Easy-to-Deploy Wireless Mesh Network System with User Authentication and WLAN Roaming Features*

Tomo NIIZUMA†, Nonmember and Hideaki GOTO††, Member

SUMMARY Wireless LAN (WLAN) roaming systems, such as eduroam, enable the mutual use of WLAN facilities among multiple organizations. As a consequence of the strong demand for WLAN roaming, it is utilized not only at universities and schools but also at the venues of large events such as concerts, conferences, and sports events. Moreover, it has also been reported that WLAN roaming is useful in areas affected by natural disasters. This paper presents a novel WLAN roaming system over Wireless Mesh Networks (WMNs) that is useful for the use cases shown above. The proposed system is based on two methods as follows: 1) Automatic authentication path generation method decreases the WLAN roaming system deployment costs including the wiring cost and configuration cost. Although the wiring cost can be reduced by using WMN technologies, some additional configurations are still required if we want to deploy a secure user authentication mechanism (e.g. IEEE 802.1X) on WLAN systems. In the proposed system, the Access Points (APs) can act as authenticators automatically using RadSec instead of RADIUS. Therefore, the network administrators can deploy 802.1X-based authentication systems over WMNs without additional configurations on-site. 2) Local authentication method makes the system deployable in times of natural disasters, in particular when the upper network is unavailable or some authentication servers or proxies are down. In the local authentication method, users and APs can be authenticated at the WMN by locally verifying the digital certificates as the authentication credentials.

key words: wireless mesh networks, WLAN roaming, RADIUS, RadSec, EAP-TLS, eduroam

1. Introduction

Wireless LAN (WLAN) roaming systems, also known as federated WLAN systems, enable the mutual use of WLAN facilities among multiple organizations. One of the successful systems is eduroam, which is for research and education institutions world-wide [2]. In a basic WLAN roaming service, identity information of a roaming user is first submitted to the network service provider (SP), and then transferred to the user’s Identity Provider (IdP) in a federation.

As a consequence of high demand for the WLAN roaming, it is utilized not only at universities and schools but also at the venues of large events such as concerts, conferences, and sports events. Moreover, it is also pointed out that the WLAN roaming is useful at the affected areas of natural disasters since controlling the access and its priority based on user’s attributes can be introduced for prioritizing the important data packets such as for first-aid and life-saving. In these kinds of use cases, it is likely that no WLAN infrastructure is deployed at first, and the administrators have to deploy it from scratch on-site. Deployment should be made quicker and easier to save labor, time, and money.

The deployment costs of a conventional WLAN roaming system are generally high since the deployment requires the new access network preparation, wiring the cables to the Access Points (APs) and/or switches, and configuring the APs and servers. Wireless Mesh Network (WMN) technologies are expected to lower the wiring cost of the wireless network deployment as the APs in WMNs are interconnected by radio. In addition, WMN helps the local network deployment at some sites where people do not have enough backbone network infrastructure. Moreover, the AP system in [3] makes it possible that the institutions or the departments joining the WLAN roaming service do not need to prepare their own access networks. The system utilizes a tunneled connection by EtherIP [4] to the centralized managed access network.

In order to deploy a secure WMN, authentication of both user and AP is needed, and the secure authentication mechanism such as IEEE 802.1X [5] (hereinafter referred to as 802.1X) should be employed. However, some additional configurations are still needed on-site to deploy a secure authentication system over WMNs. In the RADIUS protocol [6], which is generally used for user authentication in wireless networks, the configurations between the APs and the RADIUS servers are necessary so that the APs can work as authenticators in 802.1X. To deploy a secure WMN based on 802.1X, the configurations must be done on per-AP basis in the WMN and it takes more time as the number of APs increases. In [7], Winter developed an eduroam AP system which uses RadSec to generate authentication paths automatically. Nevertheless, the wiring to the AP is still required as the deployment over WMNs is not considered in the system.

In time of natural disaster, moreover, a disruption-tolerant wireless authentication mechanism is also needed. Such a mechanism enables us to deploy a secure wireless network even when the upper network is unavailable or some authentication servers or proxies are down for some reasons. The recovery process should also be automatic.

In this paper, we propose a novel WLAN roaming system over WMNs which reduces the deployment costs in-
cluding the wiring and the configurations for the WLAN roaming. In the proposed system, the APs can become authenticators automatically by using RadSec [8] instead of RADIUS. Furthermore, the local authentication deployment method on WMNs is shown. The APs in the WMN can authenticate users and other APs on-site using the digital certificates without any communication with authentication servers/proxies in the upper networks. Although our contribution is not intended to improve WMN routing performance, the automatic authentication path generation method and the local authentication method stabilize authentication delay in wireless multi-hop environments.

Our original contribution is the development of a new WMN authentication system architecture making it possible to authenticate APs and users on the WMNs in a disruption-tolerant way. The tolerance of network disruption is achieved by the automatic authentication path recovery on WMNs utilizing the certificate-based local authentication method. The automatic recovery is possible since mesh APs in WMNs can become authenticator automatically.

This paper is organized as follows. Section 2 describes the overview of conventional WLAN roaming systems. In Sect. 3, we present two WLAN roaming system deployment methods over WMNs. Section 4 shows the implementation of the proposed system and the performance evaluation. Finally, Sect. 5 summarizes this paper and mentions the future work.

2. Overview of WLAN Roaming Systems

2.1 802.1X-Based WLAN Roaming System

IEEE 802.1X is known as a secure authentication framework widely employed in enterprise and campus WLAN systems. Figure 1 shows the user authentication mechanism in eduroam. The system consists of Supplicants built into user terminals, Authenticators in APs, Authentication proxies, Authentication servers. Since RADIUS protocol is used as the authentication protocol to carry authentication traffic, RADIUS servers can be Authentication proxies and Authentication servers.

To enable a roaming user to obtain network access at a Service Provider (SP), the authentication by Extensible Authentication Protocol (EAP)[9] is executed as follows.

1) When a roaming user requests for network access, the user’s identity is sent to the AP.
2) The user’s identity is forwarded to the RADIUS authentication server of the user’s IdP through several RADIUS proxies in the federation network. The destination of the next-hop RADIUS proxy is determined by the realm [10] included in the user’s identity.
3) If the RADIUS authentication server has received the authentication request including the user’s identity, the server sends its server certificate back to the user’s terminal. The terminal validates the server certificate and then, when it is valid, a TLS tunnel is established between the user terminal and the RADIUS authentication server.
4) The terminal sends the authentication credential to the RADIUS authentication server via the TLS tunnel. The type of submitted credential varies depending on the EAP method.
5) The RADIUS authentication server validates the user’s credential and sends back the authentication result as a RADIUS Access-Accept/Reject. If the result is Access-Accept, the AP permits the user to access the network, otherwise it forbids.

2.2 RADIUS-Based Roaming System Deployment

To deploy a WLAN roaming system where EAP messages is transported by RADIUS protocol, the following tasks should be done.

(a) The new deployment of the access LAN or Virtual LAN is required besides the already existing network to enable guest network use.
(b) Wiring some APs to the backhaul network is required. After that, IP addresses need to be assigned on them.
(c) The same secret key must be configured on both the authenticator and the RADIUS proxy in the federation network. The configuration allows the AP to forward RADIUS authentication packets to the RADIUS proxy connected to the federation network.

In particular, the configuration in (c) requires writing the pairs of IP address and shared secret at both side in the RADIUS proxies/servers and the APs working as RADIUS clients. This procedure is called authentication path generation in the following part of this paper. In the practical cases, each institution which is a member of a federation has their own RADIUS proxies connected to the higher level RADIUS proxies (e.g. the national RADIUS proxy). Therefore, the shared secrets are configured between the APs and the institutional RADIUS proxies at the time of a new WLAN deployment.

2.3 Roaming System over WMNs

2.3.1 WMN Assumptions

A WMN consists of some mesh nodes having mesh routing functions. They also work as APs for other mesh nodes...
and for non-mesh devices having no mesh routing functions. This type of mesh node is referred to as mesh AP hereinafter. Non-mesh devices also can get network access by communicating with the mesh APs by 802.11 infrastructure mode.

Although a WMN itself is assumed to be operated by an organization owning the location where the WMN is deployed, the WMN allows a roaming user to connect the network, which enable mutual use of WLAN facilities among multiple organizations.

### 2.3.2 Security Requirements

To deploy campus or enterprise WLAN systems using WMN technologies, the following security mechanisms should be introduced.

**User authentication** In the same way as conventional WLAN systems, users should be authenticated by the authentication server at the users’ institutions.

**AP authentication** To prevent unauthorized mesh APs from connecting to the WMN, APs also need to be authenticated.

**Mutual authentication** To prevent mesh APs and users from connecting to malicious APs, mutual authentication should be introduced between the authentication server and the joining nodes.

**Traffic Encryption** To protect the communication over wireless links in WMNs against eavesdroppers, the traffic on the WMN must be encrypted.

To meet these requirements, it is effective to apply the 802.1X-based authentication mechanism to WMNs.

### 2.4 Deployment of RADIUS-Based Roaming System over WMNs

Egners et al. showed the real-world testbed equipped with the 802.1X-based authentication mechanism over WMNs[11]. Figure 2 shows an example of the deployment. Each arrow indicates that the supplicant (source) is connected to the authenticator (destination).

First, the mesh AP N1 is connected to the backhaul network and N1 obtains its IP address. In order for N1 to forward RADIUS authentication packets to the RADIUS server, the secret key needs to be configured manually at N1’s authenticator and the RADIUS server. When N2’s supplicant requests network access to N1’s authenticator, the AP authentication is processed based on 802.1X between N2’s supplicant and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server. A shared secret key needs to be set at both N2’s authenticator and the RADIUS server.

To meet these requirements, it is effective to apply the 802.1X-based authentication mechanism to WMNs.

![Fig. 2 802.1X authentication system over WMNs](image)

802.1X only supports a simple hop-by-hop protection. In other words, the traffic is encrypted only between an authenticator and the corresponding supplicant. On the other hand, their system protects the traffic of many communication patterns based on their security framework [12].

In this deployment method, however, there are mainly two issues. The first one is that the network administrators must configure secret keys on each AP and RADIUS server. Therefore, the deployment cost will increase as much as the number of mesh APs. Moreover, additional configurations are required if the IP addresses of some mesh APs change when renewing the IP addresses by DHCP or when the network connection to upper networks has recovered. The deployment cost should be decreased especially in temporary deployment cases such as the deployment at the venues of large events. The second one is that the user authentication and AP authentication will fail if there is a failure on the path which the authentication packets go through. In the deployment over WMNs, especially, this behavior leads to the WMN topology breakdown. In most EAP methods, each mesh AP must be re-authenticated periodically. If the re-authentication fails, the mesh AP will be excluded from the WMN.

### 3. WLAN Roaming System Deployment Methods over WMNs

#### 3.1 Automatic Authentication Path Generation over WMNs

In [7], Winter developed an eduroam AP system which generates authentication path automatically using RadSec. RadSec is a protocol which transports RADIUS datagrams over TCP/TLS. In RadSec, a client generates an authentication path to the corresponding server by the TLS tunnel establishment. The RadSec client submits its digital certificate to the RadSec server, and the RadSec server verifies the submitted certificate by the public key which can verify the certificate. If the certificate and the public key are installed on each client and server beforehand, network administrators do not need to configure any secret key on both the RadSec
Figure 3  Automatic authentication path generation over WMNs

client and RadSec server after the AP is connected to the backhaul network. However, the wiring to the AP is still required as the deployment over WMNs is not considered in the system. We extended this system to the deployment over WMN.

Figure 3 depicts how to generate the authentication paths automatically over WMNs using RadSec. To generate the authentication paths using RadSec, there needs to be RadSec clients and servers. We assume that each mesh AP has a RadSec client. The mesh APs try to establish the TLS tunnels with a RadSec server connected to the federation network. Since the server can proxy authentication packets to the appropriate IdP through the federation network, this type of server is referred to as RadSec proxy.

Preliminarily, the following configurations are required before the deployment on the service site.

**Issue certificates to mesh APs** A certificate issuer issues a certificate which will be used for the TLS establishment with the RadSec proxy. The certificate installation on the mesh AP should be included as a part of factory setting.

**Install the CA certificate of the RadSec proxy** The CA certificate of RadSec proxy’s server certificate issuer must be installed to mesh APs for the TLS establishment with the RadSec proxy. The certificate installation on the mesh AP should also be included as a part of factory setting.

**Configure the destination of the RadSec proxy** The destination of the RadSec proxy must be configured on mesh APs as a part of factory setting.

**Distribute public keys to RadSec proxies** In order for the RadSec proxy to verify the certificates from the mesh APs, the certificate issuer needs to distribute its public key to the RadSec proxy beforehand. The public key is the certificate used to verify the digital signature of the certificates installed on mesh APs.

If these configurations can be done beforehand, mesh APs will be able to generate authentication paths automatically at the time of the deployment. After a mesh AP has been authenticated and joins the WMN, the RadSec client in the mesh AP tries to generate a TLS connection with the RadSec proxy configured as the destination.

To establish the TLS connection, the mesh AP must validate the RadSec proxy’s server certificate and vice versa. The certificate validations at a client (mesh AP) and a server (RadSec proxy) are as follows.

**Server certificate validation** A RadSec proxy has a server certificate issued by a well-known CA whose CA certificate is installed to mesh APs as a factory setting. Therefore, the client (mesh AP) can validate the server certificate of the RadSec proxy using the CA certificate of the server certificate issuer. The validation is processed in the same way as a web browser validates a HTTPS web server’s certificate.

**Client certificate validation** The RadSec proxy can also validate the client certificate of the mesh AP using the public key of the issuer of the client certificate. The public key is installed to the RadSec proxy before AP deployment on-site. In fact, the public key is the CA certificate of the issuer.

After the TLS connection establishment, the mesh AP can send forward authentication packets to the federation network.

Note that what all the on-site workers have to do for the WLAN roaming system deployment are to put the mesh APs physically and to switch them on. The AP authentication and the authentication path generation are done automatically. Moreover, the automatic authentication path generation makes it possible to recover the authentication system automatically when network connection has recovered. It is because that mesh APs in WMNs can become authenticator automatically after IP addresses of mesh APs are obtained or updated.

Another benefit of employing RadSec for authentication path generation is that RadSec provides secure communication between the mesh APs and the RadSec proxy. The security mechanism in RadSec is based on TLS, whereas the one in RADIUS is based on the MD5 algorithm, which has been proven to be less secure.

In addition, RadSec proxies can verify the certificate revocation status of each mesh AP by checking Certificate Revocation Lists (CRLs) or sending an Online Certificate Status Protocol (OCSP) request to the OCSP responder. However, radsecproxy [13], which is the open source RadSec proxy implementation, only supports the revocation verification by checking CRLs at the moment.
We assume that there are several RadSec proxies that are geographically distributed. In this case, mesh APs need to select the nearest RadSec proxy from them because TCP throughput decreases with the increases of Round Trip Time [14]. The procedure that a mesh AP connects to the appropriate RadSec proxy is shown as follows (Fig. 4).

1) The FQDN of the RadSec proxy is configured in all mesh APs as a factory configuration.
2) To resolve the RadSec proxy hostname to the IP address, the mesh AP sends the DNS query to the local DNS server working as a DNS resolver.
3) The local DNS server also sends the DNS query to the authoritative DNS server. The authoritative DNS server sends back the IP address of the nearest RadSec proxy from the local DNS server.
4) The local DNS server also sends back the IP address, and then the mesh AP tries to connect the RadSec proxy having the IP address the mesh AP received.

3.2 Local Authentication over WMNs

3.2.1 Local Authentication System

Kinoshita et al. proposed a disruption-tolerant authentication system [15]. To authenticate a roaming user at SPs, the authentication packet must be sent forward to the user’s IdP in the conventional WLAN roaming system. In this conventional way, the authentication fails if there is a disruption on the path which the authentication packets go through. The proposed system utilizes EAP-TLS method [16] in which client certificates are used for the authentication credentials. In the system, user authentication and authorization are processed at the SP locally by EAP-TLS. We utilize this method for the WLAN roaming system deployment over WMNs. Further security analysis and performance analysis are also shown.

3.2.2 User Authentication and AP Authentication

Figure 5 shows an overview of the local authentication over WMNs. Preliminarily, two types of mesh AP are defined to distinguish the role of the mesh AP in the explanation of the local authentication. If a mesh AP works as an authenticator, it is referred to as authenticator AP. If a mesh AP works as a supplicant, it is referred to as supplicant AP. The supplicant AP has a certificate issued by Issuer A, which provides the certificates for the mesh APs. The user terminal has a certificate from Issuer B, which provides the certificates for their users. The authenticator AP has the public keys distributed by Issuer A and B. Since supplicant APs and user terminals work as supplicants in the authentication process, they are also referred to as joining node altogether.

After a joining node has finished the association process with an authenticator AP, the authenticator AP receives an authentication request from the joining node. By checking the realm of the identity included in the authentication request, the authenticator AP determines if the authentication can be processed by itself or not. The authenticator AP has the list holding realms of which authentication request can be verified at local as shown in Table 1. Under this configuration, the authentication request of which realm matches "*.tohoku.ac.jp" is processed at the RADIUS server in the authenticator AP by verifying the certificate of the joining node based on EAP-TLS. This type of authentication is referred to as local authentication. Otherwise the authentication request is sent to the upper RadSec proxy or the upper RADIUS proxy if there is no failure on the path which the authentication packets go through. This type of authentication is referred to as fallback authentication. In case of fallback authentication, the authentication packet will be dropped if the authenticator AP cannot connect to the upper RadSec proxy or the upper RADIUS proxy. Note that the authenticator AP does not need to communicate with any servers if it has the public key of the joining node’s certificate issuer. Thus, the authentication is possible, even if the upper network is unavailable or some authentication servers or proxies are down. This feature is useful in the natural disaster scenarios.

3.2.3 Security Analysis

The joining node also needs to verify the server certificate of the RADIUS server to meet the mutual authentication re-
requirement. In case of local authentication, the joining node verifies the certificate of the authenticator AP working as a RADIUS authentication server. To verify the certificate, the joining node uses the certificate issuer’s public key.

When an attacker succeeds in stealing a certificate from a mesh AP or a user terminal, he can connect to the WMN using the certificate. To prevent the attack, a certificate revocation verification mechanism should also be introduced at both the supplicant side and the authenticator side. To check the revocation status of the client certificate, the authenticator AP checks the CRL distributed from the Issuer of the client certificate, or sends an OCSP request to an OCSP responder.

While distributing CRLs could be a burden for CA administrators, the OCSP communication requires the connection between the authenticator AP and the OCSP responder considered to be remotely located. Thus, the OCSP communication makes the local authentication method less effective as the objective of the local authentication method is reducing communications to outside networks. Creating OSCP response cache on an authenticator AP can mitigate the OCSP communication costs. FreeRADIUS[17], which is a popular RADIUS server implementation, can create OSCP response cache.

The revocation status of the server certificate can be verified only by OCSP stapling[18] since the joining node does not have network access until the authentication completion. If the authenticator does not have network access and OCSP response cache, the client should also submit the revocation status by OCSP stapling. However, no RADIUS server implementation is known to support the OCSP stapling mechanism so far. We would like to expect the feature enhancement in the near future.

The local authentication method may affect the client side security. If the authentication is processed at the joining node’s IdP and the user have been authenticated by the IdP at least once, the user can automatically connect to the WLAN because the server certificate can be automatically verified. In case of local authentication, however, the user is asked to accept a new server certificate whenever the user connects to the authenticator AP that the user has never connected to. This might cause a security issue that users might unexpectedly connect to rogue APs if the users cannot distinguish valid certificates from invalid ones such as self-signed certificates. In theory, the users do not connect to rogue APs if the supplicant checks the validity of the offered certificate of the authentication server. However, in practice, some older versions of wpa_supplicant do not check the validity of the authentication servers’ certificates[19]. Even if the supplicant can check the validity, some users might accept invalid certificates. If a user is connected to the rogue AP, the rogue AP can perform a Man-In-The-Middle (MITM) attack and gain control over his network traffic. To prevent this attack, the public key for verifying the client certificates should be kept secret to the public and available only to the authorized network or service administrators. Unless an attacker can get the public key, the user terminals fail to connect to the rogue AP.

3.3 Deployment Procedure

Figure 6 shows the deployment procedure using the two proposed methods. If the joining node associates with the authenticator AP, the joining node sends the authentication request to the authenticator AP. If the authentication request specifies EAP-TLS as the EAP method, the authenticator AP checks the realm and examines if the client certificate can be verified locally or not. If the authenticator AP can verify the certificate, the authentication is executed at the authenticator AP. If the certificate cannot be verified at the authenticator AP or the EAP method specified in the authentication request is not EAP-TLS, the authentication request is proxied to the RadSec proxy in the federation network and is also proxied to the RADIUS server in home institution of the joining node. After the authentication, the joining node gets Pairwise Master Key by the 4-way handshake[20] and gets its IP address by DHCP. If the joining node is a mesh AP, the mesh AP tries to establish TLS sessions with the RadSec proxy in the federation network, and starts to work as an authenticator AP.

4. Implementation and Evaluation

4.1 Implementation

We implemented the proposed methods on the mesh AP using two types of hardware as shown in Fig. 7. The first one is a laptop computer equipped with Intel Core i5-2540M processor, 4GB memory. The wireless chip onboard is Intel Centrino Advanced-N. Some additional wireless USB adapters (Ralink RT8070) are attached to the laptop computer. The second one is LIVA MINI PC KIT equipped with Intel Celeron N2807, 2GB memory. Some additional wireless USB adapters (Ralink RT8070) are also at-
NIIZUMA and GOTO: EASY-TO-DEPLOY WIRELESS MESH NETWORK SYSTEM WITH USER AUTHENTICATION AND WLAN ROAMING FEATURES

Fig. 7 Mesh AP

In a mesh AP, five software programs are running on Debian 8.1.0 (Linux Kernel 3.16.7). They are batman-adv [21], radsecproxy [13], FreeRADIUS [17], hostapd [22], and wpa_supplicant [23]. Figure 8 shows the network interface architecture of the mesh AP. A mesh AP has at least two wireless interfaces. One wireless interface is used to run the authenticator using hostapd allowing other supplicant APs to connect to the WMN. The second interface is used by wpa_supplicant to connect to the authenticator APs. These two interfaces used by B.A.T.M.A.N. for routing are bridged to a virtual network interface (bat-device). In addition, two optional wireless interfaces can be installed on the mesh AP. The first one is for connecting between the WMN and the outer network. The second one is for providing an entry access point for user terminals. These two optional interfaces and the bat-device are bridged to another virtual network interface.

When a mesh AP (supplicant AP) boots up, it will automatically try to connect to the neighbor authenticator AP by using wpa_supplicant. After the association process, the mesh AP will be authenticated and will be an authenticator AP as the way described in 3.2.2 and 3.3.

We confirmed that the automatic authentication path generation method and the local authentication method worked correctly as we designed on our mesh AP system.

4.2 Evaluation of On-Site Deployment Costs

The WMN deployment cost seems to be increased by the number of on-site manual configuration. We compare the number of manual configuration between the existing method [12] and the proposed method.

The WMN deployment procedure using the existing method is already shown in 2.4, and the deployment procedure using the proposed method is shown in 3.3.

Existing method In the existing method, the secret key shared between a mesh AP and a RADIUS proxy should be configured manually after an IP address is assigned to the mesh AP. Therefore, the number of manual configuration is the number of mesh AP to be deployed. If the IP addresses are assigned dynamically by DHCP, additional manual configuration is required when another IP address is assigned to the mesh AP.

Proposed method In the proposed method, no manual configuration is needed on-site to deploy a WMN. It is because that mesh APs automatically establish a connection to the RadSec proxy.

4.3 Performance Evaluation

4.3.1 Setup

We evaluate the performance of our proposed system by measuring authentication delay. Figure 9 shows the test network and server environment. Node 1, 2 and 3 are mesh APs implemented on the laptop computer whereas Node 4 and 5 are implemented on LIVA MINI PC KIT. Node 6 is a laptop computer equipped with Intel Core i5-460M processor, 2GB memory and Intel Centrino Advanced-N wireless chip. Node 6 is considered as a user terminal that measures the authentication delay.

We measured the authentication delay as the duration from the authentication request emission to the result receipt on a supplicant. The authentication delay was measured by analyzing the log files written by wpa_supplicant. There is a Virtual Private Server (VPS) out of the LAN, which is used for a RadSec proxy and a RADIUS authentication server in fallback authentication. In this test setup environment, we measured the authentication delay in the following types of authentication mechanism.

Fallback Authentication The authentication is processed
at the RADIUS server in the VPS. In fallback authentication, the authentication request is firstly carried to the authenticator from the terminal via EAPoL. The authenticator proxies the received authentication request to the RadSec authentication server in the VPS. To investigate the overhead of our proposed method utilizing RadSec, we measured each EAP-TLS authentication delay in which the authentication protocol between an authenticator AP and the VPS is RadSec or RADIUS.

**Local Authentication** In local authentication, the authentication is firstly carried to the authenticator from the terminal via EAPoL and is processed at an authenticator AP. To see the overhead for checking certificate revocation status, we measured each EAP-TLS authentication delay in which the certificate revocation by CRL or OCSP is enabled or any certificate revocation checking is disabled.

**4.3.2 Results and Discussion**

Figure 10 shows the average authentication delay for different numbers of wireless hops. Each measurement was repeated 100 times.

This experimental results show that the fallback authentication delays increase with the number of hops between the authenticator AP and the VPS. In fallback authentication, however, the authentication delay with RadSec is less than the one with RADIUS especially where the number of hops is more than three. RadSec transports the authentication packets over TCP, whereas RADIUS transports them over UDP. Thanks to the TCP fast retransmit algorithm [24], RadSec authentication packets can be sent faster than the standard RADIUS if a packet loss happens. The experimental results have confirmed that RadSec can decrease the authentication delay in multi-hop environment that makes the packet loss rate larger. Figure 11 shows the packet loss rate for different numbers of wireless hops measured by ICMP echo from Node 6 to the VPS. In the test environment, the packet loss rate increases with the number of wireless hops as shown in Fig. 11. Note that the packet loss does not come from our proposed methods, and the WMN is responsible for it. The proposed automatic authentication path generation method works robustly against the increase of the number of wireless hops.

If the certificate revocation verification is disabled or enabled with CRL, the local authentication delay does not increase with the number of hops between the authenticator AP and the VPS. On the other hand, checking the certificate revocation status by OCSP increases the authentication delay because it requires HTTP communication between the authenticator AP and the OCSP responder in the VPS.

**5. Conclusion**

This paper presented a novel WLAN roaming system architecture based on two deployment methods. The automatic authentication path generation method does not require any configuration when deploying a WLAN roaming system over the WMN. The local authentication method makes the system deployable in time of disaster, in particular when the upper network is unavailable or some authentication servers or proxies are down. It also enables to recover the WMN authentication system automatically when network connection has recovered. We have also implemented and evaluated the WMN testbed composed of mesh APs having the B.A.T.M.A.N. mesh routing protocol. An experiment showed that the automatic authentication path generation method has more advantage when the number of wireless hops in the WMN is larger.

Future work includes designing the PKI operation scheme of the proposed WMN system because our proposal depends on PKI (Public Key Infrastructure) techniques such as issuing, updating and revoking certificates of mesh APs and RadSec proxies. The update and revoking process should also be easy and quick. Of particular importance, the operation scheme should be scalable to WMNs operated by multiple operators.
Acknowledgments

This work was partly supported by JSPS KAKENHI No.15K12015.

References


Tomo Niizuma received his master’s degree in information sciences from Graduate School of Information Sciences (GSIS), Tohoku University, Japan in 2016. His research interests include WLAN roaming, 802.1X authentication, RADIUS/RadSec, Wireless Mesh Networking and Centralized IdP.

Hideaki Goto received the M.Sc. degree in physics in 1992, and the Ph.D. degree in information 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 network, and information security. He is a member of IEICE in Japan, IPSI, and IEEE Computer Society.