Performance Analysis of Drive-thru Internet Access

by

Wenchao Xu

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2018

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External examiner	NAME	Amiya Nayak
	Title	Professor
Supervisor(s)	NAME	Xuemin (Sherman) Shen
	Title	University Professor
Internal Member	NAME	Xiaodong Lin
	Title	Professor
Internal Member	NAME	Otman Basir
	Title	Professor
Internal-external Member	NAME	Liping Fu
	Title	Professor

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Drive-thru Internet is considered to be an important solution to provide Internet access for vehicles. By deploying cost-effective and high bandwidth roadside WiFi networks, a vehicle can upload/download considerable data when drive through the coverage area, whereby a myriad of automotive applications can be employed, such as intelligent transportation system, infotainment applications like video/audio streaming, webpage browsing, etc. However, the high mobility of vehicles leads to the intermittent connection between a vehicle and roadside Access Points (APs), which would cause the Internet access delay and throughput degradation. In this thesis, we propose comprehensive modeling and analysis for the drive-thru Internet access performance considering the overhead of the access procedure, which includes the steps of network detection, user authentication and network parameters assignment. We also consider the situation that a vehicle drives through multiple roadside APs' coverage areas and evaluate the performance of traffic offloading from cellular networks to roadside WiFi networks.

In specific, firstly, we develop an analytical model to study the dependency of the drive-thru Internet access delay with different factors, i.e., the wireless channel conditions, the number of co-associated WiFi clients, and the employed authentication mechanism, such as the WiFi Protected Access II (WPA2)-Pre-Shared Key (PSK) and the WPA2-802.1X modes. The access procedure is modeled as a discrete Markov chain to calculate the time to exchange all management frames and to evaluate the Internet access delay. 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 validate the accuracy of the proposed analytical model which provides useful guidelines for future selection/development of suitable WiFi network access schemes in a vehicular environment.

Secondly, we take a further step to analyze the throughput performance of the drive-thru Internet access. The mobility of the vehicle is modeled as the transition of a series of zones in the coverage area, which is defined based on the relationship between the WiFi link rate and the distance of the AP and the vehicle. A three dimensional (3D) Markov model is proposed to combine the zone transition process and the transmission of the management frames and calculate the average throughput under conditions of different numbers of co-associated WiFi clients, channel qualities and different access protocols.

Thirdly, we consider that when the vehicle drives through multiple roadside WiFi networks, and employ the Vehicle-to-Vehicle (V2V) assisted WiFi offloading mechanism, where

nearby vehicles that associated to different APs can use their idle WiFi resource to offload part of peer's data traffic. The offloading performance is calculated by modeling the intermittent WiFi transmission as an M/G/1/K queueing process, and the performance gain of the V2V assistance is also analyzed.

In summary, the research works in this thesis should provide guidelines for future research and development of drive-thru Internet.

Acknowledgements

I would like to sincerely thank my supervisor, Professor Xuemin Shen, for his continues support, invaluable guidance and endless help during my Ph.D. study in University of Waterloo. His enthusiastic encouragement and positive attitude has not only befitted me a lot on every research work, but also helped me greatly to build a better career path. I feel extremely lucky and great privilege to be his student. I would also like to express my gratitude to Professor Weihua Zhuang for her kindly support and help in my research and system experiments.

I would like to thank Professor Xiaodong Lin, Professor Liping Fu and Professor Otman Basir for serving my defense committee. I would also like to thank Professor Amiya Nayak from University of Ottawa for serving my external examiner. Their valuable comments and insightful suggestion have significantly improved the presentation of the thesis work.

In the last four years, I also received a lot of help from my current and former colleagues in our BBCR group. I would like to express my sincere gratitude to all BBCR members. I am grateful for being with Prof. Haibo Zhou, Professor Yi Zhou, Prof. Nan Cheng, Dr. Hassan Aboubakr Omar, Dr. Ning Lu, Dr. Ran Zhang, Dr. Miao Wang, Dr. Qiang Ye, Dr. Ning Zhang, Dr. Feng Lyu, Dr. Yuanguo Bi, Nan Chen, Jianbin Ni, Jiacheng Chen, Weisen Shi, Huaqing Wu, Haixia Peng, Jiayin Chen, and many others. I will always cherish our precious friendship.

Finally, I would like to thank my dear family, for their deep and constant love and eternal care during my whole life.

Wenchao Xu

September 6, 2018

Waterloo, Ontario, Canada

This PhD thesis is dedicated to my beloved parents, Meifang Xu and Xiaoqin Feng, my sister Wenzhou Xu, and my girlfriend, Zongying Chen.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

3D	Three Dimensional
AAA	Authentication, Authorization, and Accounting
ACK	Acknowledgment
ANQP	Access Network Query Protocol
APs	Access Points
AWGN	Additive White Gaussian Noise
APIPA	Automatic Private IP Address
CIR	Channel Impulse Response
COTS	Commercial Off-The-Shelf
CTS	Clear-To-Send
DCF	Distributed Coordination Function
DHCP	Dynamic Host Configuration Protocol
DIFS	DCF Interframe Space
DSRC	Dedicated Short-Range Communications
EAP	Extensible Authentication Protocol
HT	High Throughput
IP	Internet Protocol
ITS	Intelligent Transportation System
LOS	Line Of Sight
MIMO	Multiple-Input-Multiple-Output
MPDU	MAC layer Protocol Data Unit (MPDU)
NAI	Network Access Identifier
OFDM	Orthogonal Frequency Division Multiplexing
OSU	Online SignUp

PPDU	Physical layer (PHY) Protocol Data Unit
PSK	Pre-shared Key
QoS	Quality-of-Service
RSSI	Received Signal Strength Indicator
RTS	Request-To-Send
SIFS	Short Interframe Space (SIFS)
SNR	Signal-to-Noise Ratio
TCP	Transport Control Protocol
TTLS	Tunneled Transport Layer Security
TVWS	TV White Space
WPA2	WiFi Protected Access II
UDP	User Datagram Protocol
V2R	Vehicle-to-Roadside-unit
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
VLAN	Virtual Local Area Network

Chapter 1

Introduction

Modern vehicles are expected to have high rate Internet connections, where various applications can be employed in vehicles to provide immersive experience for drivers and passengers by utilizing the abundant Internet resources, such as video streaming, voice calling, and transportation information sharing [1] [2] [3]. For example, Intelligent Transportation System (ITS) can collect and disseminate the vehicles' internal and external conditions via the Vehicle-to-Infrastructure (V2I) connections to improve the road efficiency and driving safety level [4] [5] [6]. It is predicted that the global vehicular data traffic will reach 300 Zettabytes by 2020 [7] [8], which can cause a great pressure to current Internet access technologies for vehicles. Cellular networks are initially adopted for Internet access for vehicles. However, the costs of downloading/uploading all traffic to cellular networks are usually not affordable for vehicle users. Transmitting all these traffic via cellular networks will not only cause network congestion, but also charge prohibitive communication costs to vehicle users. In addition, cellular network capacity will be drained up in dense condition where lots of vehicles are requesting heavy data tasks [9]. Drive-thru Internet has been considered as a cost-effective V2I communication method to provide Internet access when the vehicle drives through the roadside network coverage area. In this chapter, we first provide an overview of the drive-thru Internet, then elaborate the access procedure prior to the effective Internet connection between the vehicle and the AP, followed by the impact of the access procedure on the network performance. We also discuss the diagram of V2V assisted WiFi offloading in drive-thru Internet. Finally, we present our research objectives and thesis outline.

1.1 Overview of Drive-thru Internet

WiFi is chosen as the roadside wireless access technology to overcome the weakness of cellular access for vehicles. First, WiFi has been widely used for Internet access around the world for years. It is predicted that by the year of 2021, 73% percent of the global Internet traffic will be served by WiFi networks [10]. WiFi devices are universally compatible and the unlicensed spectrum is used that are not restricted over all regions of the world. Secondly, WiFi has significant link throughput. The latest 802.11ac protocol can achieve the peak link rate around 1 Gbps [11] [12], which provides enough capacity for vehicles in a WiFi cell even in dense condition. Furthermore, unlike deploying TVWS station or consuming in cellular networks, the economic cost of operating WiFi networks are relatively low. A roadside WiFi network can be agilely setup using commercial off-the-shelf devices and open source software [13].

The diagram of drive-thru Internet was firstly proposed by Ott *et al.* that utilized the roadside AP to provide temporal Internet access for drive-by vehicles [14], and proved that the WiFi hotspot can provide considerable throughput for both User Datagram Protocol (UDP) and Transport Control Protocol (TCP) data traffic [14], which is demonstrated in Fig. 1.1.

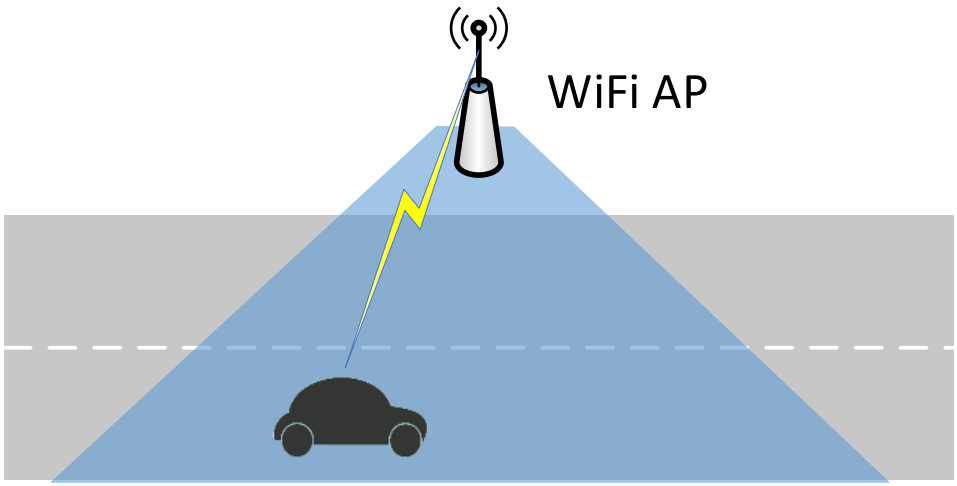

Figure 1.1: Drive-thru Internet diagram

The sojourn duration that the vehicle in the coverage area can be categorized into three phases, as shown in Fig. 1.2. When the vehicle reaches the edge of the coverage area, the signal strength rises to a certain level that AP and the vehicle can hear each other.

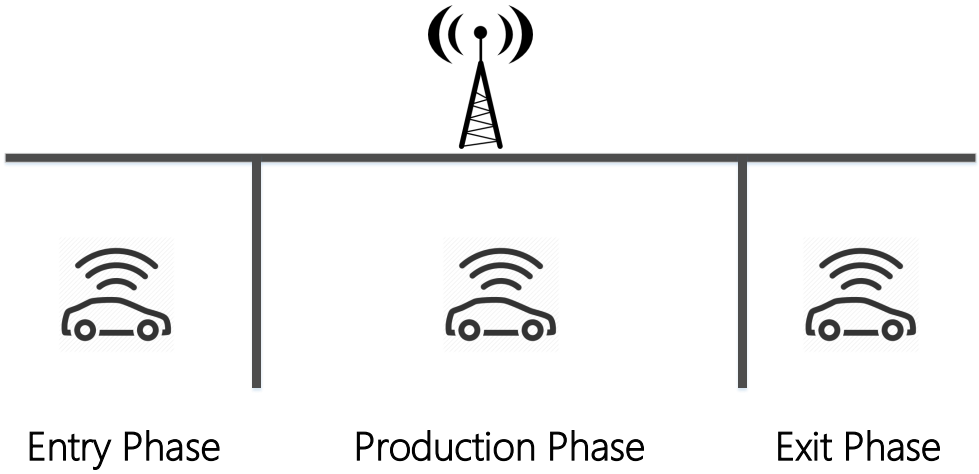

Figure 1.2: Three phases of drive-thru Internet

However, the transmission will suffer significant packet loss since the Signal-to-Noise Ratio (SNR) is low, and thus, this duration is referred to as the entry phase. And as the vehicle drives close to the AP, the SNR increases and considerable link rate can be achieved, which is referred to as the production phase. And in the exit phase when the vehicle leaves the coverage area, the SNR level decreased and the link rate falls to zero eventually.

A lot of road tests have been conducted to show that considerable data traffic can be transmitted between the roadside AP and the drive-by vehicle during the production phase, which demonstrates the feasibility of providing effective Internet access via the drive-thru Internet. Mahajan *et al.* conducted ground measurements and verified the end-to-end connectivity between moving vehicles and the roadside WiFi APs. Besides, the throughput performance between the AP and the moving vehicles are also investigated on different regions [15]. Cheng *et al.* adopted the queueing model to analyze the traffic offloading performance for vehicles using the intermittent roadside WiFi networks. The relationship between the offloading effectiveness and the average service delay of the data tasks are analyzed [16]. Similarly, Zhou *et al.* proposed a cluster based scheme to conduct cooperation between multiple roadside APs to deliver content to vehicles [17]. However, existing works seldom consider the access procedure that a vehicle user has to accomplish before he/she can actually access to Internet via a roadside hotspot, which will significantly affect the drive-thru Internet throughput performance.

1.2 Drive-thru Internet Access Procedure

Before the vehicle can actually download/upload data from/to Internet, it should accomplish the access procedure to setup effective and reliable connection with the roadside WiFi network. In this section, we will introduce the steps within the access procedure, and elaborate the impacts on the drive-thru Internet performance.

1.2.1 Related works on drive-thru Internet access

To provide Internet access by roadside APs, the impacts of the access procedure have been brought to the forefront for vehicle users. Fast access protocols have been proposed to reduce the round trips when exchanging the required management frames to setup the connection. For example, the IEEE 802.11r amendment reduces the number of authentication frames to be exchanged by caching the pairwise master key among different APs so that the time to accomplish the access procedure can be reduced [18]. Lopez *et al.* utilized the network layer information to optimize the network access in handoff process [19]. Such pre-authentication mechanisms require the cooperation between different APs or the backhaul subnets, which is not easy to apply in real environment. And the overhead for a vehicle to detect the roadside networks or the network parameters settings were not considered. Shin *et al.* utilized a selective channel scanning method to shorten the network detection delay and thus the access overhead can be reduced [20]. However, the authentication step which takes the majority part of the access delay was neglected. Most drive-thru Internet experiments and measurements in literature removed or simplified the access procedure since it is difficult to evaluate the impacts on the network performance. For example, 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 immediately, without any consideration of the access delay [14] [21] [22]. The experiment in [23] [24] did not include the authentication step, while the measurement result showed that the DHCP latency could be several seconds. Mahajan *et al.* also did not consider the overhead of authentication and IP address acquisition in their measurements in [15]. The analytical works from [16, 17, 25, 26] assumed that Internet can be accessed as soon as the vehicle drives into the cell coverage areas, where the impacts of the access procedure was omitted. However, Lu *et al.* argued that the time for access procedure cannot be neglected due to high mobility of vehicles, which can take up to ten or more seconds [1]. The steps of the access procedure are investigated, whose impacts are also analyzed in the following chapter.

1.2.2 Steps of Internet access procedure

The access procedure can be categorized into three steps based on their functions: network detection, user authentication and network parameters assignment.

Network detection

The vehicle should percept the existence of the roadside network before setup effective Internet connection. When approaching the network coverage area, the vehicle can either listen to the beacon frames broadcasted by roadside AP or send query request to APs to seek the required information, which are necessary for the vehicle to choose the most proper AP and set correct link parameters, such as network name, channel frequency, modulated rates, etc.

User authentication

The authentication step is required to setup reliable and secure wireless connections between the AP and its users. 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. In drive-thru Internet scenario, automatic authentication schemes are preferred since it's difficult for vehicle users to perform manual interactions, such as for webpage/SMS verifications which are commonly used in some public places such as airports, malls, etc. Protocols like WiFi WPA2-PSK and WPA2-802.1X (with various EAP method) are often considered in drive-thru Internet, which support automatic authentication by pre-storing the user credentials or certifications, and are suitable for commercial deployment of on-road WiFi networks.

The authentication step contributes the majority of the overhead in the access procedure, since it involves not only the message exchange between the vehicle and the roadside AP, but also the handshake with the remote authentication server.

Network parameters assignment

To setup effective Internet connection, it is required that proper network parameters should be assigned. For example, the vehicle should have an Internet Protocol (IP) address to communicate with other entities. Dynamic Host Configuration Protocol (DHCP) protocol is often used to assign the IP address for WiFi users dynamically. In some conditions, the vehicle might need to configure extra network settings. For example, the Virtual LAN (VLAN) parameters may need to be set properly to isolate the broadcast domain between the roadside networks and the backhaul network in the link layer [27].

1.2.3 Impacts on Drive-thru Performance

The sum of the durations required for network detection, authentication and IP assignment constitutes the access delay, which can last for a few seconds [23]. In such 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. The impacts of the access procedure include both the access delay and the throughput degradation.

Access delay

As shown in Fig. 1.3 the access delay refers to the average time duration that a vehicle has to wait until the access procedure is accomplished when in $S1 - S2$. 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. 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) [28]. 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. It is critical to study the dependency of the access delay on these factors, i.e., the wireless channel conditions, the number of vehicles accessing the

AP service, and the employed authentication mechanism, such as the WPA2-PSK and the WPA2-802.1X modes, which can provide useful guidelines for future selection/development of suitable WiFi network access schemes in a vehicular environment. However, limited existing works have focused 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 [29].

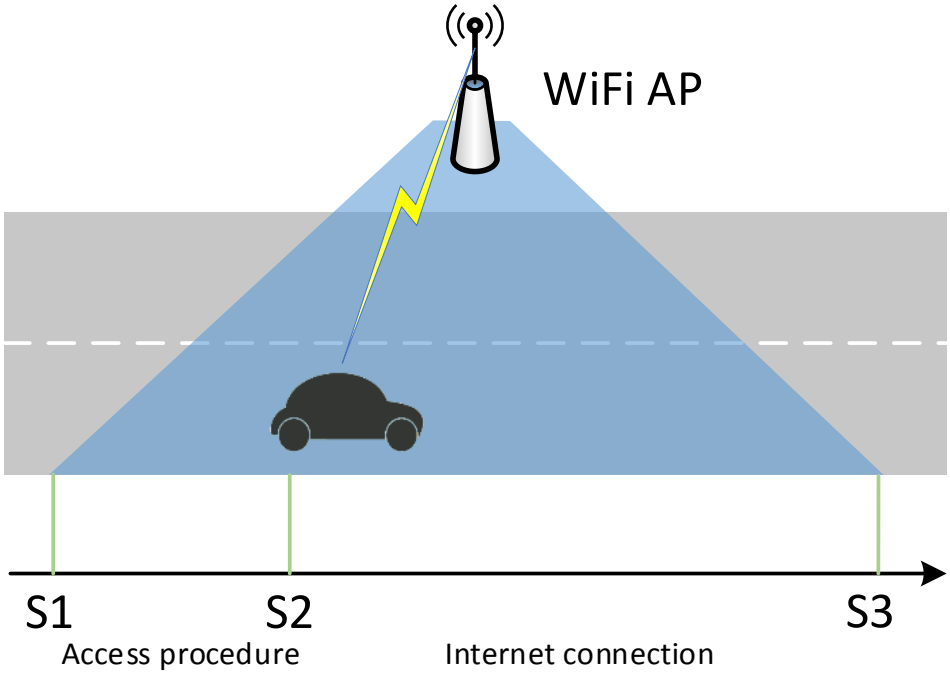

Figure 1.3: Three phases of drive-thru Internet

Throughput degradation

A vehicle cannot access to Internet via the roadside WiFi AP until the access procedure is accomplished. Since the sojourn time of a vehicle within the WiFi coverage area is limited, a fast access procedure will leave more time for downloading/uploading Internet data, and vice versa. The accomplishment of the access procedure can be deferred in the above mentioned conditions, i.e., the channel condition, the contending vehicles and the access protocols. However, given the value of access delay, it is still not enough to obtain the actual throughput performance since the WiFi link rate is varying with distance between the vehicle and the AP [**?**], e.g., Fig. 1.4 shows the relationship between the link rate and

the distance from the vehicle to the AP from a practical experiment based on the 802.11g testbeds when employing the Hotspot 2.0 access protocol from our measurement [13].

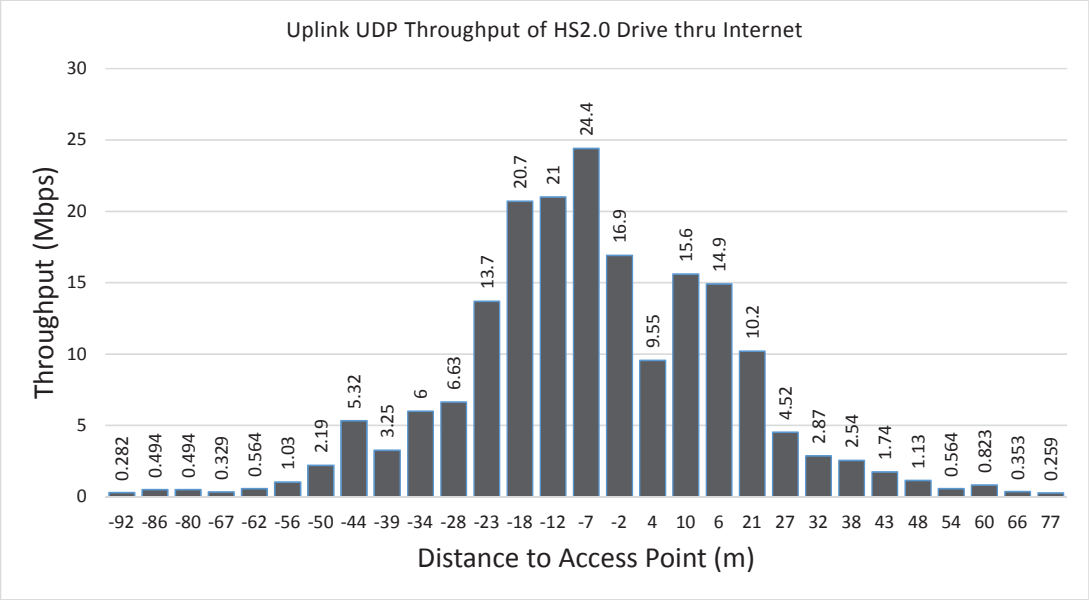

Figure 1.4: Hotspot 2.0 drive-thru Internet measurement results

Generally, the Probability Density Function (PDF) $f_a(t)$ is required to calculate the average throughput D_a, which is difficult to obtain:

$$D_a = \int_t^{\frac{L}{v}} \overline{\mathrm{R}}(vt, n) f_a(t)\, dt \tag{1.1}$$

where $\overline{\mathrm{R}}(x, n)$ is the average WiFi link rate when the distance between the vehicle and AP is x, and v, L is the vehicle velocity and the coverage range respectively and n is the number of co-associated WiFi clients. Instead of calculating $f_a(t)$, we adopt a 3D Markov process to obtain the throughput performance by combining the vehicle mobility and the Internet access procedure, which involves the transmission of all management frames.

1.3 V2V assisted Drive-thru Internet Offloading

Using the drive-thru Internet, the data traffic can be offloaded from cellular network to roadside WiFi networks to alleviate the crowdedness of cellular networks while reduce

users' cost [30]. Lee *et al.* studied the traces of near 100 mobile devices and pointed out that 65% of the wireless traffic can be offloaded to WiFi networks [31]. Dimatteo *et al.* showed that the data delivery performance can be significantly improved even in sparse network deployment via WiFi offloading for vehicles [32].

Some research works from literature also demonstrate that the direct connection between mobile users can be utilized to further enhance WiFi offloading. Han *et al.* proposed a 'tagged user' selection scheme, and let tagged users to download the popular contents and then opportunistically transmit them to encountered peers through direct WiFi or Bluetooth connection [33]. Wu *et al.* utilized the cooperation between mobile users to allow mobile users to download the target contents and share with each other via the end-to-end connection [34]. Instead of offloading the common contents shared by some users, Cheng *et al.* analyzed the performance of the vehicular traffic offloading via intermittent roadside APs and studied the relationship between the offloading efficiency and the average data service delay given certain buffer length [16]. In vehicular conditions, it is also indicated that the V2V communication could help sharing content from the 'seed user' to others [35]. Since a vehicle is allowed to associate with only one AP at a time, when multiple APs are deployed along the roadside, there is a great potential to share the AP resources via the V2V connection based on the cooperation of the vehicles that associated with different APs. Thus, it is promising to utilize the V2V assistance to further enhance the offloading performance in drive-thru Internet performance.

1.4 Thesis Objective and Outline

The objective of this Ph.D. thesis is to investigate the drive-thru Internet performance. The overhead of the Internet access procedure is investigated and the V2V assisted offloading performance is analyzed when the vehicle drive through multiple roadside WiFi networks.

(1) An analytical model is developed 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).

(2) A 3D Markov chain model is proposed to calculate the throughput performance of drive-thru Internet. The vehicle mobility is mapped to the transition of different zones in the coverage area, and the Internet access procedure is analyzed while the vehicle drive through a series of zones to obtain the performance degradation under different conditions, such as different channel level, number of contending WiFi clients and different employed

access schemes.

(3) To extend the drive-thru Internet to multiple cell scenario that a vehicle drives through multiple roadside WiFi networks, we study the performance of the data offloading from cellular networks to WiFi. An M/G/1/K queue process to analysis the intermittent WiFi connection and the V2V assistance is considered to allow neighboring vehicles to relay each others' data traffic.

The rest of this thesis is organized as follows: Chapter 2 introduces the background knowledge of the Internet access procedure and the V2V WiFi offloading diagram. Chapter 3 investigates the access delay in drive-thru Internet, Chapter 4 analyzes the drive-thru Internet throughput performance, and the dependency of the throughput degradation on different factors. Chapter 5 investigates the V2V assisted drive-thru Internet offloading performance. In Chapter 6 we conclude the thesis and give the future research directions.

Chapter 2

Background

In this chapter, we first present a literature survey about the vehicular wireless access technologies, and then provide a comprehensive overview of the steps of the access procedure to setup effective Internet connection for vehicles, including existing protocols for network detection, user authentication and network parameters assignment. We further introduce the vehicular WiFi offloading diagram in drive-thru Internet, which can be described by a queueing model with limited buffer length.

2.1 Vehicular Internet Access Technologies

With the Internet access, a myriad of infotainment applications, such as video streaming, web page surfing, etc., are becoming indispensable for passengers. Furthermore, some data-craving applications, such as High Definition (HD) map, autonomous driving, etc., is expected to be realized via the high bandwidth connection. To enable the connected vehicles, different wireless technologies have been proposed to provide alternate choices other than cellular networks. Zhou *et al.* used the TV white space (TVWS) spectrum enabled infostation to disseminate the multimedia content [36]. Zhou *et. al* further proposed a game theoretical approach to pipe the vehicle data through Dedicated Short-Range Communications (DSRC) and TVWS interfaces [37]. However, the adoption of TVWS is restricted by the geo-location where the regulation and policy of using TVWS spectrum varies place by place. Ligo *et al.* utilized the Dedicated Short Range Communications (DSRC) to offload the vehicular traffic to Internet [38]. However, the link rate is limited as the DSRC bandwidth is only half of 802.11a. Luo *et al.* investigated the inter-vehicle performance based on the visible light communication (VLC) [39], which is greatly affected by the day

light noise and line-of-sight condition and the network deployment is difficult. Chou *et al.* investigated the feasibility of using WiMAX for the V2I communication, however, WiMAX is not widely supported around the world [24].

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 APs. Bruno *et al.* analyzed the 802.11 MAC layer capacity and characterized the unfairness due to different mobilities of vehicles [40]. Joshi *et al.* investigated the rate adaption of the WiFi link in vehicular conditions [41]. Song *et al.* utilized WiFi APs to form a group of meter-sized pico-cells and achieved significant TCP throughput between the vehicle and Internet [42]. Dhondge *et al.* utilized the beacon schemes to alert the vulnerable road users of the potential collision [43]. Lv *et al.* utilized the unicast mode and set all WiFi APs the same MAC and IP address to realize the seamless Internet access for vehicle users [44]. Na *et al.* provided a solution to mitigate the interference between densely deployed WiFi APs and improved the throughput performance for vehicle users [45]. Tan *et al.* used a Markov reward process to describe the vehicular data downloading via the roadside WiFi AP to obtain the throughput performance in drive-thru Internet [46]. Chen *et al.* presented a prefetching algorithm to download the content from a series of WiFi APs [47]. Goel *et al.* proposed a traffic information dissemination scheme via the WiFi based V2V communication [48].

However, literature works have ignored the access procedure before the vehicle can be connected to Internet. Existing Internet access protocols introduces non-negligible impacts on the drive-thru Internet performance. The following section introduce the current access protocols that can be applied in vehicular conditions.

2.2 Existing Internet Access Protocols

2.2.1 Network detection

Traditional WiFi use beacon frames to exchange the information between the user and AP. The beacon scheme includes two mechanisms, i.e., passive beaconing and proactive beaconing. In passive beaconing, the AP broadcasts the beacon frames to nearby users, including the information of link parameters, network ID, etc., which are summarized in table 2.1 [49]. In proactive mode, user broadcast a probe request frame to search nearby APs, which will then reply the required information in the prove reply frames. Before access

Table 2.1: IEEE 802.11 Beacon frames

Type	**Tag**	**Usage**
Link Parameters	Support rates	Physical layer rate/modulation type
	Channel status	Signal & noise level, spectrum, etc.
	802.11 radio	RTX frequency index, current data rate, timestamp, etc.
	DS-Status	Mode (ad-hoc/BSS),
	HT info	20MHz/40MHz bandwidth
Network Info	QBSS load	Channel utilization, admission capacity, etc.
	SSID	Network Name
	Interworking	Network type & hotpsot 2.0 support
	RSN info	Authentication method
	EAP Method	Type of EAP

to the roadside WiFi network, the vehicle should detect the existence of the network via beacon frames exchange or other query protocols (e.g., the Access Network Query Protocol (ANQP) of Hotspot 2.0) [50]. This step is essential for vehicles to get the information about the wireless link parameters, e.g., 802.11 radio channel, supported rates, SSID, etc., and the backhaul information like authentication method, current load, etc. The information can also help the vehicle to select a proper nearby AP.

However, sometimes such information is not sufficient for clients to find a proper AP to associate. First, the clients have limited information about the backhaul network connected to the AP, e.g., Internet accessibility, the security level, the QoS mapping support. Secondly, according to the default AP selection policy, the WiFi clients always choose the one with the largest Received Signal Strength Indicator (RSSI) among all available nearby APs. Such AP selection policy may result in improper association, e.g., association to APs without Internet connectivity, or causing unbalance load distribution and low utilization of available APs [51]. In order to overcome these problems, hotspot 2.0 are specified that no longer rely on the SSID solely to identify a WiFi network [52]. Prior to AP association, the WiFi clients can obtain more information such as the Network Access Identifier (NAI), the operator information via multiple ways. First, new information elements are added into the beacon and probe frames, so that the client devices can obtain more information about the surrounding WiFi networks by listening to beacon frames or requesting probe response frames. The key added information elements and the purpose are listed in Table 2.2. Besides, a new query protocol called ANQP is specified for the clients to obtain further information about the AP or the backhaul network services [13]. Some of the important elements are also listed in Table 2.2.

Table 2.2: Important information elements in beacon, probe and ANQP frames in Hotspot 2.0

Parameters	Sub-field	Purpose
Extended capabilities	Interworking	Indicates if this WiFi network can interwork with other networks.
	QoS Traffic Capability	Indicates if the WiFi network can support QoS mapping between WiFi and external networks.
Interworking Adv.	Access Network Type	Indicates if the network is private or public, is connected to Internet.
	Advertisement Protocol ID	Indicate the query protocol ID and the response length limit.
Roaming consortium	N/A	Indicate the roaming consortium whose credential can also authenticate with the current AP.
ANQP element	WAN Metrics	Information about Internet connecting, downlink and uplink speed/load, etc.
	NAI Realm Data	Information about NAI realm name and authentication method.
	Domain Name	Domain information about the operators.

2.2.2 Authentication

There are several authentication mechanisms which are applied in different scenarios. Webpage/SMS verifications are used in some public places such as airports, malls, etc. However, such mechanism often requires user's manual interaction to input the verification code, which is not feasible for vehicle users, who would prefer the automatic authentication methods. In residential WiFi networks, WPA2-PSK are often used, where a pre-shared credential is stored in WiFi client devices, which will automatically perform the authentication process with the AP. However, the pre-shared credential scheme has some limitations. First, the pre-shared credential is stored at local system of the AP, which lacks of a credential management entity that a vehicle user has to negotiate with the AP when need to update the credentials. WPA2-802.1X is used in commercial WiFi access or enterprises, e.g., eduroam [53] [54], which support remote management via the authentication server. The vehicle users are assigned with a certification to better protect the user credentials. However, the handshake with the remote server requires more management frames to be exchanged and extra backhual communication delay is introduced. Hotspot 2.0 also employs the 802.1X protocol in the authentication method to provide users secure connection. The latest released version also provisions Online SignUp (OSU) ability which can enable users to automatically select proper plan with reasonable costs from service providers. This

kind of management framework makes the WiFi networks as easy and secure as cellular networks.

Literature works also investigated efficient authentication methods in vehicular conditions. Chen *et al.* developed an authentication prototype to support automatic user authentication and seamless interworking between WiFi and WiMAX [55]. Han *et al.* analyzed the security of connected vehicles and proposed a verification method to protect authenticated users [56]. Fu *et al.* presented a fast authentication method in heterogeneous WiFi and WiMAX networks to reduce the handover delay [57]. Bohak *et al.* proposed a fast authentication mechanism to reduce the round trip time between the WiFi user and the remote authentication server [58]. However, such scheme requires to distribute the access information to potential APs, which is difficult in practical deployment. Moustafa *et al.* applied the 802.11i protocol to setup reliable data transfer in high way condition [59]. These works show the importance to find out the overhead of the authentication step for vehicle users, which can provide guidance for future authentication scheme research and development.

2.2.3 Network parameters assignment

To enable effective Internet connection, the vehicle should set proper network parameters, such as valid IP address, correct VLan configuration, etc. DHCP protocol is often used to dynamically assign the IP address for a WiFi client via a local or remote DHCP server from an address pool. And the Automatic Private IP Address (APIPA) protocol is often used to auto configure the IP address if the DCHP server is not available.

2.3 Vehicular WiFi offloading

To meet the overwhelming traffic requirements, traditional network upgrade includes acquiring larger spectrum, deploying more cells and evolving new technologies (e.g., from WCDMA to LTE), which are costly and time-consuming. Offloading the data traffic from cellular networks to cost-effective wireless networks, appears as a handy-to-deploy and economic one. Drive-thru Internet provides a data pipe for vehicles to offload the vehicular traffic to roadside WiFi networks, which can reduce the communication cost and improve the network throughput for vehicle users.

2.3.1 Offloading diagram

The vehicular WiFi offloading diagram is demonstrated in Fig. 2.1, which includes the macro cellular and roadside WiFi networks. Cellular networks provide wide coverage area and can be accessed almost everywhere, while the limited coverage area of a WiFi AP will introduce intermittent Internet connection time for drive-by vehicle users. Vehicle can transmit all or part of the traffic to WiFi networks when drive through the WiFi coverage area. It is demonstrated that by applying the on-the-spot offloading strategy, the network throughput can be improved by 300%, and it can be further enhanced if the AP density is increased [60]. In terms of the vehicular WiFi offloading performance analysis, Cheng *et. al* developed an opportunistic traffic offloading method that utilized the network resources of road-side WiFi APs intermittently [25]. Wang *et al.* presented a WiFi offloading diagram for vehicle users to maximize the users' satisfaction on reducing downloading cost and delivery delay [61]. The benefit of delayed WiFi offloading is shown by the game theoretical modeling and analysis in [62], where mobile users are encouraged to delay data transmission for WiFi networks and both cellular providers and users can obtain considerable economic gains.

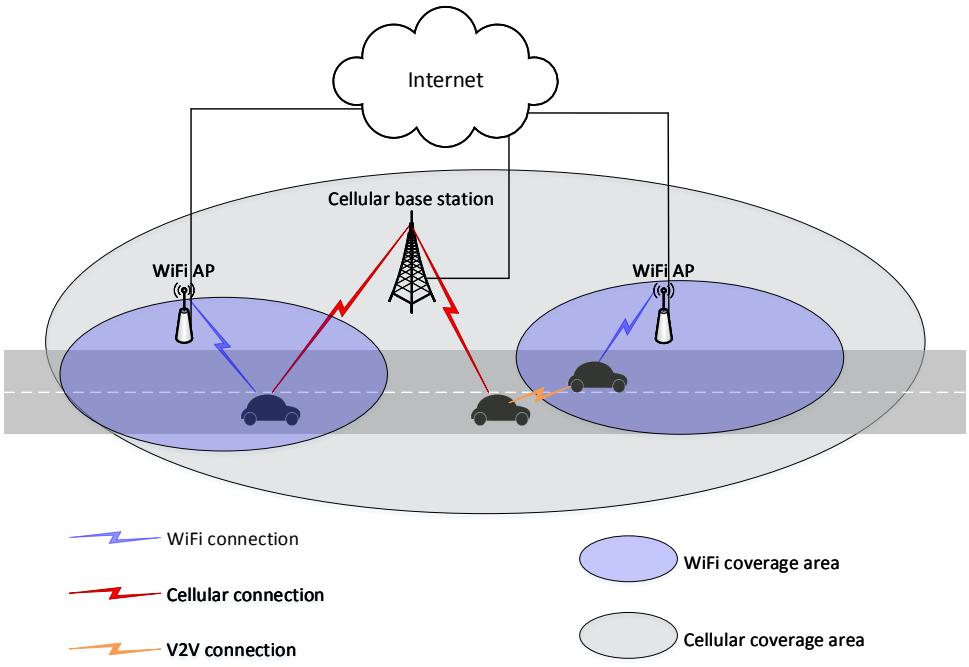

Figure 2.1: Vehicular offloading diagram

Lee *et. al* pointed out the ratio of the offloaded traffic could be further increased by 29% if the data service can be delayed [31]. Through such delayed WiFi offloading, users can wait for a certain amount of time until they encounter available APs to offload traffic opportunistically. The benefit of delayed WiFi offloading is shown by the game theoretical modelling and analysis in [62], where mobile users are encouraged to delay data transmission for WiFi networks and both cellular providers and users can obtain considerable economic gains. However, these studies mainly focused on offloading the common contents shared by all users, and assumed that they can tolerate unlimited delay of the required data, which is not practical for delay-sensitive applications such as private photo sharing via Instant Messenger, webpage requesting, etc. As users can only utilize the bandwidth of the associated AP to serve such delay-sensitive data tasks, if the service delay exceeds a certain threshold, cellular networks should take over to serve these tasks.

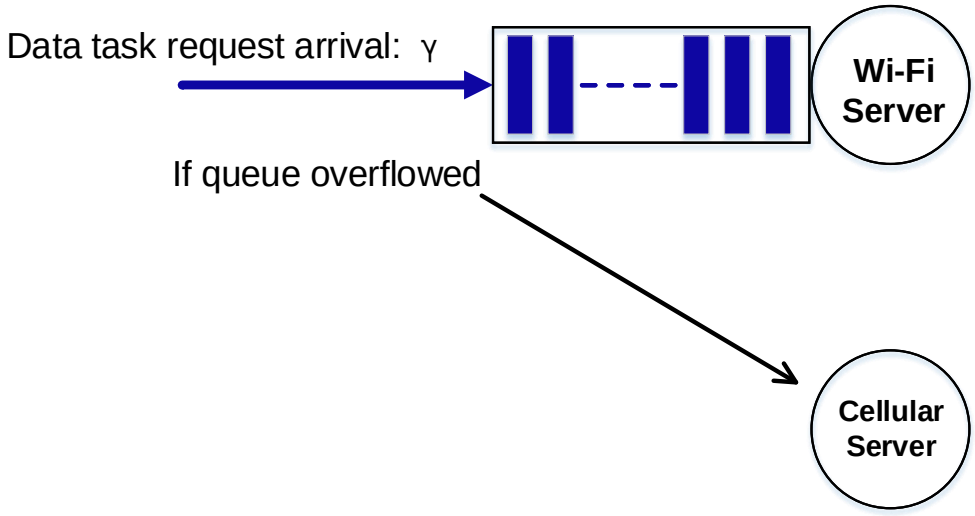

Figure 2.2: Queueing model for vehicular traffic offloading

2.3.2 Offloading queueing model

As shown in Fig. 2.2, the arrivals and fulfillments of a data task are modeled as a queueing process to analysis the trade off between the offloading performance and average data task service delay. In this thesis, we employ the M/G/1/K queue model, where M means the inter arrival time follows the exponential distribution, while G indicates the service time to fulfill a data task follows a general distribution due to the intermittent connection between

a vehicle and roadside APs. The task queue is of finite space K. When the queue is not full, the arriving task will enter into the queue and then be served by WiFi. Otherwise (namely, all K spaces are used up), the task will be blocked and be served by cellular connection to avoid the waiting time in the queue. The queue size K can be adjusted to trade off between the offloading performance and the service delay. A larger value of K results in lower probability of blocking queue, and thus more data tasks can be offloaded by WiFi, at the cost of longer delay these tasks are served. And a small value of K will lead to less offloaded data tasks but shorter service delay.

2.4 Summary

In this chapter, we have introduced the vehicular WiFi Internet access benefits, and provided background knowledge regarding to the access procedure for drive-thru Internet, including existing schemes for the network detection, user authentication and network parameters assignment steps. We have also introduced the traffic offloading diagram based on the drive-thru Internet, together with a queueing model which is used to analyze the offloading performance.

Chapter 3

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

In this chapter, we investigate the Internet access delay for vehicles via a roadside AP. 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 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 is obtained for the WPA2-PSK and WPA2-802.1X authentication methods, under various wireless channel conditions and for various numbers of contending WiFi users.

3.1 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 [63] and Hotspot 2.0 [52], and the authentication mechanism,

e.g., IEEE 802.1X [64] and Extensible Authentication Protocol (EAP) [65,66]. For instance, Figs. 3.1 and 3.2 respectively show the sequence of management frames exchanged between a vehicle and the AP for the WPA2-PSK and WPA2-802.1X authentication methods. To simplify our analysis, the delay of detecting roadside AP via reception 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 thesis. 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. 3.2, 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. 3.1 and 3.2, 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 [67].

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 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 [67], 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

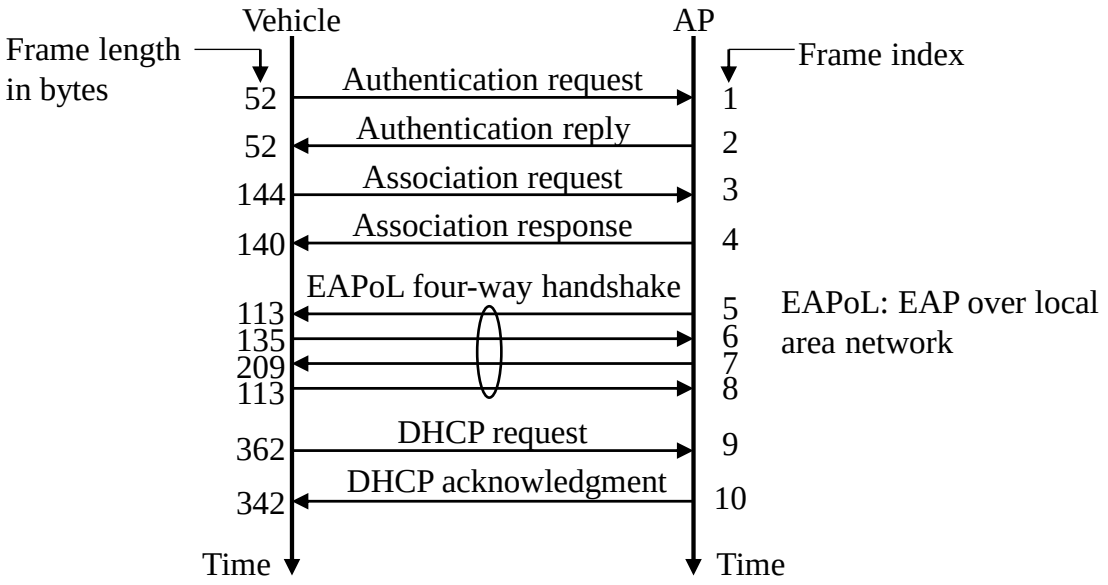

Figure 3.1: Management frames exchanged between a vehicle and an AP based on the WPA2-PSK mode for authentication ($N_f = 10$)

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 [67]. 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, 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

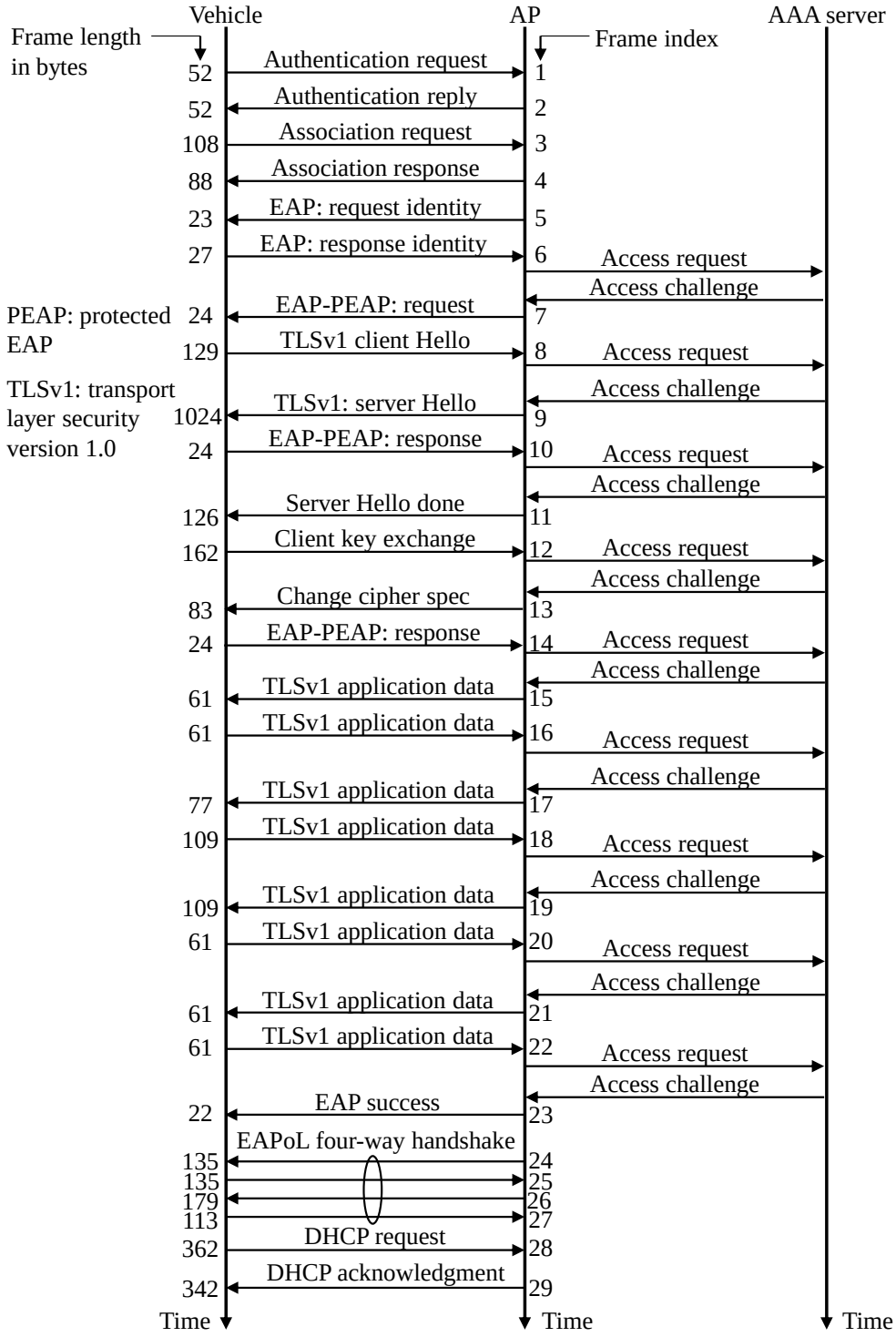

Figure 3.2: Management frames exchanged between a vehicle and an AP based on the WPA2-802.1X mode for authentication ($N_f = 29$)

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 SIFS and ACK transmission durations is neglected [67].

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.

3.2 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 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 3.1, 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[1]. 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. 3.3. Therefore, in order to calculate the average access delay, the main idea is to find the average duration

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

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.

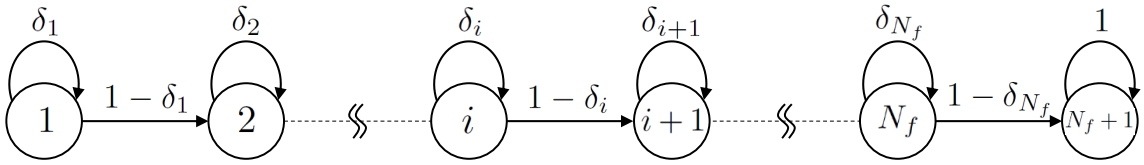

Figure 3.3: Illustration of the Markov chain and one-step transition probabilities for states 1 to $N_f + 1$

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

$$p_{ij} = \begin{cases} \delta_i, & i = j = 1, ..., N_f \\ 1, & i = j = N_f + 1 \\ 1 - \delta_i, & i = j - 1 = 1, ..., N_f \\ 0, & \text{elsewhere.} \end{cases} \tag{3.1}$$

In (3.1), the value of δ_i can be obtained by extending Bianchi's DCF model [68] to account for the frame loss due to channel conditions[2]. That is, for each $i = 1, ..., N_f$, the value of δ_i is calculated by solving the system of equations (3.2a-3.2c) in variables τ_i, α_i, and δ_i:

$$\tau_i = \frac{2(1 - 2\delta_i)}{(1 - 2\delta_i)(w + 1) + \delta_i w(1 - (2\delta_i)^{m-1})} \tag{3.2a}$$

$$\alpha_i = 1 - (1 - \tau_i)^{n_i - 1} \tag{3.2b}$$

$$\delta_i = 1 - (1 - \alpha_i)(1 - \beta_i). \tag{3.2c}$$

To show that there exists a unique value for each of τ_i, α_i, and δ_i, from (3.2c) and (3.2b) we have

$$\tau_i = 1 - \left(\frac{1 - \delta_i}{1 - \beta_i}\right)^{\frac{1}{n_i - 1}}. \tag{3.3}$$

[2]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 [68], until the i^{th} frame is successfully delivered.

Therefore, using (3.2a) and (3.3), we can prove the existence and uniqueness of the solution for the system of the three equations (3.2a-3.2c) following a similar approach as in [68]. Given the one-step transition probabilities in (3.1), the first passage time probabilities can be obtained using

$$f_{ij}^{(1)} = p_{ij} \tag{3.4a}$$

$$f_{ij}^{(n)} = \sum_{\substack{k=1 \\ k \neq j}}^{N_f+1} p_{ik} f_{kj}^{(n-1)}, \quad n > 1 \tag{3.4b}$$

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. 3.3, $\sum_{n=1}^{\infty} f_{ij}^{(n)} = 1$ 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 (3.4a-3.4b), and by noting that $f_{ij}^{(n)} \neq 0$ only if $n \geq j - i$ (Fig. 3.3), the expected value of D_{ij} is given by

$$\begin{gathered} \mathbb{E}(D_{ij}) = \sum_{n=j-i}^{\infty} \mathbb{E}(D_{ij}^{(n)}) f_{ij}^{(n)}, \\ i, j \in \{1, ..., N_f + 1\} \text{ and } i < j \end{gathered} \tag{3.5}$$

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 (3.5), by setting $i = 1$ and $j = N_f + 1$. However, in order to evaluate (3.5) 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

$$\Omega_{ij}^{(n)} = \begin{cases} \{i\}, & j = i+1 \\ \{i+1\}, & j = i+n \\ \{i, i+1\}, & \text{elsewhere.} \end{cases} \tag{3.6}$$

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

$$\begin{aligned} \mathbb{E}(D_{ij}^{(n)}) &= \sum_{k \in \Omega_{ij}^{(n)}} \mathbb{E}(D_{ij}^{(n)} | K_{ij}^{(n)} = k) \frac{p_{ik} f_{kj}^{(n-1)}}{f_{ij}^{(n)}} \\ &= \sum_{k \in \Omega_{ij}^{(n)}} \left(\mathbb{E}(D_{ik}^{(1)}) + \mathbb{E}(D_{kj}^{(n-1)}) \right) \frac{p_{ik} f_{kj}^{(n-1)}}{f_{ij}^{(n)}}, \\ i, j \in &\{1, ..., N_f + 1\}, i < j, \text{ and } n \geq \max(j - i, 2). \end{aligned} \tag{3.7}$$

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

$$\begin{gathered} \mathbb{E}(D_{ik}^{(1)}) = \mathbb{E}(U_i) + \mathbb{E}(V_i) + \text{DIFS} + \mathbb{E}(R_{ik}), \\ i \in \{1, ..., N_f\} \text{ and } k \in \{i, i+1\} \end{gathered} \tag{3.8}$$

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 [67]; 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[3]. 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

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

is given by

$$P_{B_i}(b) = \begin{cases} \delta_i^b(1-\delta_i), & b = 0, ..., m-2 \\ 1 - \sum_{q=0}^{m-2} \delta_i^q(1-\delta_i), & b = m-1. \end{cases} \tag{3.9}$$

Hence,

$$\begin{aligned} \mathbb{E}(U_i) &= \sum_{b=0}^{m-1} \mathbb{E}(U_i|B_i = b) P_{B_i}(b) \\ &= \mathbb{E}(U_i|B_i = 0) P_{B_i}(0) \end{aligned} \tag{3.10}$$

$$\begin{aligned} \mathbb{E}(V_i) &= \sum_{b=0}^{m-1} \mathbb{E}(V_i|B_i = b) P_{B_i}(b) \\ &= \mathbb{E}(V_i|B_i = 0) P_{B_i}(0) \end{aligned} \tag{3.11}$$

$$\begin{aligned} \mathbb{E}(R_{ik}) &= \sum_{b=0}^{m-1} \mathbb{E}(R_{ik}|B_i = b) P_{B_i}(b), \\ & i \in \{1, ..., N_f\} \text{ and } k \in \{i, i+1\}. \end{aligned} \tag{3.12}$$

In (3.10), the value of $\mathbb{E}(U_i|B_i = 0)$ can be found for a given probability density function of U_i, while in (3.11), 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.,

$$\mathbb{E}(V_i|B_i = 0) = h + \frac{l}{r} + \text{SIFS} + \frac{a}{r} \tag{3.13}$$

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 [67]. In (3.12), the conditional expectation $\mathbb{E}(R_{ik}|B_i = b)$ can be calculated using (3.14a)-(3.14b) as follows:

$$\mathbb{E}(R_{ii+1}|B_i = b) = \mathbb{E}(C_b)\mathbb{E}(S_i) + y_{ib} \tag{3.14a}$$

$$\begin{aligned} \mathbb{E}(R_{ii}|B_i = b) &= \mathbb{E}(C_b)\mathbb{E}(S_i) + z_{ib} \\ i \in \{1, ..., N_f\} &\text{ and } b \in \{0, ..., m-1\} \end{aligned} \tag{3.14b}$$

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

Table 3.1: Parameter values used to generate the analytical, simulation, and experimental results

Param	**Value**	**Param**	**Value**	**Param**	**Value**	**Param**	**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. 3.2
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. 3.1
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 $i = 1, ..., N_f$	—	—

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 $2^b w - 1$ [67], the expected value $\mathbb{E}(C_b)$ is given by

$$\mathbb{E}(C_b) = \frac{2^b w - 1}{2}, b \in \{0, ..., m-1\}. \tag{3.15}$$

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

$$y_{ib} = h + \frac{l_i}{r_{ib}} + \text{SIFS} + \frac{a}{r_{ib}} \tag{3.16a}$$

$$z_{ib} = h + \frac{\beta_i(1-\alpha_i)}{\delta_i}\frac{l_i}{r_{ib}} + \frac{\alpha_i}{\delta_i}\max(\frac{l_i}{r_{ib}}, \frac{l}{r}) \tag{3.16b}$$

$$i \in \{1, ..., N_f\} \text{ and } b \in \{0, ..., m-1\}.$$

Note that, in (3.16b), 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.

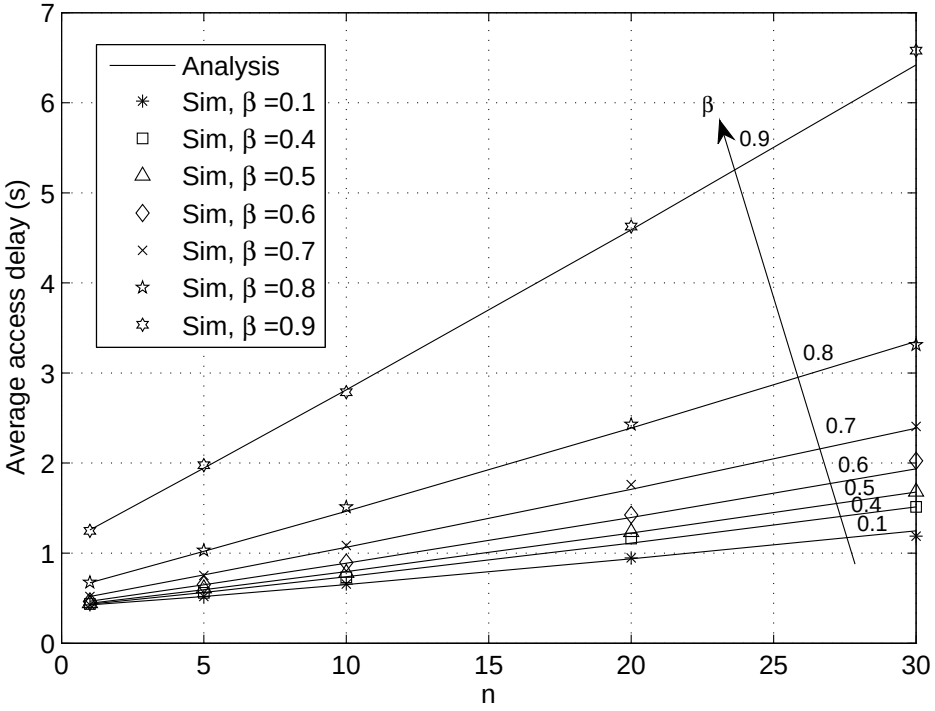

Figure 3.4: Management frames exchanged between a vehicle and an AP based on the WPA2-802.1X mode for authentication ($N_f = 29$)

Finally, the value of $\mathbb{E}(S_i)$ can be obtained using (3.17a)-(3.17c), given by

$$\mathbb{E}(S_i) = (1-\zeta_i)\sigma + \zeta_i\Big(h + \frac{l}{r} + \text{DIFS}\Big) + \nu_i\Big(\text{SIFS} + \frac{a}{r}\Big) \tag{3.17a}$$

$$\zeta_i = 1 - (1-\tau_i)^{n_i - 1} \tag{3.17b}$$

$$\nu_i = (1-\beta_i)(n_i - 1)\tau_i(1-\tau_i)^{n_i - 2} \tag{3.17c}$$

$$i \in \{1, ..., N_f\}$$

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

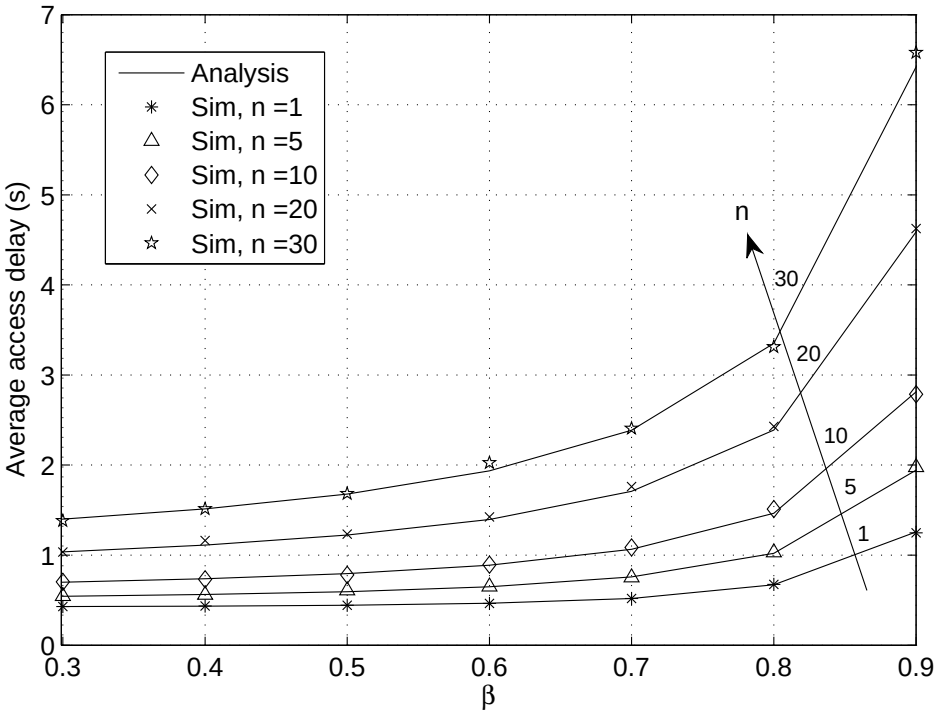

Figure 3.5: Management frames exchanged between a vehicle and an AP based on the WPA2-802.1X mode for authentication ($N_f = 29$)

using (3.1)-(3.4) and (3.6)-(3.17), the expected value of the first passage delay, $\mathbb{E}(D_{ij})$, from a state i to another state j can be obtained from (3.5). By setting $i = 1$ and $j = N_f + 1$, the value of $\mathbb{E}(D_{1N_f+1})$ represents the average access delay.

3.3 Analytical and Simulation Results

This section provides numerical results based on the mathematical analysis in Section 3.2 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 [64]; while the second authentication mechanism is based on the WPA2-PSK mode, which is mainly employed

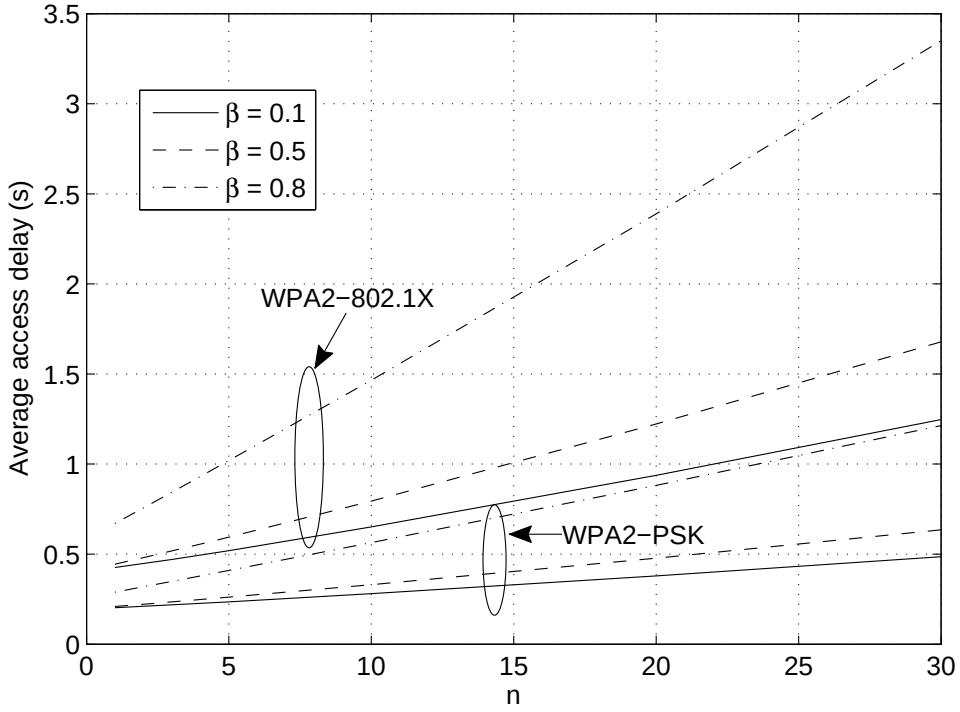

Figure 3.6: Comparison of the access delay performance for the WPA2-802.1X and WPA2-PSK authentication mechanisms

for home and small office networks and does not require an authentication server [65]. 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 3.2) 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 3.4. The experiment in Section 3.4 also provides the average processing delay for each management frame, $\mathbb{E}(U_i|B_i = 0)$ $\forall i$ in (3.10). This section also includes

Table 3.2: 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

computer simulations using MATLAB, in order to study the accuracy of the mathematical analysis presented in Section 3.2. 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 3.1. 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 3.1, which are from the 802.11n standard and measurement result from a real WiFi system.

Fig. 3.4 and Fig. 3.5 shows the access delay performance when the WPA2-802.1X mode is used for authentication. As shown in Fig. 3.4, 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. 3.4, 3.5, 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. 3.5 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. 3.5. 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 3.2. The same behavior of the average access delay illustrated in Fig. 3.4, 3.5 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. 3.1 and 3.2). Fig. 3.6 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.

3.4 Experimental Testing

To further study the accuracy of the analytical model in Section 3.2, 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.

3.4.1 Experiment Framework

As shown in Fig. 3.7, 3.8, 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 3.2, 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 [52], 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

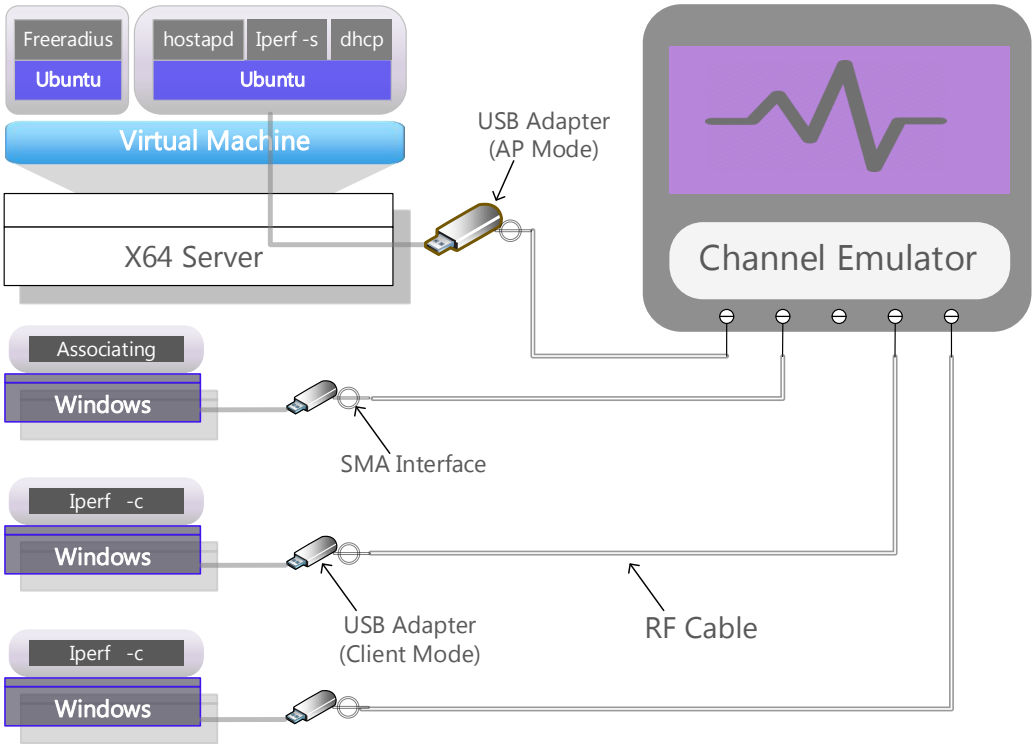

Figure 3.7: Experiment framework

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 [69].

Authentication Server: As shown in Fig. 3.2, 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 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. 3.7, and all the IP addresses are assigned on the same subnet as the AP interface.

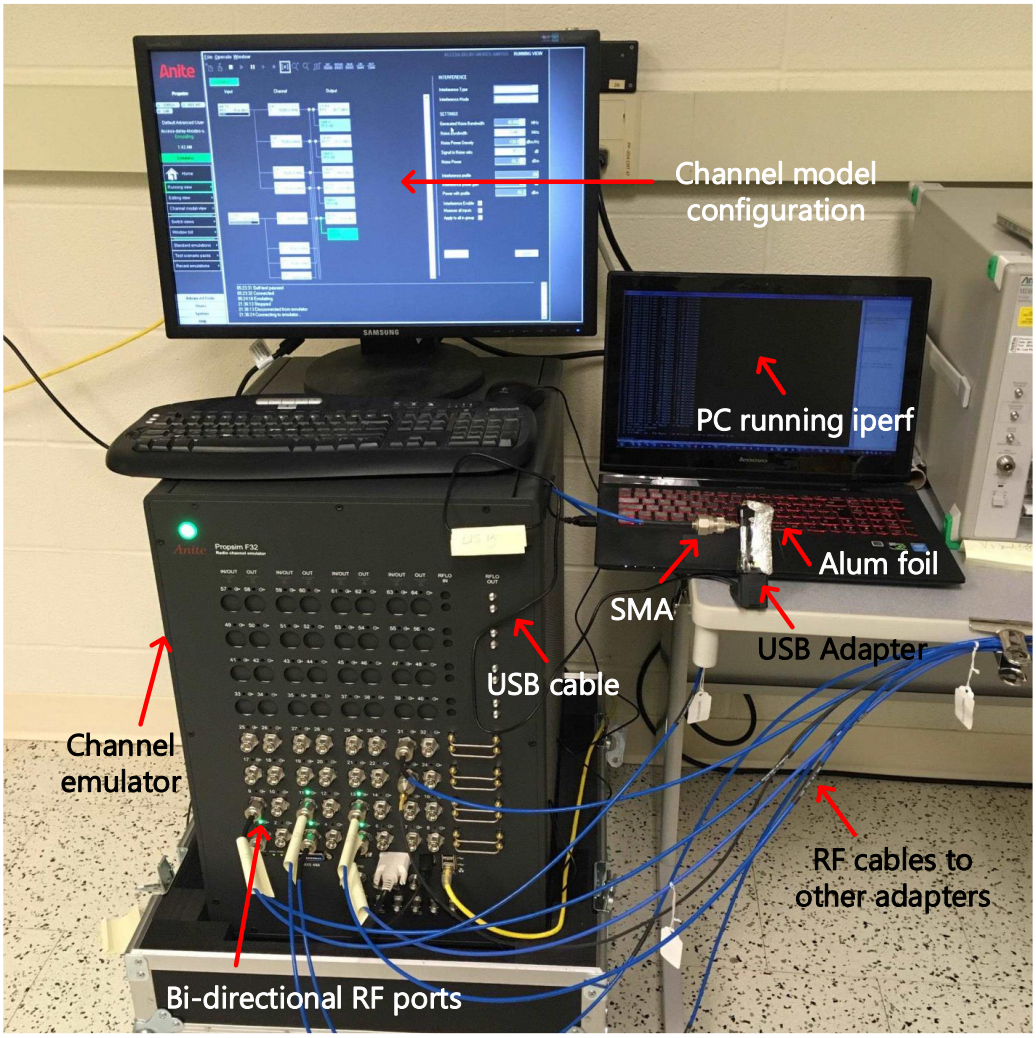

Figure 3.8: Experiment devices

Channel Emulator: We use the Propsim F32 channel emulator, which emulates the

Table 3.3: Test cases

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

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 [70][4]. The channel models used for communication between the AP and any vehicle, and between any two vehicles are illustrated in Figs. 3.9 and 3.10, 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 [70]. The signal received by the AP or any vehicle is corrupted by additive white Gaussian noise (AWGN), and the SNR is set to either 40 dB or 35 dB. These SNR values result in two different β values, as discussed next.

Test Procedure: The test cases under consideration are summarized in Table 3.3. Given the channel model between the tagged vehicle and the AP, the values of β that correspond 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 3.3. 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.

[4]The two channel models under consideration are referred to in [70] as 1) RTV expressway and 2) V2V expressway same direction with wall.

Table 3.4: Difference between the average access delay values obtained from the analysis in Section 3.2 and the experiments in Section 3.4

		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**		

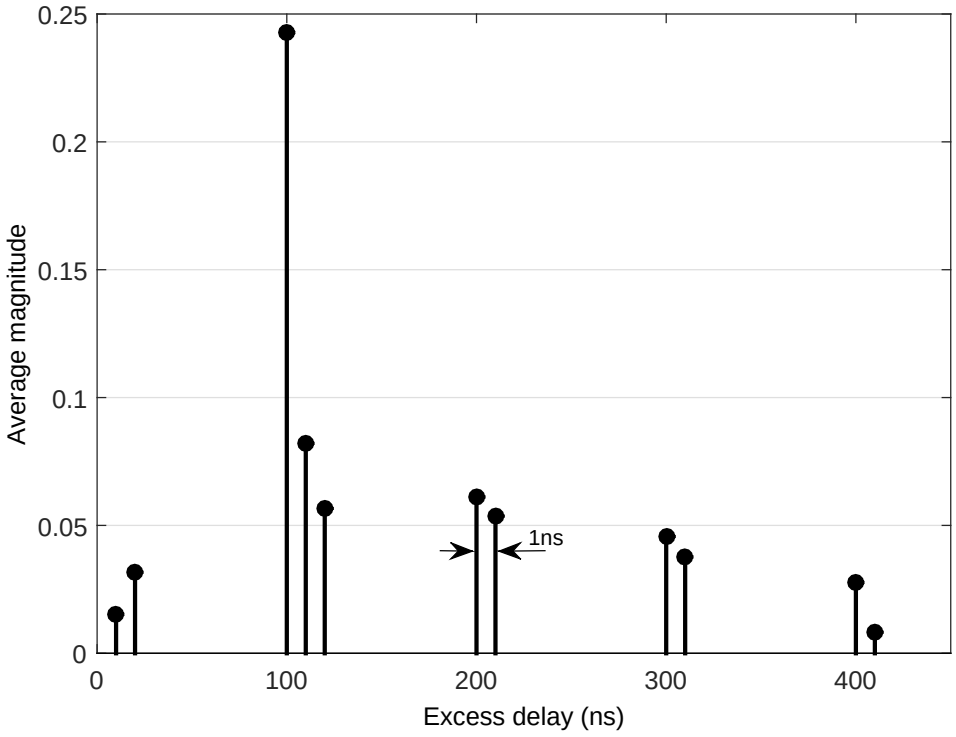

Figure 3.9: The V2R channel models used in the experiments

For each test case in Table 3.3, 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

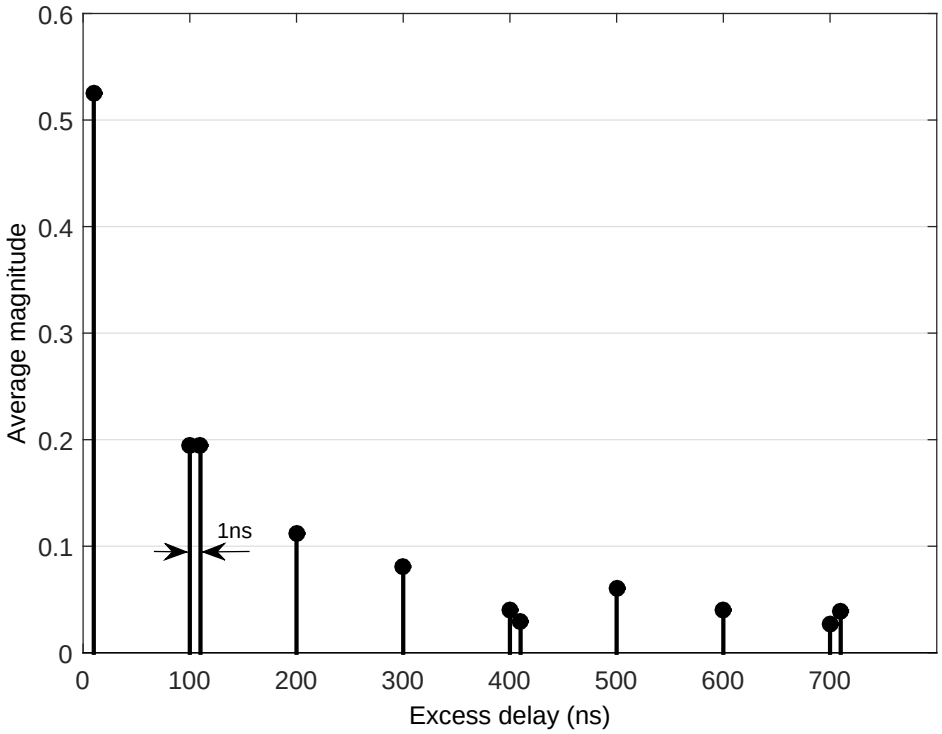

Figure 3.10: The V2V channel models used in the experiments

protocol analyzer, which captures all the frames transmitted or received by the AP[5]. 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 3.1, which are the same as those used to generate the numerical and simulation results in Section 3.3.

3.4.2 Test Results

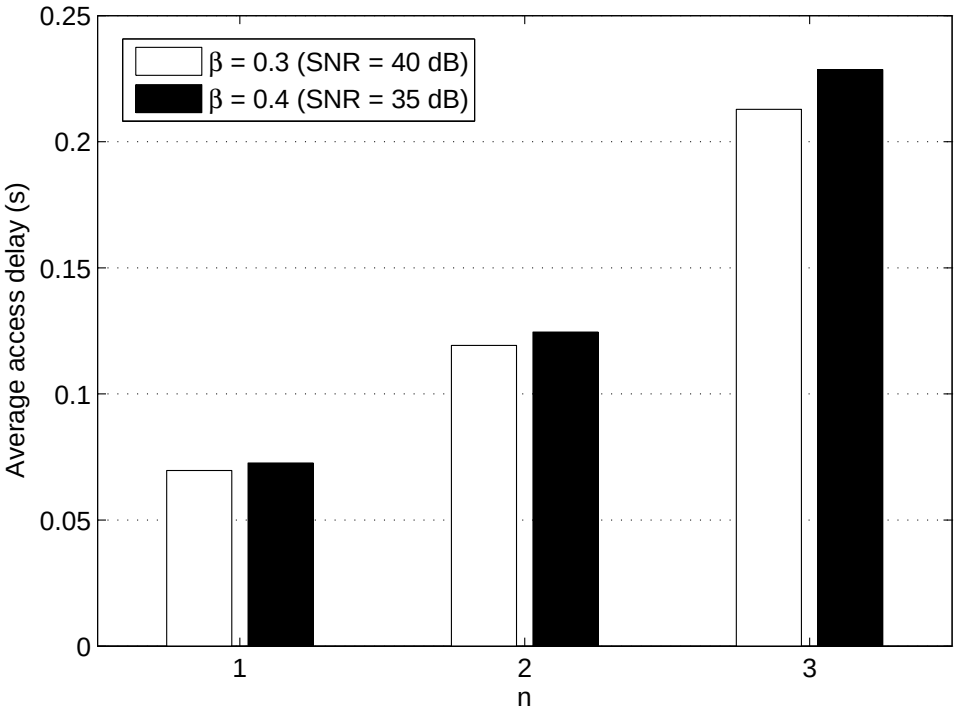

Figure 3.11: Experimental results of the access delay when the WPA-PSK mode is employed for authentication

The performance of the access delay for the test cases under consideration is shown in Figs. 3.11 and Fig. 3.12. It can be seen 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. 3.5. Table 3.4 lists the difference between the average access delay values obtained from the analysis in Section 3.2 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

[5]The first four frames in Figs. 3.1 and 3.2 could not be captured in any experiment.

experimental results are the additional (random) delay introduced by the channel emulator, which is not accounted for in the access delay calculation.

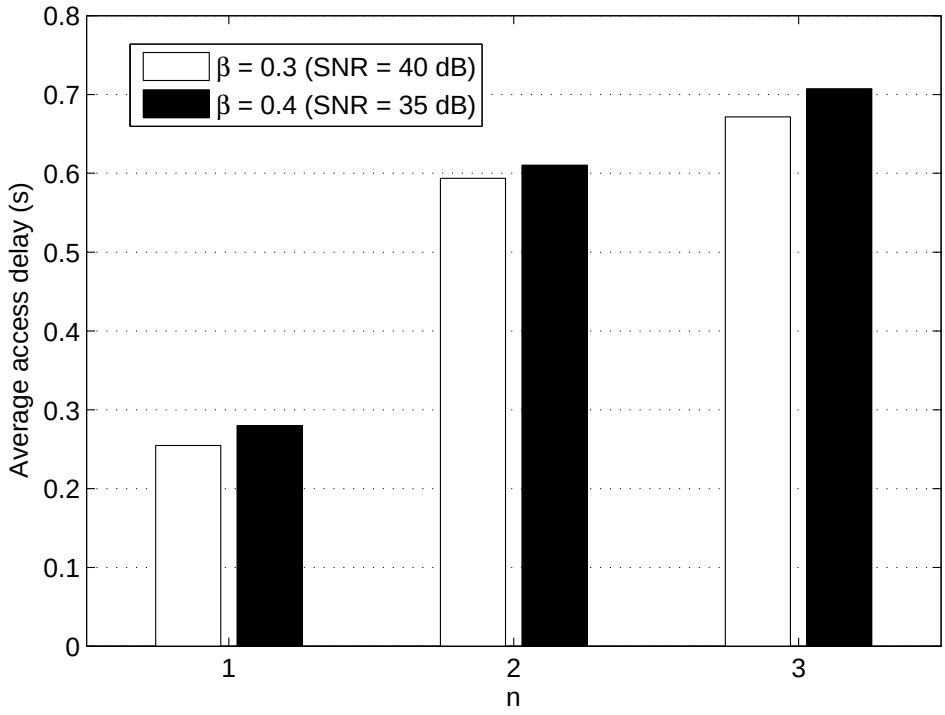

Figure 3.12: Experimental results of the access delay when the WPA2-802.1X standard are employed for authentication

3.5 Conclusion

In this Chapter, 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 Internet access schemes.

Chapter 4

Throughput Analysis for Drive-Thru Internet Access

In this chapter, we investigate the throughput performance of the drive-thru Internet considering the impact of the access procedure. Particularly, a 3D Markov model is proposed to analyze the relationship between the vehicle's position and the accomplishment of the access procedure that involves the exchange of the management frames under different conditions, e.g., number of contending WiFi clients, number of management frames, their drop rate due to channel error, etc. We also study two access schemes, namely, Hotspot 2.0 and WPA2-PSK, to show how different access protocols can affect the throughput performance. We conduct extensive simulations to validate our analysis, which could provide provident insight for future development of vehicular networks.

4.1 System Model

The system model is elaborated in the following parts, including the network model, zone transition model and Medium contention model.

4.1.1 Network model

As shown in Fig. 4.1, a stretch of road is covered by a WiFi AP located at the roadside. As soon as the vehicle drives into the coverage area where the SNR grows to certain level, the access procedure is started, and before its accomplishment the vehicle cannot transmit any

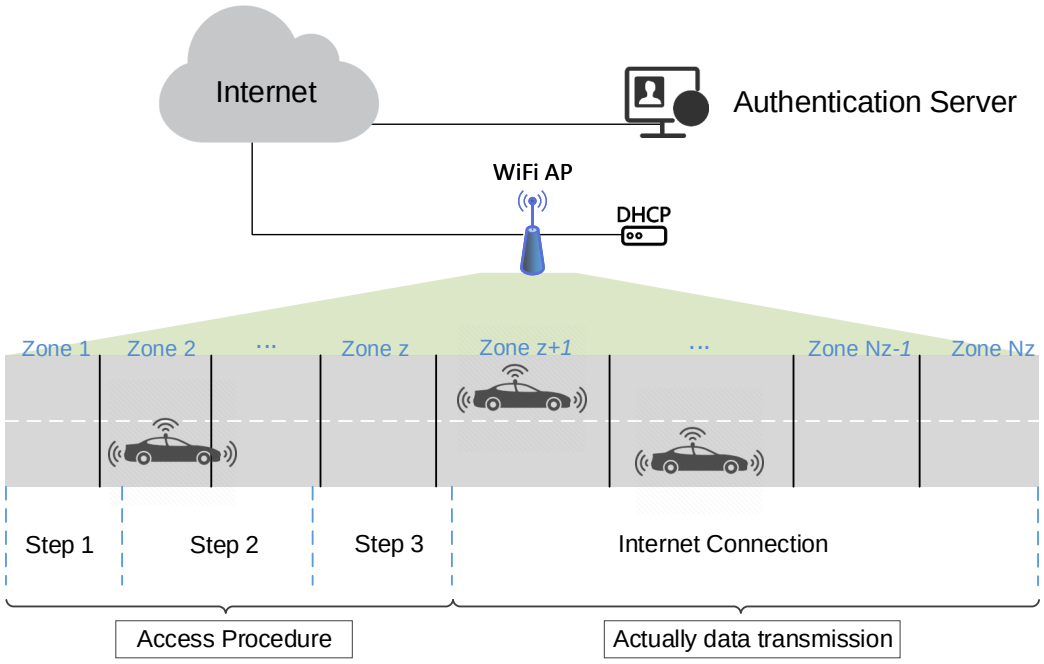

Figure 4.1: System model

data frame to the AP. Two common kinds of access protocols are considered in the access procedure, i.e., the WPA2-PSK and Hotspot 2.0. The total number of the management frames during the access procedure for the two protocols are different, and in following analysis it is denoted by N_A.

WPA2-PSK

WPA2-PSK is widely adopted in domestic WiFi networks, which verifies the user name and password locally to allow users to access to the WiFi resource. WPA2-PSk requires limited frames to be exchanged and no backhaul delay is involved. We use traditional beaconing schemes for the initial handshake between vehicle and AP for network detection.

Hotspot 2.0

Hotspot 2.0 is put forward to provide the seamless roaming for WiFi users [50]. WiFi network is detected by exchanging the ANQP frames with the network users. Hotspot 2.0 adopts the 802.1X authentication method, which requires the handshake between the

Table 4.1: Management frames of access protocols

Access Scheme	**Hotspot 2.0**			**WPA2-PSK**		
Step	Protocol	N_A	Backhaul	Protocol	N_A	Backhaul
AP Detection	ANQP handshake	2	N	Beaconing	2	N
Authentication	802.1X	27	Y	PSK	8	N
IP address	DHCP	2	N	DHCP	2	N

vehicle user and the remote authentication server, and thus introduce the backhaul delay to generate some management frames.

The IP address is assigned if the vehicle is successfully authenticated via a local DHCP server, which requires two DHCP request and reply frames to be exchanged[1]. The information of the management frames for both two access schemes are summarized in Table 4.1.

Assuming there are already n WiFi clients (except the approaching vehicle, can be other vehicles or other types of users) associated to the same AP and keep on sending packets to it, i.e., under a saturated traffic situation. As the access procedure takes places in the edge of the network coverage area, the transmission of the management frames is likely to fail due to the unreliable channel condition, whose probability is denoted by β. According to 802.11 protocol, the link modulation rate depends on the SNR level, which is mainly determined by the distance between the AP and the vehicle [26] [71]. The link rate is assumed to be the same within a specific zone in the coverage area, which is defined in the following subsection.

4.1.2 Zone model

Inspired by [26] [72], the road stretch covered by the WiFi AP can be divided into N_z zones based on the modulation link rate between the vehicle and the AP. And as the vehicle drives through the coverage area, it traverses the zones consecutively. The duration the vehicle stays in an arbitrary zone z, denoted by t_z, equals to d_z/v, where d_z is the size of the zone. The link rate when the vehicle is in zone z is denoted by r_z. Similar to [26], the time a vehicle stay in each zone is approximated as an geometrical variable with mean of t_z. Within an relatively small duration δ, the probability that the vehicle in zone z will transit to the next zone $z+1$ equals to δ/t_z, and two consecutive transitions are independent.

[1]It is also possible to deploy a remote DHCP server to assign the IP address while the AP is served as an DHCP proxy. Such case requires more DHCP management frames and introduce backhaul delay

4.1.3 Medium contention model

To investigate the affect of co-transmission from contending WiFi clients, e.g., vehicles associated to the same AP, the media access procedure for each management frame is also investigated. We apply the 802.11 DCF without employing the RTS/CTS scheme, and the minimum contention windows size is denoted by w, while the number of the back off stages is denoted by m.

4.2 3D Markov chain based Throughput Analysis

In this section, we adopt a 3D Markov chain to demonstrate the proceeding of the access procedure, which includes the dimensions of back off procedure, management frame index sequence and zone transition. We first build a 1D Markov chain for the back off stage transition when transmitting a certain management frame, and then expand it to a 2D Markov chain by considering the sequence of the management frames. And by sampling the beginning and ending moments of each status in this 2D Markov chain for the zone transition process, we finally form a 3D Markov chain model, which is used to calculate the relationship between the vehicle position and the accomplishment of access procedure, which is then used to obtain the drive-thru Internet throughput.

4.2.1 Dimension of back off procedure

Consider the kth management frame during the access procedure, which should be generated before transmission. The frame generation involves the local protocol process, potential backhaul handshake, and network framing. The whole procedure is defined as the *core process*, after that the frame is sent based on the 802.11 DCF, which incurs the back off procedure with a random back off counter C_i at stage i, $i \in [0, m-1]$, and the initial

stage i is set to 0:

1) The back off counter C_i is uniformly selected from $[0, w * 2^i - 1]$, where w is the minimum window size.

2) If the channel is sensed idle, then decrease the back off counter per time slot; if the channel is busy, then freeze the back off counter.

3) If the C_i decreases to zero, then attempt to transmit the frame to air;

4) If the transmission fails either due to collision or channel error, then increase the stage value i by one until to its maximum value, and go to step 1).[2]

5) If the transmission is successful and the corresponding ACK is received, then jump to the frame generation (*core process*) of the next management frame.

As the frame generation is independent with the frame transmission, and any transmission attempt is independent with the previous one, by sampling the end moment of each transmission attempt, the transition of the back off stage value i forms a discrete time Markov Chain [68], as demonstrated in Fig. 4.2, the triangle represents the status of *core process*, i.e., management frame generation, whose duration is denoted by $t_{c,k}$, while the circle represents the ith back off stage.

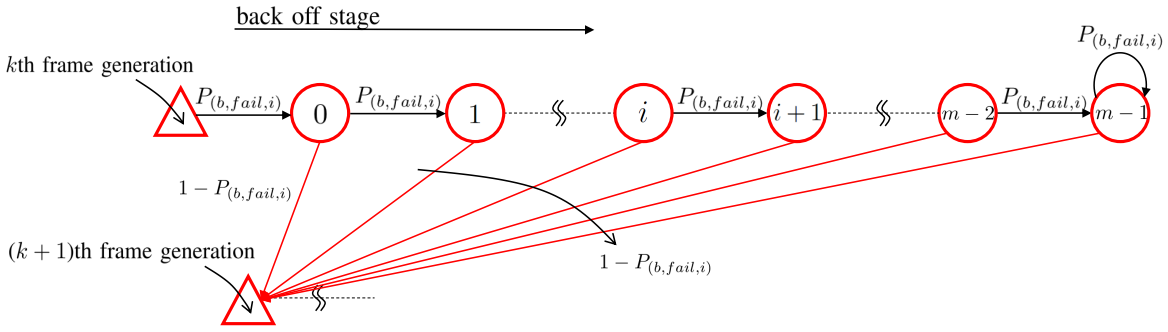

Figure 4.2: Dimension of back off procedure

The one-step transit probability when transmitting kth management frame can be obtained via Bianchi's method in equation (3.2a-3.2c), which is denoted by $P_{(b,fail,k)}$. Denote ρ_k the probability of collision for a transmission attempt of the kth frame, β_k the probability that the transmission of kth management frame fails due to channel error. Given

[2]There is no try limit to transmit a frame.

current stage is i, the next stage will be $i+1$ if the transmission fails, otherwise it will directly jump to the *core process* of the $(k+1)$th management frame.

The average time during the status of the kth frame's *core process*, $\mathbb{E}(t_{c,k})$, depends on the access protocol and the backhaul network status, and can be measured from a real WiFi system [73]. The average time during each back off stage i can be calculated by

$$\mathbb{E}(T_i) = \mathbb{E}(T_{idle}) + \mathbb{E}(C_i) * \mathbb{E}(T_\sigma) + P_s * T_s + P_{us} * T_{fail} \tag{4.1}$$

where $\mathbb{E}(T_{idle})$ is average duration to sense the channel to be idle and then the back off procedure can be invoked, which can be approximated to the time for successfully transmitting a data frame in saturated condition:

$$\mathbb{E}(T_{idle}) = T_h + \frac{L_d}{r_{d,z}} + \text{SIFS} + \frac{L_{ack}}{r_{ack}} \tag{4.2}$$

T_h is the time to transmit the physical header section of the wireless frame, such as the PLCP field, PLME field, etc. L_d is the length of the data frame and is assumed to be identical for all WiFi clients. $r_{d,z}$ is the modulated link rate of the data frame when the vehicle is located at zone z. SIFS is the length of the Short Interframe Space as specified in 802.11 protocol. L_{ack} and r_{ack} are the length and the rate of the ACK frame respectively.

The average value of the back off counter at stage i in equation (4.1) can be calculated as below since the counter is uniformly distributed in $[0, w * 2^i - 1]$

$$\mathbb{E}(C_i) = \frac{1}{2}(w * 2^i - 1) \tag{4.3}$$

$\mathbb{E}(T_\sigma)$ represents the average time spent to decrease one back off counter. Denote the length of a idle time slot in 802.11 protocol by σ, and T_σ may include several σ and back off durations, which can be calculated by considering three conditions. First, in a given slot, it is possible that all the other vehicles are not transmitting in the given time slot, whose probability is denoted by p_0, and in this situation, the time to decrease one back off counter equals to σ. Secondly, it is also possible that there is only one vehicle is transmitting in the given time slot with the probability of p_1, and if the transmission is successful, then it requires $t_{1,s}$ to decrease on back off counter:

$$t_{1,s} = T_h + \frac{L_d}{r_{d,z}} + \text{DIFS} + \text{SIFS} + \frac{L_{ack}}{r_{ack}} \tag{4.4}$$

And if the transmission fails due to channel loss with the probability of β_d, there is no

ACK frame and thus it requires $t_{(1,fail)}$ to decrease one back off counter:

$$t_{(1,fail)} = T_h + \frac{L_d}{r_{d,z}} + \text{DIFS} \tag{4.5}$$

Thirdly, if there are two or more other vehicles are transmitting, which means there will be transmission collision, whose probability is denoted to $p_{(2+)}$, then it also requires $t_{(1,fail)}$ to decrease one back off counter. And $\mathbb{E}(T_\sigma)$ can be calculated by

$$\begin{aligned}\mathbb{E}(T_\sigma) =& p_0\sigma + p_1 t_{1,s}(1-\beta_d) + t_{(1,fail)}[p_{(2+)} + p_1\beta_d] \\ =& (1-\rho_k)\sigma + p_1(1-\beta_d)(\text{SIFS} + \frac{L_{ack}}{r_{ack}}) \\ &+ (p_1 + p_{(2+)})t_{(1,fail)}\end{aligned} \tag{4.6}$$

where p_1 can be obtained by

$$p_1 = C_n^1 \tau_k (1-\tau_k)^{n-1} \tag{4.7}$$

and $p_1 + p_{(2+)}$ equals to the probability that there are one or more other vehicles are transmitting, which is ρ_k.

The probability that the management frame is transmitted successfully, denoted by P_s in equation (4.1), equals to $1 - P_{(b,fail,k)}$, while P_{us} equals to $P_{(b,fail,k)}$. The air time spent to successfully transmit the management frame T_s can be obtained via

$$T_s = T_h + \frac{L_k}{r_k} + \text{SIFS} + \frac{L_{ack}}{r_{ack}} \tag{4.8}$$

where L_k is the length of the kth management frame. And the air time spent if the transmission fails T_{fail} can be obtained by

$$T_{fail} = T_h + \frac{L_k}{r_k} * \frac{\beta_k(1-\rho_k)}{P_{b,fail,k}} + \frac{L_d}{r_{d,z}} * \frac{\rho_k}{P_{(b,fail,k)}} \tag{4.9}$$

where the second item in the above equation is an approximation of the air time to deliver the management frame given the condition that the transmission fails due to channel error, while the last item is the air time to deliver the data frame, as the transmission failure is caused by collision[3].

[3]The length of the data frame is larger than all the management frame.

4.2.2 Dimension of management frame delivery sequence

The frame generation and transmission of the $(k+1)$th management frame only depends on the previous kth management frame, and thus the frame index, namely, k, forms a discrete Markov chain that takes the value from $[1, N_A]$, as shown in Fig. 4.3. The last 'accessed' status of '$N_A + 1$' indicates that all the management frames are exchanged, i.e., the access procedure has been accomplished. A similar model based on the consecutive delivery of the management frames can be found in [73], where the accuracy is verified both in numerical simulation and experiment.

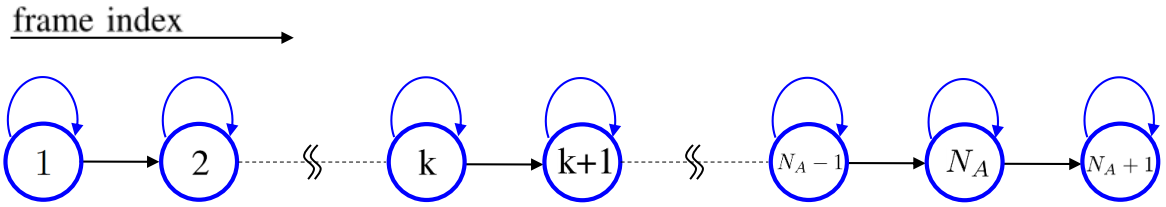

Figure 4.3: Dimension of frame delivery sequence

Since the transmission of each management frame is independent with each other, i.e., the back off stage altering of one frame is independent with another, thus, the Markov chain in Fig. 4.2 and the Markov chain in Fig. 4.3 together can form a 2D Markov chain of size $2N_A$ by m, which is shown in Fig. 4.4. In the dimension of the back off procedure, there are m status, while in the dimension of the frame sequence, there are $2N_A$ status, including the *core process* except the first frame (beaconing or ANQP query). And without loss of generality, the status of the vehicle can be denoted by a vector of (i, k) to indicate the transmission status of the management frame. The status of *core process* (in red triangles) indicates that the corresponding management frame is being generated. The last status, demonstrated in the blue square at rightmost, indicates the status of the accomplishment of the access procedure. And the average duration for each status can be obtained as stated in Section 4.2.1.

4.2.3 Dimension of zone transition: embedding 3D Markov chain

Based on the assumption that the time of the vehicle in an arbitrary zone z follows the geometric distribution, and the probability to transit to next zone $z+1$ equals to δ/t_z for a short time δ, while the vehicle transverses through the coverage area, the zone index of the vehicle forms another Markov chain, as demonstrated in Fig. 4.5. By adding the

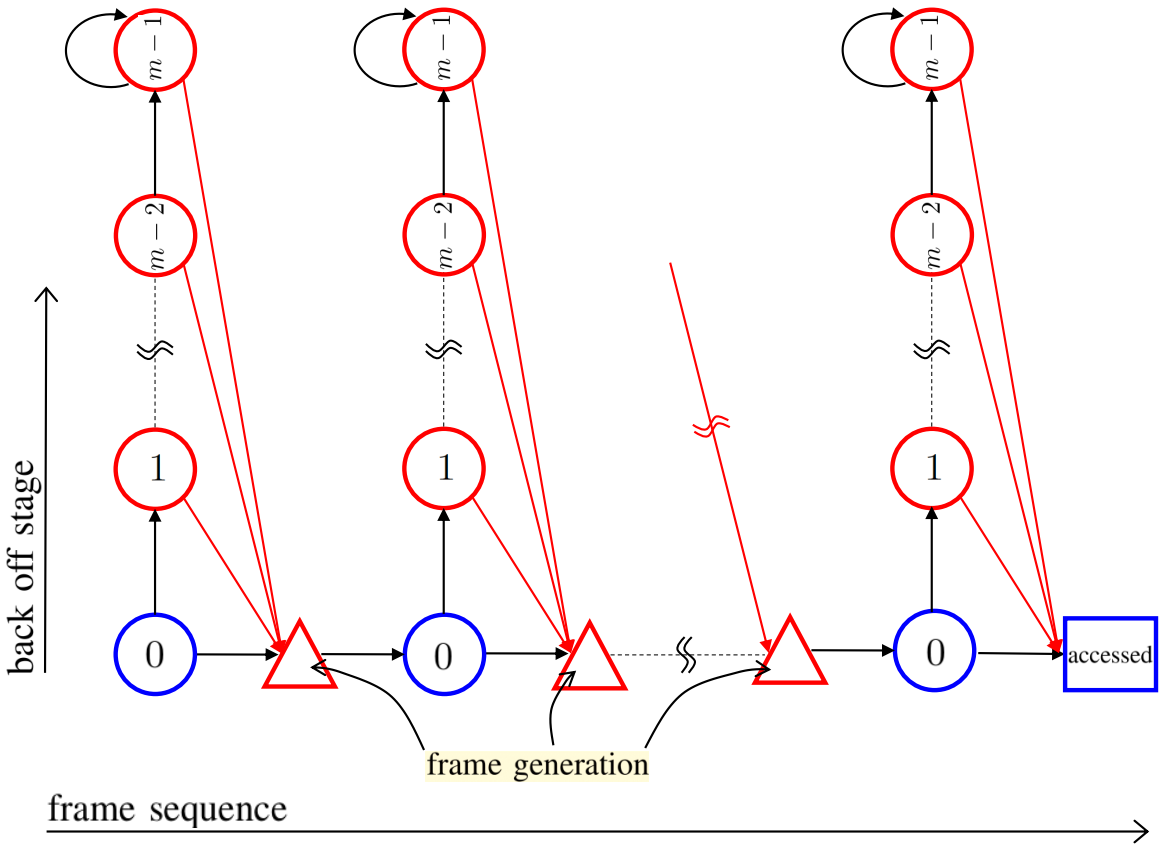

Figure 4.4: 2D Markov chain for back off procedure and frame delivery sequence

zone information to an arbitrary status in Fig. 4.4, we can describe the access procedure by three components: the back off stage i, the management frame index k and the zone index z, which are denoted by a vector of (i, k, z). As the zone transition depends solely on the mobility of the vehicle, and thus is independent with the transmission of the every management frame, by sampling the beginning moment and the ending moment of each status, the vector (i, k, z) forms an embedded 3D Markov chain, which is demonstrated in Fig. 4.6. The 3D Markov chain includes following dimensions, which indicates the relationship with the accomplishment of the access procedure and the location (in which zone) of the vehicle.

1) Back off stage dimension: the index i indicates the transmission of the currently management frame is in the back off process of stage i, i.e., the back off counter C_i is a

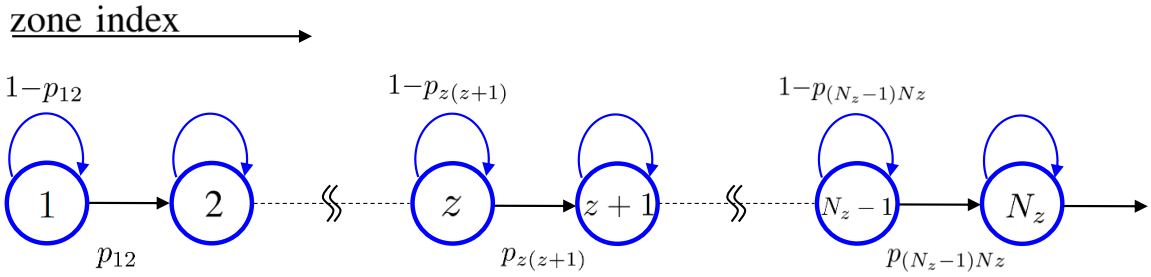

Figure 4.5: Markov chain for zone transition

uniformly distributed variable in $[0, w * 2^i - 1]$. The status begins at the ending moment of the previous transmission attempt and ends after the transmission attempt of this back off stage. In the *core process*, the frame is under construction and has not triggered the back off process, so when k is even, the corresponding back off stage index equals to 0.

2) management frame index dimension: when the index k is odd, it represents the transmission of $(k+1)/2$th management frame; when the index k is even, it means the next management frame is being generated, and when k equals to $2N_A$, it means the whole access procedure is accomplished and the data traffic can be transmitted immediately.

3) Zone index dimension: the index z indicates the location of the vehicle, i.e., the zone where the vehicle is located at the current moment. The smaller the zone index of the vehicle when finishing the access procedure, the earlier the vehicle can access to Internet, i.e., the higher the throughput can be achieved. The zone transition can possibly happen at the end of each status and the transition probability to the next zone depends on the average sojourn duration of the current status, i.e., given a status u while the vehicle is in zone z, then the probability that the next status will be in zone $z+1$ can be obtained by $P_u(z+1|z) = \mathbb{E}(T_u)/t_z$.

The one step transition probability of the 3D Markov chain can be obtained as follows. For a back off status (i, k, z) in Fig. 4.6, the next status after a transmission attempt can have four possibilities by considering the transmission result and the zone transition. If the transmission fails due to collision or channel error, while the vehicle stays in the same zone, then the next status will be $i+1, k, z$, or $m-1, k, z$ if the back off stage already reach the maximum value. The one step transition probability $\mathbb{P}(i+1, k, z|i, k, z)$ can be

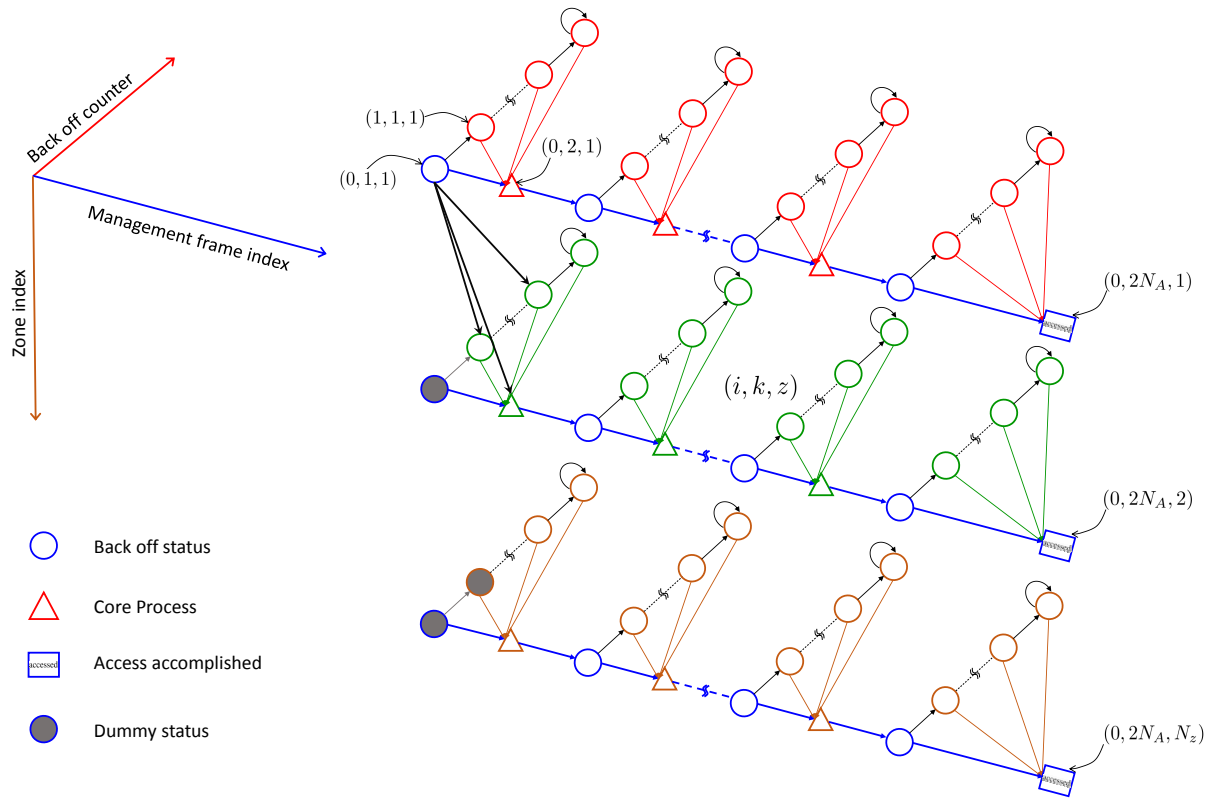

Figure 4.6: 3D Markov Chain Model for access procedure

obtained by

$$\begin{aligned}\mathbb{P}(i+1,k,z|i,k,z) &= P_{(b,fail,k)}(1-\frac{\mathbb{E}(T_{(i,k,z)})}{t_z}) \\ &= P_{(b,fail,k)}(1-\frac{\mathbb{E}(T_i)}{t_z}), \\ i \in [0,m-2], k \text{ is odd and} &\in [1,2N_A], z \in [1,N_z] \end{aligned} \tag{4.10}$$

and

$$\begin{aligned}\mathbb{P}(m-1,k,z|m-1,k,z) &= P_{(b,fail,k)}(1-\frac{\mathbb{E}(T_{(m-1,k,z)})}{t_z}) \\ &= P_{(b,fail,k)}(1-\frac{\mathbb{E}(T_{m-1})}{t_z}), \\ k \text{ is odd and} \in [1,2N_A], z \in [1,N_z] \end{aligned} \tag{4.11}$$

where $T_i, i \in [0, m-1]$ is the average duration when at the back off stage i, which can be obtained via equation (4.1). If $z \in [1, N_z - 1]$, i.e., not the last zone, and if transmission fails and the vehicle transits to next zone, then the next status will be $(i+1, k, z+1)$ (or $(m-1, k, z+1)$ if reaches maximum back off stage), whose probability can be obtained by

$$\begin{aligned}\mathbb{P}(i+1,k,z+1|i,k,z) &= P_{(b,fail,k)}\frac{\mathbb{E}(T_i)}{t_z}, \\ i \in [0,m-2], k \text{ is odd and} \in [1,&2N_A], z \in [1,N_z-1] \end{aligned} \tag{4.12}$$

and

$$\begin{aligned}\mathbb{P}(m-1,k,z+1|m-1,k,z) &= P_{(b,fail,k)}\frac{\mathbb{E}(T_{(m-1,k,z)})}{t_z} \\ &= P_{(b,fail,k)}\frac{\mathbb{E}(T_{m-1})}{t_z}, \\ k \text{ is odd and} \in [1,&2N_A], z \in [1,N_z-1] \end{aligned} \tag{4.13}$$

If the transmission is successful, then the next status will be the *core process* of the next management frame or the status of 'accessed' if all management frames are transmitted, i.e., $k = 2N_A - 1$. If the vehicle continues to stay in the current zone, then the next status will be $(0, k+1, z)$, and the one step transition probability can be obtained by

$$\begin{aligned}\mathbb{P}(0,k+1,z|i,k,z) &= (1-P_{(b,fail,k)})(1-\frac{\mathbb{E}(t_{c,k})}{t_z}), \\ k \text{ is odd and} \in [1,&2N_A], z \in [1,N_z] \end{aligned} \tag{4.14}$$

and if the vehicle moves to next zone, then

$$\mathbb{P}(0,k+1,z+1|i,k,z) = (1-P_{(b,fail,k)})\frac{\mathbb{E}(t_{c,k})}{t_z}, \\ k \text{ is odd and} \in [1,2N_A], z \in [1,N_z-1] \tag{4.15}$$

After the *core process*, the back off process is started as the management frame is ready to be transmitted. The next status will be the back off stage 0, and if the vehicle stays in current zone, the one step transition probability can be obtained by

$$\mathbb{P}(0,k+1,z|0,k,z) = (1-P_{(b,fail,k)})(1-\frac{\mathbb{E}(t_{c,k})}{t_z}), \\ k \text{ is even and} \in [1,2N_A-1], z \in [1,N_z] \tag{4.16}$$

and if the vehicle moves to next zone, then

$$\mathbb{P}(0,k+1,z+1|0,k,z) = (1-P_{(b,fail,k)})(1-\frac{\mathbb{E}(t_{c,k})}{t_z}), \\ k \text{ is even and} \in [1,2N_A-1], z \in [1,N_z-1] \tag{4.17}$$

After the N_Ath management frame is exchanged, i.e., the access procedure has been accomplished, the next status will be 'accessed', as the squares shown in the right side of Fig. 4.6. The next status depends on the zone transition, we assume that for each 'accessed' status, the average duration is set to a relatively small value, which is denoted by $T_{(accessed)}$. And the one step transition probability can be obtained by

$$\mathbb{P}(0,2N_A,z|0,2N_A,z) = 1-\frac{\mathbb{E}(T_{(accessed)})}{t_z}, \\ z \in [1,N_z] \tag{4.18}$$

and

$$\mathbb{P}(0,2N_A,z+1|0,2N_A,z) = \frac{\mathbb{E}(T_{(accessed)})}{t_z}, \\ z \in [1,N_z-1] \tag{4.19}$$

When transmitting the first management frame, if the vehicle transits to the next zone after a transmission attempt, it will never enter back to the previous back off stage, i.e., the vehicle will not enter into the status of $(0,1,1)$, whose limiting probability equals to

zero, which is defined as *dummy status*. Similarly, status of $(0,1,2)$, $(1,1,2)$, $(2,1,3)$, etc. are also *dummy status*. And hence, the number of overall status N_s is

$$N_s = \begin{cases} N_z(mN_A + N_A) - \frac{m}{2}(m-1), & m < z \\ N_z(mN_A + N_A) - \frac{z}{2}(z-1), & m \geq z \end{cases} \tag{4.20}$$

Assuming that as soon as the vehicle drives out of the WiFi network, it enters an identical WiFi coverage area and performs the access procedure again. Based on such renewal process, the expectation of the throughput of the drive-thru Internet can be obtained by letting the vehicle re-enters the same area infinitely and calculate the average value. Thus, for all status in the last zone in Fig. 4.6, i.e., $z = N_z$, the one step probability can be obtained by

$$\mathbb{P}(0,1,1|i,k,N_z) = \frac{\mathbb{E}(T_{(accessed)})}{t_z}, \quad i \in [0, m-1], k \in [1, 2N_A], \tag{4.21}$$

Denote the limiting probability of an arbitrary status (i,k,z) by $\gamma_{i,k,z}$, i.e., the stable probability that the vehicle is transmitting the kth management frame at back off stage i and located in zone z. Given the one step transition probabilities Matrix, denoted by $\mathcal{M}$, formed by equation (4.10) - (4.21), together with the following uniform condition for the 3D Markov chain, the limiting probability vector γ can be obtained by

$$\begin{cases} \gamma\mathcal{M} = \gamma \\ \gamma e^T = 1 \end{cases} \tag{4.22}$$

The probability that the vehicle is located in a certain zone $\mathcal{Z}$ can be calculated by

$$P(\text{in Zone } \mathcal{Z}) = \sum_{z=\mathcal{Z}} \gamma_{i,k,z} \tag{4.23}$$

Given the vehicle is in zone $\mathcal{Z}$, the conditional probability that the access procedure is accomplished can be calculated by

$$P(\text{accessed}|\text{in Zone}\mathcal{Z}) = \frac{\gamma_{0,2N_A,\mathcal{Z}}}{P(\text{in Zone } \mathcal{Z})} \tag{4.24}$$

Denote the throughput a vehicle can achieved in zone z given the access procedure has

been accomplished by $\mathscr{U}_z$, which can be obtained by

$$\mathscr{U}_z = \frac{r_z * t_z}{n+1} \tag{4.25}$$

where n is the number of the co-associated WiFi clients that share the bandwidth with the vehicle. And the overall throughput $\mathscr{U}_T$ can be calculated by

$$\mathscr{U}_T = \sum_{z=1}^{N_z} \mathscr{U}_z P(\text{accessed}|\text{in Zone } z) \tag{4.26}$$

4.3 Simulation Results

In this section, we conduct the simulation of a drive-thru Internet and compare the throughput performance with our analysis. We also discuss some potential usage of our model in future protocol design and development.

4.3.1 Simulation setup

The simulation scenario includes a WiFi AP at roadside, a tagged vehicle that repeatedly drive over the coverage area, several WiFi clients that representing the co-associated contending vehicles, which keep on transmitting the data frames to AP. The WiFi AP adopts the 802.11n (HT) protocol [28] and the date rate is determined based on the free space path loss model for each zone [74] [67], whose parameters are listed in Table 4.2.

According to the above specifications, the zone parameters can be calculated and are listed in Table 4.3. The link rates of the management frames are set to a constant value of 6 Mbps as observed from real access procedure, i.e., $r_k = 6$ Mbps. The link rate of the ACK frames are the same with the corresponding both management frames and data frames. The length and the *core processing* delay for the management frames are measured from a real system employing the protocols of Hotspot 2.0 and WPA2-PSK similar with which in [73].

In one simulation run, the tagged vehicle will immediately perform the access procedure by exchanging the management set of a certain protocol, and upon its accomplishment, the vehicles start to continually transmit the data frame to the AP, and the overall data amount transmitted is record when it drives out of the coverage area, whose average value is considered to be throughput performance. And the above procedure are repeated for at

Table 4.2: The WiFi parameters in simulation

Parameters	**Value**
DCF time slot size σ	9 μs
SIFS size	16 μs
DIFS size	34 μs
PHY header duration (preamble+PLCP header)	20 μs
Data frame length	1574 bytes
ACK frame length	32 bytes
AP radio power	18 dbm
Frequency	5.2 GHz
Noise level	-95 dbm

least 200 runs to obtain the average throughput, which will be presented and discussed in the next Sections.

4.3.2 Simulation result

Fig. 4.7 shows the average aggregate throughput of the vehicle, which is obtained when the tagged vehicle can exclusively use all the link bandwidth after the access procedure. The maximum back off stage is set to 7 and the minimum window size is set to 16 according to the 802.11n (HT) protocol. The aggregate throughput shows the available overall throughput of the AP for the tagged vehicle's remaining journey after the access procedure. It can be observed that aggregated throughput is not degraded severely until the management frame drop rate reach to a significant value. The aggregated throughput decreases when there are more contending clients, which leads to more collisions and result in more transmission attempts, especially when the channel condition is worse. And comparing the two access schemes, the Hotspot 2.0 protocol adopts more management frames

Table 4.3: Zone parameters

Zone index	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
d_z (m)	26.8	23.9	8.4	12	6	3	5	2.4	8.2	2.4	5	3	6	12	8.4	23.9	26.8
r_z (Mbps)	6.5	13	19.5	26	39	52	58.5	65	78	65	58.5	52	39	26	19.5	13	6.5
$r_z * t_z$ (Mb) v=60 km/h	10.4	18.7	9.8	18.7	14	9.3	17.7	9.3	38.3	9.3	17.7	9.3	14	18.7	9.8	18.7	10.4

then WPA2-PSK, and also involves the backhaul delay, and thus lead to less aggregate throughput.

As in reality, the aggregate throughput will be shared by all the associated clients, as shown in equation (4.25). To demonstrate the impact the access procedure, the 'throughput loss' is defined to evaluate the difference of the throughput that can be achieved between the case of employing and not employing access procedure, which is denoted by η.

$$\eta = \frac{\mathscr{U}_{total} - \mathscr{U}_T}{\mathscr{U}_{total}} \tag{4.27}$$

where $\mathscr{U}_{total} = \sum_{z=1}^{N_z} \mathscr{U}_z$, which is the total throughput that the tagged vehicle can achieve without the access procedure. Fig. 4.8 and Fig. 4.9 shows the throughput loss when employing the Hotspot 2.0 and the WPA2-PSK respectively. From the two figures, it is observed that when the number of the contending clients increase, the traffic loss is significantly exacerbated, especially when the frame drop rate is high, which is consistent with the results in Fig. 4.7. The traffic loss will be up to 80% when the Hotspot 2.0 is adopted, which means that the vehicle can only get around 20% of the expected throughput that no access procedure is employed. Similarly we can see a near 14% throughput loss when adopts WPA2-PSK, which requires to exchange much less management frames and no backhaul handshakes.

Fig. 4.7-4.9 shows that the vehicle will lose significant throughput in the condition of large number of co-associated WiFi clients and high management frame drop rate due to channel error. Fig. 4.10 shows that the throughput loss is related to the back off stage number, given a certain value (16) of minimum back off window size. When the back off stage number m become small, i.e., the back off stage i in equation (4.3) is limited to a small

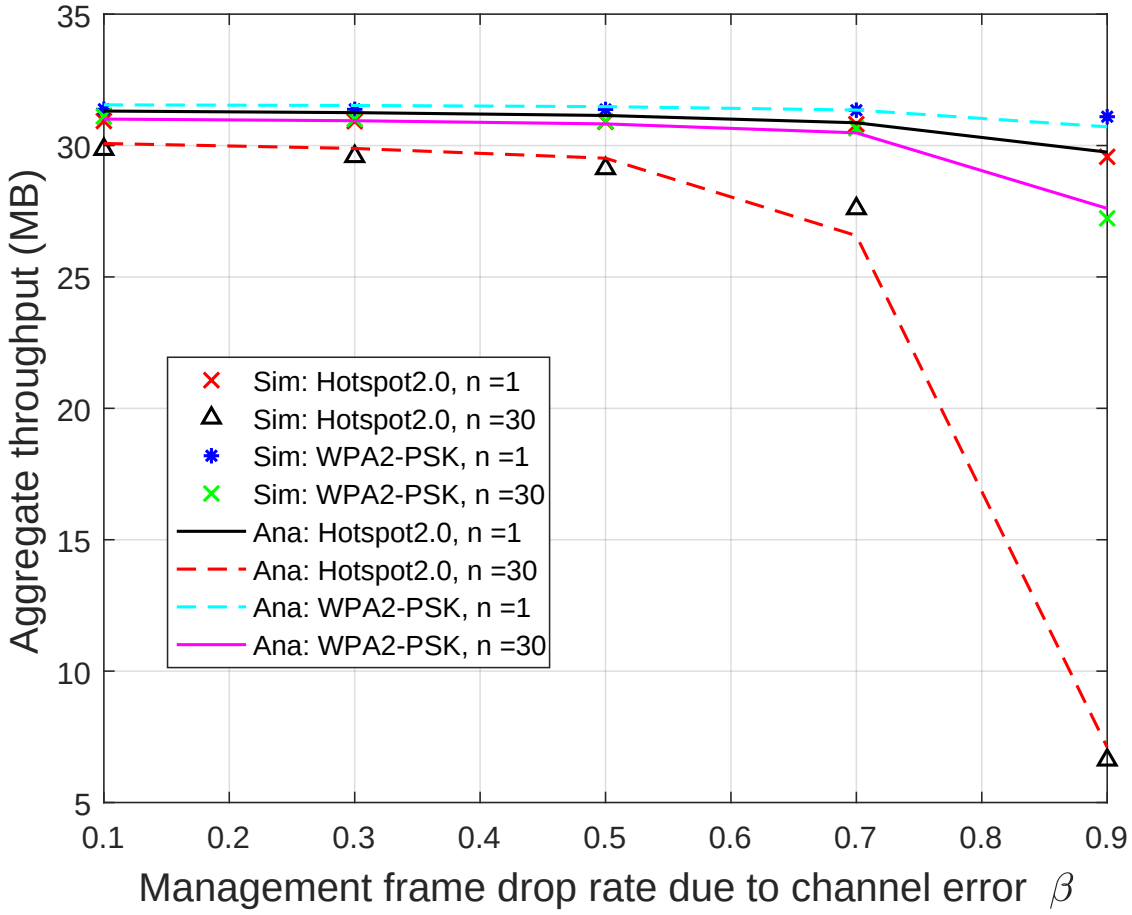

Figure 4.7: Aggregate throughput vs management frame channel error rate

value, then the average back off counter C_i is reduced, and the vehicle will have less back off waiting time before a transmission attempt, and thus lead to high collision probability, which will obstruct the access procedure as the management frame transmission will be delayed. And when the back off stage number become larger, the average back off counter is increased, which means that for each transmission attempt, the average waiting time will be increased, and thus the overall back off waiting time will be increased, and the average time to deliver a management frame will also be increased, and thus the access procedure will consume more time. From Fig. 4.10, it is possible to find an optimal value of m to minimize the traffic loss introduced by the access procedure.

A similar observation can be found in Fig. 4.11, which shows the traffic loss in the

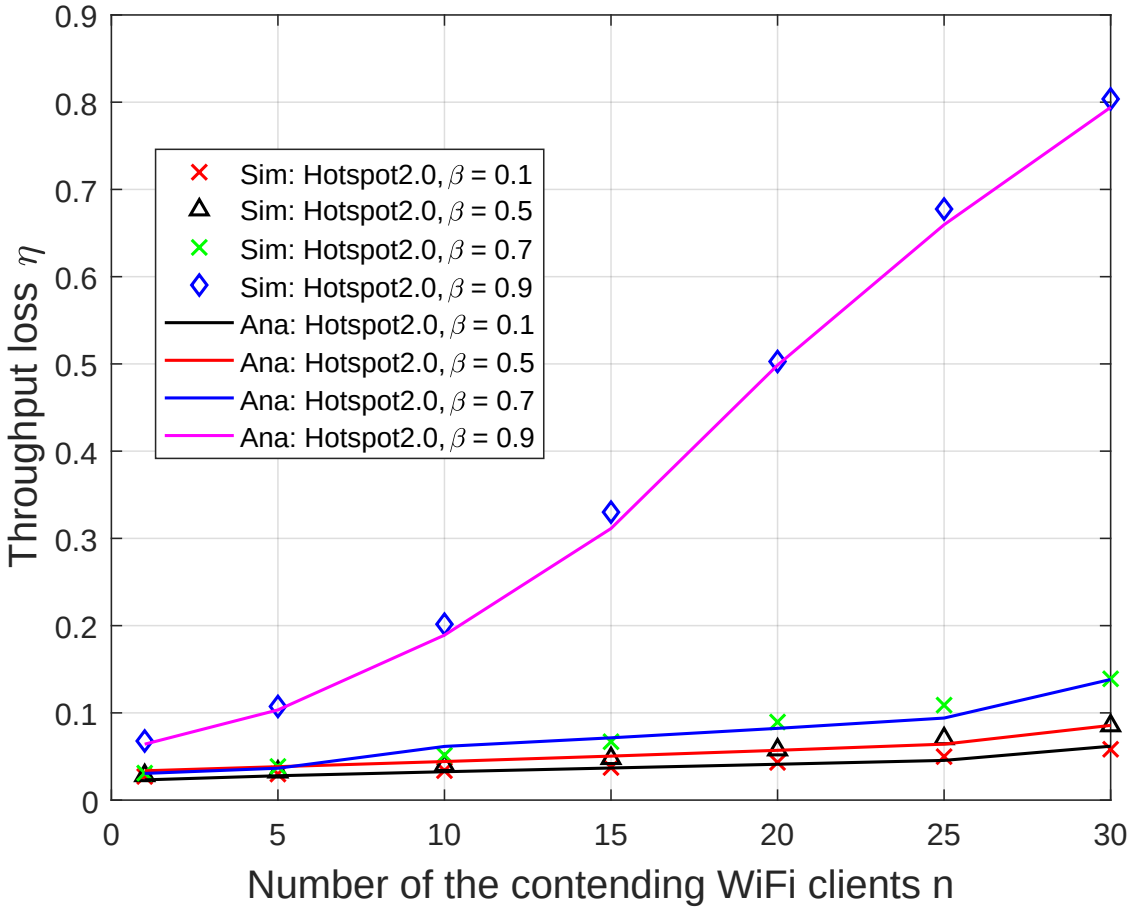

Figure 4.8: Throughput loss of the tagged vehicle with Hotspot 2.0

condition of different values of minimum back off window size w, given a certain back off stage number (7). When w is small, the back off time for a certain back off counter is limited, and thus the management frame will be attempted to transmit shortly, which will cause high collision probability in the similar way as the case of small m, and thus the duration to transmit a management frame will be increased, and the accomplish of the access procedure will need more time, which increase the traffic loss. While w is too large, the average waiting time for a given back off stage will be increased, and the average time used to transmit a management frame is thus increased, so more time will be used to finish the access procedure, which leads to high throughput loss as less Internet connection time will be available.

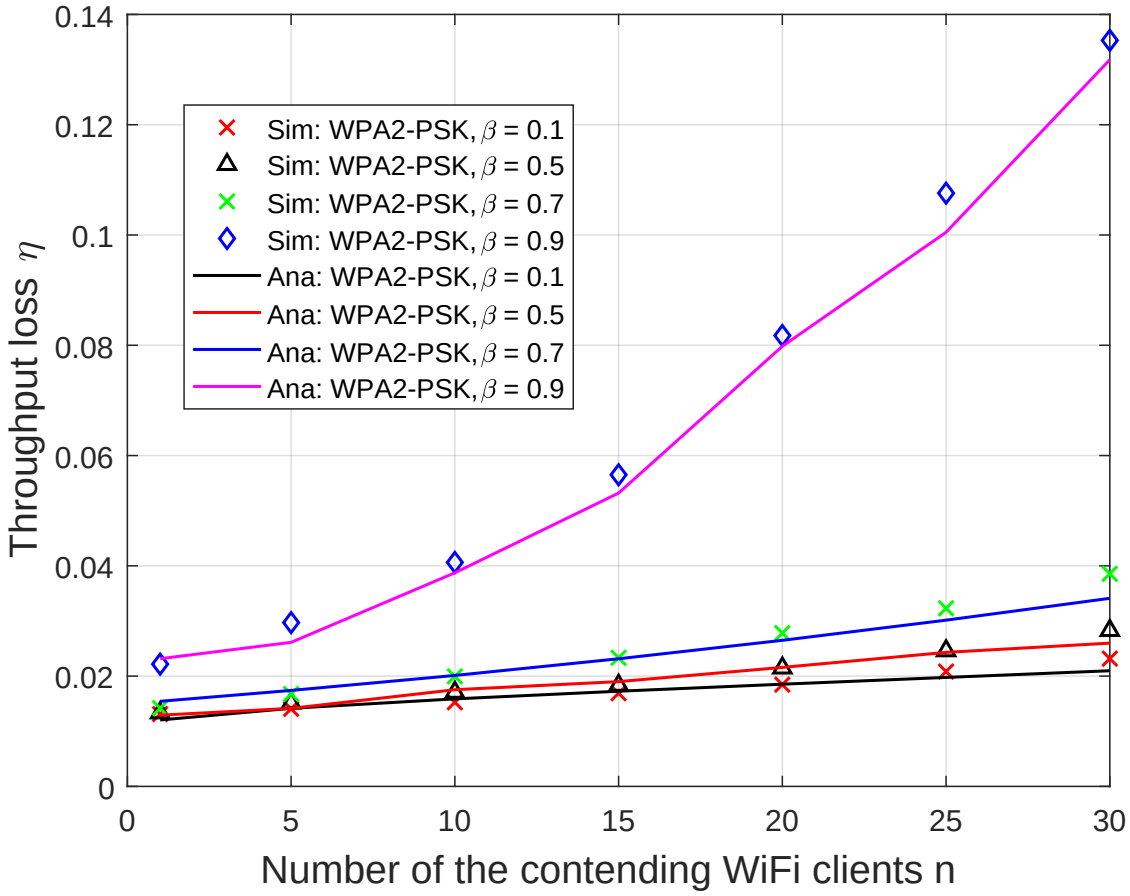

Figure 4.9: Throughput loss of the tagged vehicle with WPA2-PSK

4.3.3 Potential applications

Fig. 4.7 - 4.11 have shown the accuracy of our analytical model in all aspects of conditions, which not only can be used to evaluate the throughput performance of the drive-thru Internet, but also provide potential applications for future protocol research and design in vehicular conditions, especially in V2I Internet communications.

Group authentication evaluation

Current authentication protocol requires every vehicle to perform the user authentication procedure with the roadside WiFi network, which consumes the majority of the time in

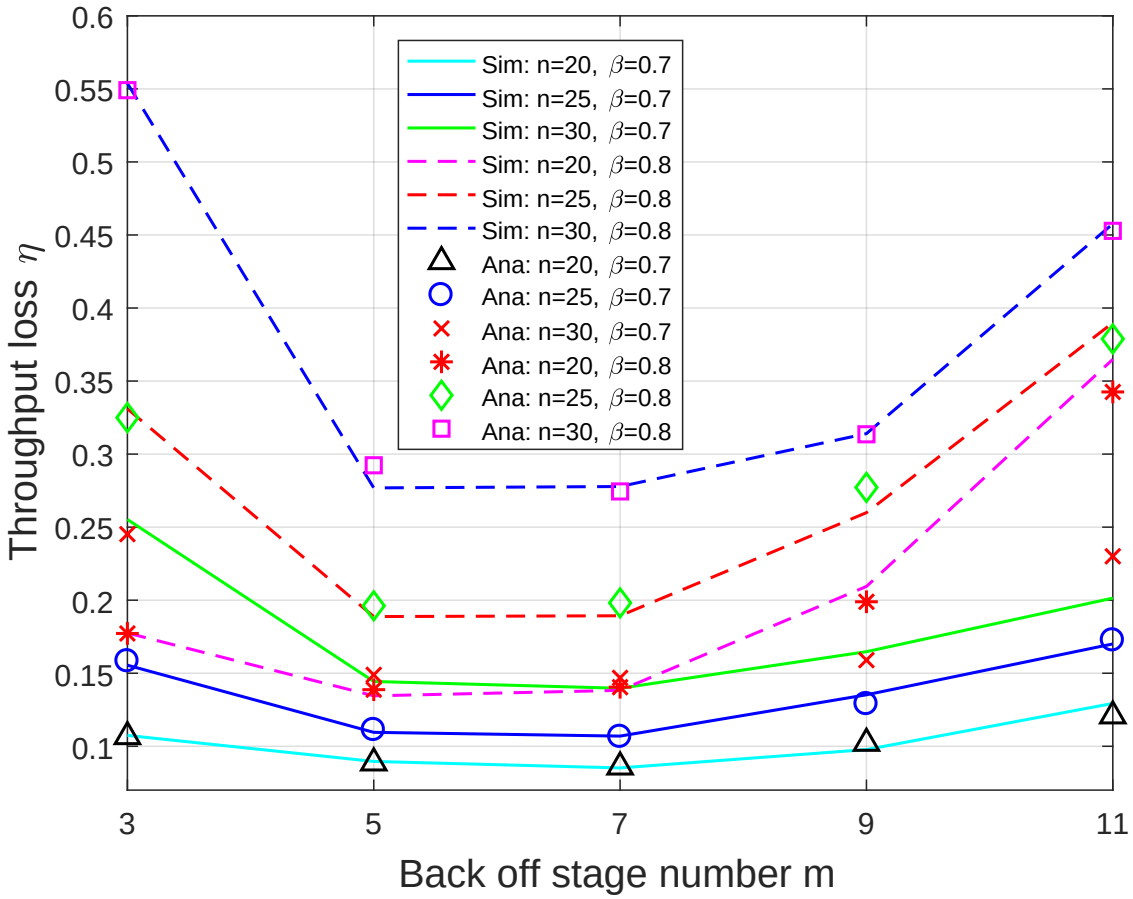

Figure 4.10: Throughput loss vs. back off stage number m

access procedure. To reduce such overhead, a number of neighboring vehicles can form a group to perform the authentication together [75], and thus the access duration can be greatly reduced, hence the throughput loss can be greatly saved. Our model can provide a tool to calculate the network overhead of such group authentication protocols.

Adaptive vehicular MAC protocol

Fig. 4.10 and 4.11 shows that given the vehicle density and the channel condition, the throughput loss can be minimized by adjusting the MAC parameters, namely, the back off stage number and the minimum back off window size. And an adaptive MAC protocol for vehicular Internet access protocol can use our model to predict and apply the optimal

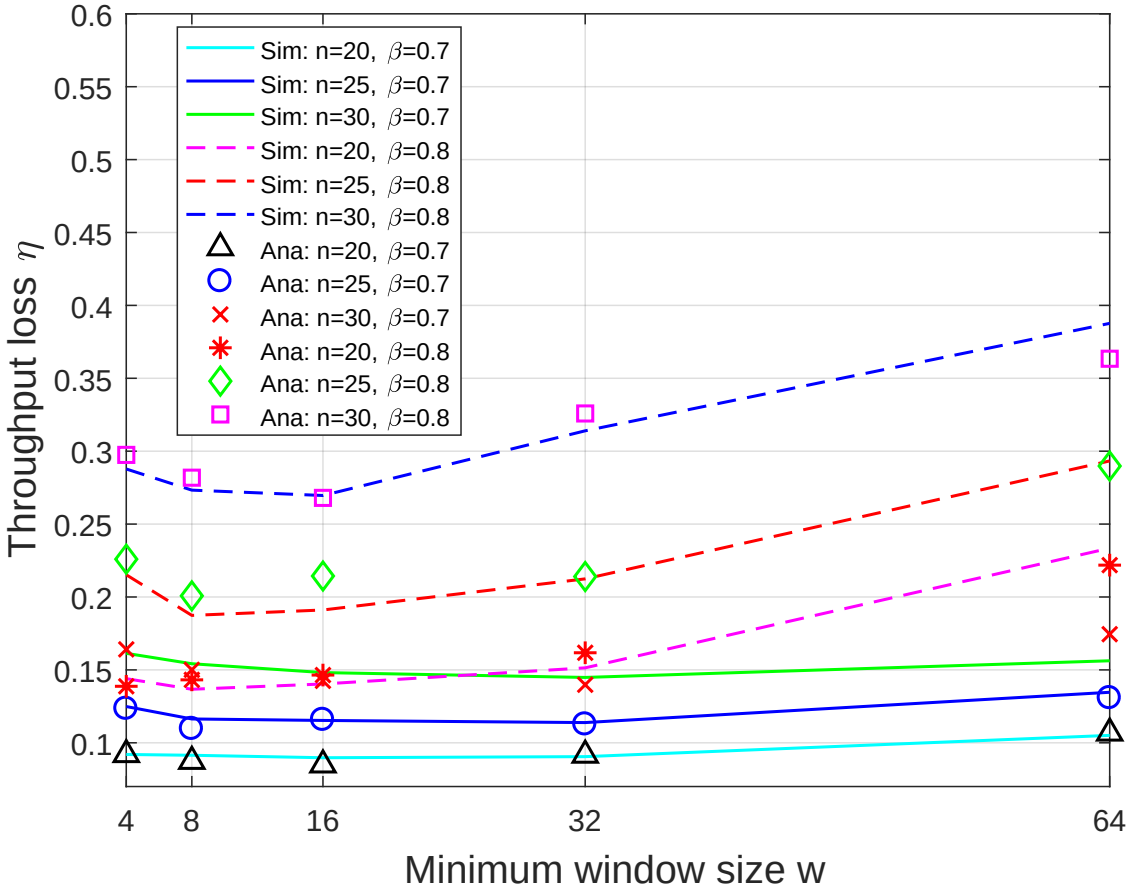

Figure 4.11: Throughput loss vs. minimum window size

values of the parameters, and thus the throughput performance can be improved [76].

Software defined vehicular networks (SDVN)

In SDVN, a central controller can collect the global information and thus can efficiently find an optimal policy for vehicles to access Internet. Our model can be used for the controller to calculate an optimal authentication policy in different vehicular conditions, e.g., traffic density, channel quality, etc. [77]

Autonomous vehicles

Autonomous vehicles may require frequent and secure authentications to enable reliable connection for safe driving, automatic parking, etc. The network delay and exchanged messages of such process can be analyzed by our method in mobile conditions, which are crucial in future network protocol design for autonomous vehicles [78].

4.4 Conclusion

In this chapter, we have investigated the access procedure for a vehicle to access to the roadside WiFi network for Internet connection. We have proposed a 3D Markov chain model to calculate the throughput performance of drive-thru Internet by considering the transition of the coverage zones, management frame index and the back off process. We have conducted extensive simulations to validate the accuracy of our analytical model, which can be applied in the development of future vehicular networks, such as group authentication, mobile MAC protocol, software defined vehicular networks and connected autonomous vehicles.

Chapter 5

ViFi: Vehicle-to-Vehicle assisted WiFi Offloading

In this chapter, we study the vehicle-to-vehicle (V2V) assisted WiFi offloading when vehicles drive through multiple WiFi networks. We also consider that neighboring vehicles can assist each other to transmit part of peer's traffic. The intermittent WiFi transmission is modeled as an M/G/1/K queue process and the 'preemptive drop' policy is adopted to show the performance gain of the V2V assistance.

5.1 System Model

In this section, the ViFi system model is described, which includes network model, vehicle mobility model, Internet access procedure, WiFi offloading queue model and V2V assistance model.

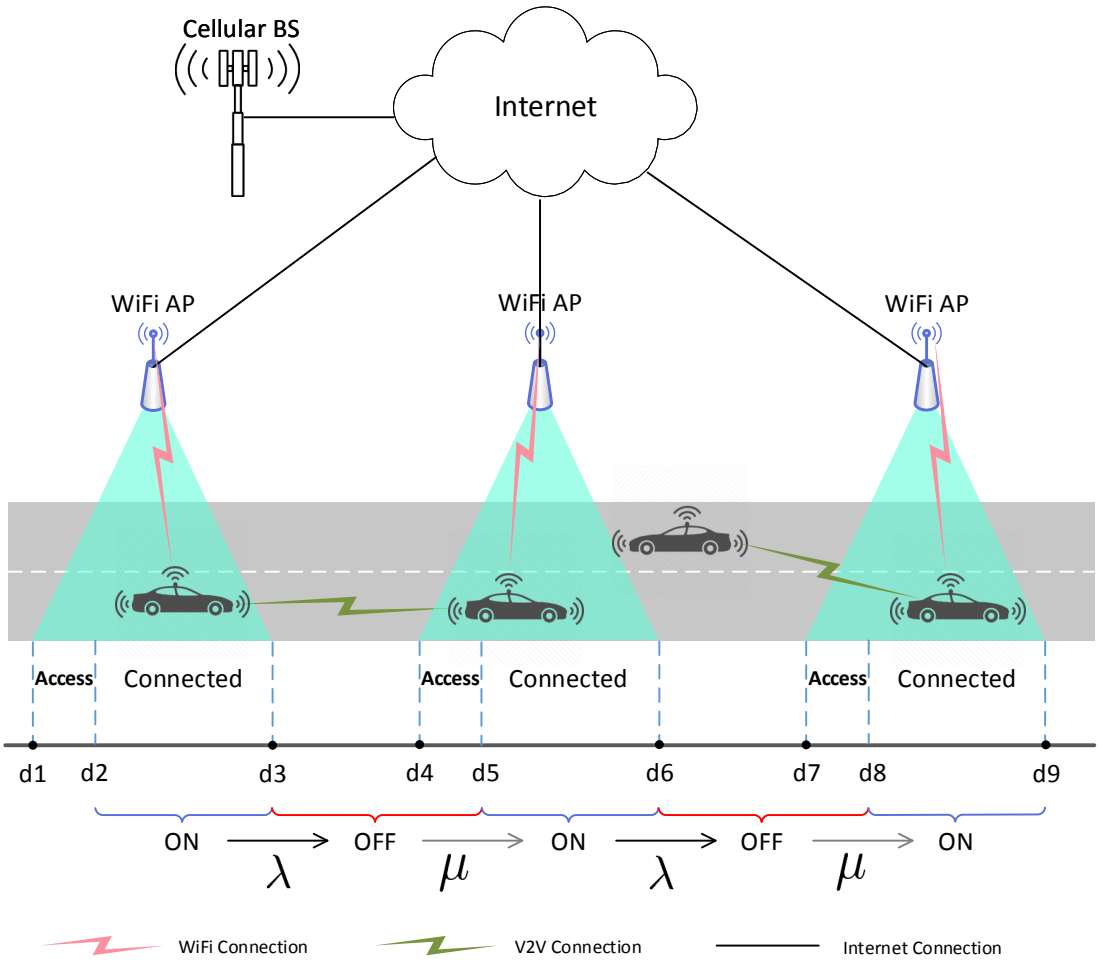

Figure 5.1: ViFi system model

5.1.1 Network Model

As shown in Fig. 5.1, assume that all vehicles can access to cellular networks at any moment. WiFi APs are deployed along the roadside and connected to backhaul Internet, and the distances between neighboring APs are the same. There are coverage hole between adjacent WiFi cells, e.g., area $d_3 - d_4$. The ratio of the uncovered area range (d_{uc}) to the

covered area range (d_c) is defined as the *uncover ratio*:

$$\eta_u = \frac{d_{uc}}{d_c} = \frac{d_3 d_4}{d_1 d_3}, \quad or \quad \frac{d_6 d_7}{d_4 d_6}, \quad etc. \tag{5.1}$$

The bandwidth of the WiFi AP is shared by all vehicles associated to it, i.e., the average link rate of the tagged vehicle r equals to R/N_a, where R is the overall achievable aggregate rate and N_a is the average number of the tagged vehicle's co-associated vehicles. Besides, vehicles can communicate with neighbors via the V2V communication, e.g., DSRC, TVWS Radio [36]. We assume that the V2V communication can connect vehicles in adjacent WiFi cells and the one-hop V2V communication latency can be neglected.

5.1.2 Vehicle Mobility Model

We assume that in a long stretch of road, vehicles drive to each lane with Poisson arrival with the parameter of λ_v at velocity of v. In an area of range d, the average number of vehicles equals to $N_l \lambda_v d/v$, where N_l is the number of lanes. Inspired by [16], the switch of the tagged vehicle(the one we consider)'s WiFi connectivity status can be modeled as an *on-off* process. The time duration that the tagged vehicle stays in the connected status can be approximated as an exponential variable with mean $1/\lambda$, while the time duration that the tagged vehicle is off connected with any WiFi AP is approximated as an exponential variable with mean $1/\mu$. And we have:

$$\begin{aligned} \frac{1}{\lambda} &= \frac{d_c}{v} - \tau_{ac}, \\ \frac{1}{\mu} &= \frac{d_{uc}}{v} + \tau_{ac} = \frac{\eta_u d_c}{v} + \tau_{ac}, \end{aligned} \tag{5.2}$$

where τ_{ac} is the average delay introduced by the access procedure.

5.1.3 Internet Access Procedure

The area the vehicle transverses during the access procedure is defined as the *access area*, which for example, is $d_1 d_2$ (or $d_4 d_5$, etc.) as shown in Fig. 5.1. The access procedure includes the following three steps, in which the management frames exchanged are summarized in Table 5.1.

Table 5.1: Frames exchanged during Internet access procedure

Step	**Function**	**Num. of frames**
1)	Beaconning, Query	4
2)	EAP-TLS, EAPoL handshake	23
3)	DHCP	2

1) Network detection: In this step, the vehicle will exchange beacon frames or query frames with the AP to obtain necessary information, e.g., radio channel, supported rates, authentication method, etc.

2) User authentication: WiFi operators use the authentication to prevent unauthorized users from stealing the WiFi resource, while WiFi users relies on this step to protect their communication privacy. The widely used WPA2-802.1X authentication method is adopted, which requires the handshake between the vehicle and the remote authentication servers.

3) IP address assignment: We use a local DHCP server on roadside AP to assign an IP address for associated vehicles.

Besides, generating a management frame requires time for local framing, and sometimes has to wait for the response from remote server (e.g., the TLS handshake frames), which will introduce the 'core delay' before the frame can be exchanged. The core delay during the access procedure used are measured from a real WiFi system.

5.1.4 WiFi Offloading Queue Model

Fig. 5.2 shows the ViFi queueing model, where the data task request arrival and the departure (means data task is fulfilled) are modeled by an M/G/1/K queueing process, where the time interval between consecutive data tasks is an exponential variable with mean $1/\gamma$. The average time required to fulfill the arrived data task equals to $\mathbb{S}/r$, where $\mathbb{S}$ is the average size of the data task and r is the average WiFi link rate of the tagged vehicle, as stated in Section 5.1.1. We then assume the time needed to transmit all the data of a task follows an exponential distribution with parameter $\lambda_{task} = r/\mathbb{S}$. However, it is possible that during one coverage area, the data task cannot be fulfilled due to limited connection time, thus the serving of the data task has to be deferred until next WiFi AP

connection. So that the actual time consumed to fulfill a data task, referred as 'effective service time', follows a general distribution, which is analyzed in Section 5.2.2.

The offloading performance O_e is evaluated by the ratio of the data tasks transmitted via WiFi APs, which can be calculated by

$$O_e = 1 - P_{B,tag} + P_{B,tag} * P_{assist} \tag{5.3}$$

where $P_{B,tag}$ is the overflowed (or blocking) probability of the WiFi data task queue of the tagged vehicle. And P_{assist} is the probability that the peer vehicle can assist the overflowed data task from tagged vehicle via his own WiFi connection.

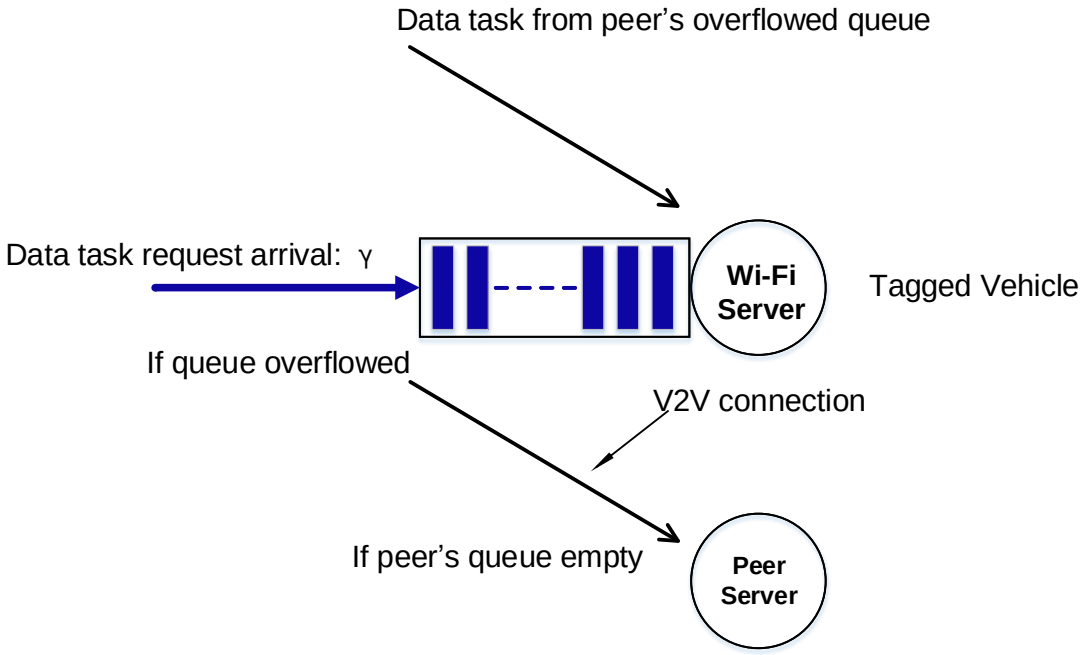

Figure 5.2: Queueing model of ViFi

5.1.5 V2V Assistance Model

Vehicles prefer using the WiFi connection to fulfill the data tasks. If the data task queue overflows, the tagged vehicle will check if his peer can help him to transmit the data through peer's idle resource, otherwise, the tagged vehicle will let the cellular network to fulfill the data task. The peer vehicle chooses the 'preemptive drop' policy, which allows

him to fulfill his own data task with priority. If there is own data task arrival when peer is assisting tagged vehicle's task, then peer will drop the data task from tagged vehicle (which has to be served by cellular network) and start to transmit the data for himself to his own WiFi data pipe. In this way, the peer's WiFi queue should not be affected by the assistance behavior. Since all vehicles' behavior and parameters are the same, the offloading performance can be obtained via the analysis of the tagged vehicle without loss of generality. As the vehicle arrival is Poisson with parameter λ_v, then the probability of the tagged vehicle can find an assistant peer is defined as:

$$\begin{aligned} P_{v2v} &= 1 - P(\text{No accessed peers in neighboring cells}) \\ &= 1 - e^{-\lambda_v * 2 * d_c / v} \end{aligned} \tag{5.4}$$

Then we have:

$$P_{assist} = P_{v2v} * P_{I,peer} * P_{I,v2v} * P_{na,peer} \tag{5.5}$$

where $P_{I,peer}$ is the probability that peer's data task queue is empty, $P_{I,v2v}$ is the probability that peer is currently not assisting any task from tagged vehicle, $P_{na,peer}$ is the probability that during the assistance of a data task, peer has no new data task arrival.

5.2 Offloading Performance Analysis

In this section, we present the calculation of the offloading performance, i.e., the traffic ratio that served via WiFi AP, including both self WiFi server and V2V connected peer's AP. We first analyze the access delay, and then derive the effective service time that a data task needs to fulfill through WiFi server. After that we apply an M/G/1/K queueing process to model the status of the data buffer queue, which are used to obtain the offloading performance.

5.2.1 Access Delay Approximation

The analysis and experiment in [73] showed that the average access delay τ_{ac} can be estimated as a linear function of the amount of contending nodes, i.e., the number of vehicles associated to the same AP. Thus the average access delay τ_{ac} can be written as:

$$\tau_{ac} = k * N_a + b_0 \tag{5.6}$$

where k and b_0 are constant under certain packet drop rate (PDR, δ) of the management frames during access procedure. The values of k and b_0 used in this article are obtained from the numerical result of [73].

5.2.2 Effective Service Time Derivation

To fulfill an arrived data task, it might need transmissions between the tagged vehicle and several APs as the WiFi connection will be interrupted due to the vehicle mobility. Denote $T(x)$ the effective service time of a data task, which requires service time x. x is an exponential variable with mean $1/\lambda_{task}$. Let Φ_λ denote the duration between the beginning moment of the data task service and the upcoming connection interruption, which is exponential with mean $1/\lambda$. Let Φ_μ denote the length of an unconnected duration, which corresponds the duration that the tagged vehicle is out of WiFi connectivity, and is an exponential variable with mean $1/\mu$. And thus:

$$T(x) = \begin{cases} x, & if \quad x \leqslant \Phi_\lambda \\ \Phi_\lambda + \Phi_\mu + T(x - \Phi_\lambda), & if \quad x > \Phi_\lambda \end{cases} \tag{5.7}$$

The Probability Density Function (PDF) of $T(x)$ can be derived using Laplace Transform (L.T.) method, which can be obtained from Eq. (5.7) [79]:

$$\mathscr{T}(s) = \frac{\lambda_{task}}{\lambda_{task} + s + \frac{\lambda * s}{s+\mu}} \tag{5.8}$$

and applying the Fourier-Series (F.S.) method in [80], the inverse L.T. of $\mathscr{T}(s)$, which equals to the PDF of the effective service time, can be approximated via the trapezoidal rules with step size σ:

$$f_T(t) \approx \frac{\sigma e^{\alpha t}}{\pi} + \frac{2\sigma e^{\alpha t}}{\pi} \sum_{m=1}^{+\infty} \mathrm{Re}\left(\mathscr{T}(\alpha + im\sigma)\right) \cos\left(m\sigma t\right) \tag{5.9}$$

where α is a real number located at the right side of all singularities of Eq. (5.8).

5.2.3 WiFi Queue Solution

Based on the PDF of the effective service time, we can solve the stable parameters of the M/G/1/K queue to obtain the probabilities to calculate the offloading performance. Denote n_i the number of remaining data tasks in the buffer queue when the ith data task is just fulfilled, then n_i satisfies:

$$n_i = \begin{cases} \min\{K-1, A_i\}, & n_{i-1} = 0 \\ \min\{K-1, A_i + n_{i-1} - 1\}, & n_{i-1} \in \{1, 2, \ldots, K-1\} \end{cases} \tag{5.10}$$

where A_i is the number of the data task arrivals from the beginning moment of the service to the fulfillment of task i, and K is the queue buffer length. From Eq. (5.10), it can be inferred that sampled at every moment a data task finishes, the number of remaining data tasks in the buffer queue forms an embedded Markov chain [81]. By solving the limiting probability of the queue status, we can obtain the blocking probability of the queue $P_{B,tag}$. The probability that k new data task arrivals during the effective service time of ith data task can be obtained by

$$\xi_k = \int_{t=0}^{+\infty} \frac{(\lambda t)^k}{k!} e^{-\lambda t} f_T(t) dt. \tag{5.11}$$

And then the transition probability matrix of all states P_t can be obtained:

$$P_{t(K\times K)} = \begin{pmatrix} \xi_0 & \xi_1 & \xi_2 & \ldots & \xi_{K-2} & \sum_{i=K-1}^{+\infty} \xi_i \\ \xi_0 & \xi_1 & \xi_2 & \ldots & \xi_{K-2} & \sum_{i=K-1}^{+\infty} \xi_i \\ 0 & \xi_0 & \xi_1 & \ldots & \xi_{K-3} & \sum_{i=K-2}^{+\infty} \xi_i \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 & \xi_0 & \sum_{i=1}^{+\infty} \xi_i \end{pmatrix}$$

Thus the steady probability P_k can be calculated together with

$$\sum_{k=0}^{K-1} P_k = 1 \tag{5.12}$$

The probability that the queue length equals to k, i.e., there are k data tasks in the queue, denoted by $\mathscr{P}_k$ equals to

$$\mathscr{P}_k = (1 - P_B) P_k \tag{5.13}$$

Since the actual load to the queue ρ_r equals

$$\rho_r = \frac{\gamma}{\overline{T}}(1 - P_B) \tag{5.14}$$

where $\overline{T}$ is the average effective service time, which can be obtained from Eq. (5.9). The probability that the buffer length is zero, i.e., no data task in the queue, can be obtained by

$$\mathscr{P}_0 = 1 - \rho_r \tag{5.15}$$

From Eq. (5.13 - 5.15), we can obtain that:

$$P_{B,tag} = \mathscr{P}_K = 1 - \frac{1}{P_0 + \frac{\gamma}{\overline{T}}} \tag{5.16}$$

The offloading ratio by the WiFi service of the tagged vehicle himself equals to:

$$O_{e,tag} = 1 - P_{B,tag} \tag{5.17}$$

5.2.4 V2V Assistance Analysis

The peer's data task queue can also be solved by the M/G/1/K queueing model following the same method in Section 5.2.3. And thus,

$$P_{I,peer} = \mathscr{P}_0 \tag{5.18}$$

And the probability that peer is not serving any overflowed task from tagged vehicle can be approximated as

$$P_{I,v2v} = \frac{1}{1 + \gamma P_B \overline{V}} \tag{5.19}$$

where $\overline{V}$ is the average sojourn time the overflowed task from tagged vehicle on peer's server. $\gamma P_B \overline{V}$ is the average number of the overflowed tasks from tagged vehicle during one sojourn time of the previous overflowed task[1]. And $\overline{V}$ can be calculated by:

$$\overline{V} = \int_0^{+\infty} \left(\int_0^l t f_\gamma(t) dt + \int_l^\infty l f_\gamma(t) dt \right) f_T(l) dl \tag{5.20}$$

[1]means only one among all the $(1 + \gamma P_B \overline{V})$ tasks can be served if peer is idle.

where $f_\gamma(t)$ is the PDF of exponential distribution with the data task arrival rate γ. And the probability that in the assistance duration for an overflowed task from tagged vehicle, peer has no new task arrived, can be calculated by

$$P_{na,peer} = \int_0^{+\infty} \left(\int_r^{+\infty} \gamma e^{-\gamma t} dt \right) f_T(r) dr \tag{5.21}$$

And then the offloading ratio contributed by the V2V assistance can be obtained from Eq. (5.3 - 5.5) combining the above results.

5.2.5 Offloading Ratio Calculation

The overall offloading ratio is give in Eq. (5.3). Besides, the benefit of V2V assistance can be calculated as the *v2v offloading gain*:

$$G_{v2v} = \frac{P_{B,tag} P_{assist}}{1 - P_{B,tag}} \tag{5.22}$$

5.3 Simulation Results

The ViFi simulation is conducted based on the parameters listed in Table 5.2. The 'core delay' mentioned in Section 5.1.3 of each frame is measured from the system described in [73]. The values of k and b_0 from Eq. (5.6) listed in Table 5.2 are obtained when the packet drop rate δ during the access procedure is set to 0.1, 0.5, 0.9 respectively. The vehicles drives through the coverage areas of a series of WiFi APs repeatedly and transmit the data packet to WiFi networks and the V2V data pipe following the 'preemptive drop' policy. The offloading performance is evaluated by calculating the ratio of the data packet task that fulfilled by WiFi. We run the offloading simulation under various conditions, including different vehicle arrival rate λ_v, data task arrival rate γ, buffer length K, vehicle velocity v and uncover ratio η_u.

Table 5.2: Simulation Parameters

Parameter	**Denoting**	**Values**
d_c	Range of WiFi coverage area	200 m
N_l	Number of lanes	2
R	Aggregate rate of an AP	54 Mbps
$\mathbb{S}$	Average size of the data arrival	8 MByte
k	in Eq. (5.6): linear function	0.025, 0.052, 0.183
b_0	in Eq. (5.6): linear function	0.47, 0.448, 1.102
σ and α	in Eq. (5.9): step size and a real number	$\sigma = 0.001$, $\alpha = 0$

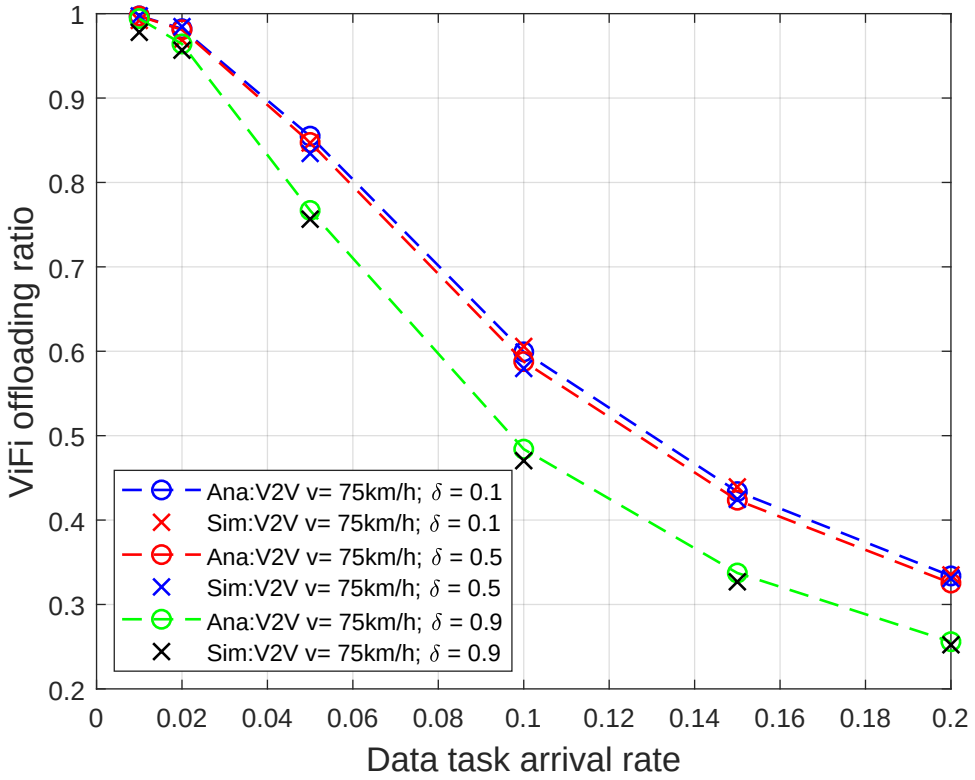

Figure 5.3: ViFi offloading performance

Fig. 5.3 shows the ViFi offloading performance defined in Eq. (5.3) under different data task arrival rate γ. It can be observed that ViFi can offload the majority of the arrived data task to WiFi APs when the traffic load is low. When γ rises, the offloading ratio decreases since more data tasks will overflow. And by comparing the three cases with different access packet drop rate δ, we can see that the offloading ratio is barely affected until δ becomes a large value. Such conclusion can be used in the access protocol design for vehicular Internet access, especial for high mobility conditions.

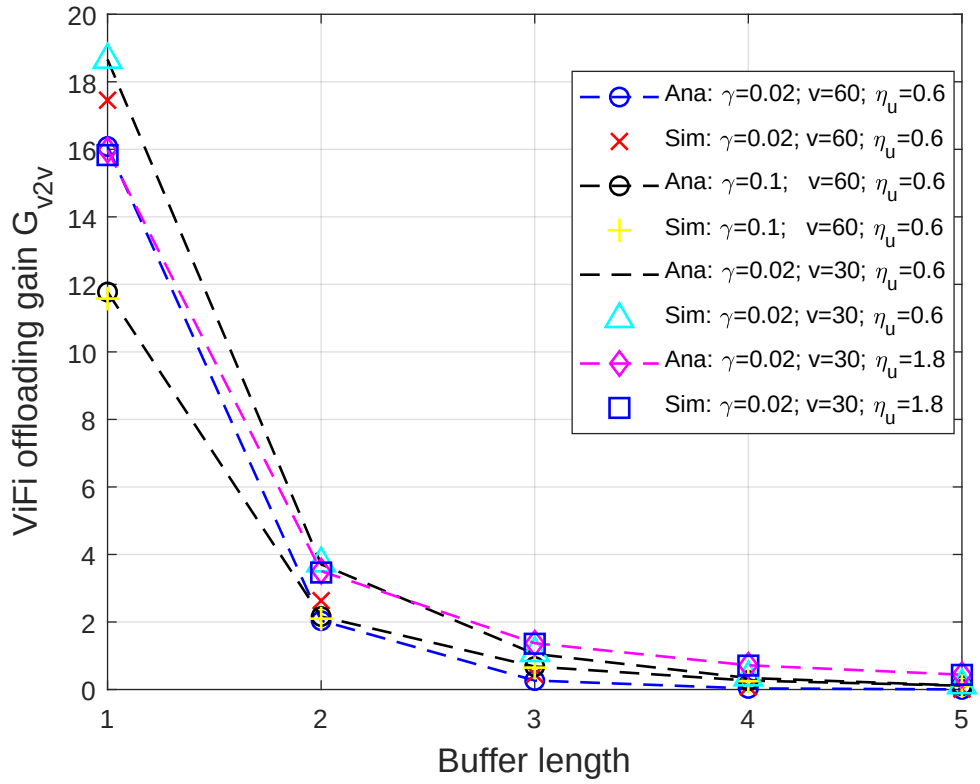

Figure 5.4: Percentage of V2V offloading gain

Fig. 5.4 shows the percentage of the offloading gain through V2V assistance defined in Eq. (5.22). It is shown that when the traffic load is low, e.g., the data task arrival rate γ is small, the V2V assistance can help the tagged vehicle to offload considerable overflowed tasks. When the data arrival rate increases, the peer will be busy to fulfill his own data task according to the 'preemptive drop' policy, and thus contribute less to the V2V assistance. When the vehicle travels with low velocity, given a certain vehicle arrival

rate λ_v, the tagged vehicle has a good chance to find an assistant peer in neighboring cells, and thus the offloading gain can be improved.

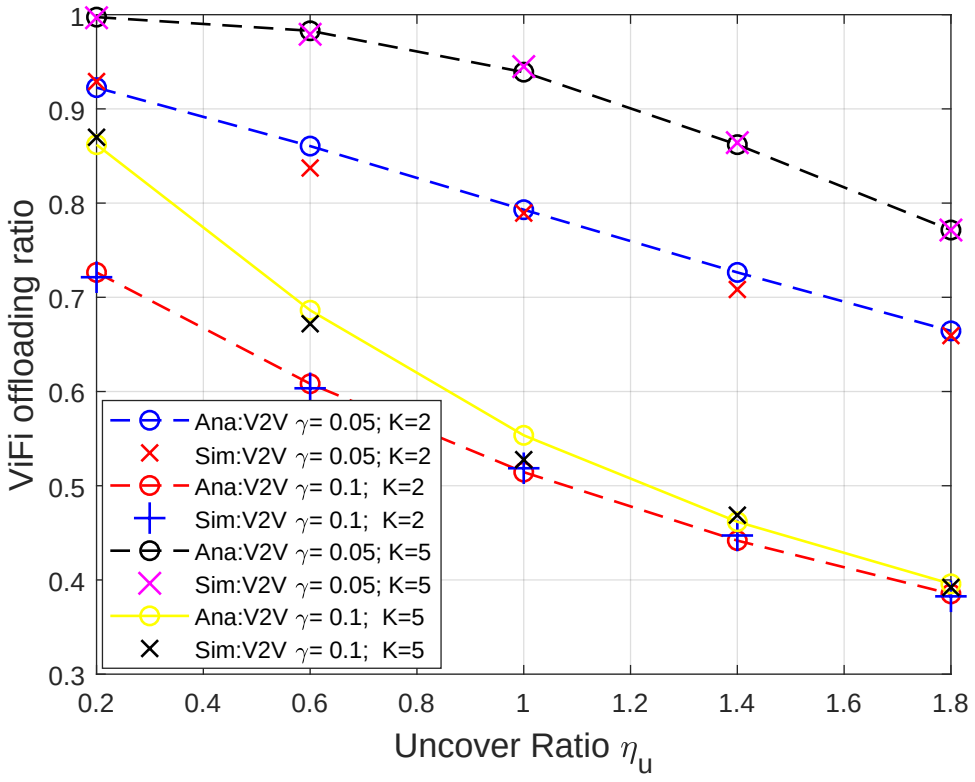

Figure 5.5: ViFi offloading ratio vs. uncover ratio

Fig. 5.5 shows the relationship between the ViFi offloading ratio and the uncover ratio η_u. It can be observed that when η_u increases, i.e., the gap areas between two adjacent WiFi cells become larger, the offloading ratio will decrease since the tagged vehicle has to drive through more WiFi cells to fulfill a data task, which leads to longer time for the data task to stay in the queue, and thus makes the queue more likely to overflow. Fig. 5.5 also shows that when η_u or the data task arrival rate γ is relatively large, applying a large queue buffer size K can still offload the majority of the data traffic. Such conclusion can be applied in the caching size selection for data delivery in vehicular conditions [**?**].

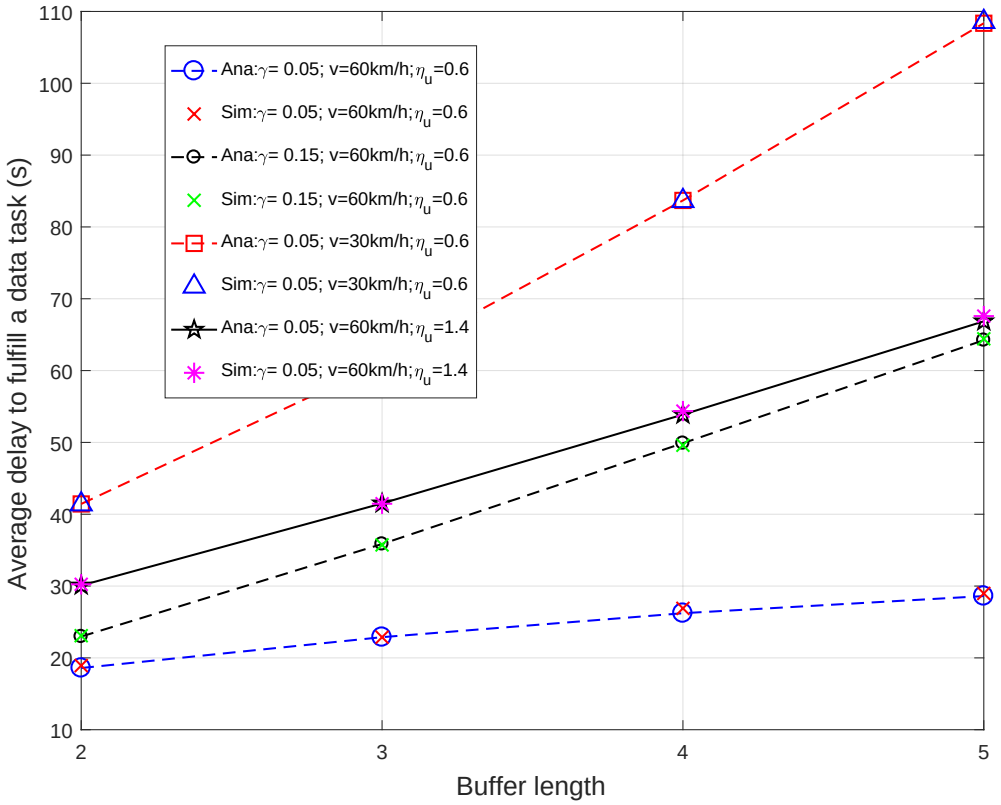

Figure 5.6: Average delay to fulfill a data task

However, maintaining a larger K value will increase the number of the data tasks buffered in the queue, and the average duration for a data task stay in the buffer will be extended. And thus, the average delay to fulfill a data task will increase, as shown in Fig. 5.6. The average delay also increases when velocity v, uncover ratio η_u or data task arrival rate γ rises, since a large v and η_u value will let the vehicle has less sojourn duration in a WiFi cell. And when γ increases, the queue length will be extended and the waiting time for a task in the queue will be increased.

5.4 Conclusion

In this chapter, we have studied the V2V assistance in WiFi offloading for vehicles. We have utilized the V2V communication between vehicles associated to different APs to help each other on offloading their overflowed data tasks from the WiFi data queue. We have

applied the M/G/1/K queueing model to analyze the offloading performance of the proposed ViFi scheme with the 'preemptive drop' policy between the tagged vehicle and his peer considering the Internet access overhead. Simulation have demonstrated the accuracy of our analysis, which provides useful implications for offloading scheme research and design.

Chapter 6

Conclusions and Future Work

In this chapter, we summarize the research results regarding to the performance analysis of the drive-thru Internet access, and the future research directions are also highlighted.

6.1 Conclusions

In this thesis, we have investigated the Internet access overhead in drive-thru Internet, including the access delay and throughput degradation. We also proposed a V2V assisted offloading method that utilize multiple roadside networks and the assistance between neighboring vehicle users to improve the drive-thru Internet performance. Specifically, the following researches are presented based on the analytical investigation and experiment/simulation discussion.

1. Delay Analysis of In-Vehicle Internet Access Via On-Road WiFi AP: we have investigated the time duration that a vehicle has to wait for accomplishing the Internet access procedure before effective connection. We developed an analytical model to find the dependency of the access delay on the factors of wireless channel condition, number of the contending WiFi users, and the access protocols. We have found that the access delay increases when the channel condition degrades, or when the number of the channel contenders increases. We have also concluded different authentication protocols have significant impacts on the access delay. We found that the average access delay increases almost linearly with the number of contending WiFi users given a certain channel condition. The analysis is verified by both simulation and

experiment measurement, and can provide important guidance for future vehicular Internet access protocol research and development.

2. Throughput Analysis for Drive-Thru Internet Access: the drive-thru Internet throughput has been analyzed considering the impacts of the access procedure. First, we apply a 3D Markov process to model the access procedure between the drive-by vehicle and the roadside AP while the vehicle moves through the coverage area, whereby the relationship between the vehicle's position and the process of the access procedure is investigated. Secondly, we validate and compare the throughput of the drive-thru Internet and find out the throughput loss due to the access procedure in various conditions, including the channel quality, number of contending WiFi users, different access protocols, etc. We also discuss the future application of our model, which is expected to be an important tool in future vehicular communication protocol research and development.

3. Vehicle-to-Vehicle assisted WiFi Offloading: we have extended the single network cell scenario of the drive-thru Internet to multiple cells scenario. Vehicles in neighboring cells can assist each other via their own WiFi resources. We use an M/G/1/K queue to find out the offloading performance when employing the 'preemptive drop' assistant policy. It has been shown that the offloading performance can be improved by up to 19% via the V2V assistance.

6.2 Future Research Directions

The research works in this thesis can be extended in several directions, including the further study on complex Internet access protocols for vehicles and more sophisticated vehicular offloading schemes.

1. Performance analysis on complex Internet access protocol: the proposed models can be further developed to consider more practical details in the vehicular Internet access procedure. First, it is possible that the management frame transmission can be interrupted during the access procedure. For example, one management frame might be re-generated due to transmission timeout, or extra authentication frame is needed to be exchanged due to safety reasons. Besides, the backhaul network status also can have significant impacts on the management frame exchange during the Internet access procedure. Furthermore, the network entities that the vehicular Internet access protocol may involve many be extended to multiple APs and access

servers. For example, the 802.11r protocol requires different APs to exchange the pairwise master key, and some quick handover protocols often require the vehicle to negotiate with the access server in different moment and locations. The analytical models in this thesis can be extended to cover such situations by adding extra status and calculating their transition probabilities, which help to better understand the Internet access performance in vehicular conditions.

2. Extension to other wireless access technologies: modern vehicles are often equipped with multiple and heterogeneous wireless access radios, as stated in Section 2.1. The interworking between the heterogeneous radio access networks can be utilized to facilitate the access procedure, e.g., use one network to help the vehicle user to access to another network [82]. Our methods can be extended to analyze the overhead of such new access diagram based on the cooperation among heterogeneous access networks.

3. Sophisticated offloading schemes: except the 'preemptive drop' policy adopted in our offloading scheme, different policy can be used in the V2V assisted offloading diagram. For example, instead of dropping neighbor's data tasks, caching them in a V2V buffer queue and suspend their transmission when WiFi is busy can further reduce the data tasks for cellular networks. And when WiFi become idle, different service restart models for those suspended data tasks can be considered. For example, when the data task resumes, if the data task service time should be re-sampled, the data transmission should start from the very beginning bit, which takes more time than the case that the data transmission start from the suspended bit. By extending our V2V assisted model, the offloading performance of different policies and resume types can be analyzed.

References

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

[2] W. Xu, H. Zhou, N. Cheng, F. Lyu, W. Shi, J. Chen, and X. Shen, "Internet of vehicles in big data era," *IEEE/CAA J. Autom. Sinica*, vol. 5, no. 1, pp. 19–35, 2018.

[3] K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of dsrc and cellular network technologies for V2X communications: A survey," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 9457–9470, 2016.

[4] H. A. Omar, W. Zhuang, and L. Li, "Vemac: A tdma-based mac protocol for reliable broadcast in vanets," *IEEE Trans. Mobile Comput.*, vol. 12, no. 9, pp. 1724–1736, 2013.

[5] F. Lyu, H. Zhu, H. Zhou, W. Xu, N. Zhang, M. Li, and X. Shen, "Ss-mac: A novel time slot-sharing mac for safety messages broadcasting in vanets," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3586–3597, 2018.

[6] X. Cheng, L. Yang, and X. Shen, "D2d for intelligent transportation systems: A feasibility study," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 4, pp. 1784–1793, 2015.

[7] A. Meola, "How the internet of things will transform private and public transportation," http://uk.businessinsider.com/internet-of-things-connected-transportation-2016-10, accessed April 2, 2018.

[8] N. Cheng, F. Lyu, J. Chen, W. Xu, H. Zhou, S. Zhang, and X. Shen, "Big data driven vehicular networks," *IEEE Network*, no. 99, pp. 1–8, 2018.

[9] K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of dsrc and cellular network technologies for V2X communications: A survey," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 9457–9470, 2016.

[10] Cisco, "The zettabyte era: Trends and analysis," https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.pdf, accessed April 2, 2018.

[11] E. H. Ong, J. Kneckt, O. Alanen, Z. Chang, T. Huovinen, and T. Nihtilä, "IEEE 802.11 ac: Enhancements for very high throughput wlans," in *2011 IEEE 22nd international symposium on Personal indoor and mobile radio communications (PIMRC)*, 2011, pp. 849–853.

[12] R. Van Nee, "Breaking the gigabit-per-second barrier with 802.11 ac," *IEEE Wireless Commun.*, vol. 18, 2011.

[13] W. Xu, H. Zhou, Y. Bi, N. Cheng, X. Shen, L. Thanayankizil, and F. Bai, "Exploiting hotspot-2.0 for traffic offloading in mobile networks," *IEEE Network*, no. 99, pp. 1–7, 2018.

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

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

[16] N. Cheng, N. Lu, N. Zhang, X. Shen, and J. W. Mark, "Opportunistic wifi offloading in vehicular environment: A queueing analysis," in *IEEE Global Communications Conference (GLOBECOM)*, 2014, pp. 211–216.

[17] 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 Trans. Intell. Transp. Syst.*, vol. 15, no. 6, pp. 2644–2657, 2014.

[18] T. C. Clancy, "Secure handover in enterprise wlans: capwap, hokey, and ieee 802.11 r," *IEEE Wireless Commun.*, vol. 15, no. 5, 2008.

[19] R. M. Lopez, A. Dutta, Y. Ohba, H. Schulzrinne, and A. F. G. Skarmeta, "Network-layer assisted mechanism to optimize authentication delay during handoff in 802.11

networks," in *Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, MobiQuitous 2007*, pp. 1–8.

[20] S. Shin, A. G. Forte, A. S. Rawat, and H. Schulzrinne, "Reducing mac layer handoff latency in ieee 802.11 wireless lans," in *ACM Proceedings of the second international workshop on Mobility management & wireless access protocols*, 2004, pp. 19–26.

[21] J. Eriksson, H. Balakrishnan, and S. Madden, "Cabernet: vehicular content delivery using wifi," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, 2008, pp. 199–210.

[22] A. Tufail, M. Fraser, A. Hammad, K. K. Hyung, and S.-W. Yoo, "An empirical study to analyze the feasibility of wifi for vanets," in *12th International Conference on Computer Supported Cooperative Work in Design*, 2008, pp. 553–558.

[23] 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 *Proceedings of the 12th annual international conference on Mobile computing and networking.* ACM, 2006, pp. 50–61.

[24] C.-M. Chou, C.-Y. Li, W.-M. Chien, and K.-c. Lan, "A feasibility study on vehicle-to-infrastructure communication: Wifi vs. wimax," in *10th International Conference onMobile Data Management: Systems, Services and Middleware, MDM'09*, 2009, pp. 397–398.

[25] 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 Trans. Intell. Transp. Syst.*, vol. 17, no. 7, pp. 1944–1955, 2016.

[26] T. H. Luan, X. Ling, and X. Shen, "Mac in motion: Impact of mobility on the mac of drive-thru internet," *IEEE Transactions on Mobile Computing*, vol. 11, no. 2, pp. 305–319, 2012.

[27] D. Passmore and J. Freeman, "The virtual lan technology report," *3COM White Paper*, 1996.

[28] "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.

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

[30] N. Cheng, N. Lu, N. Zhang, X. Shen, and J. W. Mark, "Vehicular wifi offloading: Challenges and solutions," *Vehicular Communications*, vol. 1, pp. 13–21, 2014.

[31] K. Lee, J. Lee, Y. Yi, I. Rhee, and S. Chong, "Mobile data offloading: How much can wifi deliver?" in *Proc. 6th ACM International Conference on Emerging Networking Experiment and Technologies*, 2010.

[32] S. Dimatteo, P. Hui, B. Han, and V. O. Li, "Cellular traffic offloading through wifi networks," in *IEEE 8th International Conference on Mobile Adhoc and Sensor Systems (MASS)*, 2011, pp. 192–201.

[33] B. Han, P. Hui, V. Kumar, M. V. Marathe, G. Pei, and A. Srinivasan, "Cellular traffic offloading through opportunistic communications: a case study," in *Proc. 5th ACM workshop on Challenged networks*, 2010, pp. 31–38.

[34] Y. Wu, J. Chen, L. P. Qian, J. Huang, and X. Shen, "Energy-aware cooperative traffic offloading via device-to-device cooperations: An analytical approach," *IEEE Trans. Mobile Comput.*, vol. 16, no. 1, pp. 97–114, 2017.

[35] F. Mezghani, R. Dhaou, M. Nogueira, and A.-L. Beylot, "Offloading cellular networks through v2v communicationshow to select the seed-vehicles?" in *IEEE International Conference on Communications (ICC)*, 2016, pp. 1–6.

[36] H. Zhou, N. Cheng, N. Lu, L. Gui, D. Zhang, Q. Yu, F. Bai, and X. Shen, "Whitefi infostation: Engineering vehicular media streaming with geolocation database," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 8, pp. 2260–2274, 2016.

[37] H. Zhou, N. Cheng, Q. Yu, X. S. Shen, D. Shan, and F. Bai, "Toward multi-radio vehicular data piping for dynamic dsrc/tvws spectrum sharing," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 10, pp. 2575–2588, 2016.

[38] A. K. Ligo, J. M. Peha, P. Ferreira, and J. Barros, "Throughput and economics of dsrc-based internet of vehicles," *IEEE Access*, vol. 6, pp. 7276–7290, 2018.

[39] P. Luo, Z. Ghassemlooy, H. Le Minh, E. Bentley, A. Burton, and X. Tang, "Performance analysis of a car-to-car visible light communication system," *Applied Optics*, vol. 54, no. 7, pp. 1696–1706, 2015.

[40] R. Bruno and M. Conti, "Throughput and fairness analysis of 802.11-based vehicle-to-infrastructure data transfers," in *IEEE 8th International Conference on Mobile Adhoc and Sensor Systems (MASS)*, 2011, pp. 232–241.

[41] A. U. Joshi and P. Kulkarni, "Vehicular wifi access and rate adaptation," in *ACM SIGCOMM Computer Communication Review*, vol. 40, no. 4, 2010, pp. 423–424.

[42] Z. Song, L. Shangguan, and K. Jamieson, "Wi-fi goes to town: Rapid picocell switching for wireless transit networks," in *Proceedings of the Conference of the ACM Special Interest Group on Data Communication*, 2017, pp. 322–334.

[43] K. Dhondge, S. Song, B.-Y. Choi, and H. Park, "Wifihonk: smartphone-based beacon stuffed wifi car2x-communication system for vulnerable road user safety," in *IEEE 79th Vehicular Technology Conference (VTC Spring)*, 2014, pp. 1–5.

[44] P. Lv, X. Wang, X. Xue, and M. Xu, "Swimming: Seamless and efficient wifi-based internet access from moving vehicles," *IEEE Trans. Mobile Comput.*, vol. 14, no. 5, pp. 1085–1097, 2015.

[45] W. Na, N.-N. Dao, and S. Cho, "Mitigating wifi interference to improve throughput for in-vehicle infotainment networks," *IEEE Wireless Commun.*, vol. 23, no. 1, pp. 22–28, 2016.

[46] W. L. Tan, W. C. Lau, O. Yue, and T. H. Hui, "Analytical models and performance evaluation of drive-thru internet systems," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 1, pp. 207–222, 2011.

[47] B. B. Chen and M. C. Chan, "Mobtorrent: A framework for mobile internet access from vehicles," in *IEEE INFOCOM 2009*, 2009, pp. 1404–1412.

[48] S. Goel, T. Imielinski, and K. Ozbay, "Ascertaining viability of wifi based vehicle-to-vehicle network for traffic information dissemination," in *The 7th International IEEE Conference on Intelligent Transportation Systems*, 2004, pp. 1086–1091.

[49] S. Vasudevan, K. Papagiannaki, C. Diot, J. Kurose, and D. Towsley, "Facilitating access point selection in ieee 802.11 wireless networks," in *Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement*, 2005, pp. 26–26.

[50] "Hotspot 2.0 technical task group," *Wi-Fi Alliance Technical Committee*.

[51] W. Xu, C. Hua, and A. Huang, "A game theoretical approach for load balancing user association in 802.11 wireless networks," in *Proc. IEEE Globecom'10*, pp. 1–5, 2010.

[52] "Hotspot 2.0 specification and passpoint project." [Online]. Available: http://www.wi-fi.org/discover-wi-fi/wi-fi-certified-passpoint

[53] L. Florio and K. Wierenga, "Eduroam, providing mobility for roaming users," in *Proceedings of the EUNIS 2005 Conference, Manchester*, 2005.

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

[55] Y.-T. Chen, "Achieve user authentication and seamless connectivity on wifi and wimax interworked wireless city," in *IFIP International Conference on Wireless and Optical Communications Networks*, 2007, pp. 1–5.

[56] K. Han, S. D. Potluri, and K. G. Shin, "On authentication in a connected vehicle: Secure integration of mobile devices with vehicular networks," in *2013 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*, 2013, pp. 160–169.

[57] A. Fu, G. Zhang, Z. Zhu, and Y. Zhang, "Fast and secure handover authentication scheme based on ticket for wimax and wifi heterogeneous networks," *Wireless personal communications*, vol. 79, no. 2, pp. 1277–1299, 2014.

[58] A. Bohák, L. Buttyán, and L. Dóra, "An authentication scheme for fast handover between wifi access points," in *Proc. of ACM Wireless Internet Conference (WICON)*, 2007.

[59] H. Moustafa, G. Bourdon, and Y. Gourhant, "Providing authentication and access control in vehicular network environment," in *IFIP International Information Security Conference*. Springer, 2006, pp. 62–73.

[60] L. Hu, C. Coletti, N. Huan, P. Mogensen, and J. Elling, "How much can wi-fi offload? a large-scale dense-urban indoor deployment study," in *Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th.* IEEE, 2012, pp. 1–6.

[61] N. Wang and J. Wu, "Opportunistic wifi offloading in a vehicular environment: Waiting or downloading now?" in *The 35th Annual IEEE International Conference on Computer Communications, INFOCOM*, 2016, pp. 1–9.

[62] J. Lee, Y. Yi, S. Chong, and Y. Jin, "Economics of wifi offloading: Trading delay for cellular capacity," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1540–1554, 2014.

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

[64] J. P. Craiger *et al.*, "802.11, 802.1 x, and wireless security," *SANS Institute InfoSec Reading Room*, 2002.

[65] J.-C. Chen and Y.-P. Wang, "Extensible authentication protocol (eap) and ieee 802.1 x: tutorial and empirical experience," *IEEE Commun. Mag.*, vol. 43, no. 12, pp. supl–26, 2005.

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

[67] "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.

[68] G. Bianchi, "Performance analysis of the ieee 802.11 distributed coordination function," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 3, pp. 535–547, 2000.

[69] "iperf - the ultimate speed test tool for tcp, udp and sctp," https://iperf.fr/.

[70] M. A. Ingram, "Six time-and frequency-selective empirical channel models for vehicular wireless lans," *IEEE Veh. Technol. Mag.*, vol. 2, no. 4, pp. 4–11, 2007.

[71] L. Cheng, B. E. Henty, D. D. Stancil, F. Bai, and P. Mudalige, "Mobile vehicle-to-vehicle narrow-band channel measurement and characterization of the 5.9 ghz dedicated short range communication (dsrc) frequency band," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, 2007.

[72] K.-H. Liu, X. Shen, R. Zhang, and L. Cai, "Performance analysis of distributed reservation protocol for uwb-based wpan," *IEEE Trans. Veh. Technol.*, vol. 58, no. 2, pp. 902–913, 2009.

[73] W. Xu, H. A. Omar, W. Zhuang, and X. Shen, "Delay analysis of in-vehicle internet access via on-road wifi access points," *IEEE Access*, vol. 5, pp. 2736–2746, 2017.

[74] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.

[75] J. Ni, X. Lin, and X. Shen, "Efficient and secure service-oriented authentication supporting network slicing for 5g-enabled iot," *IEEE J. Sel. Areas Commun.*, 2018.

[76] Q. Ye and W. Zhuang, "Distributed and adaptive medium access control for internet-of-things-enabled mobile networks," *IEEE Internet Things J.*, vol. 4, no. 2, pp. 446–460, 2017.

[77] N. Zhang, S. Zhang, P. Yang, O. Alhussein, W. Zhuang, and X. Shen, "Software defined space-air-ground integrated vehicular networks: Challenges and solutions," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 101–109, 2017.

[78] X. Lin and X. Li, "Achieving efficient cooperative message authentication in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 7, pp. 3339–3348, 2013.

[79] D. Fiems, T. Maertens, and H. Bruneel, "Queueing systems with different types of server interruptions," *European Journal of Operational Research*, vol. 188, no. 3, pp. 838–845, 2008.

[80] J. Abate, G. L. Choudhury, and W. Whitt, "An introduction to numerical transform inversion and its application to probability models," in *Computational probability, Springer*, 2000.

[81] S. K. Bose, *An introduction to queueing systems*. Springer Science & Business Media, 2013.

[82] T. Manku, "Using a first network to control access to a second network," 2014, uS Patent 8,630,901.

[83] H. Zhou, N. Zhang, Y. Bi, Q. Yu, X. Shen, D. Shan, and F. Bai, "Tv white space enabled connected vehicle networks: Challenges and solutions," *IEEE Network*, vol. 31, no. 3, pp. 6–13, 2017.

[84] "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 amendment 6: Wireless access in vehicular environments," *IEEE Std. 802.11p*, 2010.

[85] P. Choi, J. Gao, N. Ramanathan, M. Mao, S. Xu, C.-C. Boon, S. A. Fahmy, and L.-S. Peh, "A case for leveraging 802.11 p for direct phone-to-phone communications," in *IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED)*, 2014, pp. 207–212.

[86] W. Xu, H. Zhou, W. Shi, F. Lyu, and X. Shen, "Throughput analysis of in-vehicle internet access via on-road wifi access points," in *IEEE 86th Vehicular Technology Conference (VTC-Fall)*, 2017, pp. 1–5.

[87] M. Amoozadeh, A. Raghuramu, C.-N. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 126–132, 2015.

[88] "hostapd: Ieee 802.11 ap, ieee 802.1x/wpa/wpa2/eap/radius authenticator," http://w1.fi/hostapd/.

[89] L. Wang, H. Wu, Z. Han, P. Zhang, and H. V. Poor, "Multi-hop cooperative caching in social iot using matching theory," *IEEE Trans. Wireless Commun.*, vol. 17, no. 4, pp. 2127–2145, 2018.

[90] A.-M. Căilean and M. Dimian, "Current challenges for visible light communications usage in vehicle applications: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2681–2703, 2017.

[91] P. Calhoun and B. O'Hara, "802.11 r strengthens wireless voice," *Technology Update, Network World, Aug*, vol. 22, 2005.

[92] I. C. Society, "802.11u-2011," https://standards.ieee.org/findstds/standard/802.11u-2011.html.

Appendix List of Publications

1. **W. Xu**, W. Shi, F. Lyu, H. Zhou, N. Cheng, X. Shen, "Throughput Analysis of Vehicular Internet Access via Roadside WiFi Hotspot,"
   to be submitted.

2. **W. Xu**, H. Zhou, Y. Bi, N. Cheng, X. Shen, L. Thanayankizil, F. Bai, "Exploiting Hotspot-2.0 for Traffic Offloading in Mobile Networks,"
   IEEE Network, no. 99, pp. 1-7, 2018.

3. **W. Xu**, H. ZHou, N. Cheng, F. Lyu, W. Shi, J. Chen, X. Shen "Internet of Vehicles in Big Data Era,"
   IEEE/CAA Journal of Automatica Sinica., vol. 5, no. 1, pp. 1935, 2018.

4. **W. Xu**, H. Omar, W. Zhuang, X. Shen "Delay Analysis of In-Vehicle Internet Access Via On-Road WiFi Access Points,"
   IEEE Access, (2017): 2736-2746.

5. **W. Xu**, H. Wu, J. Chen, W. Shi, H. Zhou, N. Cheng, X. Shen, "ViFi: Vehicle-to-Vehicle Assisted Traffic Offloading via Roadside WiFi Networks,"
   accepted by Globecom 2018.

6. X. Shen, **W. Xu**, H. Zhou, 'System and Method for Automotive Wi-Fi Access and Connection', United States patent application PCT/CA2017/051292, filed, 2017