IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 26, 2021, accepted November 7, 2021, date of publication November 17, 2021, date of current version December 9, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3128974

Link Setup Time Reduction by FILS on IEEE 802.11-Based Inter-Vehicular Communications

ARATA KATO[1], (Student Member, IEEE), TAKA MAENO[2], YASUNORI OWADA[3], (Member, IEEE), GOSHI SATO[3], KATSUHIRO TEMMA[3], (Member, IEEE), TOSHIAKI KURI[3], (Senior Member, IEEE), MINEO TAKAI[4,5], (Member, IEEE), AND SUSUMU ISHIHARA[6,7], (Member, IEEE)

[1]Graduate School of Science and Technology, Shizuoka University, Shizuoka 422-8529, Japan
[2]Space-Time Engineering Japan Inc., Tokyo 101-0025, Japan
[3]National Institute of Information and Communications Technology, Tokyo 184-8795, Japan
[4]Graduate School of Information and Science, Osaka University, Osaka 565-0871, Japan
[5]Samueli School of Engineering, University of California, Los Angeles, Los Angeles, CA 90095, USA
[6]College of Engineering, Academic Institute, Shizuoka University, Shizuoka 422-8529, Japan
[7]Research Institute of Green Science and Technology, Shizuoka University, Shizuoka 422-8529, Japan

Corresponding author: Arata Kato (kato.arata.17@shizuoka.ac.jp)

This work was supported by Council for Science, Technology and Innovation (CSTI), Cross-ministerial Strategic Innovation Promotion Program (SIP) 2nd, ''Enhancement of National Resilience against Natural Disaster'' with funding from the National Research Institute for Earth Science and Disaster Resilience (NIED).

ABSTRACT This paper reports the performance of link setup time reduction outlined by IEEE 802.11ai, which is also known as Fast Initial Link Setup (FILS), in real intermittent inter-vehicular communications. Fast link establishment is a significant concern in communications between mobile devices with high mobility, such as passing vehicles on roads, because short link setup times enable vehicles to transfer larger amounts of application data. However, secure links are also important because they prevent both unauthorized access by unauthenticated users and misinformation circulation by malicious persons. Conventional security protocols such as IEEE 1609.2 and IEEE 802.11i/IEEE 802.1X, which is also known as the Wi-Fi Protected Access 2 Extensible Authentication Protocol (WPA2-EAP), archive user authentication in vehicular networks but often take several seconds to establish a secure link due to numerous frame exchanges. In contrast, FILS is designed to establish a secure WPA2-EAP link in 100 ms using cached authentication information. However, since the effectiveness of FILS in real vehicular networks has not yet been reported, this paper describes experiments that clarify its setup time reduction abilities in 2.4 GHz IEEE 802.11n-based inter-vehicular communications by measuring the initial link setup times between two passing vehicles in a real environment. The results show that FILS significantly reduces the initial link setup times between the passing vehicles to around 150 ms and increases the size of application data transferred between vehicles. Additionally, it is demonstrated that FILS always establishes a secure link, while Protected EAP (PEAP) sometimes fails. Finally, in communications between vehicles passing each other at the relative speed of 80 km/h, we confirm that the FILS link setup time reduction effectively increases transferrable application data sizes by 10 MB compared with WPA2-PEAP.

INDEX TERMS FILS, IEEE 802.11ai, inter-vehicular communications, vehicular delay/disruption tolerant network.

I. INTRODUCTION

Fast, secure link establishment can improve connectivity between highly mobile devices during inter-vehicular communications in vehicular delay/disruption tolerant networks (VDTN). Additionally, short link setup times reduce link establishment overhead and extend data transmission time. Secure links protect communications from tapping by unauthenticated users and misinformation circulation by malicious persons.

The advantages of fast, secure link establishment meet the requirements of VDTN-based disaster networks, which are robust to disasters because they can be performed using emergency vehicles with onboard units (OBUs) and physically carry application data to remote areas with relay transmission between vehicles if communication infrastructures are down

The associate editor coordinating the review of this manuscript and approving it for publication was Mohammad Ayoub Khan.

by natural disasters such as earthquakes and tsunamis. Furthermore, in VDTN-based disaster networks, fast, secure link establishment enables emergency vehicles to exchange sensitive information, such as victim medical data and images of disaster areas, which can help rescue teams understand the disaster scale quickly. In fact, the Asia Pacific Telecommunity (APT) recommends using vehicular delay/disruption tolerant networks as a means of communication during disaster in [1].

To facilitate these efforts, we are developing a VDTN-based disaster communications system that uses Wi-Fi and Digital Convenience Radio (DCR) [2], which is based on the Association of Radio Industries and Businesses (ARIB) STD-T98 standard covering one band of among Japan's narrow-band radio traffic. The communication range and bitrate of DCR devices are typically less than 10 km and 4.8 kbps, respectively. In our disaster communication system, emergency vehicles serve as DTN ferry nodes by transferring data among shelters and disaster control headquarters. In this network, the ad-hoc mode is not used. The vehicles have IEEE 802.11 access point function protected by WPA-EAP. When two vehicles pass each other, one vehicle behaves as a normal station (STA) and another behaves as an access point (AP). The STA vehicle connects to the AP vehicle and receives data stored in the AP vehicle, such as photos and videos of disaster-stricken areas.

Individual authentication is necessary to protect against unauthorized tapping and prevent the spread of misinformation in disaster networks because they often carry sensitive information such as personal medical records. Currently, the Wi-Fi Protected Access 2 Extensible Authentication Protocol (WPA2-EAP), which is also known as WPA2-Enterprise, is typically used for individual authentication on IEEE 802.11 systems, and it is also available in IEEE 802.11-based inter-vehicular communications. However, WPA2-EAP communications require a few seconds for link establishment because they must build Transport Layer Security (TLS) tunnels and exchange authentication information such as certificates and passphrases. These long link establishment times reduce the time available for application data transferred between passing vehicles and thus the amount of data that can be transferred.

To minimize this problem, our newly proposed system uses the IEEE 802.11ai protocol, which is also known as the Fast Initial Link Setup (FILS), to reduce link establishment time and increase the transfer size of application data in the VDTN-based disaster networks. In operation, FILS enables access points and station nodes to authenticate each other within about 100 ms by using cached authentication information. The link setup time is defined as a period between when a station sends an IEEE 802.11 probe request to an access point and when the station obtains its own IP address from a DHCP server. On the other hand, inter-vehicular communication environment has unidentified factors that can affect the field performance of FILS, such as vehicles' mobility and radio propagation, and measuring the FILS performance in real vehicular environment is crucially important to identify the FILS practical performance.

To clarify the effect of link setup time reduction by FILS in intermittent inter-vehicular communications, we performed both laboratory and field experiments, and we report the results of our experiments in this paper. The results of our measurements show that FILS reduces link setup time in intermittent inter-vehicular communications using 2.4 GHz IEEE 802.11n, which effectively increases the size of application data transmitted between passing vehicles by 10 MB compared with WPA2-PEAP. The IEEE 802.11ai was issued in 2017, and a few papers [6]–[8] have reported the FILS performance with mathematical models or network simulation. We will review related work on FILS performance evaluation in Section IV-E. However, to the best of our knowledge, no report to date has verified link setup time reduction via FILS in actual use, especially in vehicular networks.

As such, the present paper represents the first report of a performance evaluation of FILS in a real-world vehicular DTN. This paper extends our conference paper previously presented in [9] and shows the details of the results of a laboratory and field experiment we performed to measure the FILS performance in vehicular networks, which are not shown in [9].

The remainder of this paper is structured as follows. Section II of this paper describes the details of our newly developed disaster communication system, while Section III explores work related to the IEEE 802.11 authentication mechanisms. Section IV explains the mechanisms of WPA2-EAP and provides additional details regarding IEEE 802.11ai protocols. Section V presents experiments conducted to measure the FILS performance in 2.4 GHz IEEE 802.11n-based inter-vehicular communications, during which we show that FILS enables vehicles to establish secure links and increases transferrable application data amounts. Section VI show the results of the laboratory and field experiments. We conclude in Section VII with a brief summary and mention of future work.

II. DISASTER COMMUNICATION SYSTEM USING HETEROGENEOUS WIRELESS COMMUNICATIONS

This section describes the motivation, architecture, and technical requirements of our newly developed disaster communication system.

A. MOTIVATIONS TO DEVELOP THE DISASTER COMMUNICATION SYSTEM

The development of our new disaster communication system was motivated by the issues pertaining of disaster rescue operations in Japan, which currently face the following problems that can make rescue operations chaotic.

1) Misinformation and confusion stemming from transceiver-based oral communications
2) Dependency of communication systems on communication infrastructures

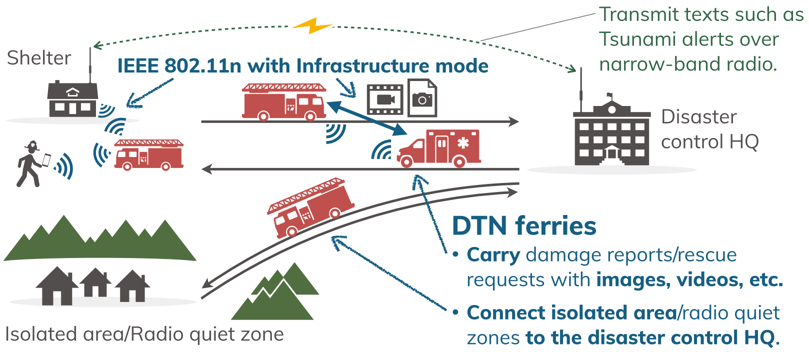

Shelter
IEEE 802.11n with Infrastructure mode
Transmit texts such as
Tsunami alerts over
narrow-band radio.
Disaster
control HQ
DTN ferries
• Carry damage reports/rescue
requests with images, videos, etc.
• Connect isolated area/radio quiet
zones to the disaster control HQ.
Isolated area/Radio quiet zone

FIGURE 1. Overview of our proposed disaster communication system.

1) MISCOMMUNICATION DUE TO TRANSCEIVER-BASED ORAL COMMUNICATIONS

Almost all Japanese local governments use public address system loudspeakers and voice transceivers for communication between residents and emergency personnel [10]. While voice messages are useful for communication between the personnel of disaster management agencies, they are insufficient for the personnel of disaster management agencies to understand the damage level of disaster-stricken areas correctly and minutely because they lack visual information such as the photos and videos of disaster-stricken areas. As the saying goes, ‘‘One picture is worth a thousand words,’’ and the one photo can give the personnel of more clear, non-contradictory about the disaster-stricken areas without a contradiction than voice messages. Because voice messages include talkers’ own expressions and impressions of the damage level of disaster-stricken regions, messages from different persons who see the same thing may confuse the receiver of the message.

Moreover, visual information can overcome comprehension and language barriers. It is difficult for foreign people to understand voice messages in non-native languages, but they can easily understand the situation of their current place from photos and videos. For these reasons, it is important for people to share photos and videos of disaster-stricken areas during a disaster. The Global Facility for Disaster Reduction and Recovery (GFDRR) reports that visual information is efficient for disaster reduction in [11].

2) COMMUNICATION SYSTEMS DEPENDENT ON COMMUNICATION INFRASTRUCTURES

Since disasters can destroy communication infrastructures such as cellular networks and optical fiber networks, communication systems used at disaster sites must be robust to infrastructure failures. Currently, a few Japanese local governments have their own local fiber networks and servers to support administrative services, such as communication systems between administrative organizations, but those networks can also be damaged in disasters. Hence, a disaster communication system that works independently of current communication infrastructures is required.

B. SYSTEM ARCHITECTURE

Disaster communication systems consist of disaster control headquarters, shelters, and emergency vehicles with heterogeneous DCR and IEEE 802.11 wireless communication systems. Emergency vehicles handle large data such as disaster-related images and videos via IEEE 802.11-based store-carry-forward transfer to the disaster control headquarters, radio blind zones unreachable by radio signals, and isolated areas. These image and video transfer significantly improve the ability of rescue teams to understand the scale of the damages and formulate rescue plans quickly.

Narrow-band radio is used to transfer text messages such as evacuation alerts and calls for help. The ARIB STD T-98 standard uses the 351, 467, or 150 MHz band. The DCR data rate depends on modulation. For example, it is 4.8 kbps during $\pi/4$-shift frequency-shift keyed (FSK) frequency-division multiple access (FDMA) communications. Since its range is typically up to a few kilometers, it is useful for broadcasting emergency messages such as tsunami/earthquake warnings.

Emergency vehicles working as DTN nodes communicate over IEEE 802.11n protocols and authenticate each other via WPA2-EAP. In the VDTN-based disaster-communication system we have proposed, OBUs installed on emergency vehicles should be able to communicate not only with the vehicle’s OBUs but also with personal mobile devices, such as smartphones and tablet PCs carried by disaster management personnel, because the emergency vehicles collect the photos and videos of disaster-stricken areas from the personal mobile devices via Wi-Fi. In addition, when wireless access points permanently installed at disaster-stricken areas are unavailable due to damage from disasters, the OBUs can be carried out from the vehicles by the personnel of disaster management agencies and used as temporary wireless access points in the disaster-stricken areas. For these reasons, we opted to use IEEE 802.11n in our research.

Although WPA2-EAP-based communications require access points to a Remote Authentication Dial-In User Service (RADIUS) server when verifying certificates, such an authentication scheme cannot be used for emergency vehicles in our disaster communication system because emergency vehicles are often unable to connect to the Internet during disaster-related activities. Therefore, the disaster communication system requires authentication servers to be included in each network node, such as emergency vehicles, shelters, and disaster control headquarters. These authentication servers synchronize certificates over general-use communication infrastructures, such as cellular and IEEE 802.11 networks before disasters, and over DCR after disasters occur. When the certificates are updated, they are broadcast by the authentication server that has the updated certificates.

C. VDTN-BASED DISASTER COMMUNICATION SYSTEM REQUIREMENTS

As stated earlier, VDTN-based disaster communication systems must restrict access to rescue teams because they handle sensitive personal information such as medical data, which means they must authenticate users or mobile devices individually. However, the following restrictions significantly impact individual authentications on disaster communication systems:

1) Short communication times between emergency vehicles: Emergency vehicles operating as DTN ferry nodes can communicate while passing each other. However, depending on their relative velocities and road conditions, they often have only a few seconds to authenticate each other and transfer data. Therefore, the individual authentication process of disaster communication systems should be completed quickly to maximize the amount of transmitted data between emergency vehicles.
2) WPA2-EAP overhead reduction: WPA2-EAP can take several seconds to complete authentication due to the numerous required frame exchanges, even though emergency vehicles serving as DTN node ferries already have short data transfer times. The frame exchange process, which is known as an EAP exchange, is necessary to securely transfer authentication information, such as certificates, usernames, and passwords. However, it is often difficult for emergency vehicles working as DTN node ferries to send certificate verification requests because they must go into radio blind zones and areas without communication infrastructures, such as mountainous regions.

To minimize the limitations described above, disaster communication systems must be able to process individual DTN ferry authentications quickly.

III. RELATED WORK

This section describes work related to individual authentication methods for IEEE 802.11 and vehicular networks and highlights the problems that may arise if the existing individual authentication methods are applied to IEEE 802.11-based inter-vehicular communications.

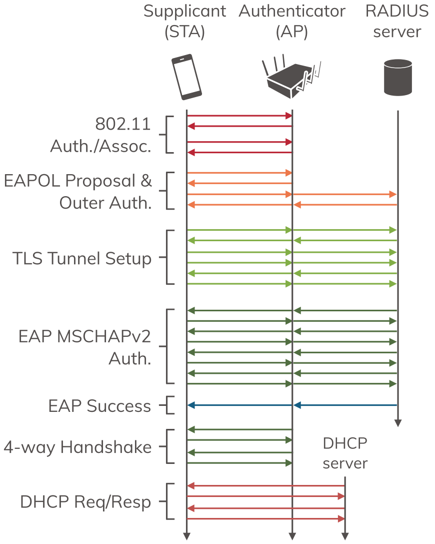


FIGURE 2. PEAP frame sequences.

A. INDIVIDUAL AUTHENTICATION ON IEEE 802.11

As stated above, the primary IEEE 802.11 individual authentication protocols are standardized in IEEE 802.11i/IEEE 802.1X [12], which are also known as WPA2-EAP. These individual authentication protocols enable access points and stations to identify each other via certificates or username and passphrase pairs. EAP [13] has a variety of authentication/certification methods, such as EAP-TLS [14] and protected EAP (EAP-PEAP) [15]. EAP-TLS provides access points and stations with a method to identify each other via their certificates, but its certificate management process is complicated because it must distribute certificates to all stations. In contrast, EAP-PEAP allows access points to identify stations with their usernames and passphrases.

Unfortunately, even though EAP-PEAP simplifies certificate management, it requires an EAP exchange between an access point and station when setting up a secure link, as shown in Figure 2. In this process, the access point and the station need to exchange at least 22 frames between the beginning of the link setup and the completion of the station's IP address assignment. Additionally, the process can take a long time in situations where the frame loss rate is high, such as inter-vehicular communications, which reduces the time available to exchange data frames after the link setup, and thus the amount of data transmitted.

Xu *et al.* showed that the WPA2-EAP authentication delays increase as the number of vehicles rises in [16], which indicates that the WPA2-PEAP and client IP address assignment delays increase when the vehicle density is high and that throughput between the vehicles declines due to those delays.

Separately, other researchers have proposed methods to reduce the WPA2-EAP's latency between mobile devices with high mobility by pre-authentication or key caching.

For example, Mishra *et al.* [17] proposed a proactive key distribution scheme using a neighbor graph, which shows the access points a station might possibly access after handoff. Their scheme allows a station to conduct authentication with access points to which the station may connect in the near future via the access point associated with the station. In another example, Hur *et al.* proposed a pre-authentication method for IEEE 802.11-based vehicular networks [18] that enhances Mishara's scheme and allows a station and an access point to cache a pairwise master key, which can reduce the authentication latency to a level lower than Mishara's method.

However, these schemes are inadequate for IEEE 802.11-based inter-vehicular communications because they assume that the access points are stationary and the station and access points are reachable. Those assumptions do not hold in IEEE 802.11-based inter-vehicular communications in disaster communication systems because emergency vehicles serving as DTN node ferries cannot rely on having sustainable links when communication infrastructures fail. Furthermore, emergency vehicles cannot link to other network nodes when they are in a radio blind zone.

B. INDIVIDUAL AUTHENTICATION ON VEHICULAR NETWORKS

Individual authentication protocols for inter-vehicular communications are standardized in IEEE 1609.2 [19] and ETSI TS 103 097 [20], which also define certificate-based authentication methods for vehicular networks. Certificate-based authentication methods help reduce authentication latency between vehicles because those vehicles only need to exchange a few frames to complete the authentication process. This is simpler than username-passphrase-based authentication methods such as WPA2-PEAP.

Individual authentication protocols also require vehicles to have multiple certificates and acquire different certificates for every authentication because it is difficult to update vehicle certificates when there are no stable links between the vehicles and trust anchors. Therefore, the standards require the trust anchors (i.e., certificate authorities) to be responsible for vehicle certificate management, and thus bear the burden of managing numerous certificates. As a result, numerous researchers have looked for ways to facilitate certificate management on vehicular networks.

For example, Sun *et al.* [21] proposed a certificate update method using roadside units (RSUs), but that method depends on communication infrastructures, which makes it unsuitable for disaster communication systems because it is highly probable that RSUs will be unavailable in emergency situations. Separately, Feiri *et al.* [22] proposed a vehicle-based certificate distribution method that forces vehicles in close proximity to each other to proactively exchange certificates. However, Feiri's method would not work in low-vehicle-density areas where vehicles rarely encounter each other because the need to encounter other vehicles to keep certificates updated would degrade disaster communication systems. This is particularly true in systems where emergency vehicles can be sent to remote areas, such as mountainous regions, where they would have no chance to communicate with other emergency vehicles for extended periods.

Böhm and Jonsson [23] proposed an IEEE 802.11p MAC enhancement that enables a roadside unit to share the authentication information of a car that has already been authenticated by another roadside unit. Since roadside units that have received the authentication information can authenticate the car with the information, they omit the authentication procedure with the car. Therefore, the MAC enhancement can reduce authentication overhead between roadside units and cars. However, the MAC enhancement does not support conventional security protocols such as WPA2-EAP and IEEE 1609.2 and only works with IEEE 802.11p.

Since, as indicated by the examples above, certificate-based authentication methods require stable links between emergency vehicles and trust anchors, as well as complicated certificate management procedures, they do not provide a realistic way to manage disaster communication systems. Therefore, we adopted the WPA2-PEAP username-passphrase-based authentication method for our disaster communication system. Mano *et al.* reported the overhead of initial authentication on IEEE 802.11 harms seamless handover between high-mobility devices based on field experiment results in [24]. Since the abovementioned authentication and IP address assignment latency will presumably occupy communication time between moving vehicles, we propose using FILS for IEEE 802.11-based inter-vehicular communications to reduce individual authentication and IP address assignment delays.

IV. FAST INITIAL LINK SETUP

This section describes the Fast Initial Link Setup (FILS) mechanisms standardized in IEEE 802.11ai, which enables the establishment of a secure connection within about 100 ms using the following four mechanisms:

A) Channel scanning enhancement
B) Active scanning optimization
C) IP address assignment during the IEEE 802.11 associations
D) Authentication information caching

A. CHANNEL SCANNING ENHANCEMENT

While authenticators broadcast a beacon frame every 100 ms, FILS also allows them to broadcast FILS discovery frames. Furthermore, while IEEE 802.11ai states that a FILS discovery frame must always have a Basic Service Set Identifier (BSSID) users have the option of including other information elements. Thus, supplicants can detect authenticators faster than usual.

B. ACTIVE SCANNING OPTIMIZATION

A supplicant in the active scanning mode actively broadcasts probe request frames to search for authenticators. If the

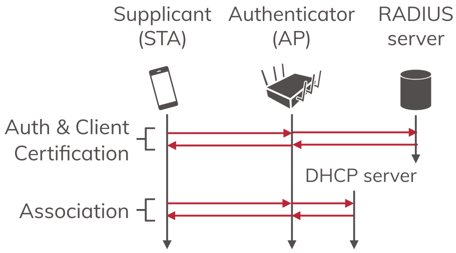


FIGURE 3. **FILS frame sequences.**

probe request frame does not have an expiration time, the authenticators will need to respond to every probe request, which causes extra traffic on the channel and degrades Layer 2 (data link layer) throughput. In contrast, FILS allows a probe request frame to include an expiration time for request replies, which means FILS can reduce the unnecessary channel scanning traffic.

C. IP ADDRESS ASSIGNMENT DURING THE IEEE 802.11 ASSOCIATION

FILS provides an IP address assignment field as an information element of an authentication response frame. The assignment function enables a Dynamic Host Configuration Protocol (DHCP) server to assign an IP address to the supplicant within the Layer 2 authentication procedure. Figure 3 shows the frame sequence of the EAP re-authentication protocol (EAP-RP), which allows the authenticators and supplicants to process the initial link setup and IP address assignment within a few exchanged frames. This allows FILS to reduce frame exchanges in the initial link setup and shortens the setup time.

FILS also allows higher-layer protocols to include a packet in IEEE 802.11 association request/response frames. More specifically, it defines an additional information element called a "FILS HLP Container Element" that contains a packet with the media access control (MAC) addresses of the source and destination in the element. This allows user applications working on different WLAN nodes to exchange packets during the IEEE 802.11 association. In IEEE 802.11ah networks, some papers [3]–[5] have proposed fast authentication procedures. These 802.11ah authentication methods mainly focus on improving the IEEE 802.11 association procedure. On the other hand, FILS not only shortens authentication procedures but also completes IP address assignment in the authentication procedure by FILS HLP Container Element.

D. AUTHENTICATION INFORMATION CACHING

FILS enables an access point and a station to cache authentication information, such as certificates, when they establish a secure link for the first time. The access point and the station use the cached authentication information to establish secure links from the second time onward. This allows FILS to complete a link set up with fewer frame exchanges than a conventional EAP exchange.

E. EFFECTIVENESS

Various papers have reported the FILS performance. For example, Mano *et al.* performed a field experiment in a situation where 40 pedestrians with mobile devices came into a stream with the speed of 4.5 km/h and passed in the front of an access point in [6], [25]. The mobile devices and the access point authenticated each other with FILS or WPA2-PEAP. The authors confirmed that the mobile devices using FILS established IEEE 802.11 links before the pedestrians passed the access point, while the mobile devices using WPA2-PEAP did not complete IEEE 802.11 link establishment even after passing in the front of the access point.

Ong theoretically analyzed the FILS authentication methodology outlined in IEEE P802.11 Group AI (TGai) in [7]. The author formulated the FILS active scanning enhancement and compared the performance of the FILS active scanning enhancement with IEEE 802.11 DCF (Distributed Coordination Function) or EDCA (Enhanced Distributed Channel Access). The author revealed that the FILS active scanning enhancement can make the responsiveness to beacon frames 20% and 250% faster than IEEE 802.11 EDCA and DCF, respectively. However, since this paper refers to TGai technical papers, the FILS performance is not sufficiently analyzed with consideration of EAP-RP and IP address assignment in IEEE 802.11 association specified in the published IEEE 802.11ai standard.

Kushida *et al.* [8] simulated the effectiveness of FILS link setup time reduction in IEEE 802.11ad wireless networks. Their simulation results revealed that FILS reduced link setup times to ten times less than WPA2-PEAP and also reduced the number of authentication failures in an IEEE 802.11ad networks. However, all simulation nodes are stationary in their simulation scenario, and the FILS effectiveness considering the mobility of network nodes is not discussed in the paper.

Although these papers showed that FILS is effective in decreasing authentication overhead, as far as we know, no paper reported has the effectiveness of link setup time reduction by FILS in vehicular networks. For this reason, this paper presents the results of laboratory and field experiments to determine the FILS effectiveness in vehicular networks.

V. EXPERIMENTAL SETUP

This section describes the setup of the laboratory and field experiments conducted to evaluate the effectiveness of FILS link setup time reduction in inter-vehicular communications. The laboratory experiment was conducted to verify whether the FILS implementation can achieve the performance outlined in IEEE 802.11ai. The field experiment was conducted to verify whether FILS can work in an actual inter-vehicular communications system.

A. DETAIL OF OUR FILS IMPLEMENTATION

We implemented the FILS functions in ARM-based on-board units equipped with the Linux operating system (OS) because

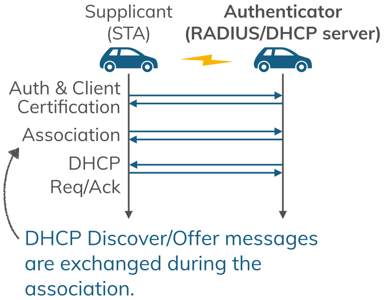

Supplicant (STA)
Authenticator (RADIUS/DHCP server)
Auth & Client Certification
Association
DHCP Req/Ack
DHCP Discover/Offer messages are exchanged during the association.

FIGURE 4. Our FILS implementation.

there are already a number of FILS implementations for that system. However, our FILS implementation had some differences related to IP address assignment compared to the original FILS functions due to limitations of the device driver of the IEEE 802.11 chips we used. Specifically:

1) Authentication (RADIUS) servers work on all the access points: Vehicles serving as DTN ferries work as authentication servers. This configuration was selected to ensure compatibility with the architecture of our disaster communication system.
2) FILS IP address assignment is not supported: In our FILS implementation, a DHCP server assigns the client's IP address using the conventional DHCP process. In other words, the DHCP server and client must exchange DHCP discover/offer messages and request/ack messages, even though the original FILS does not require these message exchanges.
3) DHCP discover/offer messages are exchanged during the IEEE 802.11 association: Our FILS implementation supports the FILS HLP Container described in Section IV, which allows higher-layer protocols such as DHCP to send a packet during the IEEE 802.11 association. We implemented a DHCP server and client that support sending discover/offer messages via the FILS HLP Container. Therefore, our FILS implementation only needs to exchange request/ack messages after completing the Layer 2 link setup.
4) Lightweight DHCP clients work on OBUs: Our DHCP client also supports exchanging discover/offer messages via the FILS HLP Container. More specifically, the client sends a request message immediately after receiving an offer message via the FILS HLP Container. In contrast, a normal DHCP client will not send a request immediately because it waits for other offer messages from multiple DHCP servers.

B. OBU CONFIGURATIONS

We performed laboratory and field experiments with OBUs, as shown in Figure 5. Table 1 shows the OBU specifications. Each OBU was equipped with two Qualcomm AR9300 Wi-Fi cards and four Wi-Fi antennas that communicate over the IEEE 802.11n protocol at 2.4 GHz. Additionally, each OBU on which we implemented the FILS functions was equipped with a customized hostapd [27] authenticator daemon program and wireless protected access wpa_supplicant [28]. We also added the EAP-RP function to the original hostapd 2.7 and wpa_supplicant 2.7 codes.

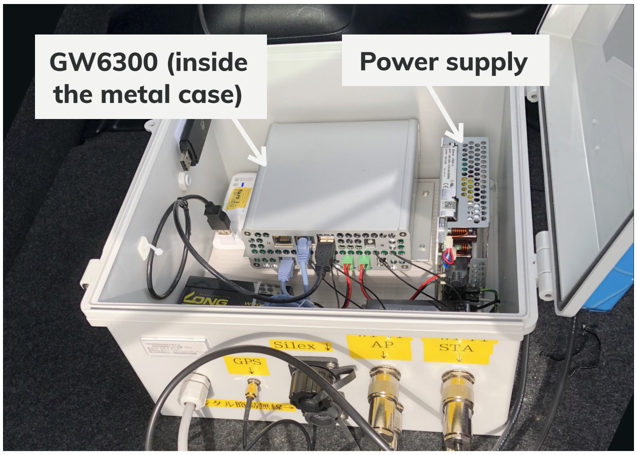


FIGURE 5. OBU overview.

TABLE 1. OBU specifications.

Base board	Gateworks GW6300
Distribution/Kernel	Ubuntu 16.04.05 LTS/Linux 4.14.4
CPU	Octeon TX Dual Core ARM CPU @ 800 MHz
Memory	DDR3 1GB
Storage	SSD 250 GB
Wi-Fi chip/driver	Qualcomm AR9300 x2 / ath9k

We implemented an embedded Structured Query Language (SQL) database in the customized hostapd to cache authentication information of stations that had previously connected to the hostapd and forced the OBUs to cache the authentication information in advance. We also utilized hostapd 2.6 and wpa_supplicant 2.6 without modification to measure EAP-PEAP performance levels. As described in the previous section, in both experiments, we used a DHCP server and client that support FILS.

Additionally, we implemented a RADIUS server in the authenticator, which reduced the delay between the two components to almost zero. We also implemented a user application to send a file between the supplicant and the authenticator via Transmission Control Protocol (TCP). The user application sends a 100 MB file for each measurement. The kernel was allowed to reuse TCP sessions that the kernel had started and were in the TIME-WAIT state. We also enabled TCP fast open [29] and Tail Loss Probe (TLP) [30] to reduce the TCP session establishment overhead. The use of TLP makes it possible to detect and recover from tail losses faster than TCP retransmission timeout. The other TCP parameters were the same as the default values.

C. LABORATORY EXPERIMENT CONFIGURATION

We connected the OBUs with coaxial cables through variable attenuators, as shown in Figure 6, and manually set their signal reception strength to either −65 dBm or −95 dBm, such that the OBUs were connected at −65 dBm and

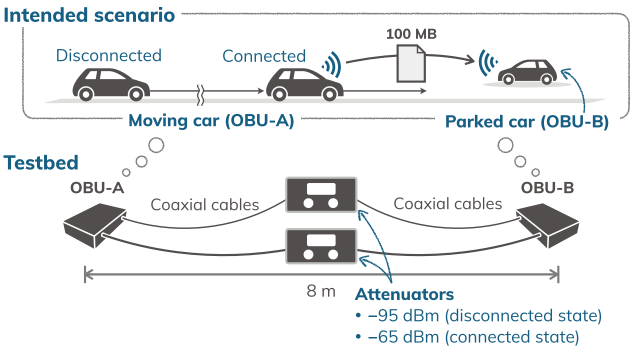


FIGURE 6. Laboratory experiment scenario.

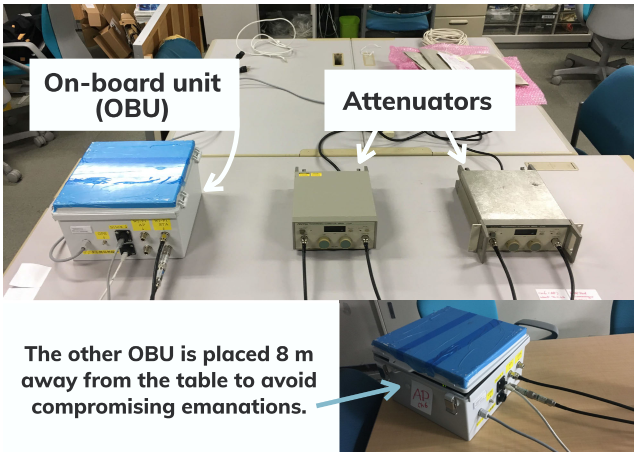


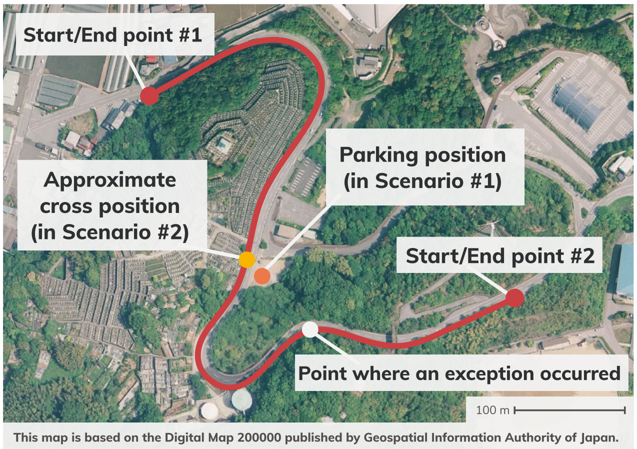
FIGURE 7. Laboratory environment overview.

disconnected at −95 dBm. We also configured the data rate on Layers 2 and 1 (i.e., on both the data link layer and the physical layer) to be automatically determined. At the start of our experiment, we launched hostapd and wpa_supplicant and used the attenuators to set the receiving signal strength of the OBUs to −95 dBm. Next, we adjusted the receiving signal strength to −65 dBm and waited for 30 seconds while they attempted to transfer a 100 MB file. Finally, we restored the receiving signal strength to −95 dBm and recorded the link setup time and the number of bytes transmitted between the OBUs.

To measure link setup times, we monitored network interfaces installed at the OBUs by ip command [31] which is the Linux network interface utility and iw command [32] which is Linux WLAN configuration utility, and recorded timestamps when the IEEE 802.11 probe request is transmitted and when an IP address is assigned to a DHCP client.

D. FIELD EXPERIMENT SCENARIOS AND CONFIGURATIONS

Our actual field experiment was conducted in Konan City, Kochi Prefecture, Japan. Figure 8 shows a map of the area and the driving route. The solid red line indicates the car trajectories while the orange dot near the center of the picture shows where we parked the car that served as the authenticator.



This map is based on the Digital Map 200000 published by Geospatial Information Authority of Japan.

FIGURE 8. Field experiment area.

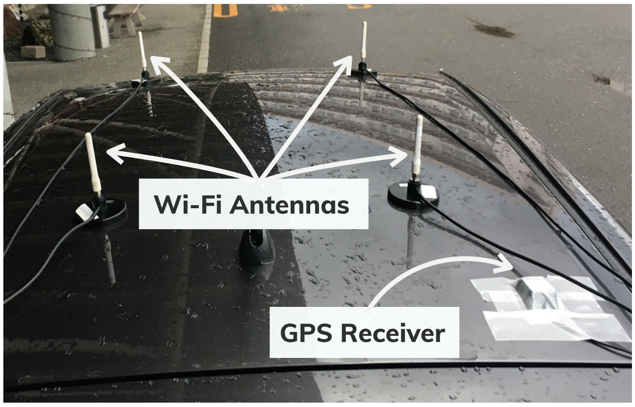


FIGURE 9. Wi-Fi antenna configuration.

We used two cars, which are referred to hereafter as Car #1 and Car #2. In this experiment, Car #1 served as the authenticator, while Car #2 served as the supplicant. We installed the OBUs and Wi-Fi antennas in both cars. Figure 9 shows the antenna placements. The antennas of each Wi-Fi card were placed on the vehicle roofs at diagonal angles. The data rates on Layers 2 and 1 were the same as used in the laboratory experiment. The height of the cars was 1.5 m. Note that we did not install the DCR functions into the OBUs for this experiment.

We moved the cars according to two scenarios, hereafter referred to as Scenario #1 and #2. In Scenario #1, we parked Car #1 at the point marked in orange in Figure 8 and drove Car #2 in both directions at 40 km/h on the route indicated by the red line in Figure 8. In Scenario #2, we drove the two cars in opposite directions at 40 km/h on the driving route so that they passed each other at the yellow point. Car #2 completed five round trips during Scenario #1, while both cars completed ten round trips during Scenario #2.

In both the laboratory and field experiments, we conducted measurements to determine if FILS shortens the link setup

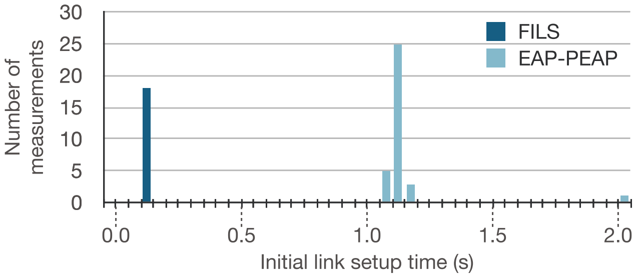


FIGURE 10. **Initial link setup time measured in our laboratory experiment.**

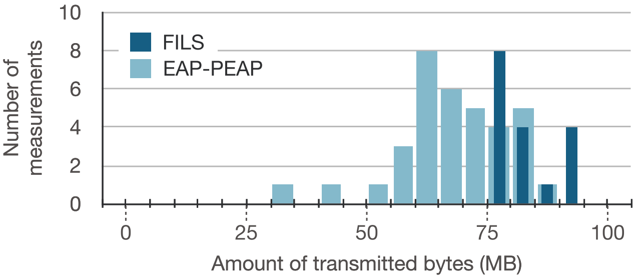


FIGURE 11. **Transmitted bytes measured in our laboratory experiment.**

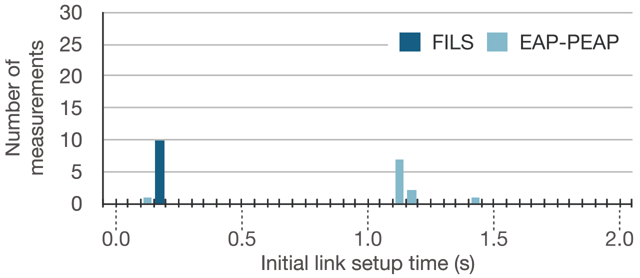


FIGURE 12. **Initial link setup time in Scenario #1.**

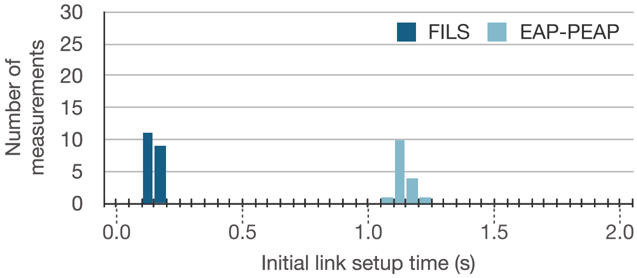


FIGURE 13. **Initial link setup time in Scenario #2.**

time and improves the amount of transmitted data. The link setup time is defined as beginning when the supplicant starts to send an association request frame to the authenticator and ending when the supplicant obtains an IP address.

VI. EVALUATION RESULTS

This section describes the laboratory and field experimental results, which suggest the existence of a bottleneck during the initial link setup for IEEE 802.11-based inter-vehicular communications.

A. LABORATORY ENVIRONMENT

Figure 10 shows a histogram comparison of the FILS and EAP-PEAP link setup times measured in our laboratory experiment. Each bin width is 0.05 s. The thin bars in deep blue and the thick bars in light blue are the FILS and EAP-PEAP results, respectively. As shown, the FILS link setup time averaged 127 ms, and the maximum and minimum setup time was 147 ms and 109 ms, respectively.

In contrast, the EAP-PEAP link setup times averaged 1.21 s with maximum and minimum setup time values of 2.81 s and 1.08 s, respectively. Since we implemented and used a DHCP server and client, the IP address assignment with our FILS implementation was performed by DHCP after the Layer 2 link was established, as shown in Figure 3. Thus, the FILS link setup times were about 30 ms longer than the link setup time of the IEEE 802.11ai standard. Figure 11 shows a histogram of the transmitted bytes between the OBUs in the laboratory experiment. Here, we can see that the number of bytes transmitted by FILS tends to exceed those transmitted by EAP-PEAP and that FILS increased the data traffic by about 14 MB. This result indicates that FILS reduced the link setup time and extended the communication time available to transfer data packets per connection.

From these results, we confirmed that our FILS implementation could shorten the link setup time based on the standard and increase the amount of transmitted data per connection.

B. FIELD EXPERIMENT

Figures 12 and 13 show histograms of the link setup times measured in the field experiments. In Scenario #1, the maximum, average, and minimum setup time of FILS were 197 ms, 173 ms, and 154 ms, respectively, while the maximum and average setup times of EAP-PEAP were 1.43 s and 1.10 s, respectively.

The minimum setup time of EAP-PEAP, except for an exceptional case, was 1.07 s. In the exceptional case, the link setup time was much shorter (137 ms) than the 1.07 s minimum because the Layer 2 link disconnected momentarily and then re-established by hostapd and wpa_supplicant without completing an EAP exchange. This occurred when the moving car passed at the point indicated by the white dot in Figure 8. At this point, the cars were visible to each other because the trees between the point and the parked car were lower than in the other areas. In Scenario #2, the maximum, average, and minimum setup times of FILS were 186 ms, 151 ms, and 110 ms, respectively, while the maximum, average, and minimum setup times of EAP-PEAP were 1.22 s, 1.13 s, and 1.09 s, respectively.

Figures 14 and 15 show histograms of the transmitted bytes in the two scenarios. These results indicate that FILS increased the data traffic by around 33 MB in Scenario #1 and around 10 MB in Scenario #2. In both cases, the numbers of bytes transmitted via FILS tended to exceed those transmitted

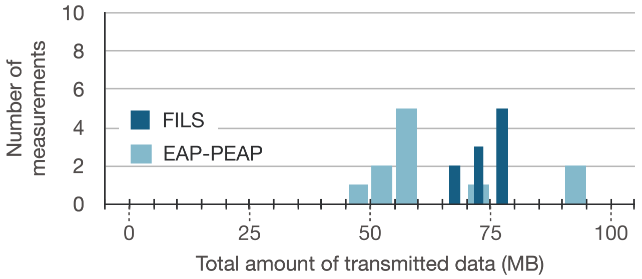


FIGURE 14. Transmitted bytes in Scenario #1.

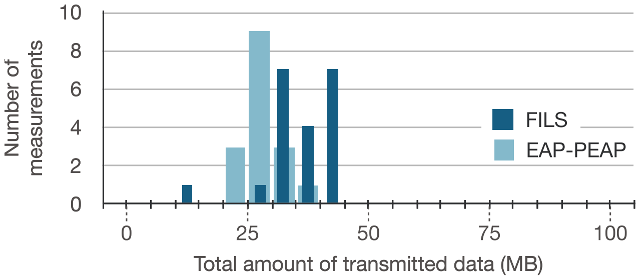


FIGURE 15. Transmitted bytes in Scenario #2.

by EAP-PEAP because FILS reduced the link setup times and lengthened the time available to transfer data packets per connection.

In Scenario #1, there was one exception in which the transmitted bytes of EAP-PEAP exceeded those transmitted by FILS. This occurred when a TCP session between the cars was maintained after the link on Layer 2 had prematurely disconnected, which means the TCP session time did not expire. Normally, the user application restarts counting transmitted bytes when a TCP session is disconnected. However, in this case, the user application did not restart counting transmitted bytes because the cars established communication when Car #2 passed by the point depicted by the white dot in Figure 8 before passing the point depicted by the yellow dot in Figure 8.

Although the cars were close to each other when reaching the white point in each round trip, the only time the cars established a link and transferred data while passing was in the case of the exception. The Layer 2 link disconnected while Car #2 traveled between the white and yellow points, but the TCP session remained active. Because of this, the transmitted bytes were summed up before and after the Layer 2 disconnection.

In another interesting finding, we confirmed that FILS always established a link during Scenarios #1 and #2, while WPA2-PEAP failed to establish a link 11 times in Scenario #2. The failures of the WPA2-PEAP case occurred because the station on one car closed the IEEE 802.11 communication link with the access point on another car before sending data via TCP. In this case, the station barely received IEEE 802.11 data frames from the access point in 30 seconds after they established the communication link. We consider frame losses and the resulting failure of TCP session establishment to be the main causes of this error. In the field experiment, frame losses could occur frequently because the cars moved at the speed of 40km/h. The frame losses that stem from high mobility of cars could prevent the access point and the station from establishing a TCP session. On the other hand, FILS can set up a link with just a few of frame exchanges and prevent vehicles from missing communication opportunities due to link establishment overhead.

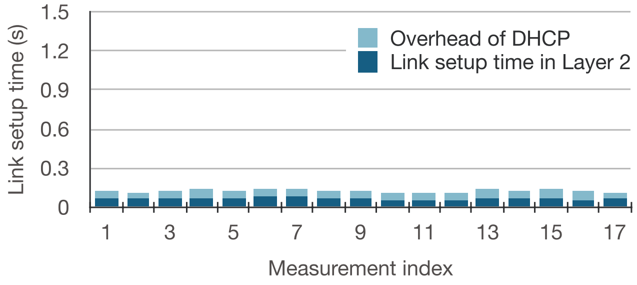


FIGURE 16. Details of FILS link setup times in laboratory experiment.

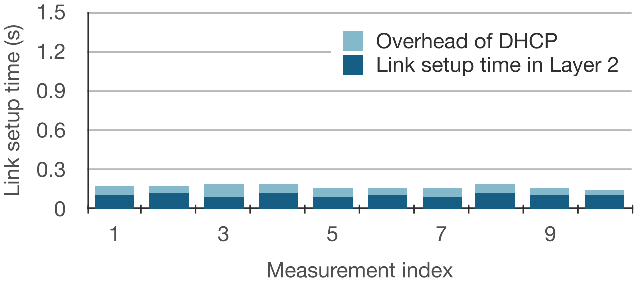


FIGURE 17. Details of FILS link setup times in Scenario #1.

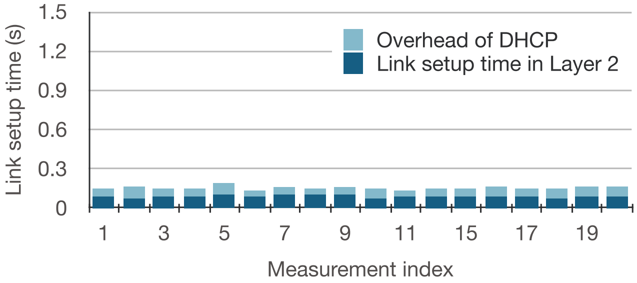


FIGURE 18. Details of FILS link setup times in Scenario #2.

C. INITIAL LINK SETUP BOTTLENECK

Figures 16, 17, and 18 are stacked bar graphs showing initial link setup times measured in the in-laboratory environment, Scenario #1, and Scenario #2, respectively, while Figures 19, 20, and 21 are stacked bar graphs showing the PEAP initial link setup times, respectively.

From these results, we can see that FILS reduced the overhead of the client's IP address assignment by DHCP. In contrast, EAP-PEAP took approximately one second to assign the client's IP address, which indicates that the exchange of DHCP messages causes an excessive overhead.

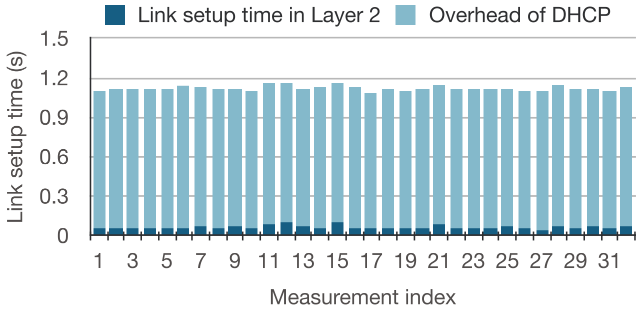


FIGURE 19. Details of PEAP link setup times in laboratory experiment.

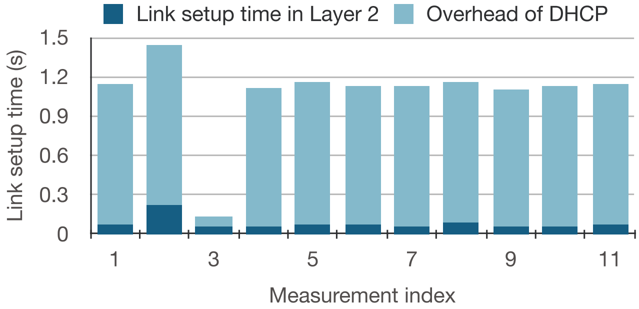


FIGURE 20. Details of PEAP link setup times in Scenario #1.

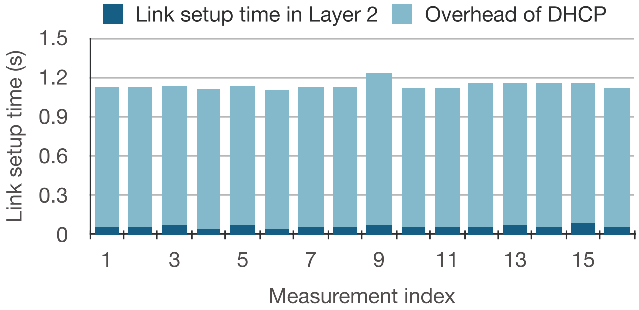


FIGURE 21. Details of PEAP link setup times in Scenario #2.

There are two potential reasons for the DHCP overhead: DHCP offer message waiting time and parsing DHCP lease files. A DHCP client waits for several seconds before responding to a DHCP offer message because it can receive these messages from multiple DHCP servers. In addition, for a major DHCP server with full DHCP implementation, such as an ISC DHCP server, records assign IP addresses in a lease file and check this file prior to each assignment to validate the IP address lease time and to avoid conflicts between assigned IP addresses. Consequently, there is a delay due to having to parse this lease file.

However, in our experiments, the delay from parsing the lease file can be ignored because we remove the lease file and reset the DHCP server prior to each measurement. Thus, unlike in the conventional case, our FILS implementation allows the DHCP server to send an offer message during the IEEE 802.11 association using the FILS HLP Container, upon receipt of which, the client immediately sends immediately a request message back via the FILS HLP Container. As a result, the DHCP overhead of the proposed FILS implementation is shorter than that of EAP-PEAP. In Figure 20, we see an exceptional case, whose index is three, in which the EAP-PEAP link setup time is shorter than in other cases. This exceptional case is due to the same reason that the cars completed the link setup time over the low trees area. In still another case, a situation occurred in which EAP-PEAP took a longer time to set up a link than the other situations, but the cause of that exception was traced to frame losses, which exceeded those of other cases.

These results show that EAP-PEAP could complete the Layer 2 link as quickly as FILS, but the results do not include the overhead of certificate verification to the authentication server. Therefore, the EAP-PEAP link setup could take longer in situations where the authentication server is accessible over other networks such as cellular networks. Furthermore, these results do not include the overhead that occurs when a DHCP server checks lease files, which could harm the initial link setup when numerous vehicles attempt to connect with each other.

However, the results described above confirm that FILS reduced link setup times and increased the size of transmitted data between two passing cars communicating over IEEE 802.11n with WPA2-EAP. Additionally, FILS was found to be capable of quickly establishing secure links in IEEE 802.11-based VDTNs with the same level of security as WPA2-EAP as well as preventing vehicles from missing communication opportunities when they pass each other.

We consider two reasons for the communication errors when using WPA2-PEAP: frame loss and the failure of TCP session establishment. Since the cars passed by each other at high speed, and frame loss easily occurred, the data transfer applications could not establish a TCP session. In addition, the frame loss could prevent the cars from transferring the file after the TCP session was established. For this reason, the station did not receive data frames and closed a communication link on Layer 2 intentionally. The communication errors we observed in the field experiment indicate that data transmission over TCP can fail when a connection on Layer 2 and lower is unstable even if the connection on Layer 2 is established successfully. UDP can be an alternative protocol of TCP, but UDP does not have a retransmission mechanism. Therefore, a cross-layer mechanism that can monitor the connection state of each network layer (e.g., TCP and user applications) and notify the upper layers like TCP and user applications of the connection states is required to avoid frame losses and transfer large amounts of data between vehicles.

VII. CONCLUSION

This paper reported the results of laboratory and field experiments showing that FILS (IEEE 802.11ai) reduces link setup times and increases the size of transferred application data in 2.4 GHz IEEE 802.11n-based inter-vehicular communications. More specifically, when cars passed each other at a relative speed of 80 km/h, our results showed that FILS reduced the initial link setup to around 150 ms between the passing cars, and that it transferred around 40 MB, which is 10 MB more than WPA2-PEAP. We also confirmed that FILS prevented vehicles from missing communication opportunities due to the link establishment overhead.

Our future research will focus on clarifying FILS capacity limitations when multiple link setups coincide, such as communications between emergency vehicles and disaster control headquarters. We will also focus on developing a method for updating cached authentication information used by FILS via intermittent inter-vehicular communications.

REFERENCES

[1] *APT Recommendation on Specification of Information and Communication System Using Vehicle During Disaster*, document APT/STAP/REC-02, Asia Pacific Telecommunity, 2018.

[2] *Digital Convenience Radio Equipment for Simplified Service*, Standard ARIB STD-T98, Version 1.4, Association of Radio Industries and Businesses, 2014.

[3] D. Bankov, E. Khorov, A. Lyakhov, E. Stepanova, L. Tian, and J. Famaey, "What is the fastest way to connect stations to a Wi-Fi HaLow network?" *Sensors*, vol. 18, no. 9, p. 2744, Aug. 2018.

[4] W. Yin, P. Hu, W. Wang, J. Wen, and H. Zhou, "FASUS: A fast association mechanism for 802.11ah networks," *Comput. Netw.*, vol. 175, Jul. 2020, Art. no. 107287.

[5] L. Zhang and M. Ma, "FKR: An efficient authentication scheme for IEEE 802.11ah networks," *Comput. Secur.*, vol. 88, Jan. 2020, Art. no. 101633.

[6] H. Mano, H. Morioka, and T. Uehara, "Experimental trial of wireless LAN FILS (fast initial link setup)," (in Japanese), in *Proc. Multimedia, Distrib., Cooperat., Mobile Symp. (DICOMO)*, 2013, pp. 1626–1633.

[7] E. H. Ong, "Performance analysis of fast initial link setup for IEEE 802.11ai WLANs," in *Proc. IEEE 23rd Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2012, pp. 1279–1284.

[8] H. Kushida, H. Mano, M. Takai, Z. Liu, and S. Ishihara, "On the effectiveness of FILS in IEEE 802.11ad wireless networks," in *Proc. 23rd Asia–Pacific Conf. Commun. (APCC)*, Dec. 2017, pp. 1–6.

[9] A. Kato, T. Maeno, Y. Owada, G. Sato, K. Temma, T. Kuri, M. Takai, and S. Ishihara, "Performance evaluation of FILS in a vehicular delay/disruption tolerant network," in *Proc. IEEE 92nd Veh. Technol. Conf. (VTC-Fall)*, Nov. 2020, pp. 1–5.

[10] Cabinet Office and Government of Japan. (2015). *Disaster Management in Japan*. [Online]. Available: http://www.bousai.go.jp/1info/pdf/saigaipamphlet_je.pdf

[11] *Information and Communication Technology for Disaster Risk Management in Japan*, Global Facility Disaster Reduction Recovery, World Bank, Washington, DC, USA, 2019.

[12] *IEEE Standard for Local and Metropolitan Area Networks–Port-Based Network Access Control*, IEEE Standard 802.1X-2010 (Revision of IEEE Std 802.1X-2004), Feb. 2010.

[13] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, *Extensible Authentication Protocol (EAP)*, document RFC3748, 2004.

[14] D. Simon, B. Aboba, and R. Hurst, *The EAP-TLS Authentication Protocol*, document RFC2716, 2008.

[15] A. Palekar, D. Simon, G. Zorn, and S. Josefsson. (Jul. 2004). Protected EAP protocol (PEAP). IETF. [Online]. Available: https://tools.ietf.org/id/draft-josefsson-pppext-eap-tls-eap-06.txt

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

[17] A. Mishra, M. H. Shin, N. L. Petroni, T. C. Clancy, and W. A. Arbaugh, "Proactive key distribution using neighbor graphs," *IEEE Wireless Commun.*, vol. 11, no. 1, pp. 26–36, Feb. 2004.

[18] J. Hur, C. Park, and H. Yoon, "An efficient pre-authentication scheme for IEEE 802.11-based vehicular networks," in *Advances in Information and Computer Security*, vol. 4752. Berlin, Germany: Springer, 2007, pp. 121–136.

[19] *IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages*, IEEE Standard 1609.2-2016 (Revision of IEEE Std 1609.2-2013), 2014, pp. 1–240.

[20] *Intelligent Transport System (ITS); Security; Security Header and Certificate Formats*, document ETSI TS 103 097 V1.3.1, ETSI, Oct. 2017.

[21] Y. Sun, X. Lin, R. Lu, X. Shen, and J. Su, "Roadside units deployment for efficient short-time certificate updating in VANETs," in *Proc. IEEE Int. Conf. Commun.*, May 2010, pp. 1–5.

[22] M. Feiri, R. Pielage, J. Petit, N. Zannone, and F. Kargl, "Pre-distribution of certificates for pseudonymous broadcast authentication in VANET," in *Proc. IEEE 81st Veh. Technol. Conf. (VTC Spring)*, May 2015, pp. 1–5.

[23] A. Böhm and M. Jonsson, "Handover in IEEE 802.11p-based delay-sensitive vehicle-to-infrastructure communication," School Inf. Sci., Comput. Elect. Eng., Halmstad Univ., Sweden, IDE Tech. Rep. 0924, 2009, pp. 1–8.

[24] H. Mano, H. Morioka, P. A. Lambert, M. Emmelmann, H. Nakano, and M. Takai. (2010). *Fast Initial Authentication—IEEE 802.11-10/0371r3*. [Online]. Available: https://mentor.ieee.org/802.11/dcn/09/11-09-1000-03-0wng-ieee802-11-for-high-speed-mobility.ppt

[25] H. Mano, "Standardization of emergent wireless LAN technology and evaluation," in *Proc. CJK Workshop 9th Int. Conf. Future Internet Technol.*, 2014, pp. 1–29. [Online]. Available: http://cfi2014.wide.ad.jp/wp-content/uploads/2014/06/02-Hiroshi_Mano.pdf

[26] Z. Cao, B. He, Y. Shi, Q. Wu, and G. Zorn, *EAP Extensions for the EAP Re-Authentication Protocol (ERP)*, document RFC6696, 2012.

[27] J. Malinen. (2013). *Hostapd: IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/EAP/RADIUS Authenticator*. [Online]. Available: https://w1.fi/hostapd/

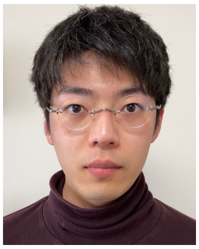
[28] J. Malinen. (2013). *Hostapd: Linux WPA/WPA2/IEEE 802.1X Supplicant*. [Online]. Available: https://w1.fi/wpa_supplicant/

[29] Y. Cheng, J. Chu, S. Radhakrishnan, and A. Jain, *TCP Fast Open*, document RFC7413, 2014.

[30] M. Rajiullah, P. Hurtig, A. Brunstrom, A. Petlund, and M. Welzl, "An evaluation of tail loss recovery mechanisms for TCP," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 45, no. 1, pp. 5–11, Jan. 2015.

[31] *IP (8) Linux Manual Page*. Accessed: Oct. 1, 2021. [Online]. Available: https://man7.org/linux/manpages/man8/ip.8.html

[32] *About IW URL*. Accessed: Oct. 1, 2021. [Online]. Available: https://wireless.wiki.kernel.org/en/users/documentation/iw



ARATA KATO (Student Member, IEEE) received the B.E. and M.E. degrees in mathematical and systems engineering from Shizuoka University, Shizuoka, Japan, in 2017 and 2019, respectively, where he is currently pursuing the Ph.D. degree with the Graduate School of Science and Technology. His current research interests include the development of wireless network systems, especially for vehicular networks, delay tolerant networks, and wireless network emulation systems.

TAKA MAENO received the M.E. degree in information engineering from Niigata University, Japan, in 2008. He joined Space-Time Engineering Japan Inc., in 2008. His research interests include wireless communication and networking systems and simulation of vehicular and other mobile networking systems.

YASUNORI OWADA (Member, IEEE) received the Ph.D. degree from Niigata University. He is currently a Senior Researcher with the Resilient ICT Research Center, National Institute of Information and Communications Technology (NICT). He has been engaged in the research and development of resilient, distributed wireless, and mobile access network system called NerveNet at NICT, since 2010. He was previously the President of Space-time Engineering Japan Inc., from 2008 to 2010, and an Assistant Professor with Niigata University, from 2007 to 2008. He was awarded with Prizes for Science and Technology, FY2019 the Commendation for Science and Technology by the Ministry of Education, Culture, Sports, Science and Technology (MEXT), Japan.

GOSHI SATO received the Ph.D. degree in software information science from Iwate Prefectural University, Japan, in 2016. Currently, he is working with the National institute of Information and Communications Technology, Resilient ICT Research Center, Japan, as a Researcher. His research interests include the SDN and disaster information systems, LPWA mesh networks, and cognitive radio networks. He is a member of the Information Processing Society of Japan (IPSJ).

KATSUHIRO TEMMA (Member, IEEE) received the B.E., M.E., and Ph.D. degrees in communications engineering from Tohoku University, Sendai, Japan, in 2010, 2012, and 2016, respectively. From April 2013 to March 2015, he was a Research Fellow at the Japan Society for the Promotion of Science (JSPS). Since April 2016, he has been with the National Institute of Information and Communications Technology (NICT). He is a member of IEICE of Japan. He was a recipient of the IEEE VTS Japan Chapter 2011 Young Researcher's Encouragement Award.

TOSHIAKI KURI (Senior Member, IEEE) joined the Communications Research Laboratory, Ministry of Posts and Telecommunications (currently, National Institute of Information and Communications Technology), Tokyo, Japan, in 1996. He has been engaged in research on optical communication systems and resilient ICT systems. He is a member of IEICE of Japan. He received the 1998 Young Engineer Award and the 2010 Electronics Society Activity Testimonial from the IEICE.

MINEO TAKAI (Member, IEEE) received the Ph.D. degree in electrical engineering from Waseda University, Japan, in 1997. He is currently a Principal Development Engineer with the Electrical and Computer Engineering Department, University of California, Los Angeles (UCLA), and also a Guest Associate Professor with Osaka University, Japan. He joined UCLA, in 1997. His research interests include the design, analysis and control of wireless communication, and mobile computing systems. He is a member of ACM.

SUSUMU ISHIHARA (Member, IEEE) received the B.E., M.E., and Dr. Eng. degrees in electronic engineering from Nagoya University, Nagoya, Japan, in 1994, 1996, and 1999, respectively. From 1998 to 1999, he was a JSPS Special Researcher. He joined Shizuoka University, in 1999. He was a Visiting Scholar at the University of California, Irvine, in 2008, and the University of California, Los Angeles, from 2014 to 2015. He is currently a Professor with the College of Engineering, Academic Institute, Shizuoka University, Japan. His current research interests include the design and implementation of communication protocols and services, especially for vehicular *ad hoc* networks and wireless sensor networks. He is a member of ACM, IPSJ, and IEICE, and a Senior Member of IPSJ.