Evaluation of WiFi Access Point Switching for Vehicular Communication Using SDN

Kaito Iwatsuki
Computer and Information Science
Graduate School of
Science and Engineering
Doshisha University
Kyoto, Japan
email:kaito.iwatsuki@nislab.doshisha.ac.jp

Nishiki Hase
Computer and Information Science
Graduate School of
Science and Engineering
Doshisha University
Kyoto, Japan
email:nishiki.hase@nislab.doshisha.ac.jp

Kenya Sato
Computer and Information Science
Graduate School of
Science and Engineering
Doshisha University
Kyoto, Japan
email:ksato@mail.doshisha.ac.jp

***Abstract*—The amount of data required by various applications continues to increase due to improved high function terminals. We expect that using Long Term Evolution (LTE) networks will also grow in the future. Networks might become very crowded depending on the places and the times at which people congregate. To reduce network congestion, carriers are offloading LTE network traffic to WiFi systems. Because the frequency resources of LTE networks are limited, movements that utilize them will increase in the future. When a mobile terminal communicates using a communication system with a narrow coverage area, such as WiFi, the frequency of switching the Access Point (AP) increases compared to using Cellular Networks. Since AP switching frequently occurs, network connections must be made more quickly. Here, the communication disconnection time denotes an efficient switching. Therefore, in this research, we select an AP for connections based on position and speed, both of which are unique to mobile terminals, and utilize the concept of a Software Defined Network (SDN). We propose a method that enables efficient network connections by executing an AP procedure that is connected before the communication is disconnected.**

Keywords–vehicular communication; Wi-Fi; SDN.

I. INTRODUCTION

In recent years, communication is often done through many mobile terminals including smartphones. Such Cellular Networks as LTE are mainly used for these mobile units. Since Cellular Networks are becoming congested by an increase in the number of mobile terminals, such applications require more data. To reduce the congestion of Cellular Networks, each carrier is offloading its cellular network traffic to unlicensed bands, such as WiFi systems. In fact, according to a Cisco survey, 58% of vehicular communication is offloaded traffic [1], which is expected to continue to rise in the future. Therefore, the importance of WiFi systems for vehicular communication will also increase in the future. We also expect to utilize WiFi systems in communication even in such fields as automobiles. However, as mentioned above, when a WiFi system is used for vehicular communication, a new problem arises: the time during which communication cannot be performed becomes longer than with a cellular system when the Access Point (AP) of the WiFi system is switched for a connection with a mobile terminal. Compared to cellular systems, existing WiFi system have a smaller coverage area that includes just one AP, and the APs belonging to a plurality of different networks cooperatively lack a function for assisting the AP's terminal switch, for example. In other words, vehicular communication using WiFi has a higher disconnection frequency and a longer disconnection time than cellular systems. When vehicular communication is done using a WiFi system with a narrow AP coverage area, if such connection procedures as authentication take too much time, the mobile terminal leaves the coverage area before the authentication is completed. Therefore, in this research, we shortened the disconnection time of communication during AP switching. Among AP-switching operations when connecting to the AP, selecting the destination of the AP being switched and the authentication operation occupy most of the entire switching operation. In this research, we use the SDN (Software Defined Network) concept [2][3] on WiFi networks to shorten these two disconnection times to solve the problem of using WiFi systems in vehicular communication. The rest of the paper is organized as follows. Section Ⅱ overviews related works and problems of conventional method. In section Ⅲ, we describe the proposed method. Simulation results are provided in Section Ⅳ, and then Section Ⅴ concludes the paper.

II. RELATED WORK

In this section, we describe the technologies that are related to WiFi vehicular communication, as well as current research on AP switching that occurs when using them.

A. Problems with current WiFi switching

When a mobile terminal communicates with a WiFi system, it must switch to the next AP as it leaves the area covered by each WiFi's AP. To switch to an AP, it must be disconnected from the system before it is connected to a new one. Then, a probe request is sent to the AP, as well as an authentication procedure.

B. Disconnection from a Connected AP

When the mobile terminal cannot receive a beacon signal that is transmitted every 100 ms by the WiFi's AP, it recognizes that communication with the AP has been disconnected and starts to scan for another AP. The allowable time when this beacon signal cannot be received varies by vendor and mounting method.

Copyright (c) IARIA, 2018. ISBN: 978-1-61208-643-9

C. Disconnection from a Connected AP

AP information of WiFi, passive, and active scans.

- Passive scan
  The mobile terminal waits to receive a beacon signal from the AP to obtain its information.
- Active scan
  The mobile terminal transmits probe request information to the AP. Upon receiving this it, the AP describes its own information in the probe response and transmits it.

In either method, when switching the AP, we must disconnect from the AP to which we are currently connected and authenticate the next AP. Therefore, communication is disconnected until the authentication processing is completed. Another problem is that no communication can be performed when the mobile terminal leaves the coverage area without completing the authentication process within the coverage area. Although several methods have achieved the same purpose as our research, we just list two related researches. The first strengthens the cooperation between APs [4]. In this method, the network AP provides information on other APs, as well as itself, and the mobile terminal recognizes them in advance, shortening the disconnection time when this new AP is connected. With this method, only information on the AP in the LAN (to which it is connected) can be obtained. Therefore, this method cannot be applied when a mobile terminal switches APs that belong to different networks. The second method scans the AP while communicating with the connected AP and selects the AP's next destination to which it will be switched [5][6]. In this method, unfortunately, an AP, which is not yet in the communication range of the movement destination, cannot be considered a switching candidate because of a feature that scans the AP within its own communication range beforehand.

III. PROPOSAL

In this section, we propose a method to improve the efficiency of connection to the WiFi network.

A. Outline

In the proposed method, a mobile terminal selects the destination of the AP being switched in advance and executes the authentication procedure necessary for the connection. This shortens the communication disconnection time that occurs at the AP-switching time. Before communication is disconnected, AP candidates are not scanned directly by the mobile system but are selected based on the information obtained from the server that holds the AP information. The following is the general operation flow. First, the mobile terminal selects the next AP to be connected based on its own position and speed. Then, the mobile terminal requests the controller to perform the authentication process necessary for the next connection. In this way, our proposed method reduces the disconnection time during switching.

B. Precondition

In the implementation environment of this research, we assume that all the APs are compatible with SDN and that the AP, which is managed by the controller and such processes as authentication, can be performed based on instructions from the controller.

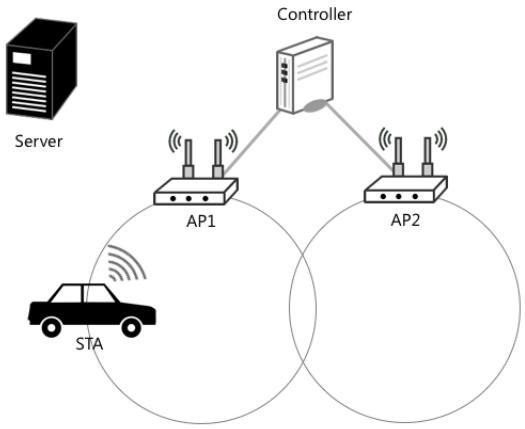

Figure 1. Component

C. Configuration

The configuration of our proposed method is shown in Figure 1.

- Mobile terminal (STA)
  The STA performs vehicular communication and obtains its own position information from GPS.
- Controller (controller)
  This controller is compatible with SDN and manages the APs in the network. When receiving an authentication request from an AP, it instructs the corresponding AP to perform authentication.
- Access point (AP)
  The AP is compatible with SDN and executes the processing when it receives an authentication instruction from the controller.
- Server (Server)
  It holds the AP's location information as well as the information of the controller that is managing the AP. When it receives a request from the STA, it provides information on the AP based on STA's position information.

D. Operating Sequence

The operation of the proposed method is roughly divided into two phases: pre-authentication and switching. Next, we describe their procedures.

E. Pre-authentication Phase

The flow of the pre-authentication phase is shown in Figure 2 and Figure 3.

1) The STA gets its position information.

2) It acquires the AP information in the vicinity by the connected AP.

Copyright (c) IARIA, 2018. ISBN: 978-1-61208-643-9

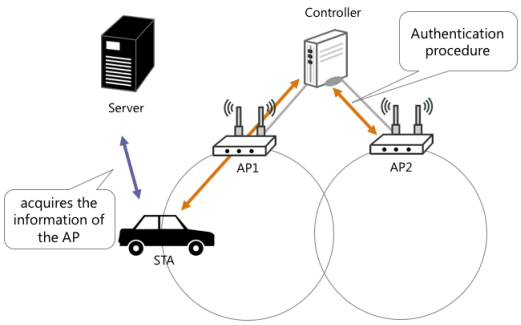

Figure 2. Acquires AP information

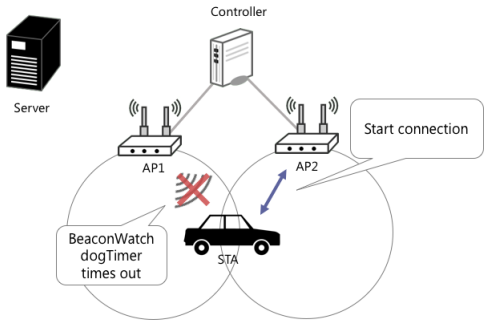

Figure 4. Switching phase

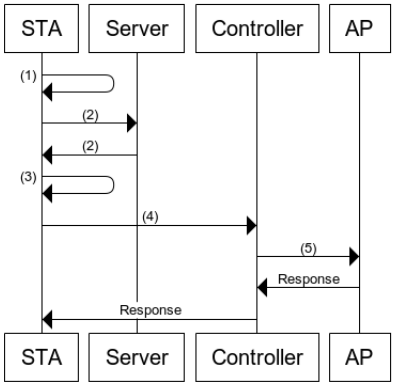

Figure 3. Sequence diagram of pre-authentication phase

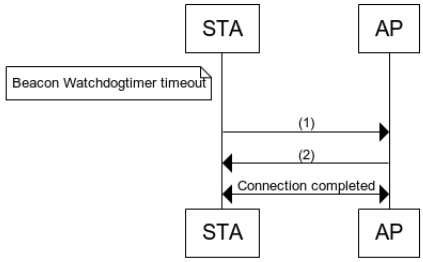

Figure 5. Sequence diagram of switching phase

3) From the server, it selects the next AP to be connected (the AP after switching) from its position and movement direction.

4) It requests controller authentication for the corresponding AP.

5) The controller sends an authentication instruction to the corresponding AP.

F. Switching Phase

The switching phase's flow is shown in Figure 4 and Figure 5. As a premise, the AP always distributes beacon signals to its surroundings.

1) The STA sends a probe request to the AP selected in the pre-authentication phase when the beacon signal times out the value specified by the Beacon Watchdog Timer. In the proposed method, its value is decreased only when the STA is fast, thereby shortening the communication disconnection time with the AP before switching.
2) After disconnection, the AP sends a probe response.
3) When the STA receives a probe response, it makes a connection by omitting an authentication because such an authentication procedure as a 4-way handshake (which are conventionally done) was carried out beforehand. Authentication procedures depend on the types of implementation. In this paper, we assume a four-way WPA2 handshake.

IV. EVALUATION AND CONSIDERATION

A. Simulator

In this research, we used NS(Network Simulator)3 [7], which is a network simulator to evaluate our proposed method's performance. The algorithm of the proposed method was implemented in the data link layer and the network layer of the network node on NS3.

B. Assumed Use Case

We used various cases that involved vehicular communication. We assumed a car as a mobile terminal. Several usage scenarios are conceivable even for automobile usage, and they are roughly classified into the following two types:

- On the highway
  When used on a highway, the moving speed is fast, and the vehicle density is generally low.
- On general roads
  When used on an ordinary road, the moving speed is slow, and the car density is higher than when used on a highway.

Based on the above items, we made the following assumptions. One is using a cellular network when communicating on a highway with low vehicle density. Second, we used the proposed method when communicating on an ordinary road with a relatively high vehicle density.

Copyright (c) IARIA, 2018. ISBN: 978-1-61208-643-9

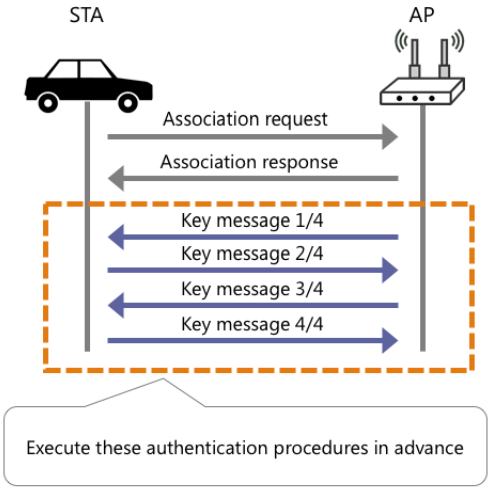

Figure 6. WPA2 key message exchange

C. Evaluation Environment

The evaluation environment is shown in Table I. Since NS3 does not have a default WiFi switching handoff function, we applied the ns3-wifi-infra-handoff patch and implemented the WiFi handoff function on NS3. We assume WPA2, which is currently the most secure authentication method, and exchange key messages among the procedures beforehand in the pre-authentication phase (Figure 6).

TABLE I. EVALUATION ENVIRONMENT

OS	Ubuntu 14.04
CPU	Intel core i7
Memory	8GB
Simulator	NS 3.22
Propagation delay model	ConstantSpeedPropagationDelayModel
Propagation loss model	LogDistancePropagationLossModel
Authentication method	WPA2

D. Evaluation Method

We modified the data link layer in the network node on NS 3 and virtually implemented our proposed method. The evaluation topology resembles that shown in Figure 7. The mobile terminal, which switches among a plurality of APs while moving. We measured it based on the disconnection time with the server that is communicating during the movement. The mobile terminal ' s speed is a constant 36 km/h, and the distance between each AP is 150 m. The disconnection time is the average of the time during which communication with the server (caused by one AP switching) cannot be performed. To measure the effect of each pre-authentication phase and switching phase, which are the two phases of the proposed method, we compared the results obtained by setting two different parameters.

1) Evaluation of Pre-authentication Phase: As described above, the evaluation criterion is the communication disconnection time during AP switching. We compared the evaluation results in the following two parameter settings.

- Conventional method
  In the conventional WiFi connection method, the Beacon Watchdog Timer uses the default value.
- Proposed method (only pre-authentication section implemented)
  The pre-authentication shown in the proposed method is done before switching, but the Beacon Watchdog Timer uses the default value. Only pre-authentication phase is implemented.

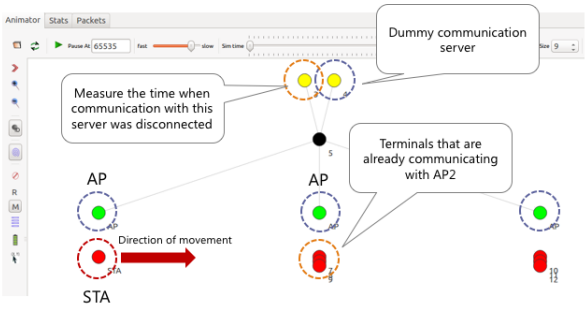

Figure 7. Evaluation topology

With these two comparisons, we measured the changes in the communication disconnection time due to the pre-authentication and its effect.

2) Evaluation of Switching Phase: The evaluation criteria are the same as the above pre-authentication phase, but we changed the parameters that were compared as follows and evaluated the switching phase:

- Proposed method (only pre-authentication section implemented)
  In the parameter settings, which were also used in the evaluation of the pre-authentication phase, we only implemented the pre-authentication part, and the Beacon Watchdog Timer uses the default value.
- Proposed method
  Evaluation when both of the two phases mentioned in the part of the proposed method are implemented.

We evaluated both above phases that were implemented with lowered disconnection times and measured the Beacon Watchdog Timer value and the switching phase effect. The topology in the actual simulator is shown in Figure 7. Apart from the elements described in the proposed section, we added terminals that have already been connected and are communicating with AP2. By adding this element, we created a more realistic environment and measured the changes in communication disconnection time by changing the numbers of this element.

E. Evaluation Result

Figure 8 shows the evaluation result of the pre-authentication phase, which is the transition of the disconnection time of the proposed and conventional methods. The x axis represents the number of terminals that are already connected, and the y axis represents the disconnection time. Both the conventional and proposed methods show that the disconnection time increases as the number of already connected

Copyright (c) IARIA, 2018. ISBN: 978-1-61208-643-9

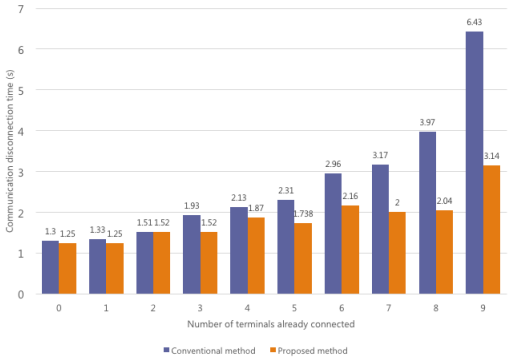

Figure 8. Evaluation result of pre-authentication phase

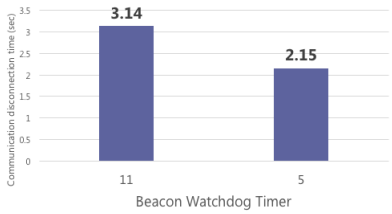

Figure 9. Evaluation result of switching phase

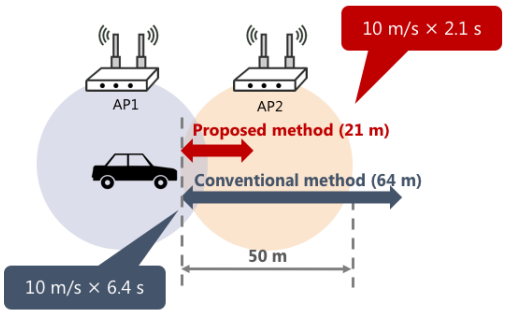

Figure 10. Distance required for authentication

terminals increases. The increase in these disconnection times is probably affected by CSMA/CA, which was used in the WiFi system. Both methods show that the disconnection time increases in proportion to the increase of the number of already connected terminals, but the increase in the disconnection time of the proposed method is more gradual than the proposed method. Figure 9 shows the evaluation result of the switching phase. The number of already connected terminals is nine. In this case, STA had the longest cutting time when evaluating the pre-authentication phase. We compared the communication disconnection time when the Beacon Watchdog Timer value has a default value of 11 and the shortened value is 5. In this experiment, the AP transmits a beacon signal at a cycle of 100 ms, and the Beacon Watchdog Timer times out when it cannot receive a specified number of beacons.

F. Consideration of Evaluation Result of Pre-authentication Phase

As seen in Figure 8, which is the evaluation result of the pre-authentication phase, the disconnection time increases in both the conventional and proposed methods as the number of already connected terminals increases. However, when the number of already connected terminals is two or more, the communication disconnection time of the proposed method is lower than the conventional method. This is probably due to the reduction of the procedure that is done at the connection time by carrying out the necessary authentication procedure. In addition, as the number of already connected terminals increases, the difference in the disconnection time between the proposed and conventional methods increases. This result shows that the maximum bottleneck in the authentication process is the waiting time of the CSMA/CA that is generated when the authentication frame is transmitted. When the number of already connected terminals increases, their communication might collide with each other, so CSMA/CA ' s back-off time increases. Since CSMA/CA collisions depend on timing, the evaluation result varies. As an example, the disconnection time with five terminals already connected is shorter than the disconnection time when the number of already connected terminals is four in the proposed method.

G. Consideration of Evaluation Result of Switching Phase

As seen from Figure 9, which is the evaluation result of the switching phase, the communication disconnection time can be shortened by reducing the Beacon Watchdog Timer value. This result is influenced by quickly disconnecting the connection with the AP that became unable to communicate and switching to the next AP. When carrying out vehicular communication, if the mobile system intends to maintain the AP connection for a long time and if the AP is actually already out of communicable range, it may lengthen the disconnection time. Our proposed method prevented this by lowering the Beacon Watchdog Timer value. However, decisive overhead exists in a technique that shortens this Beacon Watchdog Timer. If the radio waves temporarily deteriorate when the terminal is not moving, a mistaken disconnection will occur. In this research, we reduced this overhead by only shortening the Beacon Watchdog Timer when the mobile system has enough speed for this overhead.

H. Consideration of Authentication Failure

Even in the related research section, the problem is that authentication fails because the mobile terminal leaves the AP' s coverage area before the authentication process is completed, and so communication cannot be achieved. Regarding this problem, as shown in Figure 10 from the results of the pre-authentication and switching phases, the following idea can be addressed. Since the conventional method requires a maximum of 6.43 s for authentication, communication cannot be performed by exiting the coverage area before authentication is done in a general public WiFi coverage area of 50 m; authentication is completed while the proposed method can achieve a maximum of 2.15 s. That is, authentication has been completed within the coverage area and communication is achieved.

Copyright (c) IARIA, 2018. ISBN: 978-1-61208-643-9

I. Timing of Switching

This time the connected terminal spontaneously determined the switching timing led by the Beacon Watchdog Timer. However, even in such a cellular network as an LTE, the communication base station determines the time of the terminal switching. By introducing this method to our proposed method, the superiority of the controller's centralized management by SDN may be improved.

V. CONCLUSION

In recent years, research movements to use WiFi systems for vehicular communication have been growing, and offloading traffic to the WiFi systems in mobile traffic will increase in the future. However, when using a WiFi system for vehicular communication, several problems arise. In this research, for the problem of mobile terminal communication that uses WiFi systems, we examined the communication disconnection time that occurs when APs are switched. We solved this problem by switching APs based on the location speed of the mobile terminal. Our proposed method is roughly divided into two phases. First, in the preliminary authentication phase, we performed the necessary authentication processing before establishing a connection with SDN technology. The second phase shortened the Beacon Watchdog Timer in the switching phase and switched the AP. Based on the evaluation results of both phases, we shortened the communication disconnection time by making switching more efficient. We also solved erroneous disconnections, which are the overhead considered in the switching phase, based on the mobile terminal's speed. Communication can be achieved using the proposed method even for APs that leave the coverage area before authentication is completed by a conventional method.

ACKNOWLEDGMENT

This work was supported in part by JSPS KAKENHI Grant Number 16H02814.

REFERENCES

[1] "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 20152020", URL: https://www.cisco.com/c/dam/m/en_in/innovation/enterprise/assets/mobile-white-paper-c11-520862.pdf [accessed: 2017-10-10].

[2] D. Zhao, M. Zhu, and M. Xu, "SDWLAN: A flexible architecture of enterprise WLAN for client-unaware fast AP handoff", Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Hefei, 2014, pp. 1-6.

[3] M. Bernaschi, F. Cacace, and G. Iannello, "OpenCAPWAP,an open-source CAPWAP implementation for management and QoS support", 2008 4th International Telecommunication Networking Workshop on QoS in Multiservice IP Networks, Venice, 2008, pp. 72-77.

[4] S. Feirer and T. Sauter, "Seamless handover in industrial WLAN using IEEE 802.11k", 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE), Edinburgh, 2017, pp. 1234-1239.

[5] P. Macha and J. Wozniak, "A lightweight algorithm for fast IEEE 802.11 handover", Australasian Telecommunication Networks and Applications Conference (ATNAC) 2012, Brisbane, QLD, 2012, pp. 1-6.

[6] D. Lee, D. Won, and M. J. Piran, "Reducing handover delays for seamless multimedia service in IEEE 802.11 networks", in Electronics Letters, vol. 50, no. 15, pp. 1100-1102, July 17 2014.

[7] "ns-3", URL: https://www.nsnam.org/ [accessed: 2017-8-18].

Copyright (c) IARIA, 2018. ISBN: 978-1-61208-643-9