Delay Analysis of In-Vehicle Internet Access Via On-Road WiFi Access Points

Wenchao Xu*, Hassan Aboubakr Omar*†,
Weihua Zhuang*, *Fellow, IEEE*, and Xuemin (Sherman) Shen*, *Fellow, IEEE*
*Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1
†Engineering Mathematics and Physics Department, Cairo University, Giza, Egypt
{w74xu, h3omar, wzhuang, sshen}@uwaterloo.ca

Abstract*—Providing cost-effective and high throughput WiFi access for vehicle drivers and passengers is a promising solution to support the increasing demand for in-vehicle Internet applications. Prior to accessing Internet services via an on-road WiFi access point (AP), a vehicle user has to wait for a certain time duration, referred to as access delay, until the user is authenticated and assigned proper network layer parameters, such as an Internet Protocol (IP) address. Investigation of the access delay in a vehicular environment is critical, since a large access delay can significantly reduce the time duration that a vehicle actually benefits from Internet connectivity during its temporary existence within the coverage area of an on-road WiFi AP, especially with high vehicle moving speeds. In this paper, we propose an analytical model based on a Markov chain to study the dependency of the access delay on different factors, including the wireless channel conditions, the number of vehicles accessing the AP service, and the employed authentication mechanism, such as the WiFi protected access II (WPA2)-pre-shared key (PSK) and the WPA2-802.1X modes. The accuracy of the analytical model is studied via computer simulations, as well as experimental testing using commercial off-the-shelf (COTS) WiFi products, together with a channel emulator that emulates the wireless channel conditions in a vehicular environment. Simulation and experiment results highlight the accuracy of the proposed analytical model. Results in this study provide useful guidelines for future selection/development of suitable WiFi network access schemes in a vehicular environment.

I. Introduction

Recently, many car manufacturers have equipped their vehicles with Internet connectivity, which enables various in-vehicle applications by utilizing the abundant Internet resources, such as video streaming, voice calling, and transportation information sharing [1], [2]. Different wireless technologies have been proposed to support Internet connectivity for vehicles. For example, Cheng *et. al* discussed the feasibility of utilizing cellular device-to-device technology to build intelligent transportation systems (ITS) [3], while Zhou *et. al* proposed a game theoretical approach to pipe the vehicle data through dedicated short-range communications (DSRC) and TV white space (TVWS) interfaces [4]. Similarly, the success of WiFi technology and its ubiquitous deployment for indoor scenarios, together with its cost-effectiveness, universal compatibility, and high quality-of-service (QoS) provisioning, has motivated many researchers to investigate WiFi as a potential solution to support Internet access for vehicles via on-road WiFi access points (APs). For instance, Mahajan *et. al* studied the wireless connectivity between moving vehicles and WiFi base stations [5]. Ott *et. al* introduced the idea of 'drive-thru Internet' and proved that an on-road WiFi hotspot can provide considerable throughput for both user datagram protocol (UDP) and transport control protocol (TCP) data traffic [6]. Likewise, Zhou *et. al* presented a cooperative content retrieving scheme from road-side WiFi hotspots for vehicle users [7], and Nan *et. al* developed an opportunistic traffic offloading method utilizing the network resources of road-side WiFi APs [8]. However, limited existing works focus the time duration that a vehicle user needs to take before the user can access the service of an on-road WiFi AP and actually connect to the Internet [9]. This time duration, referred to as 'access delay', is required mainly to perform the authentication and Internet Protocol (IP) address assignment. In [6], the conducted drive-thru experiments employ an open access scheme and a static IP address, which allow a vehicle user to automatically associate and access the AP service, without any consideration of the access delay. Yet, except for experimental testing or research purposes, the access delay is unavoidable to perform the authentication procedure, which is essential for WiFi network users and operators. From an operator perspective, authentication is obviously required to prevent un-authorized users from utilizing the network resources by verifying the users' identities and credentials. Similarly, from a user perspective, the authentication procedure is needed to set up secure and reliable network connections via protected communication protocols.

There are several authentication methods for WiFi networks, e.g., webpage verification at some public places, WiFi protected access II (WPA2)-pre-shared key (PSK) for most of the home WiFi networks, WPA2-802.1X for enterprise WiFi networks, such as eduroam at universities [10] [11], and the Hotspot 2.0 specifications for automatic association and seamless roaming [12]. Among these standards, the WPA2 and Hotspot 2.0 networks can be automatically accessed without any manual interaction, by allowing a user to pre-store the user credentials, which is suitable for commercial deployment of on-road WiFi networks. Additionally, the IEEE 802.11r fast roaming protocol ensures fast re-association when a WiFi user leaves the coverage region of an AP and enters the coverage region of another AP [13]. However, the IEEE 802.11r cannot be applied to APs that are far away from or not connected

to each other. In addition to the time duration required to complete the authentication procedure, another duration is needed for a vehicle user to obtain an IP address, e.g., via Dynamic Host Configuration Protocol (DHCP) protocol. The sum of the durations required for authentication and IP assignment constitutes the access delay, which can last for a few seconds [14]. In such a case, a vehicle user can have a limited time to utilize the Internet resources before the vehicle moves out of the coverage area of a WiFi AP, especially with a high vehicle moving speed. Hence, a 'quickWiFi' scheme was proposed to reduce the access delay by tuning related WiFi parameters and optimizing the AP scanning strategy for clients [15].

The access delay can be affected in several ways. First, if the AP is serving a large number of users, the access delay will increase for a new user due to a high level of channel contention using the IEEE 802.11 standard distributed coordination function (DCF). Second, a poor wireless propagation channel can result in a high frame error rate, which further increases the access delay, due to retransmission of management frames that are not successfully delivered. Third, different authentication protocols require different sequences of management frame exchanges between the AP and a new user, leading to a different access delay associated with each authentication methods. To the best of our knowledge, the effects of the number of contending WiFi users, the wireless channel conditions, and the employed authentication method on the access delay have not been analyzed. In this paper, we investigate how these factors affect the access delay. We propose a Markov chain-based analytical model that can be applied for any authentication method, in order to calculate the average access delay, given the time-varying channel conditions and number of contending WiFi users in a vehicular environment. The accuracy of the proposed analytical model is studied via MATLAB simulations and experimental testing. The experimental testing is conducted using commercial off-the-shelf (COTS) WiFi products supporting the IEEE 802.11n standard, together with an advanced channel emulator that emulates the wireless channel conditions between the vehicles and a WiFi AP in an expressway scenario. The analytical, simulation, and experimental testing results of the average access delay are obtained for the WPA2-PSK and WPA2-802.1X authentication methods, under various wireless channel conditions and for various numbers of contending WiFi users.

The remainder of this paper is organized as follows. Section II describes the system model under consideration and Section III presents the analytical model to evaluate the average access delay. Section IV discusses the analytical and simulation results, while Section V introduces the experiment framework, test procedure, and test results. Finally, Section VI concludes this research.

II. System Model

We consider a single WiFi AP that provides Internet connectivity for vehicles on the road. When a vehicle enters the communication range of the AP, before connecting to the Internet, the vehicle exchanges a sequence of management frames with the AP in order to perform the necessary procedures for authentication and IP address allocation. The management frame exchanges between the vehicle and the AP depend on the WiFi network access standard, e.g., WPA2 [10] and Hotspot 2.0 [12], and the authentication mechanism, e.g., IEEE 802.1X [16] and extensible authentication protocol (EAP) [17], [18]. For instance, Figs. 1 and 2 respectively show the sequence of management frames exchanged between a vehicle and the AP for the WPA2-PSK and WPA2-802.1X authentication methods[1]. The generation of some management frames may require communication between the AP and a remote server through a core network. For instance, as shown in Fig. 2, the AP needs to connect to a remote authentication, authorization, and accounting (AAA) server before replying to some frames from a vehicle. We focus on a single vehicle, referred to as tagged vehicle, that just enters the communication range of the AP and attempts to connect to the Internet via the AP. To perform this Internet connection, the management frames exchanged between the tagged vehicle and the AP, as shown in Figs. 1 and 2, are indexed from 1 to N_f, and the length of the i^{th} management frame is denoted by $l_i, i = 1, .., N_f$. The frame length indicates the length of the data field of the physical layer (PHY) protocol data unit (PPDU), which consists of the encoded MAC layer protocol data unit (MPDU) and other fields that are included by the PHY and transmitted over-the-air using the same bit rate as the MPDU, such as the service field and tail bits added by the IEEE 802.11 orthogonal frequency division multiplexing (OFDM) PHY standard [13].

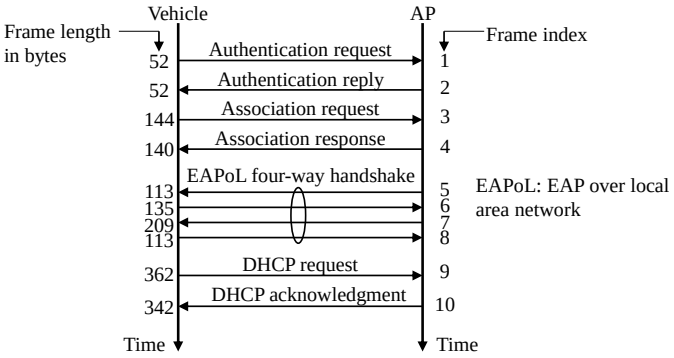


Fig. 1: Management frames exchanged between a vehicle and an AP based on the WPA2-PSK mode for authentication ($N_f = 10$)

In addition to the tagged vehicle, there exist a number of neighbor vehicles that are already connected to the Internet via the AP and uploading data to the AP. It is assumed that, each neighbor vehicle always has a data frame to upload to the AP, from the instant that the tagged vehicle enters the communication range of the AP until all the N_f management frames are successfully exchanged. Each data frame uploaded

[1]To simplify our analysis, the delay of detecting roadside AP via receiption of beacon/probe frames is neglected. Such delay mainly depends on the system parameters of broadcast interval of beacon/probe frames and is not within the consideration of this paper.

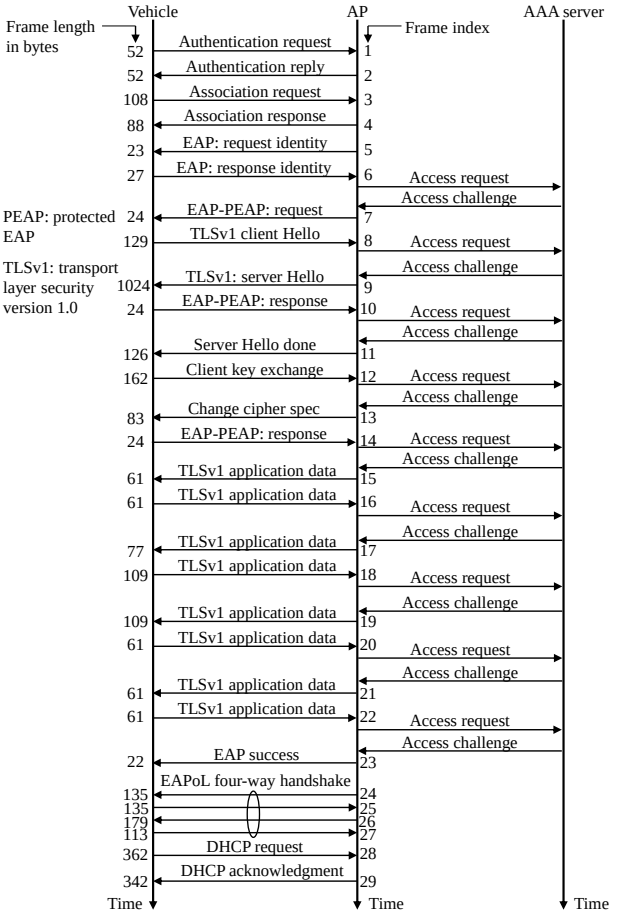


Fig. 2: Management frames exchanged between a vehicle and an AP based on the WPA2-802.1X mode for authentication ($N_f = 29$)

by a neighbor vehicle has a fixed length denoted by l, and is transmitted at a constant PHY bit rate denoted by r. All the nodes (i.e., the neighbor vehicles, the tagged vehicle, and the AP) are within the communication range of each other and employ the IEEE 802.11 DCF to access the channel [13], with a minimum contention window size denoted by w, and a number of back-off stages indexed from 0 to $m-1$, where m denotes the total number of back-off stages in the absence of request-to-send/clear-to-send (RTS/CTS) handshaking. At each back-off stage, the tagged vehicle and the AP employs a PHY bit rate, denoted by $r_{ib}, i = 1, ..., N_f$ and $b = 0, ..., m-1$, for the next transmission attempt of the i^{th} management frame that is being exchanged. For the same management frame index, i, the values of r_{ib} $\forall b$ are determined based on a certain rate switching algorithm, while for the same back-off stage index, b, the value of r_{ib} depends on whether the tagged vehicle or the AP is the source of the i^{th} management frame. If a management/data frame is successfully received, an acknowledgment (ACK) frame of length a is transmitted using the same PHY bit rate as that for the management/data frame transmission. On the contrary, if a management/data frame is not successfully delivered to its destination, the frame is referred to as a 'lost' frame. The ACK timeout duration that the source of a lost frame needs to wait for, before invoking the DCF back-off procedure, is neglected [13]. A lost frame is retransmitted by its source node until it is successfully delivered, without any maximum retry limit.

When the tagged vehicle or the AP attempts to transmit the i^{th} management frame, $i = 1, ..., N_f$, the total number of nodes that are contending to access the channel is constant and denoted by n_i, which consists of all the neighbor vehicles plus one node (i.e., either the AP or the tagged vehicle, depending on which one is the source of the i^{th} management frame). For the n_i contending nodes, $i = 1, ..., N_f$, let τ_i denote the probability that a node transmits a frame in a randomly selected slot duration[2], α_i the probability that a transmitted frame is lost due to a transmission collision, β_i the probability that a transmitted frame is lost due to a poor channel condition ($0 < \beta_i < 1$), and δ_i the probability that a transmitted frame is lost due to a transmission collision or poor channel, i.e., $\delta_i = 1 - (1 - \alpha_i)(1 - \beta_i)$. It is assumed that the value of each of α_i, β_i, and (consequently) δ_i, $i = 1, ..., N_f$, is the same for any frame transmitted by any of the n_i contending nodes, and remains constant until the i^{th} management frame is successfully exchanged between the tagged vehicle and the AP. Also, the success events of different delivery trials of the same management/data frame are independent. If a transmission collision happens among management and data frames, none of the contending nodes can successfully receive any of the colliding frames. On the contrary, if no transmission collision happens for a transmitted frame, but the frame is lost due to a poor channel condition, the back-off procedure of each node that successfully received the frame is invoked immediately at the end of transmission of the lost frame, i.e., the additional wait time that consists of short interframe space (SIFS) and ACK transmission durations is neglected [13].

In the following, the notation $\mathbb{E}(Y)$ denotes the expected value of a random variable Y, $\mathbb{E}(Y|Z = z)$ the conditional expected value of Y given the event that another random variable Z takes the value z, and $\max(a, b)$ the maximum of the two values a and b.

III. Access Delay Analysis

The objective of this section is to derive the average access delay that is required for the tagged vehicle and the AP to complete the authentication and IP allocation procedures by exchanging the necessary N_f management frames. First, we define a time step as the sum of the durations required by the source of a management frame to: a) generate the frame, b) complete the DCF back-off procedure and start the over-the-air transmission of the frame, and c) either successfully transmit the frame and receive the corresponding ACK frame or unsuccessfully transmit the frame and wait until the channel is sensed idle (the earlier of the two events). Based on the definition, the access delay from the time instant that the first management frame is being generated until all the N_f

[2]The slot duration is defined as the duration between two consecutive variations in the back-off counter or back-off stage of a contending node [19].

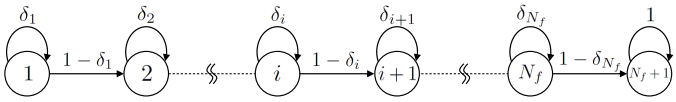


Fig. 3: Illustration of the Markov chain and one-step transition probabilities for states 1 to $N_f + 1$

management frames are successfully exchanged can be partitioned into a sequence of time steps. At the start of each time step, a management frame is required to be (re)transmitted either by the tagged vehicle or by the AP. Let X_n be the index of the management frame that should be exchanged between the tagged vehicle and the AP at the start of the n^{th} time step. Based on the system model in Section II, X_n is a discrete-time Markov chain that takes integer values from 1 to N_f. Additionally, the value of $N_f + 1$ is added to the state space of X_n to represent the event that all the N_f frames are successfully exchanged between the tagged vehicle and the AP[3]. Hence, when $X_n = i, i = 1, ..., N_f$, the Markov chain either transits to state $i + 1$ or remains at its current state, based on whether or not the transmission of the i^{th} frame is successful at the end of the n^{th} time step, as illustrated in Fig. 3. Therefore, in order to calculate the average access delay, the main idea is to find the average duration that the Markov chain X_n needs in order to transit from state 1 to state N_f+1 for the first time. The remainder of this section shows how this average duration can be obtained.

For Markov chain X_n, let p_{ij} denote the one-step transition probability from state i to state j, where

$$p_{ij} = \begin{cases} \delta_i, & i = j = 1, ..., N_f \\ 1, & i = j = N_f + 1 \\ 1 - \delta_i, & i = j - 1 = 1, ..., N_f \\ 0, & \text{elsewhere.} \end{cases} \tag{1}$$

In (1), the value of δ_i can be obtained by extending Bianchi's DCF model [19] to account for the frame loss due to channel conditions[4]. That is, for each $i = 1, ..., N_f$, the value of δ_i is calculated by solving the system of equations (2a-2c) in variables τ_i, α_i, and δ_i:

$$\tau_i = \frac{2(1 - 2\delta_i)}{(1 - 2\delta_i)(w + 1) + \delta_i w(1 - (2\delta_i)^{m-1})} \tag{2a}$$

$$\alpha_i = 1 - (1 - \tau_i)^{n_i - 1} \tag{2b}$$

$$\delta_i = 1 - (1 - \alpha_i)(1 - \beta_i). \tag{2c}$$

To show that there exists a unique value for each of τ_i, α_i, and δ_i, from (2c) and (2b) we have

$$\tau_i = 1 - \left(\frac{1 - \delta_i}{1 - \beta_i}\right)^{\frac{1}{n_i - 1}}. \tag{3}$$

[3]When $X_n = N_f + 1$, the k^{th} time step, $k \geq n$, can take any positive value.

[4]When the tagged vehicle or the AP attempts to transmit the i^{th} management frame, $i = 1, ..., N_f$, each of the n_i contending nodes always has a frame to transmit, i.e., in a traffic saturation conditions [19], until the i^{th} frame is successfully delivered.

Therefore, using (2a) and (3), we can prove the existence and uniqueness of the solution for the system of the three equations (2a-2c) following a similar approach as in [19]. Given the one-step transition probabilities in (1), the first passage time probabilities can be obtained using

$$f_{ij}^{(1)} = p_{ij} \tag{4a}$$

$$f_{ij}^{(n)} = \sum_{\substack{k=1 \\ k \neq j}}^{N_f+1} p_{ik} f_{kj}^{(n-1)}, \quad n > 1 \tag{4b}$$

where $f_{ij}^{(n)}$ denotes the n-step first passage time probability from state i to state j. Note that, for the Markov chain in Fig. 3, $\sum_{n=1}^{\infty} f_{ij}^{(n)} = 1$ iff $j > i$ or $j = i = N_f + 1$, provided that $\delta_i \neq 1 \ \forall i$. Now, let D_{ij} denote the first passage delay from state i to state j, i.e., the delay that the Markov chain requires to transit to state j for the first time, given that the Markov chain is currently at state i, where $i = 1, ..., N_f$, $j = 1, ..., N_f + 1$, and $j > i$. By using the law of total expectation and the first passage time probabilities from (4a-4b), and by noting that $f_{ij}^{(n)} \neq 0$ only if $n \geq j - i$ (Fig. 3), the expected value of D_{ij} is given by

$$\mathbb{E}(D_{ij}) = \sum_{n=j-i}^{\infty} \mathbb{E}(D_{ij}^{(n)}) f_{ij}^{(n)}, \quad i, j \in \{1, ..., N_f + 1\} \text{ and } i < j \tag{5}$$

where $D_{ij}^{(n)}$ denotes the n-step first passage delay from state i to state j, i.e., the delay that the Markov chain requires to transit to state j for the first time in n time steps, given that the Markov chain is currently at state i. Consequently, the average access delay can be directly obtained from (5), by setting $i = 1$ and $j = N_f+1$. However, in order to evaluate (5) for specific i and j values, the expected value $\mathbb{E}(D_{ij}^{(n)})$ should be calculated $\forall n \in \mathbb{N}^+$ such that $n \geq j-i$. For $n \geq j-i$ and $n \neq 1$, the value of $\mathbb{E}(D_{ij}^{(n)})$ can be obtained in a recursive way as follows. Let random variable $K_{ij}^{(n)}$ denote the index of the first state to which the Markov chain transits from state i, given that the Markov chain transits from state i to state j for the first time in n steps, where $i, j = 1, ..., N_f, i < j$, and $n \geq \max(j - i, 2)$. For these $i, j,$ and n values, let set $\Omega_{ij}^{(n)} = \{k : p_{ik} \neq 0 \text{ and } j - n + 1 \leq k < j\}$ denote all possible values of random variable $K_{ij}^{(n)}$, which is given by

$$\Omega_{ij}^{(n)} = \begin{cases} \{i\}, & j = i + 1 \\ \{i + 1\}, & j = i + n \\ \{i, i + 1\}, & \text{elsewhere.} \end{cases} \tag{6}$$

Hence, the expected value $\mathbb{E}(D_{ij}^{(n)})$ can be calculated by using

$$\begin{aligned}\mathbb{E}(D_{ij}^{(n)}) &= \sum_{k\in\Omega_{ij}^{(n)}} \mathbb{E}(D_{ij}^{(n)}|K_{ij}^{(n)}=k)\frac{p_{ik}f_{kj}^{(n-1)}}{f_{ij}^{(n)}} \\ &= \sum_{k\in\Omega_{ij}^{(n)}} \Big(\mathbb{E}(D_{ik}^{(1)}) + \mathbb{E}(D_{kj}^{(n-1)})\Big)\frac{p_{ik}f_{kj}^{(n-1)}}{f_{ij}^{(n)}}, \\ i,j \in &\{1,...,N_f+1\}, i<j, \text{ and } n \geq \max(j-i,2).\end{aligned} \tag{7}$$

In order to evaluate $\mathbb{E}(D_{ij}^{(n)})$, it is required to find the values of $\mathbb{E}(D_{ik}^{(1)}), \forall i \in \{1,...,N_f\}$ and $k \in \{i, i+1\}$. First, we have

$$\begin{aligned}\mathbb{E}(D_{ik}^{(1)}) = \mathbb{E}(U_i) + \mathbb{E}(V_i) + \text{DIFS} + \mathbb{E}(R_{ik}), \\ i \in \{1,...,N_f\} \text{ and } k \in \{i, i+1\}\end{aligned} \tag{8}$$

where U_i is the processing time at the start of a time step required to generate the i^{th} management frame, including the duration needed for communication through the core network (if exists); V_i is the time spent until the channel is sensed idle and the back-off procedure is invoked by the source of the i^{th} management frame; DIFS is the duration of a DCF interframe space [13]; and R_{ik} is the remainder of a time step, excluding the U_i, V_i, and DIFS durations, when the i^{th} management frame is either successfully ($k = i+1$) or unsuccessfully ($k = i$) delivered. The processing time, U_i, of the i^{th} management frame is nonzero only before the first transmission attempt of the frame (i.e., when the source of the frame is at back-off stage 0). When $U_i = 0$, we have $V_i = 0$ in consequence, since each time step starts at a moment the channel already starts to become idle[5]. In order to calculate $\mathbb{E}(U_i)$, $\mathbb{E}(V_i)$, and $\mathbb{E}(R_{ik}), k \in \{i, i+1\}$, for a specific value of $i \in \{1,...,N_f\}$, let random variable B_i denote the back-off stage of the source node that attempts to transmit the i^{th} management frame at the start of a time step. The probability distribution function of B_i is given by

$$P_{B_i}(b) = \begin{cases}\delta_i^b(1-\delta_i), & b = 0,...,m-2 \\ 1 - \sum_{q=0}^{m-2}\delta_i^q(1-\delta_i), & b = m-1.\end{cases} \tag{9}$$

Hence,

$$\begin{aligned}\mathbb{E}(U_i) &= \sum_{b=0}^{m-1}\mathbb{E}(U_i|B_i=b)P_{B_i}(b) \\ &= \mathbb{E}(U_i|B_i=0)P_{B_i}(0)\end{aligned} \tag{10}$$

$$\begin{aligned}\mathbb{E}(V_i) &= \sum_{b=0}^{m-1}\mathbb{E}(V_i|B_i=b)P_{B_i}(b) \\ &= \mathbb{E}(V_i|B_i=0)P_{B_i}(0)\end{aligned} \tag{11}$$

$$\begin{aligned}\mathbb{E}(R_{ik}) = \sum_{b=0}^{m-1}\mathbb{E}(R_{ik}|B_i=b)P_{B_i}(b), \\ i \in \{1,...,N_f\} \text{ and } k \in \{i, i+1\}.\end{aligned} \tag{12}$$

In (10), the value of $\mathbb{E}(U_i|B_i=0)$ can be found for a given probability density function of U_i, while in (11), the value of $\mathbb{E}(V_i|B_i=0)$ can be approximated as the duration of a successful over-the-air delivery of a data frame, i.e.,

$$\mathbb{E}(V_i|B_i=0) = h + \frac{l}{r} + \text{SIFS} + \frac{a}{r} \tag{13}$$

where h is the transmission duration of PHY information other than the PPDU data field, e.g., PHY convergence procedure (PLCP) preamble and signal fields of the IEEE 802.11 OFDM PHY [13]. In (12), the conditional expectation $\mathbb{E}(R_{ik}|B_i=b)$ can be calculated using (14a)-(14b) as follows:

$$\mathbb{E}(R_{ii+1}|B_i=b) = \mathbb{E}(C_b)\mathbb{E}(S_i) + y_{ib} \tag{14a}$$

$$\begin{aligned}\mathbb{E}(R_{ii}|B_i=b) = \mathbb{E}(C_b)\mathbb{E}(S_i) + z_{ib} \\ i \in \{1,...,N_f\} \text{ and } b \in \{0,...,m-1\}\end{aligned} \tag{14b}$$

where C_b denotes the value of the back-off counter of the source node at back-off stage b, S_i the duration required to decrease the back-off counter of the source node by 1 when attempting to transmit the i^{th} management frame, and y_{ib} (z_{ib}) the remainder of a time step after the over-the-air transmission of the i^{th} management frame starts, when the transmission is successful (unsuccessful) and the source node is at the b^{th} back-off stage. Since at the b^{th} back-off stage, the value of the back-off counter is equally likely selected from 0 to $2^b w - 1$ [13], the expected value $\mathbb{E}(C_b)$ is given by

$$\mathbb{E}(C_b) = \frac{2^b w - 1}{2}, b \in \{0,...,m-1\}. \tag{15}$$

The values of y_{ib} and z_{ib} can be calculated (by neglecting the propagation delay) using

$$y_{ib} = h + \frac{l_i}{r_{ib}} + \text{SIFS} + \frac{a}{r_{ib}} \tag{16a}$$

$$\begin{aligned}z_{ib} = h + \frac{\beta_i(1-\alpha_i)}{\delta_i}\frac{l_i}{r_{ib}} + \frac{\alpha_i}{\delta_i}\max(\frac{l_i}{r_{ib}}, \frac{l}{r}) \\ i \in \{1,...,N_f\} \text{ and } b \in \{0,...,m-1\}.\end{aligned} \tag{16b}$$

Note that, in (16b), the values of $\frac{\beta_i(1-\alpha_i)}{\delta_i}$ and $\frac{\alpha_i}{\delta_i}$ respectively equal the probability that a failure of delivering the i^{th} management frame is due to a poor channel condition only (i.e., no transmission collision) or involves a transmission collision with a data frame. Finally, the value of $\mathbb{E}(S_i)$ can be obtained using (17a)-(17c), given by

$$\begin{aligned}\mathbb{E}(S_i) = (1-\zeta_i)\sigma + \zeta_i\Big(h + \frac{l}{r} + \text{DIFS}\Big) \\ + \nu_i\Big(\text{SIFS} + \frac{a}{r}\Big)\end{aligned} \tag{17a}$$

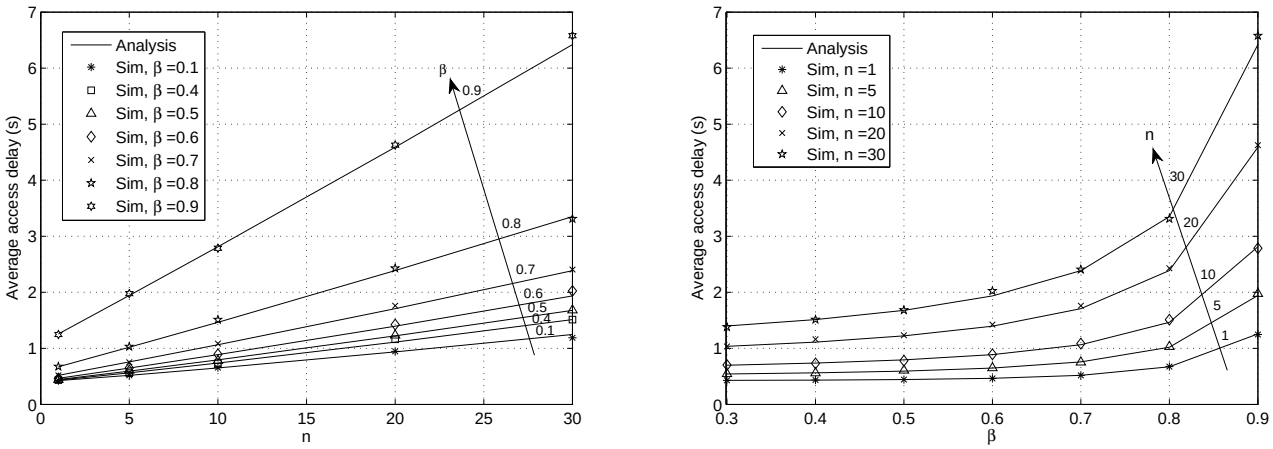
$$\zeta_i = 1 - (1-\tau_i)^{n_i-1} \tag{17b}$$

$$\begin{aligned}\nu_i = (1-\beta_i)(n_i-1)\tau_i(1-\tau_i)^{n_i-2} \\ i \in \{1,...,N_f\}\end{aligned} \tag{17c}$$

[5]An exception is the first time step when $i = 1$, for which the value of V_1 is neglected.

TABLE I: Parameter values used to generate the analytical, simulation, and experimental results

Parameter	Value	Parameter	Value	Parameter	Value	Parameter	Value
w	16	DIFS	SIFS + 2σ	N_f for WPA2-802.1X	29 frames	a	32 bytes
m	7	Preamble length	16 μs	N_f for WPA2-PSK	10 frames	l	1574 bytes
σ	9 μs	PLCP header length	4 μs	r_i (i^{th} frame transmitted by the AP)	24 Mbps	l_i for WPA2-802.1X	Fig. 2
SIFS	16 μs	h	Preamble length + PLCP header length	r_i (i^{th} frame transmitted by the tagged vehicle)	6 Mbps	l_i for WPA2-PSK	Fig. 1
r	24 Mbps	$\mathbb{E}(U_i)$ for WPA2-802.1X	Varies from 45 μs to 64 ms for $i = 1, ..., N_f$	$\mathbb{E}(U_i)$ for WPA2-PSK	Varies from 87 μs to 70 ms for $i = 1, ..., N_f$	—	—



(a) Average access delay versus n

(b) Average access delay versus β

Fig. 4: Analytical and simulations (Sim) results of the access delay when the WPA2-802.1X standard is employed for authentication

where σ is the idle slot duration, ζ_i and ν_i respectively denote the probability of a transmission and the probability of a successful transmission in a slot duration from the $n_i - 1$ nodes that are contending with the source node of the i^{th} management frame. By using (1)-(4) and (6)-(17), the expected value of the first passage delay, $\mathbb{E}(D_{ij})$, from a state i to another state j can be obtained from (5). By setting $i = 1$ and $j = N_f + 1$, the value of $\mathbb{E}(D_{1N_f+1})$ represents the average access delay.

IV. Analytical and Simulation Results

This section provides numerical results based on the mathematical analysis in Section III to investigate the access delay performance with respect to the number of contending nodes, the wireless channel conditions, and the associated authentication mechanisms. The first authentication mechanism under consideration is based on the WPA2-802.1X mode, which is used for enterprise networks and requires an authentication server [16]; while the second authentication mechanism is based on the WPA2-PSK mode, which is mainly employed for home and small office networks and does not require an authentication server [17]. The two authentication mechanisms result in two different sequences of management frame exchanges between the AP and the tagged vehicle, as well as different values of the additional delay introduced for some management frames due to possible communication between the AP and an authentication server through the core network. The numerical results are generated based on the IEEE 802.11n standard, which (together with the authentication mechanism) defines the sequence of management frames that should be exchanged for the tagged vehicle to connect to the Internet through the AP. When delivering the management frames, the values of each of β_i and n_i $\forall i$ (Section III) are set to fixed values, denoted by β and n, respectively. Similarly, for the i^{th} management frame, the values of r_{ib} $\forall b$ are set to a fixed value, denoted by $r_i, i = 1, ..., N_f$, where each r_i is set to the bit rate employed by the source of the i^{th} management frame at back-off stage 0, as obtained from the experimental testing in Section V. The experiment in Section V also provides the average processing delay for each management frame, $\mathbb{E}(U_i|B_i = 0)$ $\forall i$ in (10). This section also includes computer simulations using MATLAB, in order to study the accuracy of the mathematical analysis presented in Section III. We simulate the exchange of the N_f management frames between the tagged vehicle and the AP, for the WPA2-PSK and WPA2-802.1X authentication modes, based on the IEEE 802.11 DCF for channel access by all nodes, as described in Section II. For each combination of n and β values in the simulations,

the average access delay required to exchange the N_f frames is estimated by using 200 samples (i.e., 200 repetitions of successful delivery of all the N_f frames), which result in acceptable 95 percent confidence interval for all the n and β values under consideration for each authentication mode. The parameter values used to obtain the analytical, simulation, and experimental results are summarized in Table I.

Fig. 4 shows the access delay performance when the WPA2-802.1X mode is used for authentication. As shown in Fig. 4a, the average access delay increases almost linearly with the number of contending nodes, n, for a given wireless channel represented by the probability, β, that a frame is lost due to a poor channel condition. The rate of average access delay increase with n is higher when the β value increases. For instance, in Fig. 4, the rate of increase of the curve corresponding to $\beta = 0.6$ is approximately double that of the curve corresponding to $\beta = 0.1$. The effect of β on the average access delay is illustrated in Fig. 4b for different n values. When the value of n is small ($n \leq 5$), increasing β up to 0.5 does not result in a significant increase in the average access delay. The reason is that, if a management frame is lost due to channel conditions, the additional delay required to regain access of the channel and retransmit the fame is not significant when n is small, due to a low channel contention level. On the contrary, when the n value increases, the effect of β on the average access delay becomes more noticeable, as shown in Fig. 4b. When β approaches 1, the average access delay tends to ∞, as expected, since no management frame can be successfully delivered. There is a good match between the analytical and simulation results, which indicates the accuracy of the analytical model presented in Section III. The same behavior of the average access delay illustrated in Fig. 4 for the WPA2-802.1X standard is observed for larger n values (up to 150) and when the WPA2-PSK mode is used for authentication. However, when WPA2-PSK is employed, the average access delay is considerably lower than that of the WPA2-802.1X mode, due to a smaller number of management frames required to achieve the Internet access (Figs. 1 and 2). Fig. 5 compares the average access delay for the WPA2-802.1X and the WPA2-PSK modes for different n and β values. The average access delay and its rate of increase with respect to n are higher for the WPA2-802.1X mode as compared with the WPA2-PSK for all the n and β values shown. Results in this section help to understand the behavior of the average access delay under various channel conditions, with different number of contending nodes, and using the different authentication methods, which is useful to select or develop a suitable WiFi network access scheme for a vehicular environment.

V. Experimental Testing

To further study the accuracy of the analytical model in Section III, we conduct experimental testing with COTS WiFi products and a cutting-edge channel emulator, to investigate the average access delay with different number of contending nodes, under realistic channel conditions in a vehicular environment, and by using the WPA2-802.1X and the WPA2-PSK authentication mechanisms. The experiment framework, test procedure, and test results are presented in the following.

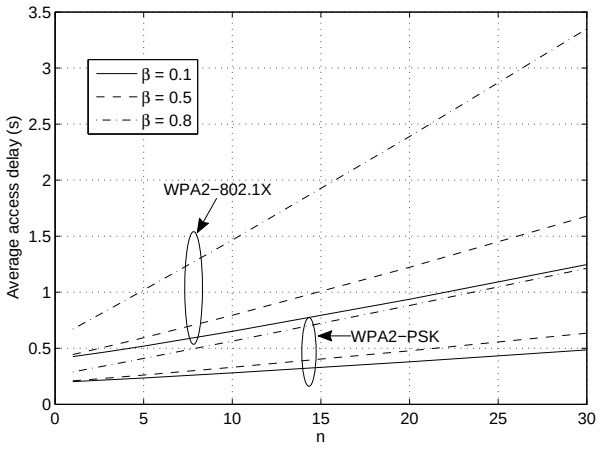


Fig. 5: Comparison of the access delay performance for the WPA2-802.1X and WPA2-PSK authentication mechanisms

A. Experiment Framework

As shown in Fig. 6, the experiment framework consists of a WiFi AP, multiple WiFi clients (representing the tagged vehicle and its neighbor vehicles), and a channel emulator. The testware of the experiment is summarized in Table II, and each component of the experiment framework, as well as the testing procedure, is described as follows.

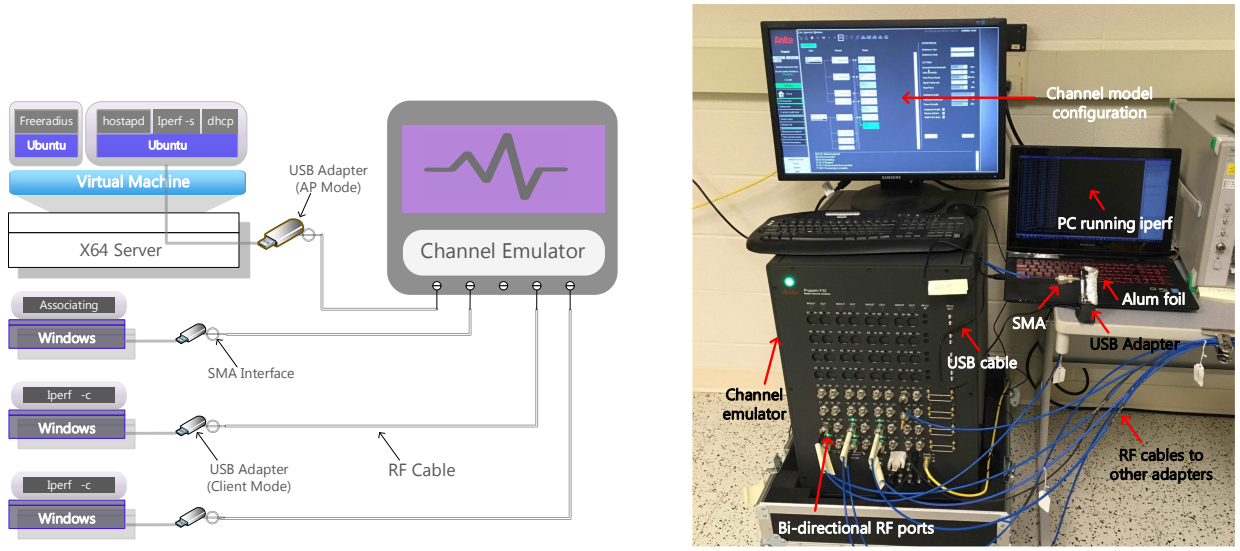
WiFi AP: The WiFi AP functionalities are performed by using a universal serial bus (USB) wireless adapter, together with the hostapd software [20], which supports WiFi AP operation on COTS wireless adapters. The AP operates over the 5.2 GHz WiFi channel, based on the high throughput (HT) PHY defined in the IEEE 802.11n amendment. While the IEEE 802.11n HT PHY supports multiple-input-multiple-output (MIMO) antenna configuration, only one antenna is used by the AP and each WiFi client, in order to reduce the number of physical connections from the wireless adapters to the channel emulator and simplify the emulation of the channel conditions among the wireless adapters.

WiFi Clients: Similar to the WiFi AP, the WiFi client operation is achieved by using a USB wireless adapter. One of the WiFi clients represents the tagged vehicle, while the other clients represent the neighbor vehicles. The client representing the tagged vehicle is configured to connect to and then disconnect from the AP, continuously for the whole duration of each experiment. In each experiment, the other clients (neighbor vehicles) are set up to continuously generate and upload data frames to the AP, by using the iperf tool [21].

Authentication Server: As shown in Fig. 2, the WPA2-802.1X mode requires communication between the AP and an AAA server in order to authenticate a WiFi client. Hence, in our experiments involving the WPA2-802.1X authentication mechanism, the Freeradius software is used to authenticate the WiFi client that represents the tagged vehicle, by applying

TABLE II: Testware of the experiment

Type	Hardware	Operating System	Software
WiFi AP	USB wireless adapter	Linux	Hostapd v2.6, Iperf, Wireshark
WiFi client	USB wireless adapter	Windows	Iperf
Authentication server	Virtual machine	Linux	FreeRadius v2.1
DHCP server	Virtual machine	Linux	ISC DHCP server



(a) Schematic diagram

(b) Testbed

Fig. 6: Experiment framework

the EAP and the tunneled transport layer security (TTLS). The Freeradius server runs on a virtual machine on the same computer that runs the hostapd server for the AP operation.

DHCP Server: We use DHCP for the AP to automatically provide a valid IP address for a client to set up the Internet connection after authentication. The DHCP server runs on the same virtual machine as the hostapd server, as shown in Fig. 6a, and all the IP addresses are assigned on the same subnet as the AP interface.

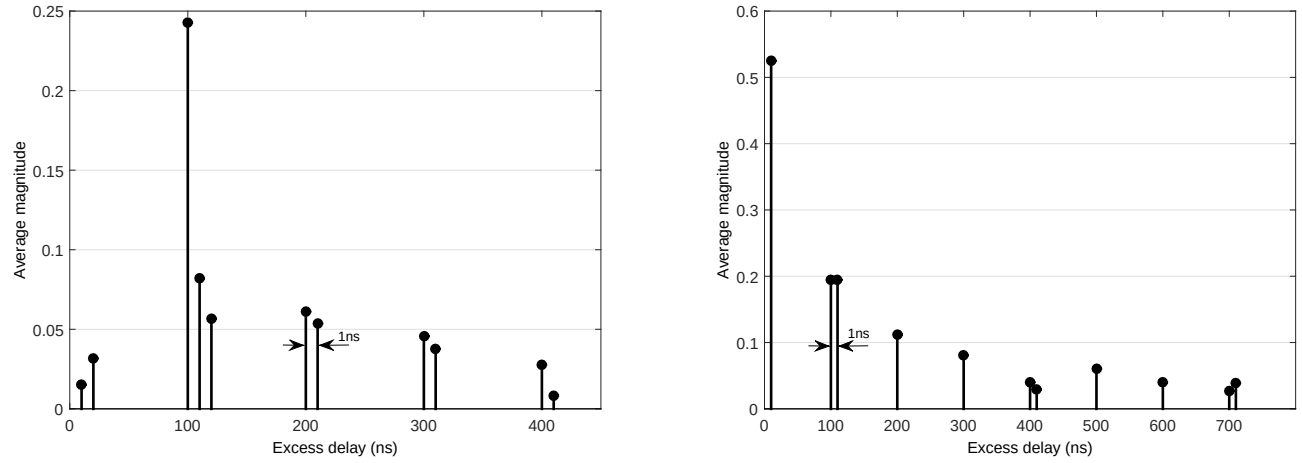
Channel Emulator: We use the Propsim F32 channel emulator, which emulates the effect of the wireless channel, such as noise, fading, delay, shadowing, and transceiver mobility, in order to conduct the experiments under realistic wireless channel conditions in a vehicular environment. The channel impulse response (CIR) is defined for the Propsim emulator in the form of a tapped delay line, where each tap represents a combination of line of sight (LoS) or non-LoS (nLoS) paths, through which the transmitted signal propagates to the destination. Each tap specifies the characteristics of the CIR component that is received through the propagation paths corresponding to the tap, such as the excess delay value, average received power, magnitude probability density function, and Doppler power spectral density (PSD). In our experiments, we use two channel models that are developed for vehicle-to-vehicle (V2V) and vehicle-to-roadside-unit (V2R) communications in the 5.9 GHz band in an expressway scenario [22][6]. The channel models used for communication between the AP and any vehicle, and between any two vehicles are illustrated in Figs. 7a and 7b, respectively, where the average power of the tap that involves the LoS path, referred to as the LoS tap (occurring at 0 excess delay), is normalized to unity. The magnitude of the LoS tap follows a Rician distribution, while the magnitude of each of the other taps follows a Rayleigh distribution. The Rician K-factor of the LoS tap and the Doppler PSD characteristics of all taps are specified in [22]. The signal received by the AP or any vehicle is corrupted by additive white Gaussian noise (AWGN), and the signal-to-noise ratio (SNR) is set to either 40 dB or 35 dB. These SNR values result in two different β values, as discussed next.

TABLE III: Test Cases

Number of clients (n)	β	Authentication protocol
1, 2, and 3	0.3 and 0.4	WPA2-PSK and WPA2-802.1X

Test Procedure: The test cases under consideration are summarized in Table III. Given the channel model between the tagged vehicle and the AP, the values of β that correspond

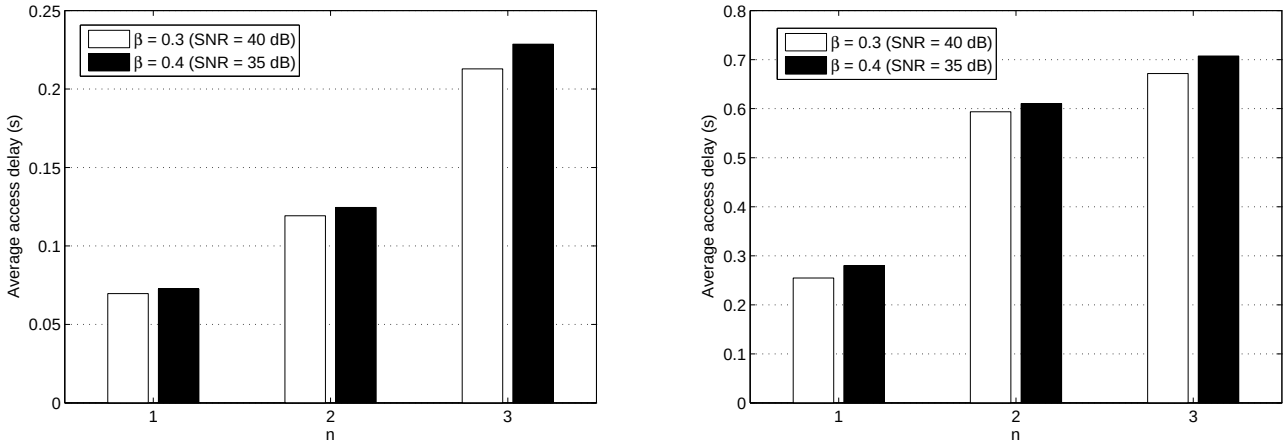
[6]The two channel models under consideration are referred to in [22] as 1) RTV expressway and 2) V2V expressway same direction with wall.



(a) V2R channel model

(b) V2V channel model

Fig. 7: The V2R and V2V channel models used in the experiments. The average magnitude of the LoS tap is normalized to unity (the LoS tap is not shown).



(a) WPA2-PSK

(b) WPA2-802.1X

Fig. 8: Experimental results of the access delay when the WPA-PSK mode and the WPA2-802.1X standard are employed for authentication

to the SNR values of 40 dB and 35 dB are found to be approximately 0.3 and 0.4, respectively, as indicated in Table III. For each SNR value, the corresponding β value is estimated by conducting a separate test using the AP and a WiFi client that continuously sends data frames to the AP. The β value is estimated by calculating the ratio of the number of data frames received by the AP for the channel model and the SNR value under consideration to the number of received frames by the AP for an ideal channel (an option in the emulator) over the same time duration.

For each test case in Table III, the tagged vehicle continuously connects to and then disconnects from the AP for a duration of one hour. Each time the tagged vehicle completes a connection to the AP, the exchanged management frames are recorded using a Wireshark protocol analyzer, which captures all the frames transmitted or received by the AP[7]. The Wireshark generates a trace file that includes the contents of each captured management frame and a time stamp indicating the time instant the frame was received or transmitted by the AP. By analyzing the Wireshark trace file generated for a certain test case, the access delay can be obtained for each connection performed by the tagged vehicle to the AP, then the average access delay for the test case is calculated over all the connections achieved during the one-hour test duration. The parameter values employed for all test cases are summarized in Table I, which are the same as those used to generate the numerical and simulation results in Section IV.

[7]The first four frames in Figs. 1 and 2 could not be captured in any experiment.

TABLE IV: Difference between the average access delay values obtained from the analysis in Section III and the experiments in Section V

		n					
		1	2	3	1	2	3
β	0.3	0.135	0.094	0.011	0.175	0.137	0.186
	0.4	0.133	0.092	0.041	0.155	0.145	0.210
		WPA2-PSK			**WPA2-802.1X**		

B. Test Results

The performance of the access delay for the test cases under consideration is shown in Fig. 8. It can be seen from Figs. 8a and 8b that, for both the WPA-PSK and WPA2-802.1X authentication mechanisms, increasing the β value (from 0.3 to 0.4) does not result in a significant increase in the average access delay for the n values, which is consistent with the analytical result in Fig. 4b. Table IV lists the difference between the average access delay values obtained from the analysis in Section III and the experiments. It is observed that, for all the n and β values under consideration, and for the two authentication mechanisms that we tested, there is a good match between the analytical and experimental results. The maximum difference between the analytical and experimental values of the average access delay is around 0.2 s. One reason of some mismatch between the analytical and experimental results is the additional (random) delay introduced by the channel emulator, which is not accounted for in the access delay calculation.

VI. Conclusions

In this paper, we have developed an analytical model to evaluate the access delay for a vehicle user to connect to the Internet through an on-road WiFi AP. The access delays of the WPA2-PSK and WPA2-802.1X authentication protocols are analyzed for different numbers of contending nodes and under various channel conditions (represented by frame error rates). It is shown that the access delay increases almost linearly with the number of contending nodes and the rate of increase is higher when the channel conditions result in a high frame error rate. Additionally, for a small number of contending nodes, increasing the frame error rate (e.g., up to 50 percent) does not result in a significant increase in the average access delay. It is also shown that the access delay of the WPA2-PSK authentication method is significantly less than that of the WPA2-802.1X, which highlights the importance of carefully selecting a suitable authentication method for WiFi access in a vehicular environment. The proposed analytical model and experiment framework can be applied to evaluate the access delay performance of newly developed authentication schemes.

VII. Acknowledgment

We would like to sincerely thank our students Feng Lyu and Alexander Kozachuk for their help to conduct the experiment in Section V.

References

[1] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected vehicles: Solutions and challenges," *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 289–299, 2014.

[2] K. Abboud, H. Omar, and W. Zhuang, "Interworking of DSRC and cellular network technologies for V2X communications: A survey," *IEEE Transactions on Vehicular Technology*, 2016 (to appear).

[3] X. Cheng, L. Yang, and X. Shen, "D2D for intelligent transportation systems: A feasibility study," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 4, pp. 1784–1793, 2015.

[4] H. Zhou, N. Cheng, Q. Yu, X. Shen, D. Shan, and F. Bai, "Toward multi-radio vehicular data piping for dynamic DSRC/TVWS spectrum sharing," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 10, p. 2575, 2016.

[5] R. Mahajan, J. Zahorjan, B. Zill, "Understanding WiFi-based connectivity from moving vehicles," *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, pp. 321–326, 2007.

[6] J. Ott and D. Kutscher, "Drive-thru Internet: IEEE 802.11b for automobile users," in *Proc. IEEE INFOCOM 2004*, vol. 1, 2004.

[7] H. Zhou, B. Liu, T. H. Luan, F. Hou, L. Gui, Y. Li, Q. Yu, and X. Shen, "Chaincluster: Engineering a cooperative content distribution framework for highway vehicular communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 6, pp. 2644–2657, 2014.

[8] N. Cheng, N. Lu, N. Zhang, X. Zhang, X. Shen, and J. W. Mark, "Opportunistic WiFi offloading in vehicular environment: A game-theory approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 7, pp. 1944–1955, 2016.

[9] J. Wu and P. Fan, "A survey on high mobility wireless communications: challenges, opportunities and solutions," *IEEE Access*, vol. 4, pp. 450–476, 2016.

[10] WiFi Alliance, "Wi-Fi protected access: Strong, standards-based, interoperable security for today's Wi-Fi networks," *White paper, University of Cape Town*, pp. 492–495, 2003.

[11] "eduroam: secure, world-wide roaming access service for international research and education community," https://www.eduroam.org/.

[12] WiFi Alliance, "Hotspot 2.0 specification and passpoint project," http://www.wi-fi.org/discover-wi-fi/wi-fi-certified-passpoint.

[13] "IEEE standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)*, pp. 1–2793, 2012.

[14] V. Bychkovsky, B. Hull, A. Miu, H. Balakrishnan, and S. Madden, "A measurement study of vehicular Internet access using in situ Wi-Fi networks," in *Proc. ACM MobiCom*, pp. 50–61, 2006.

[15] J. Eriksson, H. Balakrishnan, and S. Madden, "Cabernet: vehicular content delivery using WiFi," in *Proc. ACM MobiCom*, pp. 199–210, 2008.

[16] J. P. Craiger *et al.*, "802.11, 802.1X, and wireless security," *GIAC security essentials certification Practical Asssignment*, 2002.

[17] J.-C. Chen and Y.-P. Wang, "Extensible authentication protocol (EAP) and IEEE 802.1X: tutorial and empirical experience," *IEEE Communications Magazine*, vol. 43, no. 12, pp. 26–32, 2005.

[18] K. Ramezani, E. Sithirasenan, and K. Su, "Formal security analysis of EAP-ERP using casper," *IEEE Access*, vol. 4, pp. 383–396, 2016.

[19] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE Journal on selected areas in communications*, vol. 18, no. 3, pp. 535–547, 2000.

[20] "hostapd: IEEE 802.11 AP, IEEE 802.1x/wpa/wpa2/eap/radius authenticator," http://w1.fi/hostapd/.

[21] "iperf - the ultimate speed test tool for TCP, UDP and SCTP," https://iperf.fr/.

[22] G. Acosta-Marum and M. A. Ingram, "Six time- and frequency- selective empirical channel models for vehicular wireless LANs," *IEEE Vehicular Technology Magazine*, vol. 2, no. 4, pp. 4–11, Dec 2007.