Continuous and Secure In-Flight Wireless LAN with Roaming

Hideaki Goto
Cyberscience Center, Tohoku University
Sendai, Miyagi, Japan

1 INTRODUCTION

In-Flight Wireless LAN, or simply In-Flight Wi-Fi in a casual wording, has become an attractive service and many airlines are providing in-flight internet connection today. Some companies are providing free Wi-Fi service only for text messaging, while some others are providing a regular service for free in domestic flights. Paid service is common in international flights since the airlines have to keep the costly equipments and backhaul network usage. Some airlines provide roaming service for some Internet Service Providers (ISPs) and telecom operators in addition to the airlines' own charging system.

The In-Flight Wi-Fi today suffers from various problems regarding security and usability. Open network without encryption is commonly used despite various security threats including eavesdropping and rogue Access Point (AP) attacks. One of the biggest obstacles is the disruption of the internet connection to the ground. Introducing a secure connection means like WPA2 Enterprise, preferably combined with roaming, can solve most security problems and some usability issues [1]. However, user authentication in the current roaming systems depends on the servers on the ground and suffers from network disruption. Since In-Flight Wi-Fi is becoming indispensable not only for internet connection but also for various in-flight services, user devices need to stay connected to the APs during the entire flight.

We developed earlier a disruption-tolerant Public Wi-Fi system to realize secure user authentication and to maintain local network use in temporary isolated areas affected by natural disasters [2]. Since we noticed that the airline use case shares many aspects in our previous application, we have developed a continuous and secure In-Flight Wi-Fi system based on the previous system. This presentation[1] provides an overview of prospective use cases, problems, and the current development status.

2 IN-FLIGHT WI-FI USE CASES AND CHALLENGES

2.1 In-Flight Wi-Fi and Prospective Use Cases

It is important to think about not only the current In-Flight Wi-Fi but also prospective use cases and emerging technologies. Figure 1 depicts the current internet connection means for passenger aircrafts. Use of any radio equipments used to be prohibited before, and still is on older aircrafts, during taxiing, take-off, and landing. Although some regulations have been relaxed and wireless LAN usage has been allowed in some newer aircrafts, internet connection may not be available until the aircraft reaches a certain altitude, typically 10,000 ft., due to some technical difficulties, operation rules, and/or regulations.

Use of In-Flight Wi-Fi service is no longer limited to internet connection today. Many systems provide some flight information, travel information, weather and transportation information at the destination, and even allow in-flight shopping. Music/video streaming using an onboard media server is becoming popular. Since many people are carrying electronic gadgets today, they would probably want to use their own players, headphones, smart glasses, etc. In-Flight Wi-Fi service has a great potential for improving the services in the air, duplicating or replacing the current service / entertainment system with seat screens. Many prospective services may not always need internet connection. Therefore, it is becoming more important for airlines to provide hassle-free Wi-Fi service for any passengers at any time from gate to gate.

Some airlines provide roaming services to make it easy for passengers to get onboard the network. However, the current roaming systems have some security and usability problems, and the Wi-Fi industry is trying to introduce secure wireless LAN system with automatic roaming [1].

2.2 Security and Usability Problems

In order to avoid connecting to a rogue AP, server authentication needs to be enabled on user devices. Profile-based configuration is becoming popular to allow users configure their devices easily in a secure way. Since the profile may contain some digital certificates and cannot be manually typed in, a user has to install it before connecting to the secure network in an aircraft. With a roaming, the passengers do not need to sign-up for a special profile only for the flight. However, the current roaming systems are based on web-based authentication, and both the security and the usability are sacrificed.

User (or client) authentication is needed to enable per-user authorization and encryption. In a roaming environment, the authentication process basically runs between the user device and the authentication server at the user's Identity Provider (IdP), e.g., an ISP. The conventional methods require that the APs and IdPs are always connected. As shown in Figure 1, the backhaul network depends on satellite or Air-To-Ground (ATG) communication, and its disruption is inevitable due to safety regulations, weather conditions, radio coverage, etc. When the internet connection is disrupted, the user authentication is also affected and user devices may be disconnected from the AP, leading to bad user experiences.

2.3 Continuous Connection and Roaming

Continuous connection to the local network in an aircraft is crucial even when the internet connection is lost. We need a secure authentication method that can be used on an isolated network. A roaming feature is also desired in order to provide passengers with hassle-free and seamless network use while they are using multiple airlines. The roaming feature also needs to be disruption-tolerant, and therefore the conventional method is not appropriate.

[1] This work was submitted to AINTEC 2021 for review and accepted for poster presentation.

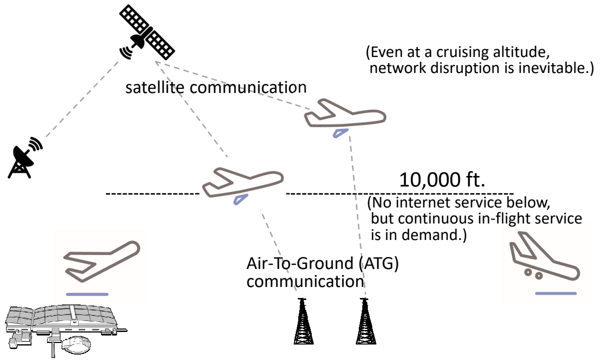

(Even at a cruising altitude,
network disruption is inevitable.)
satellite communication
10,000 ft.
(No internet service below,
but continuous in-flight service
is in demand.)
Air-To-Ground (ATG)
communication

Figure 1: In-Flight Wi-Fi service and internet connection.

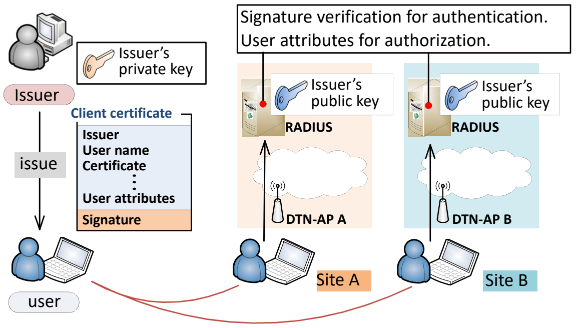


Figure 2: Certificate-based local authentication for disruption-tolerant wireless LAN service [2].

3 SECURE AND CONTINUOUS IN-FLIGHT WI-FI USING LOCAL AUTHENTICATION METHOD

3.1 Certificate-based Local Authentication

We developed earlier a secure Public Wi-Fi system whose authentication is tolerant of network disruption. The system was intended to enable local network use in temporary isolated areas affected by natural disasters [2]. Figure 2 shows the local authentication method.

The local authentication is realized by using EAP-TLS [3], which is one of the methods of Extensible Authentication Protocols used in WPA2 Enterprise. An account issuer creates a CA (Certificate Authority) certificate with its public key and distribute it to the regional RADIUS (Remote Authentication Dial-In User Service) servers in advance. The users receive client certificates in advance. By using the CA certificate, user authentication is possible at each region even without a wide area network connection. Our proposal of continuous and secure In-Flight Wi-Fi system is based on this local authentication method.

We assume that an airline or an ISP becomes an account issuer and that each aircraft corresponds to a service site. If a passenger receives a client certificate in advance, prior to getting onboard an aircraft, continuous connection to the in-flight service is realized. For roaming, the in-flight system needs to have CA certificates from multiple account issuers.

However, there is a limitation here. In our previous work [2], it was supposed that each prefecture was responsible for account issuing and that there were not so many network operators. The number of prefectures in Japan is 47 and the scalability was thought to be acceptable. The presented method would not work if there were hundreds of IdPs. Thus, it is not practical to accept directly the accounts from regular ISPs. A solution would be to delegate the user account handling to some airline alliances or solution providers of in-flight services since the number is limited to some extent.

Another challenge is the secure operation and handling of the CA certificates. There might be a threat of certificate leakage since the CA certificates are loaded on many aircrafts. User devices may not be able to use Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP) responders when the network is disrupted. A shorter life time of certificates would work, but it will increase expirations of client certificates leading to a bad user experience. Some developments will be needed in this regard.

3.2 Profile Issuing and Roaming

In-Flight Wi-Fi needs to provide various means for passengers to obtain a profile electronically at any time. In our system, the profile for the local in-flight connection can be downloaded at an airline website upon reservation, at home, airport, or anywhere on the ground where the internet is available, and also on the local online sign-up (OSU) system onboard the aircraft. Although such in-flight OSU may fail in the user and/or credit card verification process due to network disruption, a semi-online method using a voucher could help passengers get onboard the In-Flight Wi-Fi.

If a customer is subscribing to a Wi-Fi plan with roaming, associating the regular profile with the in-flight profile would be useful for enabling payment through the roaming partners like telecom companies and ISPs. There may be some possible ways and we are developing an automatic profile association method.

4 CONCLUSION

We have developed a disruption-tolerant user authentication method with roaming capability using digital certificates for realizing continuous and secure In-Flight Wi-Fi. Some more technical developments are under way. From the roaming business point of view, secure and trusted accounting is quite important. Some modification or adaptation of accounting will also be needed.

ACKNOWLEDGMENTS

This work was supported in part by JSPS KAKENHI No.19H04090.

REFERENCES

[1] Wireless Broadband Alliance. 2019. *In-Flight Connectivity – Wi-Fi Deployment & User Experience (Issue May 2019).* Retrieved Nov. 8, 2021 from https://wballiance.com/in-flight-connectivity/

[2] S. Kinoshita, T. Watanabe, Y. Yamasaki, H. Goto, and H. Sone. 2013. Fault-Tolerant Wireless LAN Roaming System Using Client Certificates. In *IEEE 37th International Conference on Computer Software and Applications (COMPSAC2013).* 822–823.

[3] D. Simon, B. Aboba, and R. Hurst. 2008. The EAP-TLS Authentication Protocol. In *RFC5216.*

AINTEC 2021 (Virtual)
14-17 Dec. 2021

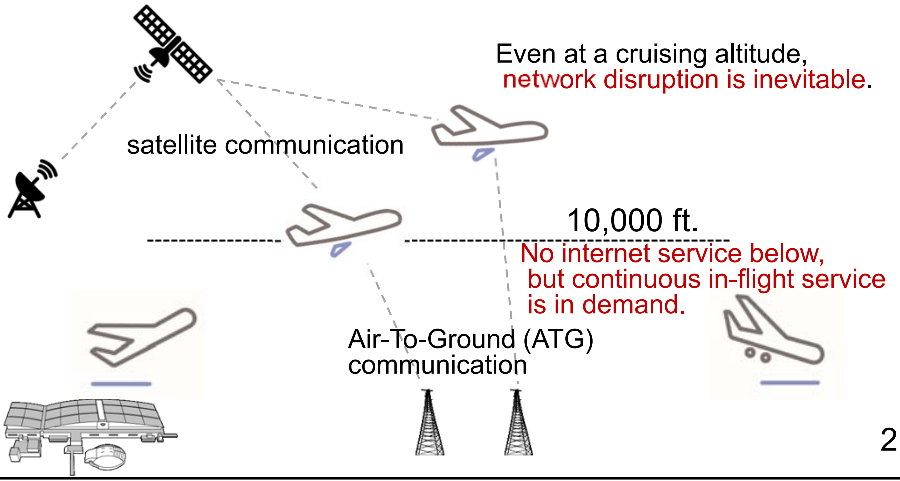
Continuous and Secure In-Flight Wireless LAN with Roaming

Hideaki Goto
Tohoku University, Japan

(Supported in part by JSPS KAKENHI No.19H04090)

In-Flight Wi-Fi and backhaul network

- Satellite / ATG network is evolving, but network disruption is inevitable. (weather, regulations, etc.)
- We want to avoid interruption of *in-flight services* such as music/video streaming, shopping, etc.


Even at a cruising altitude,
network disruption is inevitable.
satellite communication
10,000 ft.
No internet service below,
but continuous in-flight service
is in demand.
Air-To-Ground (ATG)
communication

In-Flight Wi-Fi in new era

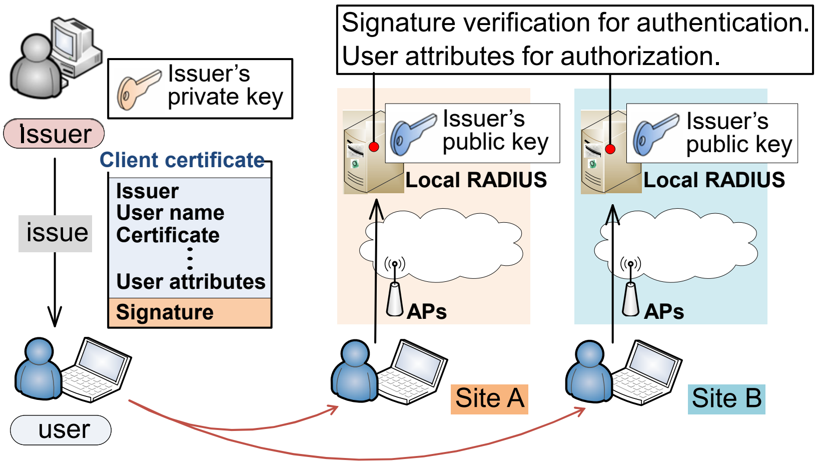
- *Various services* are depending on Wi-Fi connection.
- *Continuous connection* to the aircraft network is necessary for every passenger,
  even during backhaul network disruptions.
- *User (client) authentication and secure connection means* (802.1X, Passpoint) are required for
  - □ security and privacy protection,
  - □ hassle-free, automatic connection with *roaming* (e.g. OpenRoaming),
  - □ better services for subscribers / valued customers.

Research Objectives

- Sort out prospective use cases and challenges.
- Develop a continuous and secure In-Flight Wi-Fi system capable of roaming with many telcos and ISPs.
  (disruption-tolerant authentication method)

Certificate-based local authentication

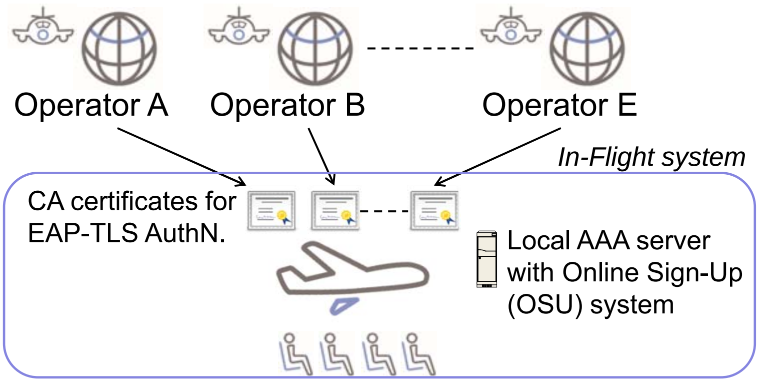
- Originally developed for disaster- and disruption-tolerant Wi-Fi system for disaster-affected areas. (COMPSAC 2013)
- User (client) authentication is possible locally by using EAP-TLS.



Signature verification for authentication.
User attributes for authorization.

Local authentication in In-Flight Wi-Fi

- A limited number of operator groups, such as airline alliances, provide CA certificates and issue client certificates.
- A challenge exists in secure operation and handling of the CA certificates as many aircrafts are carrying them.
  (detailed architecture design is in progress)


Operator A
Operator B
Operator E
In-Flight system
CA certificates for EAP-TLS AuthN.
Local AAA server with Online Sign-Up (OSU) system

Summary

- We have analyzed some prospective use cases of In-Flight Wi-Fi and technical challenges to realize them.
- We have developed an adaptation of the certificate-based local authentication method to the In-Flight Wi-Fi system.
  - Roaming is possible, accepting user credentials from some operators.
  - A Proof-of-Concept system is under development.
  - Some more refinements will be needed, especially in secure system operation and business perspectives.

Hope you enjoy much better In-Flight Wi-Fi in the near future.