Abstract: Wireless LAN Roaming enables users to be authenticated and authorized for access to networks at various places they visit. The largest roaming federation today is probably eduroam developed for research and education institutions. There have been some projects for developing roaming federations for public wireless LAN services as well. Since the introduction of the Next Generation Hotspot concept, the need to interconnect these roaming federations has emerged. However, some technical problems exist and these need to be addressed simultaneously. In this paper, we analyze existing roaming systems and develop an inter-federation roaming architecture with the aim of realizing a worldwide Wireless LAN roaming system that would accommodate eduroam. To realize realm-based routing of authentication requests across different federations and to achieve system scalability, the roaming architecture is designed to use regional hubs instead of a single exchange hub. We also aim to develop an actual roaming platform for secure public wireless LAN services based on the developed architecture. The developed platform was implemented and tested in the City Wi-Fi Roaming trials conducted by the Wireless Broadband Alliance.

Keywords: inter-federation roaming, wireless LAN roaming, identity federation, eduroam, next generation hotspot (NGH)

1. Introduction

Network roaming enables users to be authenticated and authorized for access to the Local Area Networks (LANs) at various places they visit. As Wireless LANs (WLANs) have become more popular, WLAN Roaming, also known as Wi-Fi Roaming, has drawn more attention for its ability to improve the usability and security of WLAN systems. The core technology used in WLAN Roaming is an identity federation[1], which mutually exchanges users’ digital identities and attributes stored across multiple WLAN operators. A Roaming Federation, also called Roaming Consortium (RC), is a group of operators providing the identity and/or access network services. The largest roaming federation in terms of the number of operators is probably eduroam developed for research and education institutions[2], [3]. There have been some projects for developing roaming federations for public WLAN services as well. Since the introduction of the Next Generation Hotspot (NGH) concept[4], the need to interconnect these roaming federations has emerged. This paper examines inter-federation roaming as a means to fulfill this need. The main objective of this work is to develop an inter-federation roaming architecture capable of realizing a worldwide WLAN roaming system that would accommodate eduroam. We also aim to develop an actual roaming platform based on the developed architecture. In addition, this paper provides an overview of the latest WLAN roaming system designs and explains recent directions in research and development.

A WLAN roaming system consists of some Authentication, Authorization and Accounting (AAA; read as “triple-A”) servers, intermediate proxies, and Access Points (APs). One of the widely used protocols in network roaming is Remote Authentication Dial-In User Service (RADIUS)[1], [5]. Commercial roaming systems are often realized by exchanging bilateral roaming agreements between operators. However, the architecture of the identity federation network, and the protocol used, are not always disclosed. To set a technical standard for WLAN roaming systems, the Wireless Broadband Alliance (WBA) has developed the Wireless Roaming Intermediary eXchange (WRIX) specification suite[6]. WRIX uses the RADIUS protocol, which supports the IEEE802.1x standard[7] (802.1x, hereinafter).

To date, only a few large-scale WLAN roaming federations have been established. As of this writing, eduroam[3] is one such federation and comprises about 100 member countries/territories. Some countries have hundreds of member institutions[8]. Another system called goviroam, launched in 2013 for public services and government organizations[9], is based on the same technology as eduroam. In the WLAN industry, on the other hand, the WBA is promoting Next Generation Hotspot (NGH) based on a technology called Passpoint[4], [10]. Passpoint, also known as Hotspot 2.0, is a new standard for improving the security and usability of public WLAN systems.

There is a great demand for deploying eduroam and govroam services at various off-campus sites. Suppose that some cities invite eduroam and govroam users to use their public WLAN services. If such a use case is achieved, we can expect that these services will contribute to the development of a better digital so-
ciety. Accordingly, the inter-federation roaming architecture that we develop must be able to accommodate eduroam and govroam. A conventional method for realizing this kind of service is to use the multi-SSID (Service Set Identifier) function of AP systems as shown in Fig. 1 (a). However, in this scheme, every individual WLAN operator has to have multiple gateway proxies and connect them to the proxies of all federations. Proxy-to-proxy connection work is laborious because it involves some negotiations between the operators, exchanging the IP addresses and shared secret keys of the proxies, firewall settings, and so on. To realize large-scale WLAN roaming, reducing the number of tasks required of human operators is crucial. More importantly, the multi-SSID scheme is not suitable for NGH environments because the basic idea of Passpoint is to realize sophisticated network selection by using wireless profiles from the operators (Fig. 1 (b)) instead of using dedicated SSIDs. Therefore, a new scheme for sharing the identity federation network is needed.

When we connect some large identity federation networks, we face problems with (1) routing, (2) scalability, and (3) access control. These three things are important for realizing an inter-federation roaming system. A widely used routing mechanism for exchanging authentication requests uses the “realm name” attached to the user’s credential. Both the eduroam and govroam federations have a dedicated and isolated identity federation network. It is not always easy to determine which federation the user has come from, simply by looking at the realm. If we directly connected the eduroam and govroam federation networks to provide users with both services via public WLAN APs, and if realm-based routing were available between the networks, eduroam users would be able to access any other APs dedicated to govroam and vice versa, despite the lack of a roaming agreement between the federations. To avoid such an access violation problem, an access control mechanism is required. Thus, to realize inter-federation WLAN roaming, the three abovementioned problems need to be addressed in the architecture design.

Some methods have been developed to deal with the routing and/or the scalability problems. The “Roaming Consortium Selection element,” introduced in Hotspot 2.0 Version 3.0[11], can be used to show the user’s home federation to intermediate proxies. Yamaki et al. proposed a similar approach[12]. However, these methods depend on the Passpoint and cannot provide backward compatibility for 802.1x-only devices. Although RadSec[13] combined with Dynamic Peer Discovery[14] has potential for addressing the routing and scalability problems, some development work for an access control scheme in multi-federation environments will still be needed.

The remainder of this paper is organized as follows. In Section 2, we analyze the identity federation networks of some existing roaming systems, derive a roaming architecture taxonomy, and identify the obstacles to realize inter-federation roaming. Section 3 proposes a roaming architecture for connecting large roaming federations. System operation and regulatory aspects are also discussed because they may strongly influence whether the system is adopted. In Section 4, we present our national roaming platform for public WLAN services based on the developed architecture as well as our field study through the WBA City Wi-Fi Roaming trials[15]. Then, we analyze the system performance, evaluate the scalability, and discuss the pros and cons of our architecture. Section 5 presents the conclusions.

2. Network Roaming and Identity Federation

2.1 Wireless LAN Roaming

2.1.1 Overview and Terminologies

Public WLAN services, which are probably better recognized by the name “Public Wi-Fi,” are intended to be used by various people in public spaces. There are some categories of Public Wi-Fi.

(1) Commercial (billed) Public Wi-Fi by WLAN Internet Service Providers (ISPs),

(2) Carrier Wi-Fi by telecom operators, mostly for traffic off-loading purposes, and

(3) Free Wi-Fi supported by governments, facility and shop owners, advertisers, and others.

Most current Free Wi-Fi systems worldwide are based on open wireless networks, and they are inherently insecure in terms of eavesdropping, session hijacking, content tampering, malicious code insertion, and even active attacks by rogue APs. 802.1x provides the means for detecting rogue APs and ensuring connection to genuine networks. For example, both eduroam and its variant govroam utilize 802.1x to provide users with a secure and automatic means of connection. Many Paid Wi-Fi and Carrier Wi-Fi services support 802.1x in addition to web-based user authentication over open wireless networks. As more and more people become aware of the security threats inherent in Free Wi-Fi, interest in 802.1x and its extension, Passpoint (Hotspot 2.0), continues to grow.

More recent Free Wi-Fi systems provide secure options as well. For example, Wireless@SG in Singapore[16] is accompanied by Wireless@SGx SSID, which supports 802.1x. LinkNYC in the United States (US)[17] provides Passpoint, which is also included in the technical specifications of the WiFi4EU program in the European Union (EU)[18] and are expected to be adopted in the future. To realize secured Free Wi-Fi, some kinds of user/client credentials are needed. Because each conventional system requires users to register individually, users had to sign up at every place they visited. To expand the footprint of service areas and to reduce on-site registrations, network roaming among different operators is quite useful as we see from the success of eduroam. In the eduroam system, users can access eduroam APs worldwide by using only one credential issued by his/her home institution. However, as of this writing, there is no worldwide
roaming system for Free Wi-Fi users, but the development of such a roaming federation has recently begun at the WBA.

Some key terminologies in this paper are as follows. Two parties exist in the simplest form of network roaming. Service Provider (SP) is defined as the entity providing network services. The term SP may refer to either the operator or the network system itself. Identity Provider (IdP) is defined as the entity providing users’ credentials and, in most cases, performing user authentication. IdP can be either an organization or an Authentication/Authorization/Accounting (AAA) server. An operator may play the role of IdP, SP, or both.

A Roaming Federation, also referred to as Roaming Consortium (RC), is a group of operators providing identity management and/or network services for mutual use of WLANs. Because the term RC is more common in the WLAN industry specification documents, we use RC instead of Roaming Federation in the explanations closely related to system implementation.

2.1.2 Identity Federation Network

There have long been some commercial WLAN roaming systems. However, the architecture of the identity federation network, and the protocol used, are not always available to the public. In general, open architectures and specifications are preferable from the perspective of security since they allow many security experts to challenge the security of the system and to ensure that no breach has been found. Since the roaming standard WRIX [6] was developed by the WBA and is based on a combination of 802.1x and RADIUS, we focus on RADIUS-based identity federation systems in this paper. In addition, we assume the use of the Extensible Authentication Protocol (EAP) [19], which has become indispensable in modern roaming systems for clearing various security and privacy problems.

The simplest form of identity federation network in a WLAN roaming system is as follows. An SP has one or more APs. An IdP is running a AAA server that handles user authentication. The APs are connected to the AAA server via RADIUS proxies, some of which may be run by third-party operators. After a user device has finished wireless network association with an AP, the authenticator inside the AP sends Access-Request messages to the AAA server and waits for a reply in the form of Access-Accept or Access-Reject. The authenticator grants or declines the access of the user device to the LAN based on the reply.

The roaming system of a federation can be realized by connecting the proxies and enabling the routing of RADIUS messages. The network topology may be different from system to system. Realm name has been widely used to identify the user’s home IdP where the user’s identity is stored. The username consists of “user ID” and “realm” concatenated using the @ symbol. The realm is often an operator name or a name aligned with the operator’s domain name of the Domain Name System (DNS). In the hub-and-spoke model, for example, multiple operators are connected to a hub, which is a RADIUS proxy run by a hub operator. The hub is in charge of finding the correct destination of RADIUS messages based on the realm. In general, the hub needs to have a pre-configured table for translating the realm to the IP address of the proxy at the user’s home IdP. The hub operator has some intermediary roles including the authentication of connected proxies, access control between the operators, and financial clearing/settlement when necessary.

2.1.3 eduroam and govroom

The eduroam system was developed for research and education institutions and has become a de facto standard for campus WLAN systems [2], [3]. The eduroam federation is probably the largest in the world in terms of the number of operators. As of this writing, more than 100 countries/territories are participating in eduroam [3], and some countries have hundreds of member institutions. For example, there are roughly 970 member institutions in Germany, 640 in the US, 360 in the United Kingdom (UK), and 280 in Japan, according to the eduroam website.

Figure 2 shows the basic architecture of eduroam [20]. The identity federation network of eduroam has hierarchically-connected RADIUS servers, proxies, and APs. The figure shows a scenario in which a user from institution D in Japan visits institution A in Australia and tries to connect a device to the LAN. When the user device is connected to the AP, RADIUS server A receives an Access-Request message. Because the realm attached to the username does not match that of institution A, the server determines that the user is a visitor and forwards the message to the federation-level RADIUS (FLR) proxy (.au) operated by an organization in Australia. Then, the proxy determines that the user is from a foreign country and forwards the request to one of the top-level proxies operated by the global eduroam operation team. Because the realm has the .jp country code top-level domain, the Access-Request message is forwarded to the FLR proxy in Japan, and it is finally delivered to the RADIUS server at the user’s home institution. User authentication is performed on the server at institution D, and the result is sent back to the AP.

The hierarchical structure of the network has some benefits not only in system scalability but also in system administration. Given that some countries may have several hundreds of universities, the administration of each FLR proxy may require a heavy workload. The administrator in each country is in charge of roaming system operations including compiling service operation rules, checking the eligibility of institutions, connecting the institutions’ proxies to the FLR proxy, and mediating necessary communications between operators. The system operation must follow the laws and regulations of that region in addition to the global rules defined in the eduroam Compliance Statement. Thus, the distribution of administration is important in many aspects.

2.1.4 Passpoint and the Next Generation Hotspot

This section provides a brief introduction of Passpoint and the Next Generation Hotspot (NGH). Because some technical information about Passpoint/NGH, particularly that of the network
architecture and the system operation, has not been well documented, we had to independently gather the information necessary to develop our inter-federation roaming architecture. The following contains some information we collected through our participation in the NGH trial conducted by the WBA in preparation for their roaming federation development.

Many shops, hotels, conference sites, and cities prefer using their own SSIDs for various reasons such as branding. However, using many different SSIDs substantially lowers the usability of a roaming system. Users need to configure their devices at each new location to access conventional WLAN roaming systems. The Wi-Fi Alliance and the WBA, both of which consist of network operators, have jointly addressed this problem and developed a new standard called Passpoint, also known as Hotspot 2.0[10]. Passpoint provides users with high usability and security similar to that of cellular phones by adding an automatic SSID selection mechanism to be used with the automatic connection function of 802.1x.

NGH is a conceptual standard based on Passpoint and WRIX standards. As of this writing, there are five NGH hub operators in the world and they form a hub group. Each WLAN operator is connected to one or more NGH hubs, thereby enabling roaming with other operators. There may be multiple RCs on the identity federation network created by the group of NGH hubs. NGH hub operators are in charge of access control to the respective roaming systems and can enable/disable roaming between particular operators.

In the current architecture in the NGH trial, a single RADIUS inter-connection between an operator and an NGH hub may be shared by identity federation networks of multiple RCs. Therefore, each operator does not need to establish multiple connections even when it belongs to multiple RCs. This is a great advantage in terms of reducing system administration workload and hardware. Some redundant connections may exist for improving service availability.

NGH hub operators perform access control for the RADIUS messages to separate the traffic of different roaming groups or federations. Access control can be based on realms, RADIUS attributes such as Operator-Name, IP addresses of proxies, and so on. An NGH hub operator acts as a neutral intermediary that enforces access control between the IdPs and the SPs.

2.2 Roaming Federation Taxonomy

Some roaming federations contain only a few realms, whereas others have many. Here we introduce two classes of federations according to the complexity of realm names.

Simple-realm Roaming Federation:
This class consists of roaming federations having only a limited number of realms or realms easily distinguishable from those of other federations by using regular expressions. If the number of realms is small, WLAN/hub operators can use a small realm—federation lookup table for the realm-based routing. Even if the number of realms is large, the federation can be easily identified by detecting a keyword specific to the federation in the realm. WLAN operators having only a few realms also fall into this class.

Complex-realm Roaming Federation:
This class consists of all the roaming federations not included in the other class. Federations have many realms that cannot be easily separated from the realms of other federations. No operator can easily identify which federation the presented realm belongs to. The eduroam and govroam systems are the typical examples. WLAN operators having a large number of realms also fall into this class.

2.3 Challenges in Inter-federation Roaming

When we try connecting the identity federation networks of large federations, routing and scalability problems arise. The simplest way to connect federations is probably to use a single global hub, as shown in Fig. 3. The figure shows the architecture of an inter-federation roaming system and explains the problems in the realm-based routing. Suppose we have some roaming federations and independent network operators connected to the hub. There are some SPs available to provide WLAN service to all users. Although many SPs may belong to the federations shown at the top of this figure, we intentionally separate them to simplify the flow of RADIUS messages. Every federation has at least one gateway proxy connected to the hub. Each SP receives an authentication request in the form of a RADIUS message from the user’s device and sends it to the user’s home federation or operator.

If the number of operators is small, the hub can easily identify the user’s home IdP by using a small Realm–Operator lookup table consisting of realms, roaming operator names, and their RADIUS proxy addresses. Realm-based routing is simple in this case. Suppose there are one or more complex-realm federations which have hundreds of realms. The hub may not always be able to find the user’s home federation simply by looking at the realm because generally no federation identifier is embedded in it. It would be possible to assemble a large Realm–Operator list if the number of realms is limited. However, this scheme is not sufficiently scalable to accommodate the current large federations.

In the eduroam federation, there are tens of thousands of realms. It is not practical for the hub operator to compile a list of all the realms in the world and keep it up to date. We will analyze the scalability problem in depth in Section 4. In addition, as long as the destination federation remains unknown, access control such as enabling/disabling inter-federation RADIUS message forwarding is also impossible.

2.4 Other Solutions

Solutions addressing routing and scalability problems have been proposed or are under development.
A new element called “Roaming Consortium Selection element” was introduced in Hotspot 2.0 Version 3.0[11]. During the profile matching process between the user’s device and the AP, the element points to the user’s home roaming federation and makes the selection of the identity federation network possible. Thus, both routing and scalability are solved naturally. Yamaki et al. proposed a similar method[12] using the Organization Identifier (OI) defined in the Hotspot 2.0 specification[10]. The user’s device has to prepend the OI to the username in this method so that the AP can find the user’s home federation. These methods require new hardware that is compliant with the Passpoint standard and works only in Passpoint-enabled environments. Accordingly, these solutions do not provide backward compatibility for 802.1x-only devices whereas current Passpoint-based AP systems generally can.

The inter-federation roaming system that we develop needs to support both 802.1x-only and Passpoint devices because it does not seem practical to upgrade all devices in the world to support Passpoint in a short period of time. Passpoint is still in an early stage of adoption around the world, and a Passpoint-based eduroam system is under development, as this paper represents.

Thus, support for legacy devices is crucial for faster adoption of an inter-federation roaming system in preparation for an NGH system.

Another approach is to use RadSec[13] combined with Dynamic Peer Discovery (DPD)[14]. This method uses Naming Authority Pointer (NAPTR) records in the DNS to allow the SP to find the AAA server of the user’s home institution, and ultimately enables a direct and secure connection between the SP and the home IdP. The SP (or hub) does not need to have a lookup table showing which federation the IdP belongs to. Thus, the routing problem, and the scalability problem, can be solved naturally. Access control remains as the problem to be addressed. Public Key Infrastructure (PKI) is used for authorization in peer-to-peer connections. However, the PKI and its operation designs for large-scale, inter-federation roaming systems remain to be developed.

Although we expect a good roaming system utilizing RadSec+DPD sooner or later, constructing a roaming system based on conventional static RADIUS networks has some advantages. First, such system can be used as a fall-back identity federation network when discovery has failed for a reason, most likely related to DNS lookup failure or missing NAPTR records. Second, system adoption would be much easier for participating operators. Even in the eduroam federation, hierarchical networks are still widely used because of their simple system configuration.

Only about 10 countries have introduced DPD as of this writing.

3. Inter-federation Roaming Architecture

This section presents the inter-federation roaming architecture we developed and explains the details. As discussed earlier, the following problems need to be addressed.

1. RADIUS message routing
2. Scalability
3. Access control

Although the combination of RadSec and DPD has received high expectations, its potential remains difficult to measure because the PKI design and operation have not been fully developed or reported. Therefore, in our primary work presented here, we use a static RADIUS network based on the conventional architecture. A fall-back identity federation network is indispensable, as can be seen in eduroam, and the static network should still be useful.

The simplest and most straightforward way to realize an identity federation across multiple federations might be the establishment of a global hub, as shown in Fig. 4. We assume that a global hub would have a federation list of all the realms in the world. The list may use some regular expressions to group some realms into clusters. For example, if the hub sees the realms with the .ac.jp base realm attached, they can be captured by the regular expression “*\.ac\.jp” immediately associated with the eduroam federation.

However, there are still a large number of realms that cannot be grouped, and this single-hub architecture suffers from routing and scalability problems. In addition, the hub operator will need to frequently communicate with federation representatives and IdP operators to compile a list of all the realms in the world and to keep it up to date.

Some countries in the eduroam federation have hundreds of member institutions. The number of potential members exceeds one thousand in some countries. Thus, there are tens of thousands of realms in the world. If we used one global hub only as a federation exchange point, the Realm–Federation translation table would inevitably become huge. In addition, using regular expressions for realm matching is necessary in eduroam to allow each member institution to use arbitrary sub-realms in addition to the institution’s own base realm. For example, the use of <subRealm>.example.ac.jp is allowed in addition to the base realm (example.ac.jp), where the sub-realm part can be arbitrarily changed without registering with the hub. Therefore, the hub suffers not only from congestion of RADIUS messages but also from higher computational costs for the realm matching because the search algorithm may fall back to a linear search when regular expressions are used.

Here, we propose an inter-federation roaming architecture using “regional hubs.” Figure 5 shows a diagram of the architecture, and Fig. 6 shows the details of the regional hubs. We have adopted the eduroam architecture[20] because its routing capability and scalability have been verified by worldwide operations for around fifteen years.

Suppose there are several complex-realm federations and each federation has a local operator in each country. Not all countries have joined all federations and there are some missing hubs.
Simple-realm federations and operators are omitted in Fig. 5 for simplicity. We add an inter-federation hub layer in which each country has a regional hub and a national hub. The national hubs of all federations are connected to the regional inter-federation hub. The inter-federation hub layer and the NGH hubs are in charge of exchanging RADIUS messages between countries. The NGH hub operators provide roaming and financial clearing services to various operators including telecoms. Thus, roaming via telecom operator, WLAN operator, or another federation can be achieved via the NGH network. The internal architecture of the NGH hub operator group is not included in our proposed architecture.

When the NGH hubs can easily locate the operators simply by looking up the realms in a small realm list, the corresponding RADIUS messages are sent to the operators directly. The regional hub in each country receives all the other RADIUS messages with the realms having the corresponding country code Top Level Domain (ccTLD) from one of the NGH hubs. The reason for gathering all messages is that the NGH hubs cannot always find the correct destination when complex-realm federations are involved. For Japan, for example, we ask NGH hub operators to send all RADIUS messages with the .jp realm to the regional hub as the default destination. If we are sure that some particular groups of realms will never be handled by the regional hub, the NGH hub operators may block the sending of messages with such realms to the regional hub by detecting the keywords specific to the groups.

Figure 6 shows the regional hub in a given country. The regional hub is in charge of RADIUS message routing in that country. RADIUS message routing and forwarding are realized by using the regional federation list that contains the exact realms and some grouped realms in regular expression in that country. Thus, once an authentication request reaches the regional hub, the correct federation can be identified. When the regional hub receives a RADIUS message with a foreign realm, it forwards the message to the sibling hub in the country specified by the Top-Level Domain (TLD) in the realm because the destination hub is probably in charge of handling the RADIUS message. The message may alternatively be sent to an NGH hub and delivered to the regional hub in the corresponding country through the NGH hub network.

We assume that the local operator of each federation publishes a local realm list and keeps it up to date. The regional hub operator collects the local realm lists from all the federations and assembles the regional federation list. The means for collecting realm lists is not specified in our proposal in this paper. One plausible way is to run a web crawler on the hub to collect the realm lists periodically and automatically. Another way is to implement automatic roaming consortium discovery, a method we presented in our previous paper [21].

Note that the regional federation list is much smaller than the federation list in the global hub solution. This contributes to increasing the scale of the entire roaming system.

4. Field Study and Discussions

4.1 NGH Testbed and City Wi-Fi Roaming Trials

In addition to our main objective of developing an inter-federation roaming architecture, we aimed to develop an actual inter-federation WLAN system for realizing secure and convenient Public WLAN combined with eduroam and govroam. To achieve this, we developed an NGH testbed system as our national roaming platform and began a pilot service for NGH-based public WLAN. The service was later named “Cityroam” for better publicity and recognition. In addition, we participated in the City Wi-Fi Roaming trials [15] conducted by the WBA in 2017 and 2018 to test, demonstrate, and promote our inter-federation roaming architecture. The trials were part of the NGH trial, in which major telecom operators and cities around the world participated. We provide only a summary here because the details of Cityroam and the trials were reported in our previous conference paper [22].

We developed the NGH testbed based on the proposed inter-federation roaming architecture (Fig. 6). A RADIUS proxy called “JP hub” acts as the regional hub. The hub is connected to the eduroam network via the eduroam infrastructure in Japan. Although Japan is not a member of govroam, we assumed that it exists as a dummy federation. The JP hub is connected to some telecom operators and WLAN ISPs around the world via the NGH hub operator group. Some WLAN ISPs in Japan are directly connected to the hub and provide Cityroam, the nationwide federated Public WLAN service. We tested the roaming system and confirmed that it worked as intended by using some eduroam accounts and Passpoint profiles to connect to the service. Thus, we confirmed that the Cityroam member operators successfully developed Japan’s first Public WLAN service based on Passpoint/NGH. Because most APs are configured to emit the dedicated “eduroam” SSID in addition to the SSID with Passpoint, users from participating institutions can access the WLANs in public areas without changing the configuration of their devices. Thus, a seamless, off-campus eduroam service has been realized.

Tohoku University participated in the second City Wi-Fi Roaming trial conducted by the WBA in 2017, becoming the
world’s first eduroam member on the NGH infrastructure [22]. When we connected the JP hub to one of the NGH hubs, we asked the group of NGH hub operators to forward all .jp realms, except those of known operators, to the JP hub as the default route. We also enabled Passpoint-based WLAN roaming on the APs provided by our member operators in Japan to accept users from the telecom and WLAN operators during the trial. We conducted field tests in some cities where Passpoint-based Public WLAN services were available. Figure 7 shows one of our test scenes. The smartphone was successfully authenticated and accessed the Public WLAN in Leeds, UK, by using an eduroam credential issued by Tohoku University. In the next year, we invited Norway and the Netherlands to participate in the third trial.

### 4.2 Performance Analysis of Realm-based Routing

A large number of realms, as well as RADIUS messages for roaming, are dispersed naturally in the proposed inter-federation roaming architecture. Because we have not seen much actual traffic, a traffic analysis will be performed in a future study. Here, we analyze the system scalability and performance in terms of the number of realms and the RADIUS message traffic. To estimate the prospective performance of the inter-federation roaming system, we conducted an experiment to analyze performance degradation on an actual proxy.

RADIUS proxy software can benefit from a fast search technique, such as a hash table, if the realm search can be performed by exact string matching. However, as explained in Section 3, a federation search at the regional hub would fall back to a linear search and affect the proxy performance when some large complex-realm federations exist and when regular expressions are used. In fact, use of regular expressions is common in many eduroam member countries, as described in the next section.

We used FreeRADIUS installed on a personal computer equipped with an Intel Core i5-6500 (3.2 GHz) processor since the RADIUS software has long been commonly used in the eduroam federation. Table 1 shows the memory space required and the running time for various numbers of realms. We created 10,000 dummy realms with random institution names in the form of `<instName>.jp`, where `<instName>` is a random string consisting of 12 alphanumeric characters. We created test accounts on the same proxy to enable smooth authentication.

We created regular expressions "<~(".+\.)?<instName>\.jp$" using the created random realms, and registered some or all of them in the proxy.conf configuration file. For example, in the first row of Table 1, 100 random realms are registered, and the user authentication is performed for each realm by using radtest command. Note that the measured running time includes overhead originating from the radtest command startup, communications, authentication process, and so on.

The server clearly shows linear behaviors in space and time. As the number of realms grows, the authentication time per user grows proportionally. When we loaded 10,000 realms, the authentication time per user became 6.15 ms. Because the value is obtained by taking the average of all users (with the same number of realms), the maximum time required is nearly double this figure, which is for a user whose realm is listed at the end of the proxy configuration file. The matching process per realm regular expression took roughly 0.6–0.7 μs.

The program startup time was also affected as the number of realms grew. In this test scenario, the realms in regular expression could be loaded statically only once at the program startup. FreeRADIUS does not support dynamic changes in the proxy configuration file. When we registered 10,000 realms, the startup time increased significantly (>3.7 s).

It would be possible to mitigate the performance degradation in the realm matching process by introducing a mechanism to extract the institutions’ base realms from the regular expressions so that a fast search algorithm can be used in the proxy software. However, the linear-time processing during startup cannot be eliminated and its long duration would be problematic in real services. It is therefore recommended to add a mechanism that enables adding and removing realms in regular expression dynamically without restarting the software.

### 4.3 Scalability Analysis

In this section, we analyze the scalability of the system by using the measured proxy performance described in Section 4.2 and the scales of some existing roaming systems.

The eduroam federation is currently thought to be the largest in the world, and the govroam federation is probably the second largest with complex realms. In the eduroam federation, the use of three-level realms is common in some limited countries. For example, most universities in Japan use `<instName>.ac.jp`, where `<instName>` is the institution name. These realms can be easily associated with the eduroam federation. Similar base realms are .ac.uk in the UK, .edu.au in Australia, and .edu.cn in China. As of this paper writing, 279 institutions are participating in eduroam JP, the eduroam federation in Japan, while about 1,170 higher education institutions exist in the country. The breakdown of the registered realms is as follows:

- .jp
- .ac.jp
- .go.jp
- .or.jp
Pros and Cons

Table 2 shows a comparison of roaming systems including contributions to the solution for each problem as well as limitations, which may affect its adoption and operation.

Pros:
The developed roaming architecture realizes an inter-federation roaming system with worldwide scalability, thereby achieving the objectives of our work. Although other solutions would be possible, we are not aware of any that have been developed. Our architecture is able to accommodate eduroam and govroam, both of which are complex-realm federations, and supports both conventional 802.1x-based WLAN and Passpoint-based roaming systems.

Regional hubs are introduced to increase scalability in terms of the number of realms and RADIUS message traffic, as described above. In addition, a hierarchical architecture similar to the eduroam architecture [20] has some advantages from a system administration point of view. Each federation has a local operator in each country as described in Section 2.1.3. The operator is in charge of the roaming system operation in the country and has to communicate with the federation member institutions such as universities. Using the local language makes the operation within each country much easier, while the local operator has to use English only when communicating with the federation’s global operation team. The regional hub operator in the inter-federation roaming system can act as a representative of the federations in the country and help the federations’ local operators to connect their infrastructure to other federations, public WLANs, and/or telecom operators around the world. Joining international roaming systems was previously cumbersome, especially for small operators, because the work includes exchanging roaming agreements.

Hub operation on a per country basis also has some advantages from the perspective of business operations and regulatory compliance. Some countries have stricter regulations on network use and thus institutions may not be able to join all WLAN roaming federations. Some operators do not want to allow roaming within their own countries to avoid business conflicts. Because the regional hub can be made as a third-party independent intermediary, the presented architecture is also expected to be useful in implementing and ensuring access controls on a per country basis even after the introduction of RadSec+DPD in the future.
erator that can be independent and neutral across multiple federations. Because all RADIUS messages go through the regional hub, some operators might feel uncomfortable with the arrangement and disputes might arise over the operation of the hub. These issues may be considered cons. A prospective solution would be that the country delegates the operation of its regional hub to one of the NGH hub operators, which is considered to be neutral.

Another limitation might exist in access controls. In the current NGH system, NGH hub operators are in charge of access control based on roaming agreements. An NGH hub must block RADIUS message forwarding between operators or federations who do not have a roaming agreement. As written in Section 2.1.4, an operator acting as an SP can be identified by the RADIUS Operator-Name attribute. If there is more than one complex-realm federation, the NGH hubs will be unable to find the federation to which the RADIUS messages should be delivered by the regional hub. In this case, the possible options may be (1) delegating access control to the regional hubs, and (2) handling the complex-realm federations as a unified group, giving up separate access controls.

To avoid further complexities in the inter-federation roaming system, we strongly recommend embedding federation-specific identifiers in realms when new WLAN federations are developed.

5. Conclusions

Providing users with secure and convenient public WLAN services is quite important. WLAN roaming with user authentication is crucial for solving various security and usability problems. Considering the emerging need to interconnect large roaming federations, we have developed an inter-federation roaming architecture that realizes a worldwide WLAN roaming system, which also accommodates eduroam. Technical problems exist in (1) RADIUS message routing, (2) scalability, and (3) access control, which must be addressed simultaneously in the development of our inter-federation roaming architecture, which has successfully provided solutions to all three problems.

Based on our architecture, we implemented an NGH-based WLAN roaming system in Japan and established a nationwide secure public WLAN service supporting both conventional and Passpoint-enabled devices. The functionalities of our roaming system have been confirmed through experiments including those conducted as part of the WBA City Wi-Fi Roaming trials. We have achieved (a) an inter-federation roaming architecture, (b) the world’s first eduroam service based on NGH infrastructure, and (c) Japan’s first NGH-based secure public WLAN service.

The distributed architecture using regional hubs has some advantages, not only in terms of scalability but also system administration and regulatory aspects, which may differ from country to country. Our architecture is expected to contribute to increased scalability compared with the current global hub architecture. Although RadSec-based roaming system will be fully developed and widely adopted in the near future, we think that a roaming system using static RADIUS networks will still be necessary, particularly as supplemental and/or fall-back systems. Regional hubs will also remain useful for implementing an inter-federation gate-way that has some intermediary roles.

Given that we have not seen much traffic so far, we will conduct a performance analysis using real traffic in a future study. Once the inter-federation roaming network becomes widely used, it will be necessary to support multiple virtual roaming federations on the shared identity federation network, and thus further research is needed.

Acknowledgments

This work was supported in part by JSPS KAKENHI No.19H04090. Collaboration with the Wireless Broadband Alliance (WBA) was made possible thanks to a Memorandum of Understanding between the WBA and GÉANT.

References

[1] Pérez-Méndez, A., Pereñíguez-García, F., Martín-López, R., López-Millán, G. and Howlett, J.: Identity Federations Beyond the Web: A Survey, IEEE Communication Surveys & Tutorials, Vol.16, No.4, pp.2125–2141, Fourth Quarter (2014).
[2] Florio, L. and Wierenga, K.: Eduroam, providing mobility for roaming users, Proc. EUNIS2005 (2005).
[3] eduroam, available from (https://www.edurom.org) (accessed 2020-04-27).
[4] Wireless Broadband Alliance: NEXT GENERATION WI-FI, available from (https://www.wbballiance.com/what-we-do/b/next-generation-wi-fi) (accessed 2020-04-27).
[5] Rigney, C., Willens, S., Rubens, A. and Simpson, W.: Remote Authentication Dial In User Service (RADIUS), IETF RFC2865 (2000).
[6] Wireless Broadband Alliance: Wi-Fi Roaming Standard (WBA WRIX), available from (https://wbballiance.com/resource/wi-fi-roaming-standard-wba-wrix/) (accessed 2020-04-27).
[7] IEEE Std 802.1X-2010, Port-Based Network Access Control (2010).
[8] eduroam JP, available from (https://www.edurom.jp/) (accessed 2020-04-27).
[9] govroam, available from (https://www.govroam.be/) (accessed 2020-04-27).
[10] Wi-Fi Alliance: Wi-Fi CERTIFIED Passpoint™ (Release 2) Deployment Guidelines Rev. 1.1, December 7 (2016).
[11] Wi-Fi Alliance: Hotspot 2.0 Specification Version 3.0, Feb. 28 (2019).
[12] Yamaki, H., Yamada, Y., Kato, Y., Kobayashi, E., Saotome, Y. and Matsumoto, D.: Integration of Wifi Services Based on the IEEE802.11u Standard, Proc. CCATS 2015, pp.132–137 (2015).
[13] Winter, S., McCauley, M., Vennaas, S. and Wierenga, K.: Transport Layer Security (TLS) Encryption for RADIUS, IETF RFC6614 (2012).
[14] Winter, S. and McCauley, M.: Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS Based on the Network Access Identifier (NAI), IETF RFC7585 (2015).
[15] Wireless Broadband Alliance: City Wi-Fi Roaming, available from (http://worldwidoday.com/city-wi-fi-roaming/) (accessed 2020-04-27).
[16] Wireless@5G, available from (https://www.imda.gov.sg/programme/listing/Wireless-At-5G/) (accessed 2020-04-27).
[17] LinkNYC, available from (https://www.link.nyc/) (accessed 2020-04-27).
[18] European Commission: WiFi4EU | Free Wi-Fi for Europeans, available from (https://ec.europa.eu/digital-single-market/en/policies/wifi4eu-free-wi-fi-europeans) (accessed 2020-04-27).
[19] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J. and Levkowetz, H.: Extensible Authentication Protocol (EAP), IETF RFC3748 (2004).
[20] Wierenga, K., Winter, S. and Wolniewicz, T.: The eduroam Architecture for Network Roaming, IETF RFC7593 (2015).
[21] Irie, K. and Goto, H.: Automatic Roaming Consortium Discovery and Routing for Inter-federation Wireless LAN Roaming System, Journal of Information Processing (JIP), Vol.28, pp.378–386 (2020).
[22] Goto, H.: Cityroam, Providing Secure Public Wireless LAN Services with International Roaming, Proc. RTUWO’18, pp.204–208 (2018).
Hideaki Goto received his M.Sc. degree in physics in 1992, and his Ph.D. degree in engineering in 1995 from Tohoku University in Japan. He has been an Associate Professor of Tohoku University since 2001. His research interests include pattern recognition, document image analysis and recognition, identity federation, wireless networks, and information security. He is a member of IPSJ, IEICE, and IEEE Computer Society. He has been a member of the Global eduroam Governance Committee (GeGC) at GÉANT for four terms.