# Handshake Time and Transmission Rate of 802.11g Measurement in Vehicular Networks

Lei Zhao, Xiaoyan Hong, Bo Gu
University of Alabama
Wireless, Mobile and Networking Research Lab
{lzhao, hxy, bgu}@cs.ua.edu
http://wiman.cs.ua.edu

***Abstract*— Wireless network access from moving vehicles can be challenged by many factors such as connection opportunities, mobility, handshake phase, and data sizes, etc. The handshake time and transmission rate can be influenced differently in vehicle-to-roadside networks than a static wireless LAN access. The radio signal strength changes and Doppler shift occur when the vehicle is moving. Switching among APs could cause significant connection stale, which could have a major impact on the handshake phase and transmission rate. The purpose of our paper is to enhance the understanding of these influential factors and study the feasibility of mobile vehicle access for a hybrid environment that contains sparse and dense access point deployments. Experiment data was collected in a moving vehicle, which traveled around the campus of the university. In the data analyze part, the above factors are analyzed for packet inter-arrival time, response time and transmission rate; Our main results are focused in security enabled protocols such as HTTPS and SSH, as well as TCP file transmission. Our data shows that IEEE 802.11g is still weak in supporting mobile vehicle access to the Wireless LAN. We expect that IEEE 802.11p, designed specifically for vehicle networks, can provide better mobile services.**

***Keywords* — Vehicular Networks, wireless LAN, secure communications, Doppler shift, response time**

## I. INTRODUCTION

Vehicular Networks (VANETs) are envisioned to be a significant part of ITS, the Intelligent Transportation Systems. They contribute to improve the safety and the efficiency of road networks by exchanging information between vehicles and roadside base stations. There are two ways of connections in vehicular networks, namely, vehicles to communicate with each other via Vehicle-to-Vehicle communication, and vehicles to communicate with roadside base stations via Roadside-to-Vehicle communication [1]. Moreover, vehicular networks are also envisioned to be a part of the future globe network where mobility and mobile accesses are a norm.

Applications run over VANETs will go beyond the primary transportation safety applications such as driving alarming, road condition reporting, etc. In many applications, reliable and secure communications are demanded, e.g., email services, payment [14]. The transport layer protocols will typically have handshake phase before actual data and transmission. In TCP connection, handshaking is an automated process of synchronization protocols between servers and clients. When secure communication is demanded, more steps will be needed on handshake phase. On the other hand, researchers have been developing solutions for secure vehicular communications. Public key infrastructure has been recommended as the basic mechanism.

As such, both the road side base stations and vehicle-to-vehicle communications provide connectivity. However, the available communication time for an application can still be short. Whether and how useful data could be successfully exchanged given factors like various connection opportunities, mobility, handshake phase, and the data sizes remain an intriguing issue.

To enhance our understanding of the aforementioned practical issue, we performed measurements riding in a car using our campus wireless network. We are interested in the various handshake protocols and the corresponding latencies for real data transmissions and also the influence of the speed on the access latency and throughput. We don't have a dedicated vehicular network testbed, so we used our campus wireless network and private car to create the testing scenario. The coverage of the campus wireless network reveals uneven distributions of the outdoor access points. The public wireless network of the University (UA) covers all the indoor areas and a part of outdoor areas, such as the Quad. The Quad is the heart of UA campus with a large lawn. It is used for various activities and for outdoor study by students. Our measurements were chosen to around the Quad. We believe this test field reflects some of the vehicular networks deployed either in the metropolitan areas or along the highways. In this paper, we present our measurement data and analysis.

To analyze the performance of current network, we compared data captured along the same route with two different vehicle speeds. Per the IEEE 802.11p device, we believe that they will be available in the future. As a result, the research of vehicular networks based on 802.11g still useful and important.

In the rest of this paper, we introduce the measurement methodology, metrics, data and analysis. In Section II, we present brief review of related work and background. In Section

978-1-4244-8389-1/10/$26.00 ©2010 IEEE

III, we introduce various protocols and the handshake times we measure in the experiments. Following that, we present the design and implementation of our experiment and the results and analysis in Section IV and then conclude in Section V.

## II. Background and Related Work

Early work has studied the communications time period for vehicular networks. In an early work, the connection time to a road side access point was measured as around 15 seconds and only 1/3 of this period showed high link quality [11]. In [12], the authors conduct the experiment on communication between vehicle and roadside unit (RSU) so as to study the features of opportunistic Internet access in vehicles. The experimental scenario include an access point with 802.11 a/b/g wireless card, two network sniffers and a vehicular client with 802.11 a/b/g wireless card at highway speed of 80km/h. The result of measurement shows that the 802.11 based protocol can only gain about half of the overall available throughput. In addition, they summarize ten mechanisms that have a great impact on vehicular communication in three different phases. The authors also suggest that the environment information for the vehicle network should be integrated into the protocol design in order to improve the performance. Other measurement results have shown multi-hop latency [4].

In [9], the real trace data derived from more than two thousands operational taxies are used to study the feature of inter-contact time between each pair of vehicles. By equipping the GPS receiver, a taxi periodically sends a group of location information to data center through the GPRS channel. The result shows that the tail distribution of inter-contact time exhibits an exponential distribution. The inter-arrival time and inter-arrival distance for highway vehicle traffic are investigated in [8]. Their analysis results show that the vehicle headway follows a Poisson arrival process and vehicles in the same direction indicate a similar mobility behavior.

A novel mechanism for improving the vehicle to RSU communication is proposed in [10]. In order to decrease the interference when multiple vehicles contend for the limited transmission opportunity, a special vehicle called vehicle proxy is selected to aggregate and relay the data. A new proxy is elected when the buffer in the proxy reaches certain amount or the current proxy enters the region within which the distance to a RSU is less than three times of the transmission range of RSU. The results of simulation in NS2 indicate that the proxy based method performs better than the other existing protocols in terms of aggregate throughput, reliability of data and impact of vehicle speed.

The measurements we presented here differ from these work in that we focus on handshake time for the Internet applications that need secure communications. Our results suggest the feasibility of using vehicle network links. Solutions to protocol design are not the intension of this paper.

IEEE 802.11p in the IEEE 802.11 standard family is developed for vehicular networks by adding WAVE, wireless access in vehicular environments. The standard includes physical layer suitable to high-speed vehicles, network architecture for vehicle-to-vehicles and vehicle-to-roadside infrastructure in the licensed band of 5.9 GHz, and also adaptations to many common applications such as toll collection, vehicle safety messaging, and commerce.

## III. Measurement of Handshake Phase

Our study bases on IEEE 802.11g wireless networks on campus of University of Alabama. IEEE 802.11g can support up to a maximum raw data rate of 54 Mbit/s.

To analyze network performance of 802.11g, we choose Wireshark to capture network data. Wireshark is an open-source packet analyzer used for network monitoring, troubleshooting, analysis, software and communications protocol development, and education. We use Wireshark to dump and save packets from live network connection. It also helps us to understand the structure of different networking protocols through displaying the encapsulation and the fields..

The main measurement is on the handshake time for different protocols. Specifically, we define the handshake time to be the time period from the client's first contact packet to the serve till the time that the client sends its first data packet. Though building on top of TCP, the handshake times are different for the diversified security protocols. Generally, secure protocols need more steps in the handshake phase to exchange security information. In our experiments, we will measure handshake time between three distinct applications, HTTP, HTTPS, and SSH, which use different security protocols. We use the time stamps of the corresponding packets in calculating the handshake time. We'll elaborate our measurements below.

We also measure the throughput of each type of connection. When the handshake time measurement stops at the time of the first data transferring, the throughput measurement counts the time until the data transferring ends. In fact, when data packets are large, the influence from the handshake phase on the throughout can be small.

### A. HTTP Handshaking

HTTP doesn't contain any security protocol. Handshaking of HTTP is a standard TCP 3-way handshake process. Client sends a TCP Synchronize packet to server. Server receives client's SYN, and then sends a Synchronize-acknowledgement to client. After client receives server's Synchronize-acknowledgement, client sends acknowledgement to server. Server receives acknowledgement and connection is established.

The process of TCP connection only needs 3 steps. Fig 1 is a typical HTTP handshake process we captured in our experiments. After the 3-way handshake, client starts to send "GET /HTTP/ 1.0" in the 4th packet.

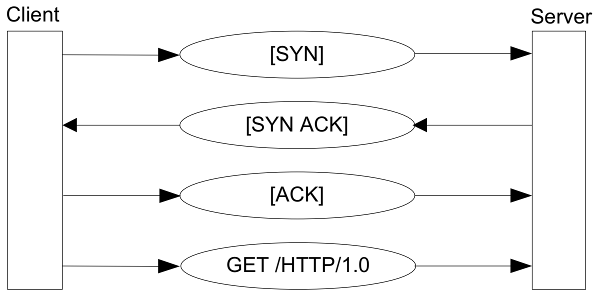


Fig. 1. HTTP handshaking

### B. HTTPS Handshaking

HTTPS, Hypertext Transfer Protocol Secure, is a combination of the HTTP Protocol with the SSL/TLS protocol to provide encryption and authentication of the server. In our experiments, TLS 1.0 is used in HTTPS as the security protocol.

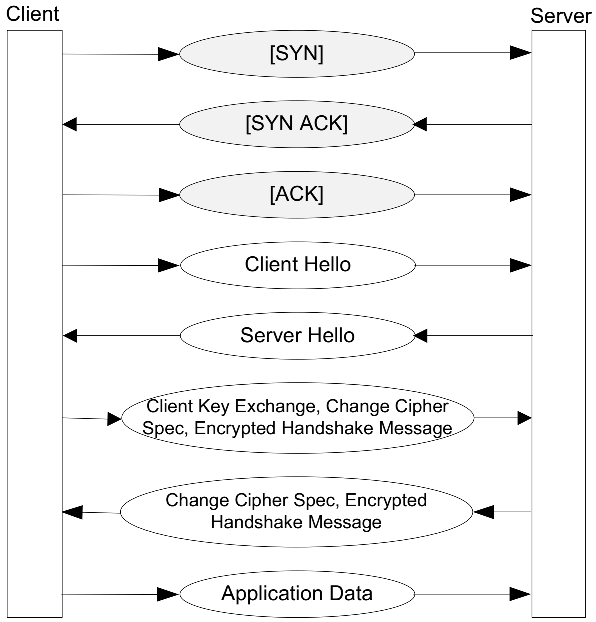

Client
Server
[SYN]
[SYN ACK]
[ACK]
Client Hello
Server Hello
Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
Change Cipher Spec, Encrypted Handshake Message
Application Data

Fig. 2. HTTPS handshaking

In the HTTPS handshaking of Fig. 2, there is a TLS handshake follow a TCP handshake. After a successful TCP hand shake, a client sends a Client Hello message specifying the highest TLS protocol version it supports, a random number, a list of suggested Cipher Suites, and suggested compression methods. The server responds with a Server Hello message, containing the chosen protocol version, a random number, Cipher Suite, and compression method from the choices offered by the client.

After this, the client responds with a Client Key Exchange message, which contains an Encrypted Handshake Message. Finally, the server sends a Change Cipher Spec message with an Encrypted Handshake Message. Connection established after this message, and the client starts sending Application Data.

### C. SSH Handshaking

SSH (Secure Shell) is a network protocol that allows data to be exchanged using a secure channel between the client and the server [3]. After the handshake phase in SSH, the two ends of the connection are able to ensure confidentiality and data integrity via message authentication codes. SSL secure protocol is used in SSH transmission.

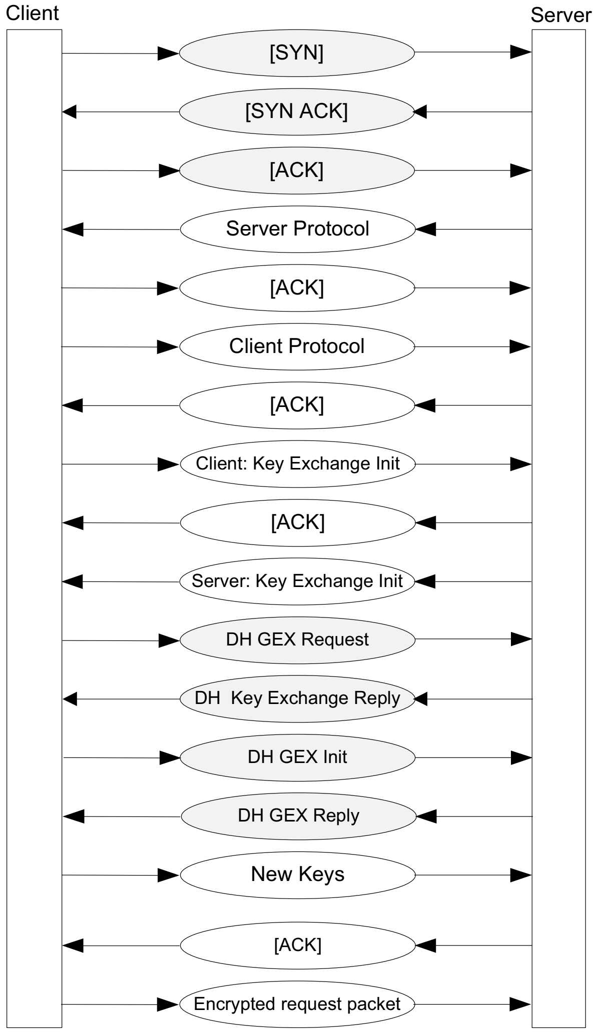


Fig. 3. SSH handshaking

Fig. 3 shows handshaking processing of my client and a SSH-2 server. The exact programmatic details of the messages exchanged during the SSL handshake may different between different clients and servers. However, the steps captured in our experiments can be summarized as follows:

1. TCP handshaking.
2. The server sends the client the server's SSL version number. The client responses an acknowledgement.

3. The client sends the server the client's SSL version number. The client responses an acknowledgement.
4. The client sends Client Key Exchange Init message. The server responses an acknowledgement, and then sends Server Key Exchange Init message.
5. Diffie-Hellman key exchange. The client sends a Diffie-Hellman request and then gets an exchange reply from the server. Then the client sends a GEX Init. The server responses a GEX reply and the Diffie-Hellman key exchange part finished.
6. New Keys generated by the client and sends to the server. The server sends an acknowledgement after verify the New Keys.
7. The SSL handshaking is now complete, and then the client and the server start transmitting encrypted data. They use the session keys to encrypt and decrypt the data they send to each other and to validate its integrity.

## IV. Experiments

The experiments and data collection implemented on campus of University of Alabama. About 100,000 effective packets captured in these experiments. These packets were supposed to measure response time of HTTP, HTTPS, and SSH connections, as well as transmission rate of file transfer. Fig. 4 shows the route of our test vehicle.

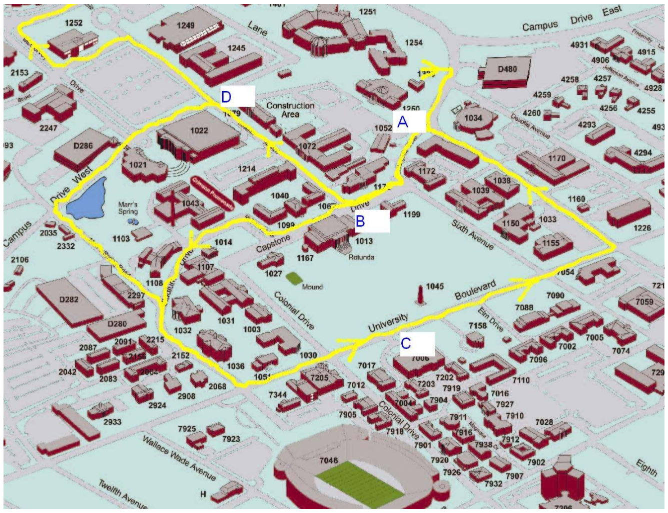


Fig. 4. Route of data collections

We captured five traces in our experiments. Three of the five trace were responding to the road segments of B→C, C→A, and A→B→D. Our client machine was an iBook G4 with AirPort Extreme 802.11g wireless interface. The operation system running this client was Debian 5.0. The other two traces used a second client of a Lenovo ThinkPad T60. This machine had an Intel 3495 wireless card and Ubuntu 9.04 as OS. The traces are located as A→B→C→A→B→D→C→A→B and B→C→A→D.

The measurements are taken repeatedly through scripts. The scripts only perform the handshake phase with the servers and collect the wireless packets for the handshake phase. In the experiment, we recurrently connect HTTP, HTTPS, and SSH servers. In addition, we repeatedly download files to measure throughput.

### A. TCP and HTTPS

We use the web server http://www.ua.edu for normal TCP handshake. HTTPS connection is made to https://mybama.ua.edu.

### B. SSH connection

The SSH server is located at the UNIX server of bama.ua.edu. We used a pair of username and password to login this server. To repeat the SSH connection, we exit the connection immediately after being connected.

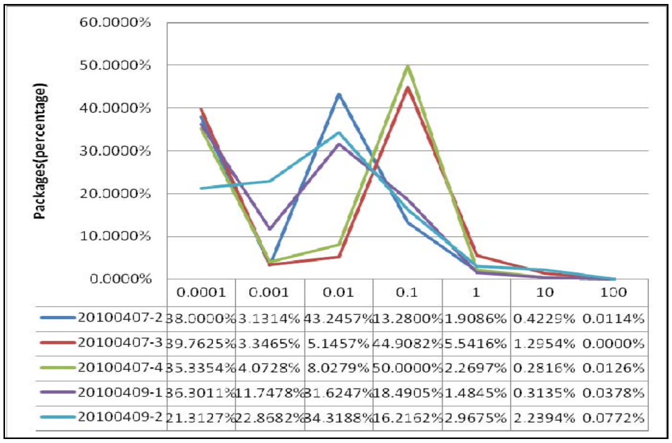
### C. File transmission

The files to be downloaded were at the web server http://cs.ua.edu. There are three different sizes of the files. We download one file each time and calculate the throughput by processing the packets with the time stamps.

## V. Performance Evaluation

We analyze the collected data in this section. In addition to the aforementioned handshake time of HTTP, HTTPS, and SSH, we measure a few more quantities. One is the packet interarrival time. It is calculated as the time period between the current packet arrival time and the previous packet arrival time. Another one is the overall packet transmission rate between our client and servers. The thrid factor is the influence on access latency from access points switching. In vehicle networks, especially in vehicle-to–roadside communication, access points switching is an essential characteristic that cannot be ignored. Finally, we analyze relationship between file size and transmission rate.

### A. Distribution of Packet Interarrival Time



| | 0.0001 | 0.001 | 0.01 | 0.1 | 1 | 10 | 100 |
|---|---|---|---|---|---|---|---|
| 20100407-2 | 38.0000% | 3.1314% | 43.2457% | 13.2800% | 1.9086% | 0.4229% | 0.0114% |
| 20100407-3 | 39.7625% | 3.3465% | 5.1457% | 44.9082% | 5.5416% | 1.2954% | 0.0000% |
| 20100407-4 | 35.3354% | 4.0728% | 8.0279% | 50.0000% | 2.2697% | 0.2816% | 0.0126% |
| 20100409-1 | 36.3011% | 11.7478% | 31.6247% | 18.4905% | 1.4845% | 0.3135% | 0.0378% |
| 20100409-2 | 21.3127% | 22.8682% | 34.3188% | 16.2162% | 2.9675% | 2.2394% | 0.0772% |

Fig. 5. Packet interarrival time of traces

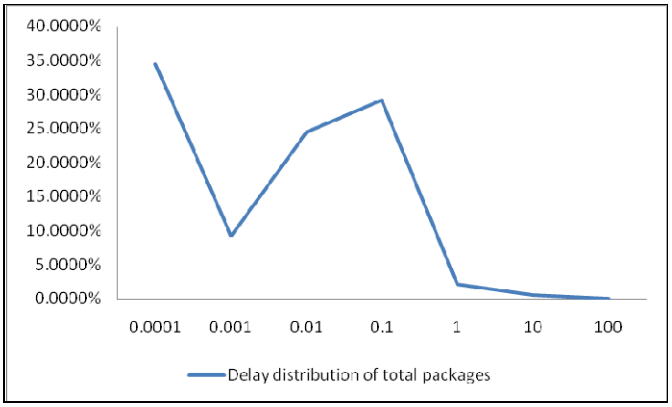


Fig. 6. packet interarrival time distribution of all traces

We have 5 separate network traffic trace files captured in our experiments. The dark blue, the red and the green traces are captured on April 7th, 2010. The locations of data collection were different. The dark blue trace is captured from A to B as shown in Fig. 1, and the red trace is capcured from B to C, green trace from C to A. The data of purple and light blue traces are collected on April 9.

The distributions of packet interarrival time are similar between the 5 files. The sizes of most of the packets are not bigger than 1500 bits. In Fig 5, we can find all five traces have high percentage of the interarrival time being less than 0.0001 second. The green trace and the red trace are similar that the peaks appear at 0.01 second to 0.1 second. The peaks of the other three trace occur at 0.001 to 0.01 second. The interarrival time longer than 0.1 second only happened in a few packets. The packet interarrival time of all the packets (distribution shows in Fig. 6) is similar with each separate traces. The peaks appear while response time less 0.001 second and between 0.01 to 1 second.

### B. *Access Point Switching Event*

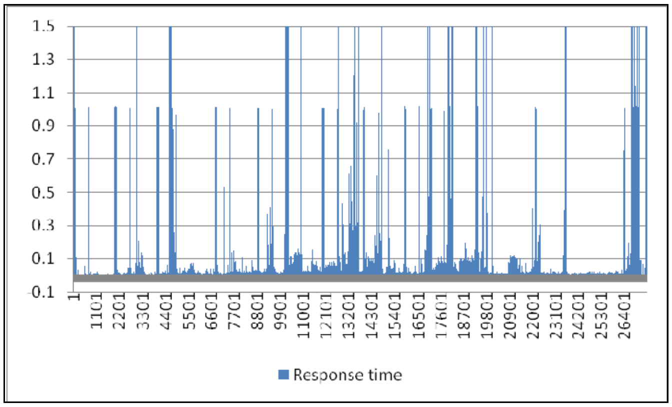


Fig. 7. packet interarrival time of trace 20100409-1. The minimum interval time is 0.006ms, maximum time is 51.6s, and average interval time is 0.024s

Access point switching event cannot be avoided in vehicular networks. = A time series of the is shown in Fig .7 of the packet interarrival time from one trace we captured. Typically, in an area covered by one access point, the transmission rate can be fast and the response time is low. However, while the client switches the access points it connects, the interarrival time becomes large. As shown in Fig. 7, the interarrival time can reach as high as 1 second while the client connection switches from one access point to another one. The result means that most packets can still be transmitted in long delay. We also observed that in some cases, the transmission turned to stale.

The vehicle speed also would change the packet interarrival time and packet rate. The two traces shown in the Fig. 8 and Fig. 9 are captured from the same location, i.e., in front of the Quad of UA, on the road marked C in Fig.1. They came from the first round and the second round passing by the location . In the first round of our experiment, our experiment vehicle kept 20MPH constant speed. However, the speed was increased to 25MPH in the second round. We intercepted both 20 second length of packet traces in the two rounds. But the two figures show distinct features. In the first round, we get 2747 packets in 20 seconds, while we only get 58 packets at the faster speed in the second round. The packet interarrival time of Fig. 9 is also longer than that of Fig. 8, at a lower vehicle speed.

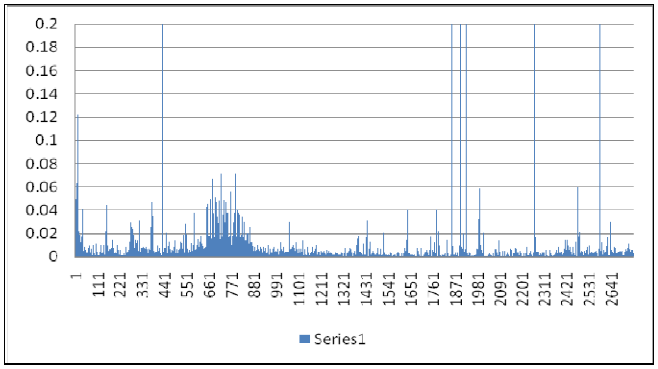


Fig. 8. Packet Response time at 20MPH (second)

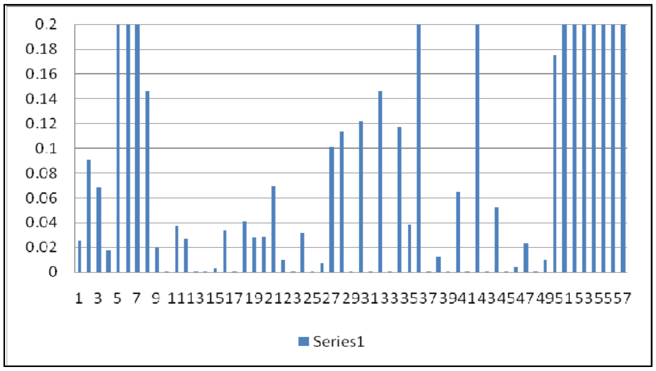


Fig. 9. packet interarrival time at 25MPH (second)

There are two reasons for this comparison. The first one is Doppler shift. A lot of studies discussed the effect of Doppler shift for IEEE 802.11g [6][7]. Doppler shift caused packet transmission in low data rate, especially for larger packet sizes. The other reason is the access point switching. The AP switching time of IEEE 802.11g is much longer than that of cellular networks. But the coverage area of 802.11g AP is much smaller than cellular base station. As a result, the moving 802.11g client only has a small time slot in the coverage area of one AP, and a big part of this time slot used for access points switching. Only a little time is used for packet transmission. Plus the affection of Doppler shift, the transmission rate of higher vehicle speed, shown in Fig.9, is much lower than that of lower speed, shown in Fig.8.

### C. *Handshake time of HTTP HTTPS, and SSH*

Handshaking steps have dicussed in section II. Because of distinct security protocols used in diverse applications, the handshake time is also varied. Fig. 10 showsthe handshake time in the second trace of April 9th. In this trace, we captured 55 times of HTTP handshakes, 56 times of HTTPS handshakes, and 56 times of SSH handshakes . The handshake time of HTTP is the shortest , the handshake times of HTTPS and SSH are much longer than those of HTTP's, And SSH takes the longest time.

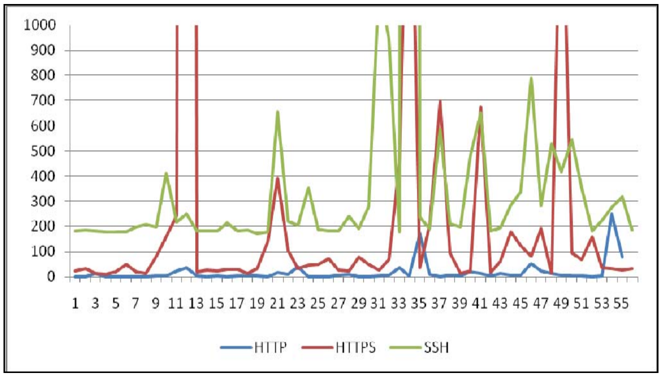


Fig. 10. Handshake time of HTTP, HTTPS, and SSH (ms)

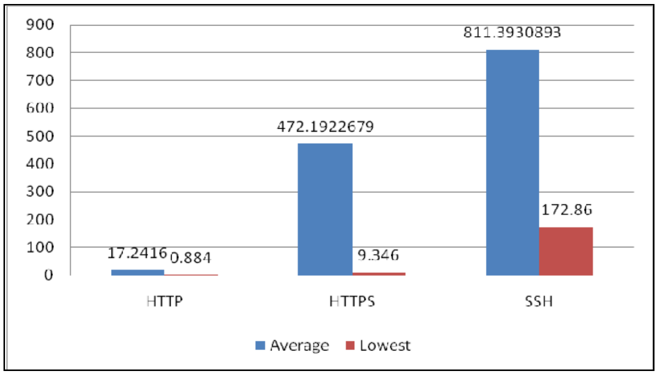


Fig. 11. Lowest and average Handshake time (ms)

As discussed in Section II, HTTP needs 3 packets to finish handshaking, while HTTPS needs 8 packets and SSH needs 17 packets to complete it. We calculate the average handshake time for each application and pick up the lowest time for each application (see Fig 11). It is interesting to note that the ratio of the handshake time of the three application protocols is not 3:8:17. Inspecting the handshake packets carefully, we find that HTTPS and SSH not only include TCP handshake packets but also include some large packets such as encrypted messages. HTTPS includes 2 encrypted messages and SSH includes 4. Transmiting these large packets dominates the total handshaking time. As a result, the average handshake time of HTTPS and SSH is almost 1:2.

### D. *File transmission*

In the file transmission experiment, we failed many times because of the long time slots needed. But we are still able to have 27 successful transmissions of a 486,912 bytes small file and 23 successful transmissions of a 1,057,280 bytes large file. The throughouts for each file transmission are given in Fig 12.

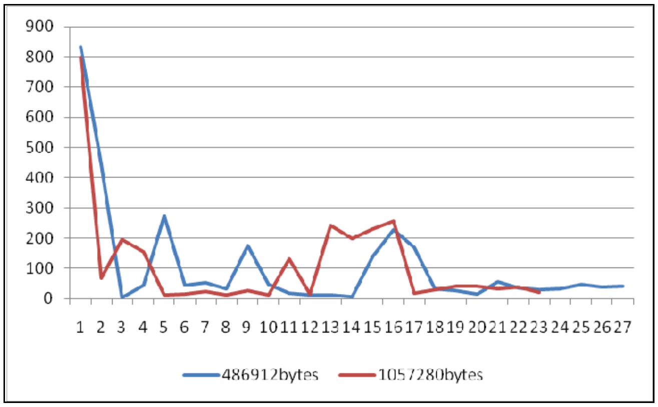


Fig. 12. Transmission rate of two files (KB/s)

Table I shows the transmission rates of of successful transmission by iBook. Comparing the two files at different places in our experiments, we find that the transmission rates of the two files are close at each time point. Also, the table shows that the transmission rate is not related to the size of files transferred.

TABLE I
TRANSMISSION RATE (CAPTURED BY IBOOK)

| | Position | The smaller file | The bigger file |
|---|---|---|---|
| *1* | *Library(B)* | -- | 241.8KB/s |
| *2* | | 141.5KB/s | 198.3KB/s |
| *3* | | 228.3KB/s | 231.5KB/s |
| *4* | | 170.4KB/s | 257KB/s |
| *5* | | 32.4KB/s | 16.7KB/s |
| *6* | *Rose Adm(C)* | 26.8KB/s | Failed |
| *7* | | 16.3KB/s | Failed |
| *8* | | Failed | Failed |
| *9* | *Fugerson(D)* | 54.6KB/s | 30.9KB/s |
| *10* | | 34.1KB/s | 42.5KB/s |
| *11* | | 30.2KB/s | 41.2KB/s |
| *12* | | 32.6KB/s | 33.7KB/s |
| *13* | | 47.2KB/s | 37.9KB/s |
| *14* | | 38.1KB/s | 19.8KB/s |
| *15* | | 40.8KB/s | Stopped |

The table compared transmission rate of two files in different area and different time.

Table II shows files transmission captured by ThinkPad. The transmission rates vary when our measurement vehicle running in different speeds. Line 5 to Line 8 in Table II show the transmission rates while the car passes in front of Rose Administration Building at 20MPH; Line 13 to Line 15 show the transmission rates at the same place in another round with a higher speed 25MPH. We got 8 successful transmission in the first round while only 4 success and 2 faild in the second round. The transmission rates of the first round were faster than those of the second round.

TABLE II
TRANSMISSION RATE (CAPTURED BY THINKPAD)

| | Position | The smaller file | The bigger file |
|---|---|---|---|
| *1* | *Museum(A)* | 832.8KB/s | 799 KB/s |
| *2* | | 443.2 KB/s | 68.1 KB/s |
| *3* | *Library(B)* | 3.3 KB/s | Failed |
| *4* | | Failed | Failed |
| *5* | *Rose Adm.(C)* | 42.9 KB/s | 194.9 KB/s |
| *6* | *(20MPH)* | 275 KB/s | 153.4 KB/s |
| *7* | | 45.5 KB/s | 11.4 KB/s |
| *8* | | 52.8 KB/s | 13.9 KB/s |
| *9* | *Library(B)* | 32.9 KB/s | 25.2 KB/s |
| *10* | *Fugerson(D)* | 175.1 KB/s | 13.4 KB/s |
| *11* | | Failed | Failed |
| *12* | | 46.6 KB/s | 27 KB/s |
| *13* | *Rose Adm.(C)* | 17 KB/s | 11.3 KB/s |
| *14* | *(25MPH)* | Failed | 130.8 KB/s |
| *15* | | 12.5 KB/s | Failed |
| *16* | *Library(B)* | 13.2 KB/s | 13.8 KB/s |
| *17* | | 6.2 KB/s | Failed |

File transmissions captured by ThinkPad.

We also calculate the average transmission rates, the best and the worst transmission rates for the two files. According to the results shown in Fig.13, the average transmission rates of the two files are similar as well as the highest transmission rates. The lowest transmission rate of the smaller file is lower than that of the bigger one. Considering the fact of less successful download of bigger file, we think the results are reasonable because only the fast transmission rate suvivled the long time needed for the large file download. We conclude that the transmission rates of different file sizes are similar in moving clients on average. However, smaller files can get more successful transmissions than bigger files.

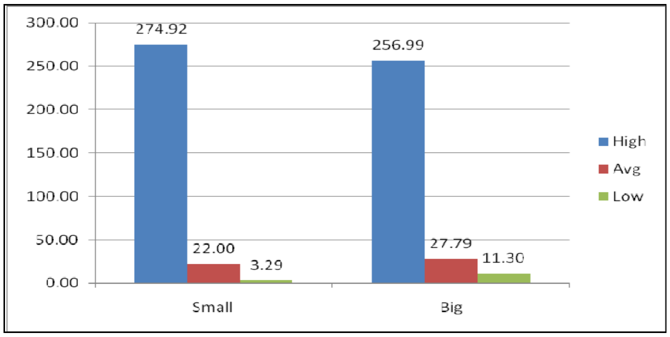


Fig. 13. Highest, Lowest, and average rate for two files (KB/s)

## VI. CONCLUSION

In this paper, we presented wireles LAN access data which was collected from a moving vehicle and analyzed the performance metrics of packet interarrival time, handshake time and transmission rate. We investigated the factors that are unique to the vehivle-to-roadside communications, including access points switching and the vehicle speed. Our main results are focused on security enabled protocols such as HTTPS and and SSH, as well as TCP file transmission. Our data shows that IEEE 802.11g is still weak in supporting mobile vehicle access to the Wireless LAN. We expect thtat IEEE 802.11p, designed specifically for vehicle networks can provide better mobile services.

## REFERENCES

[1] http://ivc.epfl.ch/

[2] http://en.wikipedia.org/wiki/HTTP_Secure

[3] http://en.wikipedia.org/wiki/Secure_Shell

[4] J. Tao, X. Hong, and P.G. Bradford “Single-Hop and Multi-Hop Delay Characteristics of Ad-Hoc 802.11b Wireless Network,” in *Proc. 19th IASTED*, Cambridge, Massachusetts, 2007, pp. 162–167.

[5] G. Resta, P. Santi, and J. Simon, "Analysis of Multi-Hop Emergency Message Propagation in Vehicular Ad Hoc Networks," in *Proc. 8th ACM international symposium on Mobile ad hoc networking and computing*, Montreal, Quebec, Canada, 2007, pp. 140–149.

[6] A. Silvennoinen, M. Hall1 and S. Häggman, “The Effect of Terminal Movement on the Performance of IEEE 802.11 g Wireless LAN Systems in Simulated Radio Channels,” *Proc. of Wireless Personal* Communications, Volume 41 , Issue 4, Pages487-505, June 2007.

[7] S. F. Mason, C. R. Berger, S. Zhou, and P. Willett, “Detection, Synchronization, and Doppler Scale Estimation with Multicarrier Waveforms in Underwater Acoustic Communication,” *Proc. of Communications, IEEE Journal* on Volume 26, Issue 9, 2008, Pages 1638 – 1649.

[8] F. Bai, and B. Krishnamachari, "Spatio-temporal variations of vehicle traffic in VANETs: facts and implications," *Proceedings of International Conference on Mobile Computing and Networking*, Beijing China, 2009, pp. 43-52.

[9] H. Zhu, L. Fu, G. Xue, Y. Zhu, M. Li, and L. M. Ni , "Recognizing Exponential Inter-Contact Time in VANETs," *Mini-Conference at IEEE INFOCOM* 2010.

[10] Ming-Fong Jhang, Wanjiun Liao, “Cooperative and Opportunistic Channel Access for Vehicle to Roadside (V2R) Communications,” Mobile Networks and Applications Volume 15 , Issue 1, 2010, pp. 13 - 19

[11] J. Ott, D. Kutscher, “Drive-thru Internet: IEEE 802.11b for Automobile“ Users,” in Proceedings of the IEEE INFOCOM’2004 Conference, Hong Kong, March 2004.

[12] D. Hadaller, S. Keshav, T. Brecht, S. Agarwal, “Vehicular opportunistic communication under the microscope,” ACM MobiSys’07, June 2007

[13] V. Bychkovsky, B. Hull, A. Miu, H. Balakrishnan, S. Madden, “A measurement study of vehicular internet access using in situ WiFi networks,” ACM MobiCom ’06, Sept 2006.

[14] J.T. Isaac, J.S. Camara, S. Zeadally, and J.T. Marquez, A Secure Vehicle-to-Roadside Communication Payment Protocol in Vehicular Ad Hoc Networks. Computer Communications, Volume 31, Issue 10, 25 June 2008, Pages 2478-2484.