Final Report

Research Grant 2015

ATRANS

ASIAN TRANSPORTATION RESEARCH SOCIETY

A Study of Data Dissemination on Vehicular Ad Hoc Networks using IEEE802.11p Communication System

Passakon Prathombutr
Kultida Rojviboonchai
Kulit Na Nakorn
Kiattikun Kawila

A Study of Data Dissemination on Vehicular Ad Hoc Networks using IEEE802.11p Communication System

ATRANS
ASIAN TRANSPORTATION RESEARCH SOCIETY

902/1 9th Floor, Glas Haus Building, Soi Sukhumvit 25 (Daeng Prasert),
Sukhumvit Road, Klongtoey-Nua, Wattana, Bangkok 10110, Thailand
Tel. (66) 02-661-6248   FAX (66) 02-661-6249
http://www.atransociety.com

March, 2016
Printed in Thailand

ATRANS

ASIAN TRANSPORTATION RESEARCH SOCIETY

List of Members

• Project Leader •

Passakon Prathombutr, Ph.D
National Science and Technology Development Agency (NSTDA), Thailand

• Project Members •

Kultida Rojviboonchai, Ph.D.
Kulit Na Nakorn, Ph.D.
Kiattikun Kawila
Information System Engineering Lab (ISEL), Department of Computer Engineering,
Faculty of Engineering, Chulalongkorn University, Thailand

Abstract

Vehicular network is a hot research topic and gains a lot of interests because Intelligent Transport System (ITS) can significantly improve quality of life on the road. In recent years, many applications on ITS have been developed such as collision avoidance applications, public transport applications and traffic management services. However, all of existing applications require cellular networks for both data retrieving and data disseminating. Although IEEE802.11p has been a standard for vehicular networks, there is still no work that applies this standard to completely support ITS services in the real world. A reason is that IEEE802.11p has just been published in 2011. Most of devices are prototypes and in developed process.

In this research, we study a system that integrate all communication types in vehicular network (V2V, V2I and V2P) with a real IEEE802.11p communication device. In the study system, all data have to be delivered using IEEE802.11p standard. All vehicles can directly communicate with each other as a multi-hop ad hoc concept. An advantage of this concept is this system can operate without any help of infrastructures such as cellular base stations or servers. In order to accomplish the research objective, this system should consist of a well design structure that can collect data from each vehicle to users and an efficient protocol that can disseminate data to all nearby vehicles in the area of interest with a reliable and efficient solution.

Table of Contents

List of Figures

ATRANS

ASIAN TRANSPORTATION RESEARCH SOCIETY

CHAPTER I INTRODUCTION

Background

Vehicular network is a hot research topic and gains a lot of interests because Intelligent Transport System (ITS) [1] can significantly improve quality of life on the road. Applications for ITS such as traffic management, public transport management and emergency notification require an efficient communication solution that can deliver information to all vehicles in an area of interest. Currently, there are three types of communication in vehicular network. 1) *Vehicle-to-Vehicle (V2V)* allows vehicles directly communicate to each other without any help of infrastructure. This type of communication is appropriate for collision avoidance or emergency service that require least delay. 2) *Vehicle-to-Infrastructure (V2I)* extends a range of communication and also increase reliability of system. Moreover, V2I connects the communication between vehicle networks and other network standards. 3) *Vehicle-to-Pedestrian (V2P)* is considered as a new communication in vehicular networks. Many researchers believe that vehicular network standard will be included in the next generation of smart phones to connect with ITS applications and services. These three mentioned communication types must be connected to each other in order to exchange their valuable information of success ITS services and applications.

In recent years, many services and applications on ITS have been developed such as emergency management, traffic management, arterial management and public transportation management which is one of the most interesting application. The public transportation service can provide an arrival time of each bus or train from servers that collects positions of public transport vehicles. This lets passengers know that how long they have to wait for their transport. Moreover, drivers' behavior can be monitored via communication system so any risk activities will be reported and warned the drivers. However, all of existing applications require cellular networks for both data retrieving and data disseminating. Although IEEE802.11p [2] has been a standard for vehicular networks, there is still no work that applies this standard to completely support ITS services in the real world. A reason is that IEEE802.11p has just been published in 2011. Most of devices are prototypes and in developed process. Very few brands install IEEE802.11p devices on their cars. Therefore, this research aims to motivate the utilization of IEEE802.11p in public transport.

Objective

The objective of this research is to study a system that integrates all communication types in vehicular network (V2V, V2I and V2P) with a real IEEE802.11p communication device. In the study system, all data have to be delivered using IEEE802.11p standard so all vehicles in the system can directly communicate with each other as a multi-hop ad hoc concept. An advantage of this concept is this system can operate without any help of infrastructures such as cellular base stations or servers. The communication between vehicles and pedestrians use Wi-Fi access points because there is no phone that support IEEE802.11p at this time. To accomplish the research objective, the system should consist of a well design structure that can collect data from each vehicle to users and an efficient protocol that can disseminate data to all nearby vehicles in the area of interest with a reliable and efficient solution.

Literature Review

There are many researches that related to the real vehicular-based evaluation. Because a device with IEEE802.11p standard is just released and can be obtained shortly, so many researchers try to evaluate the performance of device to understand characteristic of IEEE802.11p PHY and MAC standard. Therefore, most of previous researches have a common purpose that is to evaluate the communication range and analyze the propagation loss model in both LOS and NLOS of device. Although these works are tested on the real field, none of them were tested on many nodes such as a public transport environment.

Andre´ Cardote et al proposed a statistical channel model for realistic simulation in VANET [3], which is a loss propagation model based on real-world signal measurements. This research using the framework presented in [4] and [5]. This measurement performs an observation on path loss and fading in Line-of-Sight (LOS) communication. The communication of vehicle to infrastructure on IEEE 802.11p in urban environments also was studied to analyze the impact of urban characteristics in roadside unit (RSU) deployments of Vehicle to Infrastructure (V2I) [6].

Toutouh and Alba [7] evaluated the performance of a new VANET protocol, called Vehicular Data Transfer Protocol (VDTP). The experiment is conducted in real urban environment using two vehicles with IEEE 802.11b transceivers. The average distance between vehicles is 77 meters. The authors reported that the speed of vehicles impacted in low data rate and high packet loss.

Sukuvaara, Ylitalo, and Katz [8] compared the performance of IEEE802.11g and IEEE802.11p in one-hop and multi-hop scenarios. Tested vehicles are drove with various speed: 70, 80, 90 and 100 km/h. The average distance between vehicles is 100 meters. As a result, IEEE802.11p outperform than IEEE802.11g.

Vivek, Srikanth, Saurabh, Vamsi and Raju [9] study the performance of WAVE Short Message Protocol (WSMP) on IEEE802.11p in term of loss, delay and jitter. The experiment also deployed one Road Side Unit (RSU) to generate network traffic with 400-byte packet every 10 seconds. The results show that the distance between source and receivers relates to packet loss rate.

Mangel, Michl, Klemp, and Hartenstein [10] conducted the experiment to evaluate the performance of IEEE802.11p for non-line-of-sight scenarios. The experiment took place at intersections in Munich. Giordano, Frank, Pau, and Gerla [11] also evaluated non-line-of-sight scenarios at building's corner. However, communication devices are IEEE802.11b/g which is not a standard for vehicular networks.

Although there are many researches that evaluate the performance of IEEE 802.11p [3-13], most of them aim to analyst the loss propagation model of the IEEE 802.11p device. There are no any researches that study on real-world public transport system especially in the data dissemination topic. All of previous works also have done on limited number of transceivers so studying the performance of IEEE 802.11p devices on real-world public transport is essential for a direction of future development of ITS applications and services on public transportation.

CHAPTER 2 RESEARCH METHODOLOGY

System Structure

An important concept of this research is to prove that this system can operate without any cellular communication but only uses IEEE802.11p standard to exchange information between vehicles. For more clarification, let us explain an overview of mechanisms in our experiment system. First, vehicles need to exchange their information among their neighbors to get local data (a list of 1-hop neighbors and traffic density) using beacon message then this information will be used for broadcasting protocol.

A message from each vehicle will be disseminated to other vehicles in the area. The message can contain a position, an announcement or a bus status. Each vehicle also exchanges this message with an intelligent bus stop to provide important information to passengers. If passengers have a smartphone, they can connect the smartphone with Wi-Fi hotspot of bus or the bus stop to retrieve the information. This overall system be illustrated in Fig. 1 and its mechanism can be illustrated in Fig. 2.

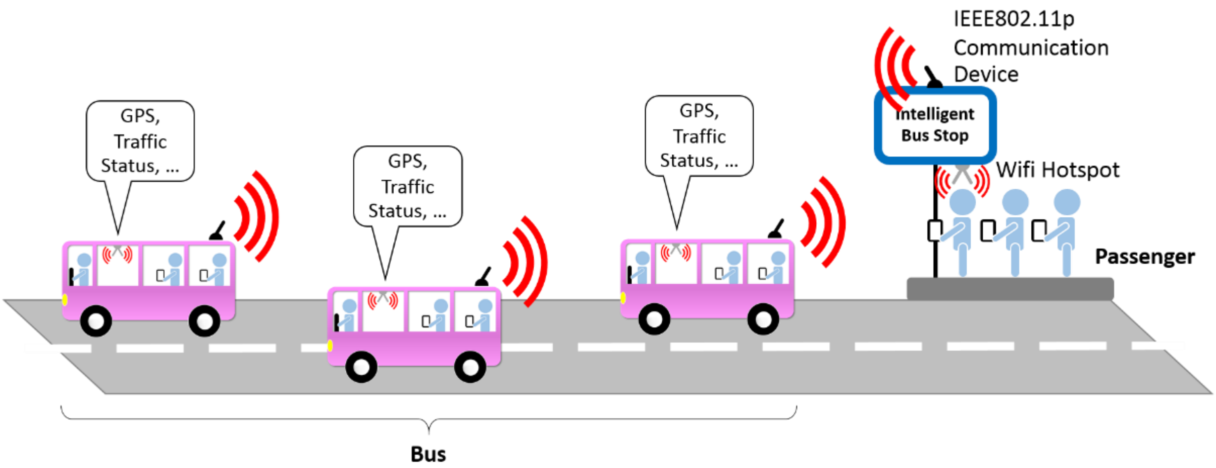


Figure 1. A Communication System in Study System.

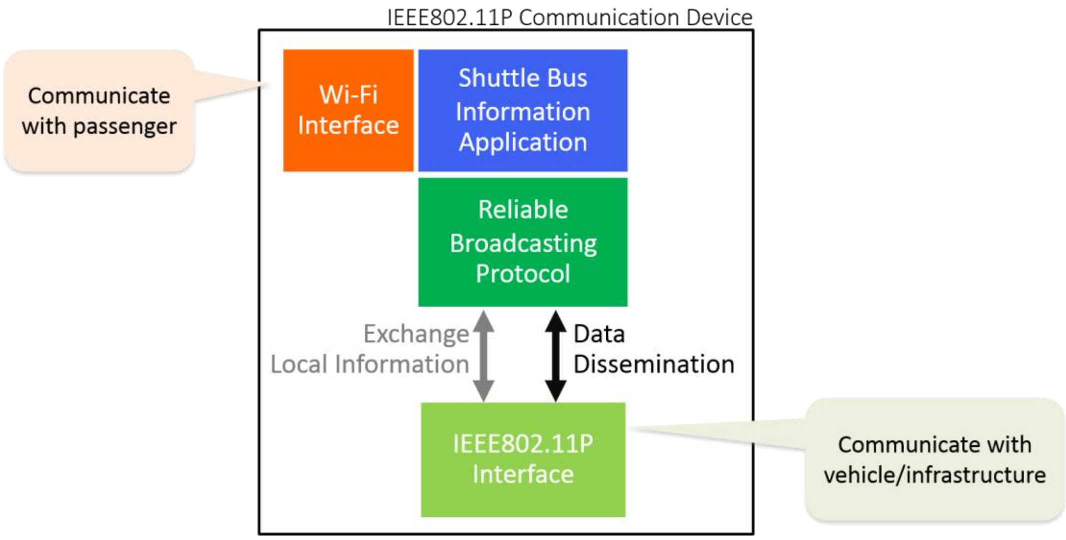


Figure 2. Mechanism in IEEE802.11p Communication Device.

The system consists of three important parts; application, reliable broadcast protocol and IEEE802.11p communication device.

Application

There are two types of application. The first application can be considered as a service or a middleware on IEEE802.11p communication device. This application will support the other applications in the system. It will received any data from Wi-Fi interface and disseminate the data through reliable broadcasting protocol and IEEE802.11p standard then send the data back to mobile application. Moreover, it can provide any local information from vehicle sensors. In our system there are six types of sensors: GPS, accelerate sensors, gyroscope, light sensor, humidity sensor and temperature sensor. An example of application that we implemented in this research can be illustrated in Fig. 3. The application shows the information from all of sensors. These data can be used for further knowledge such as drivers' behavior or traffic jam information.

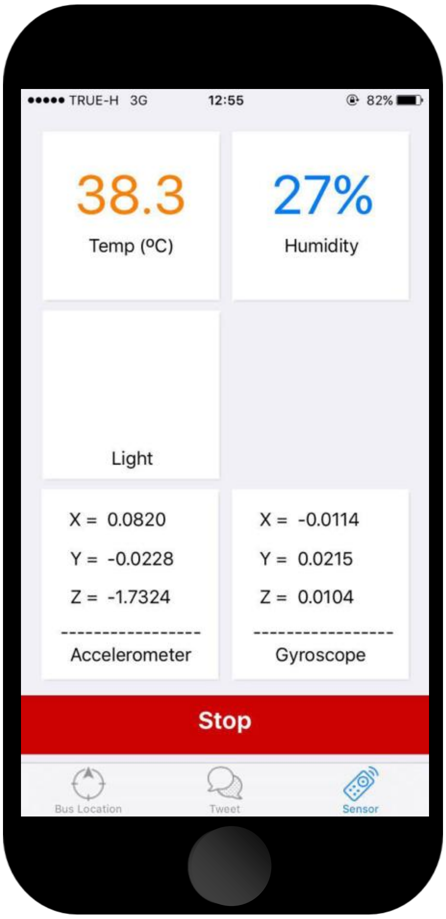


Figure 3. Bus Information Application.

The second application is a mobile application on a smart device or an application on a smart bus stop. It analyses data and provide useful information to user. For example, the application retrieves position of a shuttle bus and calculates an arrival time of incoming bus or it can show an announcement to passenger. Figure 4 shows our smart bus stop application that get bus information from IEEE802.11p standard. This application can work on both a standalone roadside unit and an infrastructure that get information from server.

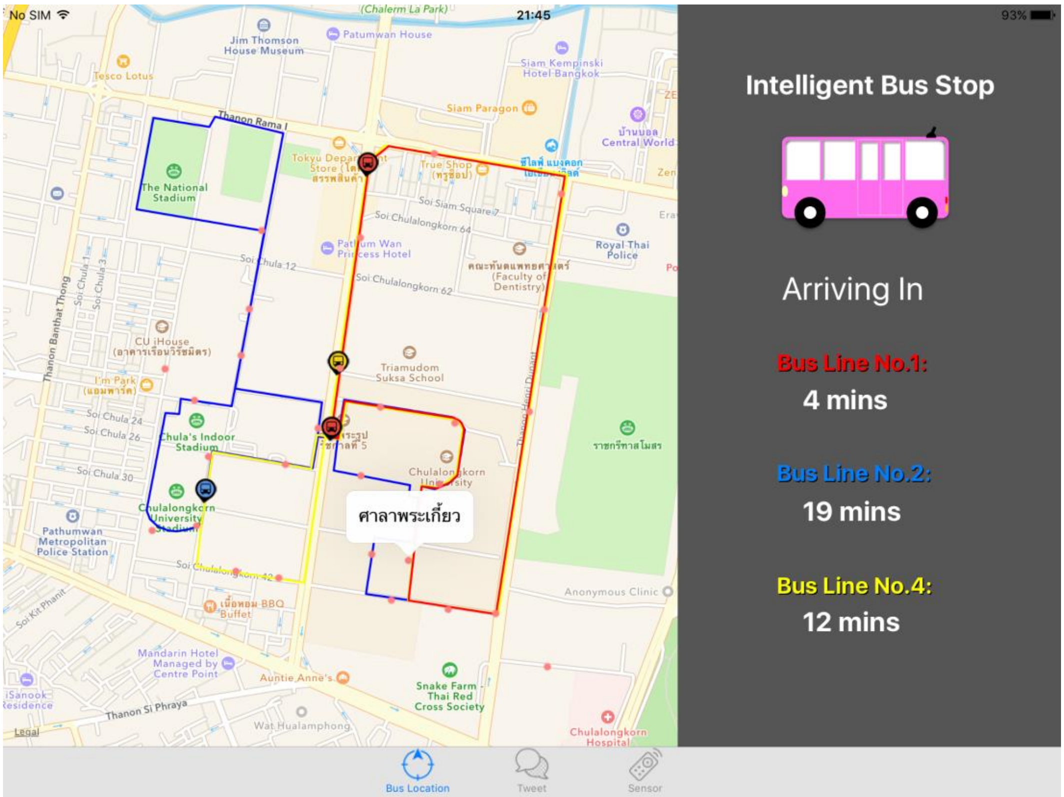


Figure 4. Shuttle Bus Arrival Time Application.

Reliable Broadcasting Protocol

In order to provide a reliable and efficient data dissemination service. The system need a reliable broadcasting protocol that can handle connectivity issue in vehicular network such as an intermittent connectivity problem and a long-time disconnection. The reliable broadcasting protocol is deployed on IEEE802.11p communication device to support data transmission in the system.

In this research, we use density-aware reliable broadcasting protocol (DECA) [14]. DECA is designed to maximize the data dissemination rate with low overhead in vehicular network. It uses the store and forward technique with periodic beacons to choose a next vehicle that has the highest density to rebroadcast a message. DECA's mechanism can be illustrated in Fig. 5.

There are three main module in DECA. First, a node selection mechanism is a module that select the next forwarder node. The next forwarder node is selected from a node that has the highest number of neighbors to maximize the number of receivers. Second, a beacon mechanism helps a node discover its neighbor and neighbor's information such as a number of neighbors and a list of received packets. Therefore, DECA can recover a missing packet using information from neighbor's beacon. Finally, a waiting timeout mechanism provides an appropriate waiting timeout to a node to avoid collision due to distributed system. The waiting timeout mechanism is activated when a node receives a new package or it notices a missing package from neighbor.

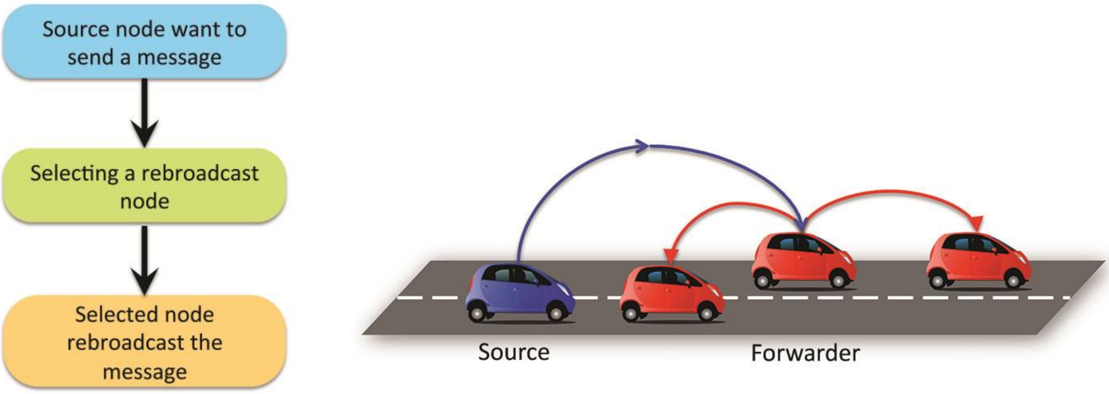


Figure 5. DECA Mechanism.

IEEE802.11p Communication Device

An IEEE802.11p communication device has the most important role in this system. The reason is all of data need to be exchanged and collected by this device. It also will be deployed on both shuttle buses and bus stops. The device requires two wireless interfaces; an IEEE802.11p interface used for exchanging information between vehicles and bus stops and a regular Wi-Fi interface used as a Wi-Fi hotspot.

We use DENSO WSU model 5001 (WSU-5001). Its available Input/Output interfaces are shown in Fig. 6. The device also supports the full version of WAVE standards including IEEE P1609.3 [15], IEEE P1609.4 [16], and IEEE 802.11p [2]. We also deploy Raspberry Pi with various sensors to collect more information from our testing vehicle.

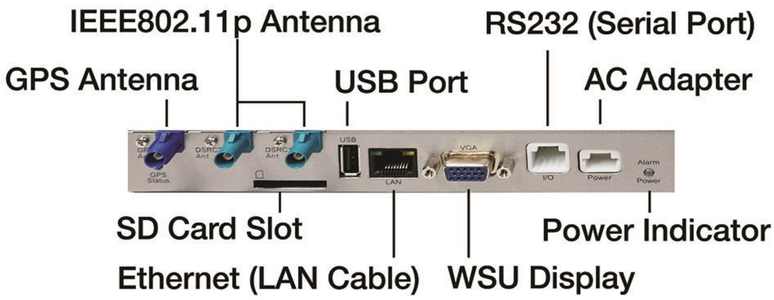


Figure 6. Available Interfaces on DENSO WSU Model 5001.

CHAPTER 3 SYSTEM IMPLEMENTATION

Communication Structure

The communication stack of the system can be illustrated in Fig. 7. Currently, there is no any available mobile devices that can communicate via IEEE802.11p standard so this system uses a Wi-Fi access point to be in the middle between IEEE802.11p devices and IEEE802.11a/b/g/n devices. The data exchanging between bus-to-bus and bus-to-bus stop (infrastructure) directly transferred with IEEE802.11p and the communication between a bus and a passenger uses a tradition standard that is available on any mobile devices.

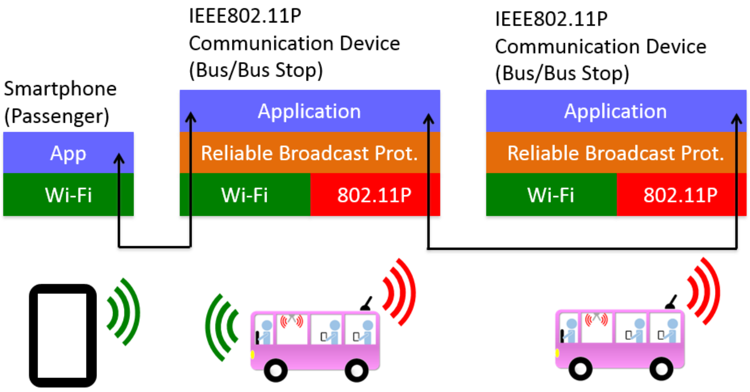


Figure 7. Communication Stack.

The Wi-Fi access point, the raspberry pi and sensor is connected to DENSO WSU through Ethernet switch. Our testing device for installing can be shown in Fig. 8. Therefore, the data that needed by mobile applications are delivered through the standard Wi-Fi access point and other communications with a node is exchanged via Ethernet.

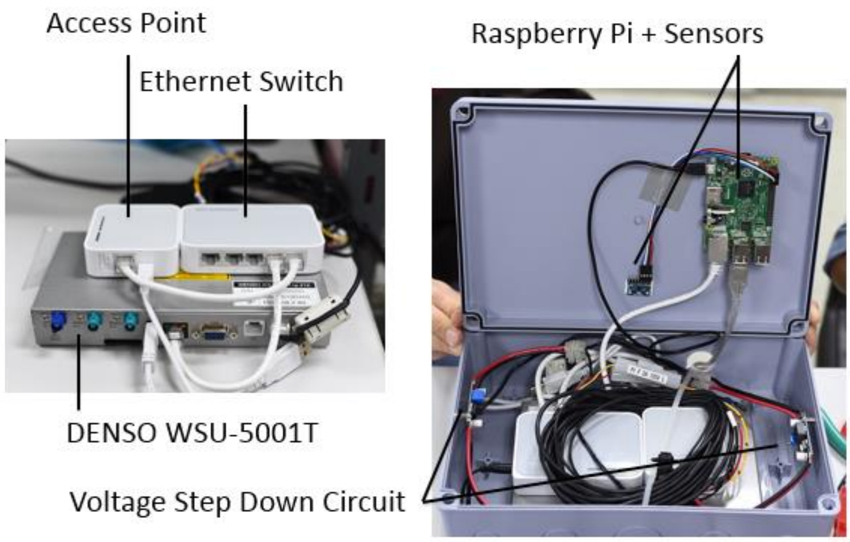


Figure 8. System Structure.

System Installation

Each testing device is installed at the front of shuttle bus in Chulalongkorn University. Two antennas of IEEE802.11p communication and a GPS antenna are placed on the roof of the bus as shown in Fig.9 and Fig.10. The sensor is placed at the front glass of the bus to get an accurate data from a light sensor, a humidity sensor and a temperature sensor. An acceleration sensor and gyroscope are placed inside the box that tightly fixed with bus body. There are 15 shuttle buses that installed the testing devices.

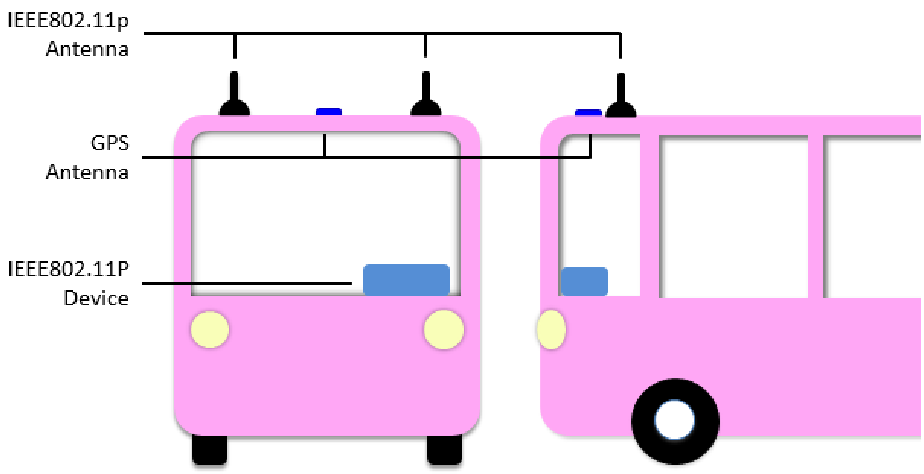


Figure 9. Position of Testing Device on Shuttle Bus.

Figure 10. Testing Device Installation on Shuttle Bus.

Our system also consists of two base stations that collect the information and recover missing packages to passing buses. The base station is located on covered walkway at coffee shop in Faculty of Engineering near central bus stop (Sala Phrakeaw Station) as illustrated in

Fig.11 and Fig.12. Another one is placed on covered way in front of Charoen Visawakarma Building (ENG4) in Faculty of Engineering, Chulalongkorn University.

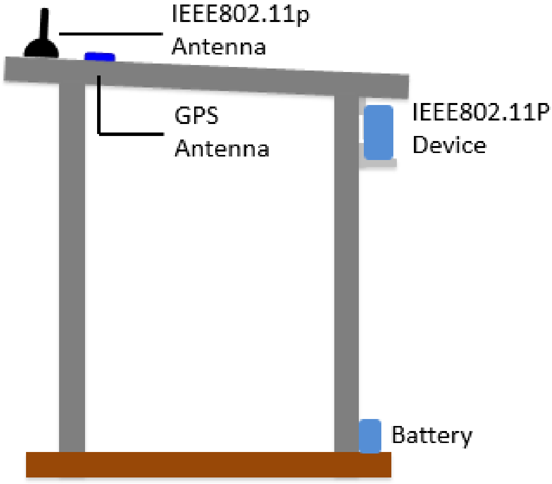


Figure 11. Position of Testing Device on Covered Walkway.

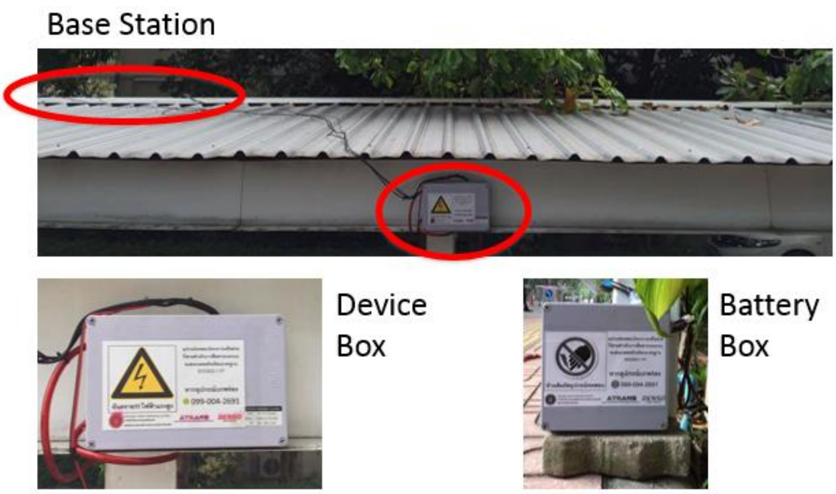
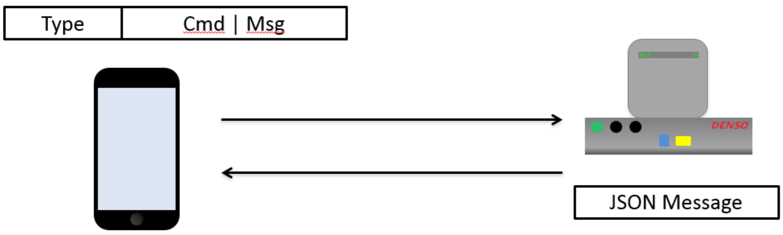


Figure 12. Testing Device Installation on Covered Walkway.

Application Programming Interface

In order to support any mobile applications, the system provide a standard API that can be called from mobile device. Figure 13 shows current available APIs that support short message communication and also position of bus. These APIs can provide important information to many ITS applications such as emergency warning, traffic report, bus management and monitor.

An example when a mobile device sends “hi” message to other devices is shown in Fig. 14. The system will start with “hello” message to register this communication to WSU device. This message is implemented in JSON format so it can flexibly adapted to use in any purposed. After the communication is initiated, an application will send data via “send” message. The system also includes "req" message for requesting any from the others and "gps" message for requesting the current position of the bus. Fig. 15 shows our smart bus stop application while our short message communication, bus tracking and bus monitoring application is illustrated in Fig. 16.



CMD	Detail
hello	Register device to WSU for short message notification
send	Send a short message to WSU; Send along with Msg
req	Request for short message
gps	Request for buses GPS

Figure 13. Application Program Interfaces of System.

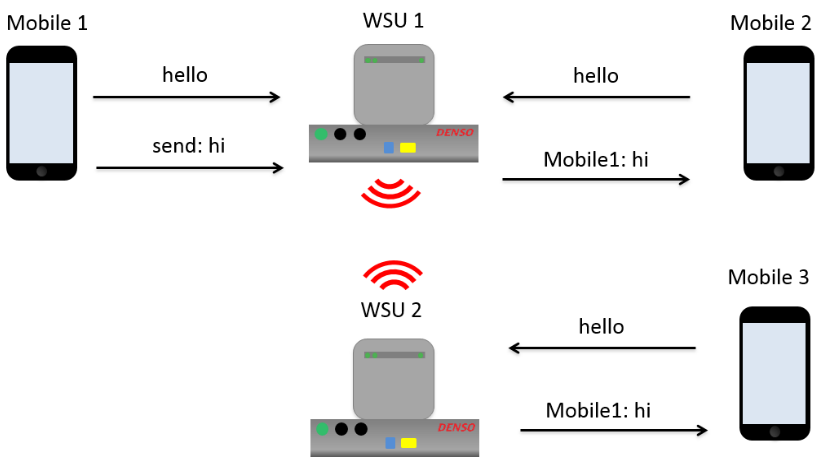


Figure 14. Short Message Communication.

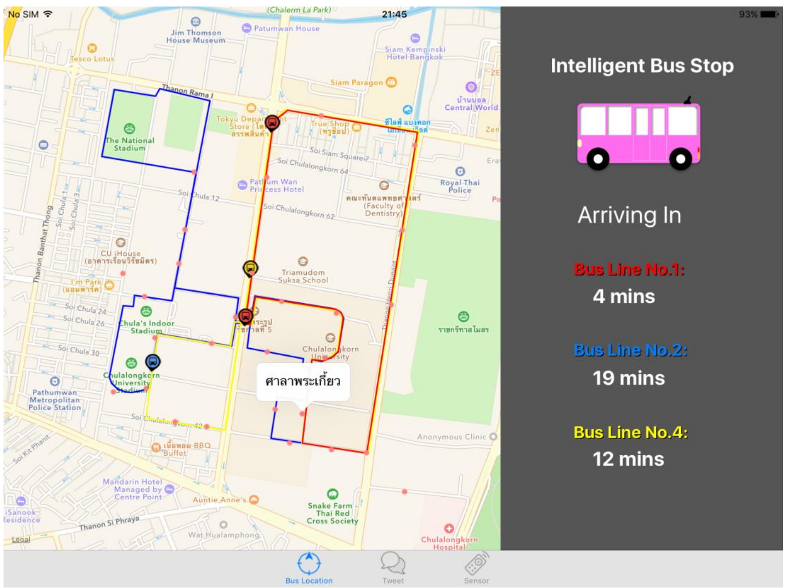
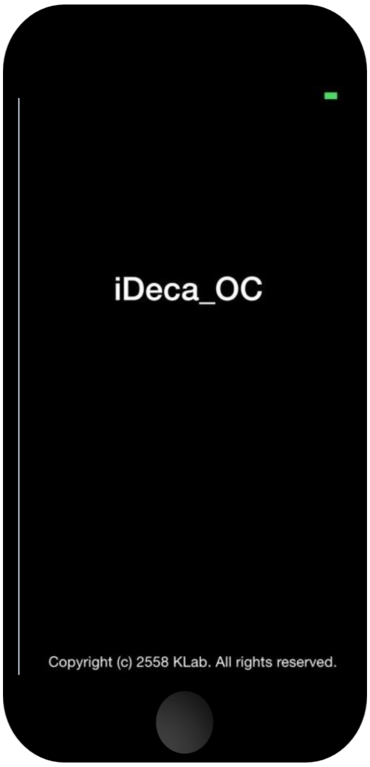
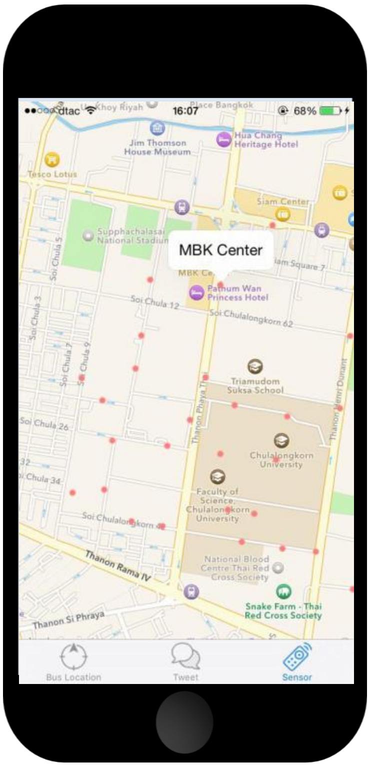


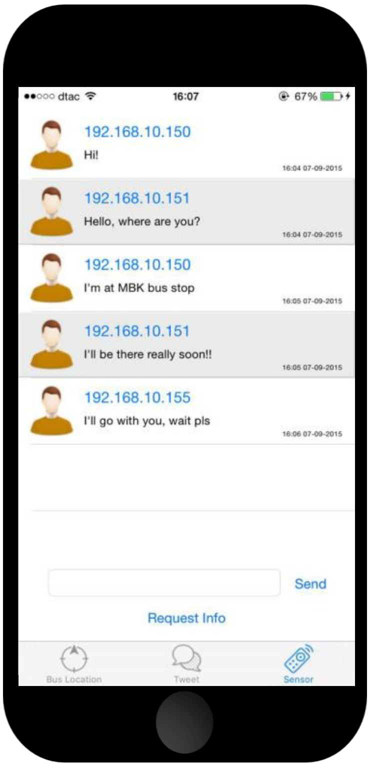
Figure 15. Smart Bus Stop Application.



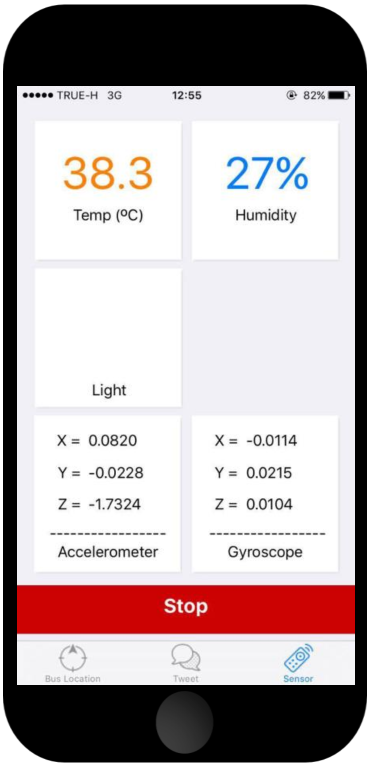
a) Startup Screen



b) Bus Location



c) Short Message Communication



d) Bus Monitoring

Figure 16. A Short Message Communication, Bus Tracking and Bus Monitoring Application.

CHAPTER 4 PERFORMANCE EVALUATION

Environment Detail

In our environment testbed, we deployed the testing devices on the shuttle bus system in Chulalongkorn University which is represented the intelligent public transport system. The shuttle bus system has a few specific bus lines cover several areas of Chulalongkorn University. Due to restricted resources such as number of 802.11p devices, we cannot deployed the testing devices to all buses. Thus, we chose some specific bus lines that cover the areas as possible. The bus lines that we chose were line number one, line number two, and line number four. Figure 17 displays routes of the selected bus lines by separated colors. All selected bus lines, the number of buses that we has deployed on line one, line two and line four are 6, 5, and 4 buses respectively. In addition, we deployed two testing devices for representing base stations. Two locations with green symbols on Fig. 17 were chose for base station deployment. These locations were represented a backbone of network that were placed nearly at the terminal of buses.

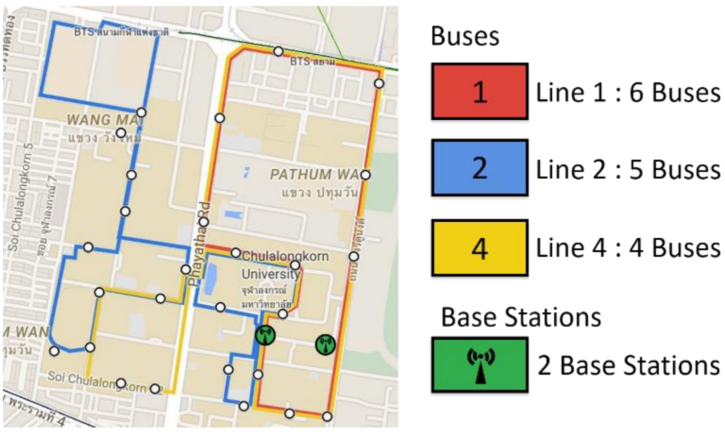


Figure 17. Bus Routes and Position of Base Stations.

Message Configuration

To study the data dissemination over vehicular ad hoc network based on realistic behavior, we assumed that all buses will generate their unique message as a data packet and send the message to other buses every a minute when they are online. As mentioned assumption gives us how our system can operate the worst case situation that has a lot of in-fight messages over network traffic efficiently. All in-fight messages can keep alive with a static period or a message lifetime. After their static period had expired, they will be removed from the network. In our environment, we scheduled the static period for 30 minutes. An initial message size is 512 bytes. In the figure 18 gives more details about the message including message header. The header format consists of IP address of source, ID number of message, information of GPS, and timestamp of message. Therefore, one message will have at least 544 bytes size, which is generated and sent to network every a minute.

Source IP (4 bytes)	Msg ID (4 bytes)	GPS (16 bytes)	Timestamp (8 bytes)	Payload (512 bytes)

Figure 18 Packet Header.

Study Results

For comprehensive discussion, we firstly will explain some serious characteristics of shuttle bus system. These characteristics can affect the performance of data dissemination directly. Next, we will investigate the results of environment testbed with two importance metrics: *Packet Delivery Ratio* and *Transmission Delay*.

The shutter bus characteristics:

- All shuttle buses are built in an electric engine.
- All shuttle buses stop their engine when they have arrived their terminal station for saving power.
- Battery of shuttle bus can deliver power up to half day.
- Battery of shuttle bus is only recharged at the bus garage.
- The bus with low battery power can be rescheduled the destination station from original terminal station to the bus garage immediately.
- The line number of bus can be changed due to demand from passengers or traffic jam.

Investigating results:

Online Activity Ratio

Online activity ratio demonstrates in the figure 19-22, the graphs implies significantly two observations. First, all buses that were deployed testing devices were not available at the same time. Some of them were disconnected from the network due to engine stopping. In this case, a range number of online buses per day is approximately 6 to 8 buses. Second, there are three period of times that a number of available buses is significantly high: the morning period between 06:00 and 08:30 as before starting morning class, the noon period between 10:30 and 13:00 as after finishing morning class or before starting afternoon class, and the evening period between 14:30 and 18:30 as after the last class of day.

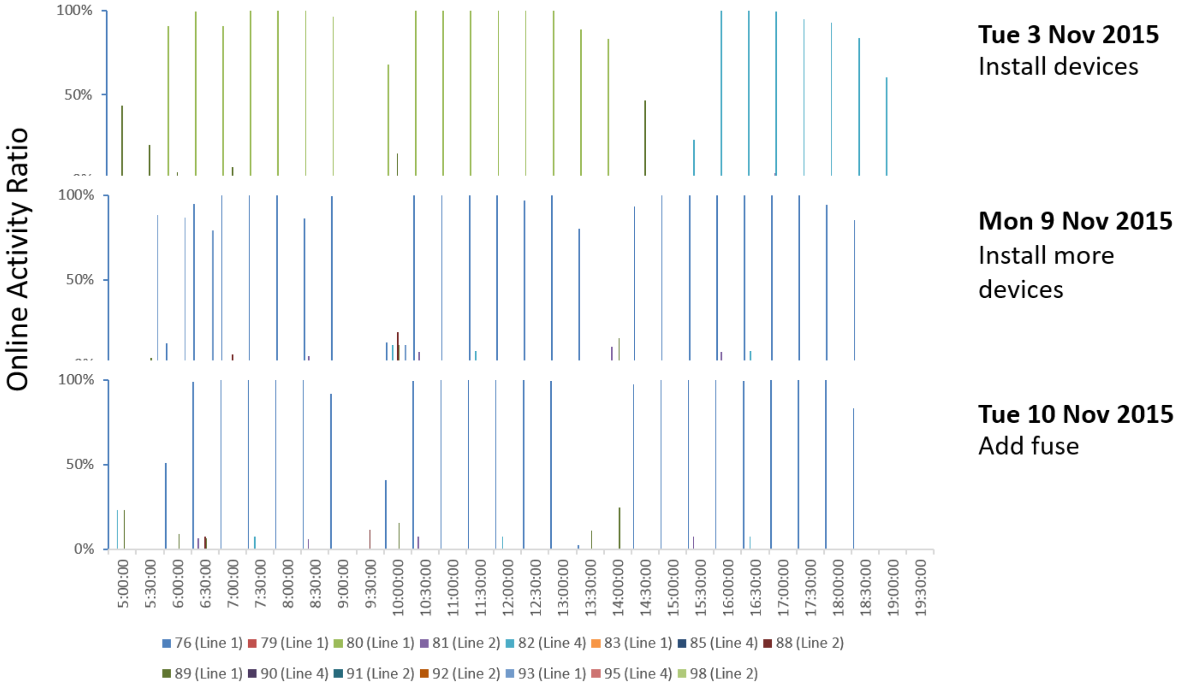


Figure 19. Online Activity Ration Results on Nov 3-10, 2015.

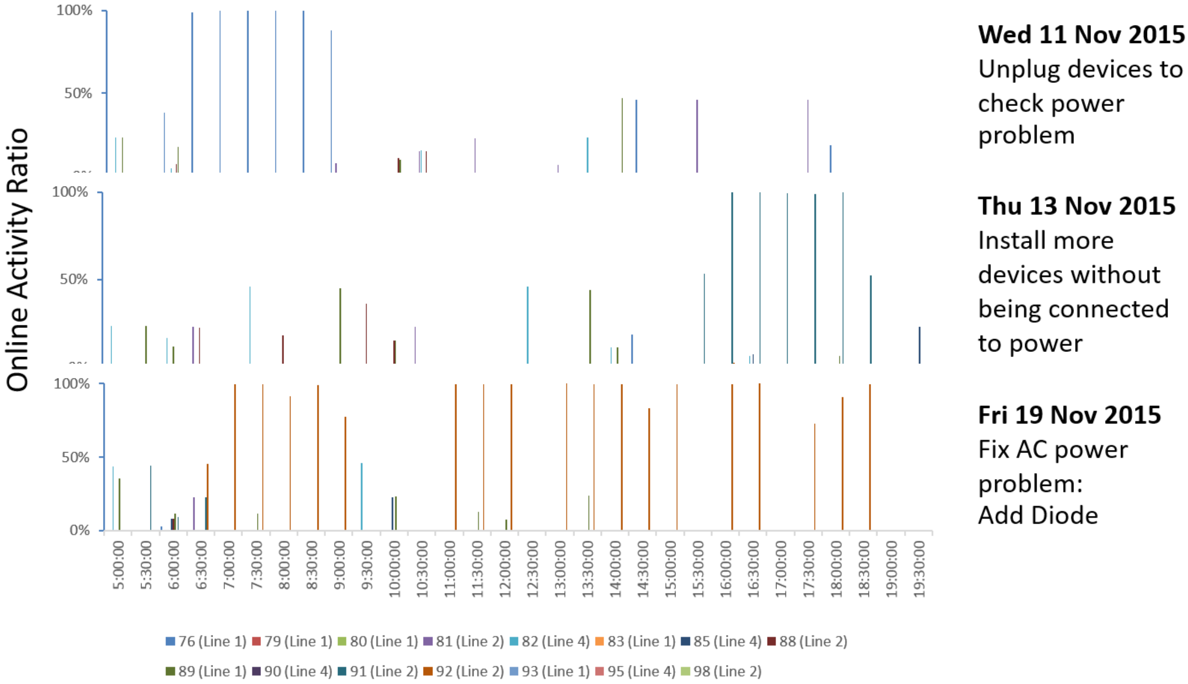


Figure 20. Online Activity Ration Results on Nov 11-19, 2015.

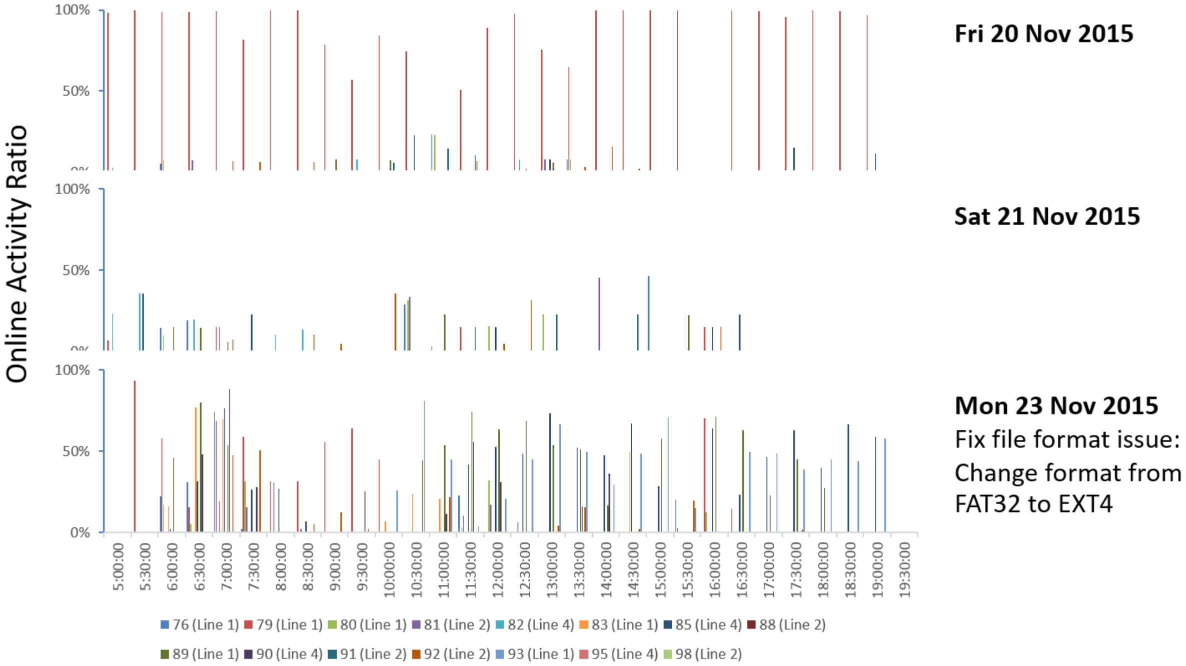


Figure 21. Online Activity Ration Results on Nov 20-23, 2015.

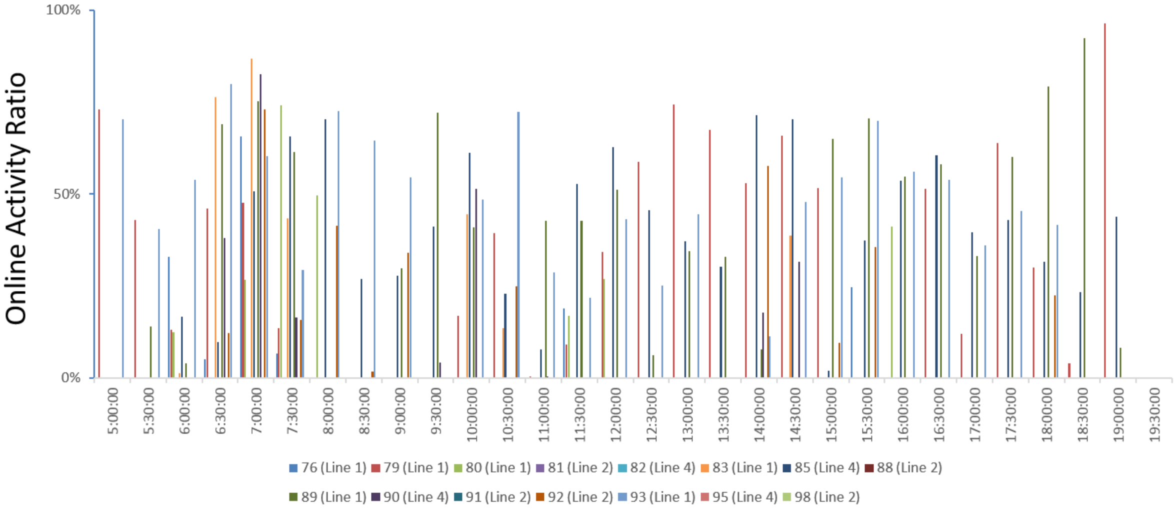


Figure 22. Online Activity Ration Results on Nov 24, 2015.

Packet Delivery Ratio

Packet Delivery Ratio demonstrate in Fig. 23. At beginning period of graph, Packet Delivery Ratio is lower than 50% because we did not deploy the device boxes completely as deployment phase. Obviously, the ratio was rising up when we deployed more testing devices. However, packet delivery ratio was going down dramatically between 11/17/15 and 11/23/15. This is because some device boxes stopped working. The cause of problem is the bus engine had distributed AC power and the unexpected issue made our power system of device boxes to explode. This took a long time for finding the cause of problem. After the problem was fixed and we redeployed our testing devices again the ratio had risen up to 83.93%.

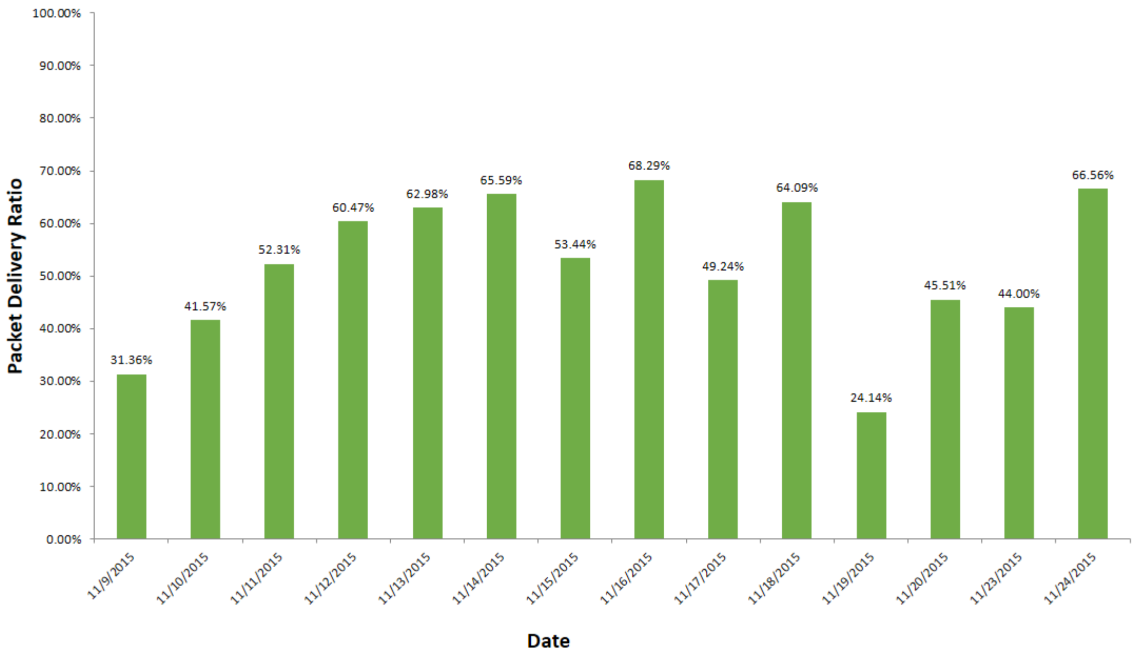


Figure 23. Packet Delivery Ratio of All Buses.

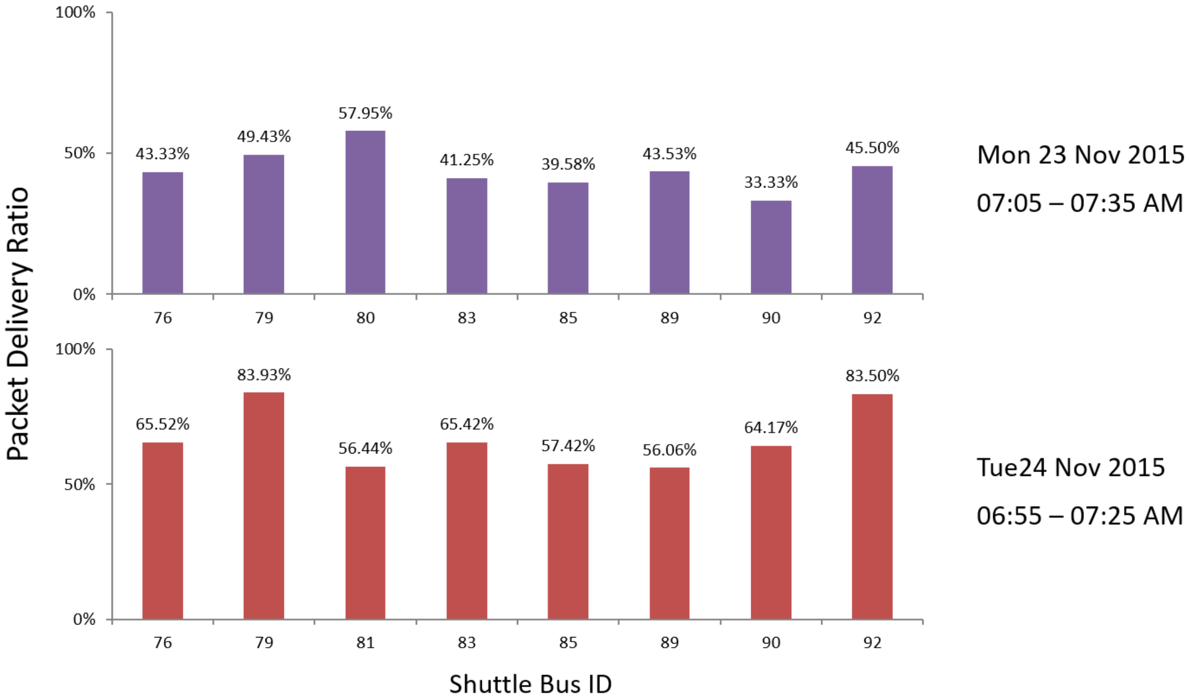


Figure 24. Packet Delivery Ratio of Each Bus.

Transmission Delay

Transmission delay is an average time that buses had begun to send their message within one-hop bus neighbor until the message were broadcasted by trigger events. This metric was affected by restricted resources such as limited number of available 802.11p devices, and a few bus lines was selected for testing), so most of delay are from traveling time when there is no bus in the area, a source or received buses have to wait to encounter a new bus. This additional delay will significantly decrease if there are enough buses that equip the communication devices to cover most of areas. However, the result shows the reasonable trend of number of rebroadcast events grew up within a linear function.

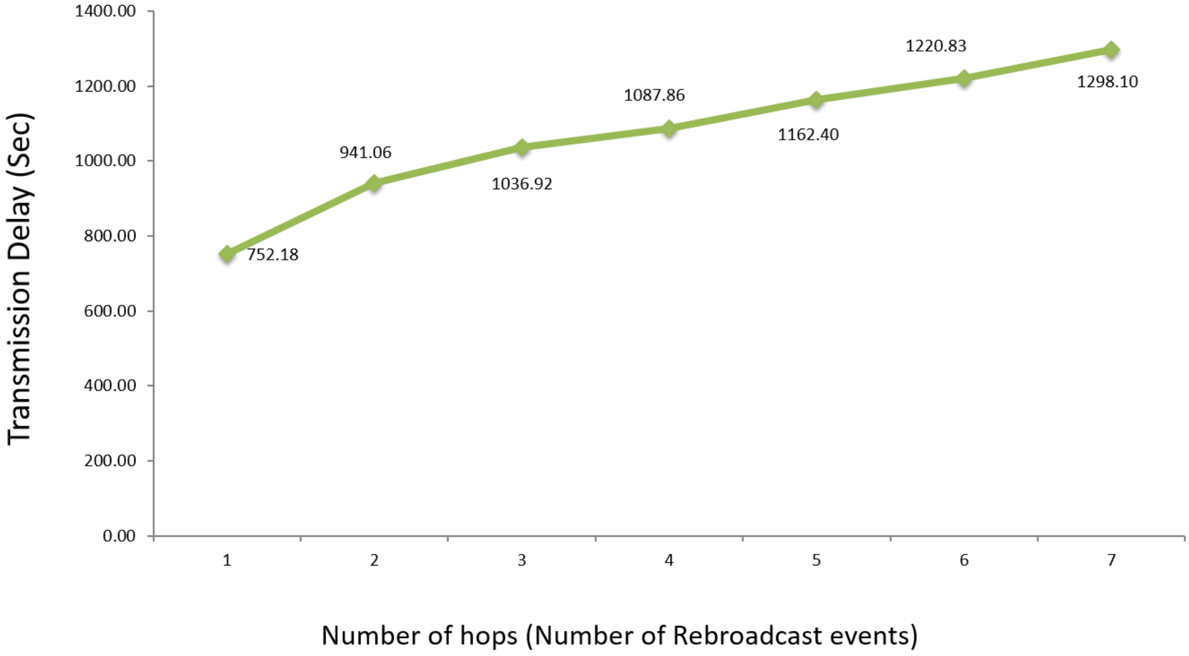


Figure 25. Transmission Delay.

Conclusion

This research aim to study the performance of IEEE802.11p standards on public transport networks and also to integrate vehicular-to-vehicular, vehicular-to-infrastructure and vehicular-to-pedestrian communication within one system. We implemented the application program interfaces to link each type of communication so any data are exchanged between vehicles using IEEE 802.11p. Our testing system consists of 15 shuttle buses and 2 base stations. To study the performance of testing system, the equipped buses will generate a message every minute and try to disseminate this message within 30 minutes. The results show that more than 50% of message are delivered to all of buses and the maximum delivery ratio is upto 83.93%. After we investigate in detail, we found that most of lost data are from disconnected problems which can be happen from two major reasons. The first one is the testing buses use electrical engine so when the buses even temporary stop at bus stops, drivers will shut the engine down. Then there is no power for testing devices and this vehicle will miss the important data from data. Therefore, we suggest that the public transport should have the separated power source to avoid intermittent connection and avoid missing important data from other vehicles. The second reason is due to limited number of devices, from the fact that every testing buses does not operate at the same time. Thus, the number of online buses is quite low which lead to disconnected network. A bus that acted as source node need to carry its message for a while to meet a new bus that never received the data. This also affect to the additional delay from traveling time. In order to handle this issue, the number of buses that installed the communication device should be increased. On the other hand, base station would be necessary to cover most of area in the beginning phase of using this technology in real environment. However, our system can communicate across devices and platform as design.

According to the mentioned issue, studying the performance of vehicular network in sparse area with help from base station is interesting topic because in the beginning of connected vehicle system, the number of vehicles that have capability to connect to others would be low. Our future work is to study a solution that can minimum number of base stations while significantly improve the performance of network. Another further study is to analyse data from sensors that are integrated with our testing devices in various points such as network quality, driver’s behavior or traffic condition.

References

[1] M. Conti and S. Giordano, “Multihop ad hoc networking: The reality,” IEEE Commun. Mag., vol.45, no.4, pp.88–95, April 2007.

[2] IEEE Standard for Information technology-- 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 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009) , vol., no., pp.1,51, July 15 2010.

[3] Cardote, A.; Neves, F.; Sargento, S.; Steenkiste, P., "A statistical channel model for realistic simulation in VANET," Vehicular Networking Conference (VNC), 2012 IEEE, vol., no., pp.48,55, 14-16 Nov. 2012.

[4] Ameixieira, C.; Matos, J.; Moreira, R.; Cardote, A.; Oliveira, A.; Sargento, S., "An IEEE 802.11p/WAVE implementation with synchronous channel switching for seamless dual-channel access (poster)," Vehicular Networking Conference (VNC), 2011 IEEE , vol., no., pp.214,221, 14-16 Nov. 2011.

[5] Fernandez, J.A.; Borries, K.; Lin Cheng; Kumar, B.V.K.V.; Stancil, D.D.; Fan Bai, "Performance of the 802.11p Physical Layer in Vehicle-to-Vehicle Environments," Vehicular Technology, IEEE Transactions on , vol.61, no.1, pp.3,14, Jan. 2012.

[6] Gozalvez, J.; Sepulcre, M.; Bauza, R., "IEEE 802.11p vehicle to infrastructure communications in urban environments," Communications Magazine, IEEE, vol.50, no.5, pp.176,183, May 2012.

[7] Toutouh, J. and Alba, E., “Performance analysis of optimized VANET protocols in real world tests,” in Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International, 2011, pp. 1244–1249.

[8] Sukuvaara, T.; Ylitalo, R. and Katz, M. “IEEE 802.11p Based Vehicular Networking Operational Pilot Field Measurement,” IEEE Journal on Selected Areas in Communications, vol. 31, no. 9, pp. 409–417, Sep. 2013.

[9] Kumar, V.; Mishra, S. and Chand, N. “Applications of VANETs: Present and Future,” Communications and Network, vol. 05, no. 01, pp. 12–15, 2013.

[10] Mangel, T.; Michl, M.; Klemp, O. and Hartenstein, H., “Real-World Measurements of Non-Line-Of-Sight Reception Quality for 5.9GHz IEEE 802.11p at Intersections,” in Communication Technologies for Vehicles, Eds. Springer Berlin Heidelberg, 2011, pp. 189–202.

[11] Giordano, E.; Frank, R.; Pau, G. and Gerla, M., “CORNER: a realistic urban propagation model for VANET,” in 2010 Seventh International Conference on Wireless On-demand Network Systems and Services (WONS), 2010, pp. 57–60.

[12] Biddlestone, S.; Redmill, K.; Miucic, R.; Ozguner, U., "An Integrated 802.11p WAVE DSRC and Vehicle Traffic Simulator With Experimentally Validated Urban (LOS and NLOS)

Propagation Models," Intelligent Transportation Systems, IEEE Transactions on , vol.13, no.4, pp.1792,1802, Dec. 2012.

[13] Sen, I.; Matolak, D.W., "Vehicle–Vehicle Channel Models for the 5-GHz Band," Intelligent Transportation Systems, IEEE Transactions on, vol.9, no.2, pp.235, 245, June 2008.

[14] Na Nakorn, K. and Rojviboonchai, K. “DECA-bewa: Density-aware reliable broadcasting protocol in VANETs,” (2013) IEICE Transactions on Communications, E96-B (5), pp. 1112-1121.

[15] IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services," IEEE Std 1609.3-2010 (Revision of IEEE Std 1609.3-2007), vol., no., pp.1, 144, Dec. 30 2010.

[16] IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation," IEEE Std 1609.4-2010 (Revision of IEEE Std 1609.4-2006), vol., no., pp.1, 89, Feb. 7 2011.

Appendix A: Log Extraction

Our log from testing system is illustrated in Fig. A1 and Fig. A2. There are 8 types of entry in our log system. Each type of entry has own meaning which described as follows:

```
23-10-0115 04:31:02.551 RecvBeacon 13.736445 100.524953 192.168.2.93::7 1 -32
23-10-0115 04:31:02.972 RecvSensor 13.736493 100.524948 -715,-86,-24,1344,-644,-16676,-2.20443003343,-4.60436889346,791,2760,46.8,26,6,2.999
23-10-0115 04:31:03.192 SendBeacon 13.736493 100.524948 192.168.2.85::53 1
23-10-0115 04:31:03.598 RecvBeacon 13.736445 100.524953 192.168.2.93::8 1 -33
23-10-0115 04:31:03.611 RecvSensor 13.736493 100.524948 -658,-138,253,696,-480,-18192,-1.51030690374,-2.19022479016,791,2769,46.8,26,0,2.999
23-10-0115 04:31:04.242 SendBeacon 13.736493 100.524948 192.168.2.85::54 1
23-10-0115 04:31:04.250 RecvSensor 13.736493 100.524948 -689,-113,-15,980,456,-18244,1.42972198234,-3.07380349932,792,2764,46.8,26,1,2.9.999
23-10-0115 04:31:04.694 RecvBeacon 13.736445 100.524953 192.168.2.93::9 1 -33
23-10-0115 04:31:04.892 RecvSensor 13.736493 100.524948 -682,-174,7,1296,-560,-17804,-1.79681388245,-4.16131660641,791,2760,46.8,26,2,2.9999
23-10-0115 04:31:05.304 SendBeacon 13.736493 100.524948 192.168.2.85::55 1
23-10-0115 04:31:05.531 RecvSensor 13.736493 100.524948 -679,-179,4,368,-452,-17652,-1.46648607072,-1.19390930356,791,2755,46.8,26,2,2.99999
23-10-0115 04:31:05.758 RecvBeacon 13.736445 100.524953 192.168.2.93::10 1 -33
23-10-0115 04:31:05.173 RecvSensor 13.736493 100.524948 -703,228,4,1452,1088,-17128,3.62168739436,-4.83587636264,791,2764,46.8,26,3,2.999999
23-10-0115 04:31:06.360 SendBeacon 13.736493 100.524948 192.168.2.85::56 1
23-10-0115 04:31:06.806 RecvBeacon 13.736445 100.524953 192.168.2.93::11 1 -33
23-10-0115 04:31:06.814 RecvSensor 13.736493 100.524948 -776,-119,254,1700,1412,-16532,4.85630654515,-5.84998869085,791,2760,46.8,26,4,2.999
23-10-0115 04:31:07.438 SendBeacon 13.736493 100.524948 192.168.2.85::57 1
23-10-0115 04:31:07.455 RecvSensor 13.736493 100.524948 -705,-116,2,916,-60,-17740,-0.193526499044,-2.95580985116,791,2760,46.8,26,1,2.9.999
23-10-0115 04:31:07.878 RecvBeacon 13.736445 100.524953 192.168.2.93::12 1 -33
23-10-0115 04:31:07.094 RecvSensor 13.736493 100.524948 -697,-120,13,756,-476,-18416,-1.47935405433,-2.34996006579,791,2760,46.8,26,0,2.9999
23-10-0115 04:31:08.500 SendBeacon 13.736493 100.524948 192.168.2.85::58 1
23-10-0115 04:31:08.735 RecvSensor 13.736493 100.524948 -728,-72,1,1140,520,-17056,1.7423963667,-3.82211433238,790,2755,46.8,26,0,2.9,2.9999
23-10-0115 04:31:08.935 RecvBeacon 13.736445 100.524953 192.168.2.93::13 1 -32
23-10-0115 04:31:08.376 RecvSensor 13.736493 100.524948 -758,-104,251,1028,332,-17620,1.07762016649,-3.33841943799,791,2760,46.9,26,0,2.9999
23-10-0115 04:31:09.552 SendBeacon 13.736493 100.524948 192.168.2.85::59 1
23-10-0115 04:31:09.927 SendData 13.736493 100.524948 192.168.2.85::60 192.168.2.93
23-10-0115 04:31:09.017 RecvSensor 13.736493 100.524948 -732,-121,8,1016,832,-17804,2.6712071387,-3.26253611257,790,2760,46.9,26,0,2.92.9999
23-10-0115 04:31:09.083 RecvData 13.736445 100.524953 192.168.2.85::60 192.168.2.85
23-10-0115 04:31:10.086 RebcData 13.736493 100.524948 192.168.2.85::60 192.168.2.93
23-10-0115 04:31:10.225 RecvData 13.736445 100.524953 192.168.2.85::60 192.168.2.85
23-10-0115 04:31:10.652 SendBeacon 13.736493 100.524948 192.168.2.85::61 1
23-10-0115 04:31:10.656 RecvSensor 13.736493 100.524948 -679,-87,42,448,-48,-17940,-0.153251601977,-1.43049518999,791,2764,46.9,26,1,2.99999
23-10-0115 04:31:10.106 RecvBeacon 13.736445 100.524953 192.168.2.93::15 1 -33
23-10-0115 04:31:10.297 RecvSensor 13.736493 100.524948 -710,-50,9,616,396,-17456,1.29875863795,-2.02053697906,790,2760,46.9,26,1,2.92.99999
23-10-0115 04:31:11.700 SendBeacon 13.736493 100.524948 192.168.2.85::62 1
23-10-0115 04:31:11.939 RecvSensor 13.736493 100.524948 -687,-96,17,268,412,-18420,1.28118506783,-0.83335216184,791,2764,46.9,26,0,2.9.99999
23-10-0115 04:31:11.168 RecvBeacon 13.736445 100.524953 192.168.2.93::16 1 -33
23-10-0115 04:31:11.579 RecvSensor 13.736493 100.524948 -724,-76,3,940,-260,-16436,-0.904804272027,-3.27285905114,792,2764,46.9,26,0,2.99999
23-10-0115 04:31:12.753 SendBeacon 13.736493 100.524948 192.168.2.85::63 1
23-10-0115 04:31:12.221 RecvSensor 13.736493 100.524948 -774,-197,-251,340,-256,-16700,-0.878055842652,-1.16620279232,792,2769,46.9,26,0,2.9
23-10-0115 04:31:12.236 RecvBeacon 13.736445 100.524953 192.168.2.93::17 1 -33
23-10-0115 04:31:13.804 SendBeacon 13.736493 100.524948 192.168.2.85::64 1
23-10-0115 04:31:13.860 RecvSensor 13.736493 100.524948 -755,-123,9,1180,-244,-17072,-0.816890208869,-3.95353736693,792,2764,46.9,26,0,2.9.9
23-10-0115 04:31:13.319 RecvBeacon 13.736445 100.524953 192.168.2.93::18 1 -33
23-10-0115 04:31:13.502 RecvSensor 13.736493 100.524948 -679,-50,-13,800,468,-18124,1.47773122073,-2.52657499741,791,2760,46.9,26,0,2.92.9.9
23-10-0115 04:31:14.857 SendBeacon 13.736493 100.524948 192.168.2.85::65 1
23-10-0115 04:31:14.142 RecvSensor 13.736493 100.524948 -680,-166,11,812,636,-18588,1.95778063248,-2.49986310109,791,2760,46.9,26,0,2.92.9.9
23-10-0115 04:31:14.384 RecvBeacon 13.736445 100.524953 192.168.2.93::19 1 -32
23-10-0115 04:31:14.783 RecvSensor 13.736493 100.524948 -689,-129,3,-52,-468,-17268,-1.55245198692,0.172473820002,791,2764,46.9,26,1,2.9.9.9
```

Figure A-1. An example of Log File from Testing System.

Send Data

Timestamp	Flag	Latitude	Longitude	Source IP	Seq #	Selected IP
7:05:18 AM	SendData	13.735795	100.531882	192.168.2.85	735	192.168.2.83

Receive Data

Timestamp	Flag	Latitude	Longitude	Source IP	Seq #
7:05:18 AM	RecvData	13.735795	100.531882	192.168.2.76	735

Rebroadcast Data

Timestamp	Flag	Latitude	Longitude	Source IP	Seq #	Selected IP
7:05:19 AM	RebcData	13.73504	100.531815	192.168.2.83	735	192.168.2.76

Figure A-2. Log Type Format

1. SendBeacon

SendBeacon entry means to exchange the local density information with 1-hop neighbors. It is periodically broadcasted to every node. The beacon is sent every one second. Each field in *SendBeacon* message format is described as follows:

- Date and time
- Message type
- Latitude and longitude
- Source IP address
- Sequence number
- A number of neighbors

2. RecvBeacon

RecvBeacon entry shows that the receiver is received the beacon from 1-hop neighbors. After that, the receiver adds or updates the sender IP address into the neighbor list as 1-hop neighbor. *RecvBeacon* entry format contains elements similarly as *SendBeacon*.

- Date and time
- Message type
- Latitude and longitude
- Source IP address
- Sequence number
- A number of neighbors
- RSSI

3. SendData

In fact, each device can send the specific messages depend on the application. It can be a message from a user or traffic information from base station or other devices. In our experiment, we use a 512-byte message as the data message. There are 5 fields in the *SendData* entry:

- Date and time
- Message type
- Latitude and longitude
- Source IP address
- Sequence number
- Selected IP address

4. RecvData

When a message reaches a destination node, the destination node write *RecvData* entry into the log file. It contains all information as same as *SendData* entry but it stores in different node.

- Date and time
- Message type
- Latitude and longitude
- Source IP address
- Sequence number
- Destination IP address

5. RecvSensor

In our experiment, we have collected the buses information with embedded sensors. There are 6 sensors: gyro meter, accelerometer, light sensors, infrared light sensor, temperature sensor, and humidity sensor. Every node has to write the sensor information into the log file when it receive sensor data from Raspberry Pi.

- Date and time
- Message type
- Latitude and longitude
- Tri-axial gyroscope data
- Tri-axial accelerometer data
- Two-axial rotation data
- Light and infrared light
- Temperature
- Humidity

6. RebcSNData

The node that has the highest neighbor density is selected by the sender node to be a selected node. It will rebroadcast the data immediately to other nodes after received the data from the sender node. The RebcSNData is written into log file after the data has been rebroadcasted.

- Date and time
- Message type
- Latitude and longitude
- Source IP address
- Sequence number
- Selected IP address

7. RebcWTData

After the sender selects the node that has the highest neighbor density as the selected node to rebroadcast data, other node which is not selected by sender have to set timeout interval for rebroadcasting data if they do not receive data from the selected node within the timeout period. Then, the RebcWTData entry is written into the log file.

- Date and time
- Message type
- Latitude and longitude
- Source IP address
- Sequence number
- Selected IP address

8. neighborMisses

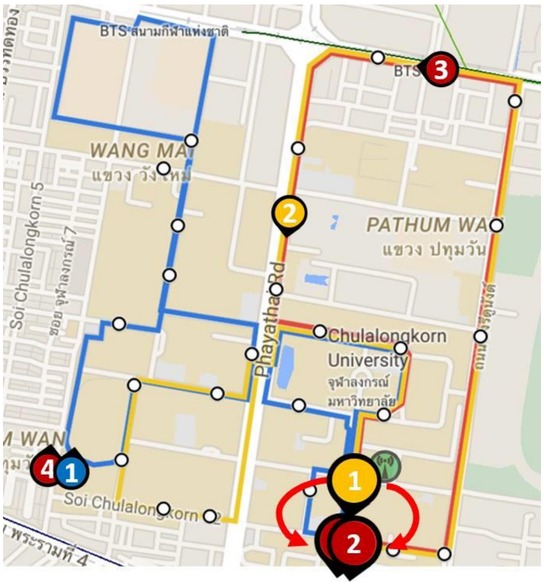
When there is a new node meet other nodes by broadcasting the beacon message. The node which receives the beacon message will check the list of message that the neighbor node has with its list. If there are some missing messages, the received node writes the neighborMisses entry into the log file. Then, the waiting timeout interval has been set. If it do not get the data from other nodes before the waiting timeout interval is expired, it will rebroadcast the data to the new node.

- Data and time
- Message type
- Source IP address
- IP address of source data
- Sequence Number of missing data

Appendix B: Data Traveling

In this section shows how the data is transmitted from the source node to the other nodes. We used the real mobility trace from our experiment to explain in this section which consisted of eight nodes with three different bus lines. All of the bus lines are represented with three colors are yellow, red, and blue.

As starting point view of data dissemination as shown in Fig. B-1, *Yellow-1* was a given source node. The node generated a data packet including a unique sequence number with 735 in this case. After that data packet was broadcasted to all 1-hop neighbors: *Red-1*, and *Red-2*. The right hand of figure demonstrates some related entries from log files. More details of each entry were described at Appendix A.



At 07:05 AM

7:05:18 AM SendData 13.735795 100.531882 192.168.2.85 735 192.168.2.83
7:05:18 AM RecvData 13.735795 100.531882 192.168.2.76 735
7:05:18 AM RecvData 13.735795 100.531882 192.168.2.83 735
7:05:19 AM RebcData 13.73504 100.531815 192.168.2.83 735 192.168.2.76
7:05:19 AM RecvData 13.735013 100.531803 192.168.2.85 735
7:05:19 AM RecvData 13.735795 100.531882 192.168.2.76 735

Figure B-1. Source Sent A Message Scenario.

Five minutes later as shown in Fig. B-2, after *Yellow-1* moved to a new area and discovered *Red-3* by the beacon mechanism. It rebroadcasted the data message to *Red-3* because *Red-3* had not received the data and the data had not expired yet. *Red-1* also had the same scenario as *Yellow-1*, *Red-1* received the beacon message from *Yellow-2* and then had to rebroadcast data to *Yellow-2*.

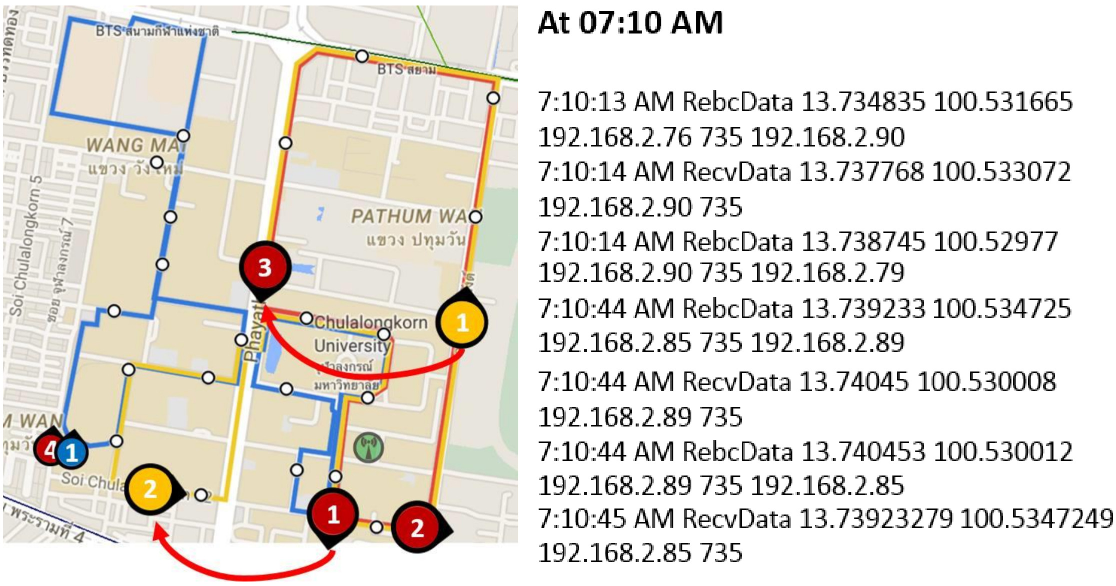


Figure B-2. Missing Message of Red-3 and Yellow-2 Scenario.

Next, *Yellow-1* had reached the first round and met the new active node which is *Blue-2*. Because the data timeout period was still counting down and *Yellow-1* received the beacon message from *Blue-2*, it found that *Blue-2* had missing data. It set the data timeout interval and waited until it was expired before rebroadcasted the missing data message to *Blue-2*. *Yellow-2* received the beacon message from *Blue-1* and found the same scenario as *Yellow-1*. *Yellow-2* randomized waiting timeout for rebroadcasting data to *Blue-1* because it found that *Blue-1* had missing data. The data message was not rebroadcasted until the waiting timeout expired or received the data message from other nodes. Next, *Blue-1* received the data message and there was *Red-5* in the neighbor list so it had to rebroadcast the data message to *Red-5*. Finally, *Red-5* did the same thing of *Blue-1* as shown in Fig. B-3.

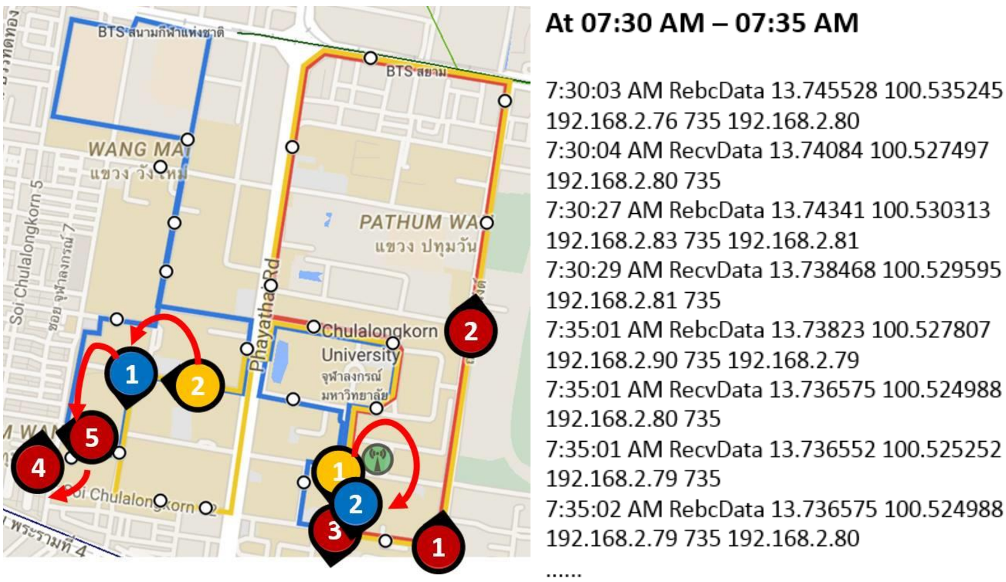


Figure B-3. Missing Message Chain Recovery Scenario.

Final Report
Research Grant 2015

ATRANS