Mutual Authentication Method in Public Wireless LAN by Using BLE Beacon

Yoshihiro Niitsu, Shunsuke Sakai and Kouta Tezuka
Shibaura Institute of Technology, Saitama-City, Saitama Japan
niitsu@shibaura-it.ac.jp

Abstract— **Demand of public wireless LAN has rapidly increased owing to growing overseas visitors. However, security measures such as encryption or authentication are insufficient because present public wireless LANs place a significance on easiness of its use. This produces an increasing risk of attacks for intercepting data. Furthermore, as it is impossible to validate correctness of access points, users can easily be connected with spoofed access points and can be guided toward malicious sites. This paper proposes the mutual authentication method for public wireless LANs based on BLE beacon data and clarifies its effectiveness.**

Keywords— mutual authenticaion, public wireless LAN, BLE beacon, UUID, access point, SSID, publibc key.

I. Introduction

Lately overseas visitors to Japan have increased rapidly and they will be expected to increase much more thanks to Tokyo Olympics in 2020. This will forward to increase demand of public wireless LANs.

However, security measures such as encryption or authentication are insufficient because present public wireless LANs place a significance on easiness of its use. This produces increasing risks of attacks for intercepting data. Furthermore, as it is impossible to validate correctness of access points, users can easily be connected with spoofed access points and can be guided toward malicious sites [1].

This paper proposes the mutual authentication method for public wireless LANs based on BLE (Bluetooth Low Energy) beacon data and clarifies its effectiveness.

II. Existing method and its problem

A. Existing method

The previous study [2] proposed the mutual authentication method by using NFC (Near Field Communication). This NFC system generally has a low risk of man-in-the-middle attacks and everyone can simply operate it. Mutual authentication procedures of existing method are shown as follows.

Step 1: A user touches a user terminal to an issuing machine of authentication data.
Step 2: The issuing machine of authentication data asks an authentication server for authentication data.
Step 3: The authentication server generates authentication data and sends it to the issuing machine.
Step 4: The issuing machine sends it to the user terminal.
Step 5: The user terminal connects with an access point by using it.
Step 6: Both the authentication server and the user terminal validate the authentication data. If it has no problem, the user terminal starts accessing to the Internet.

B. Problems of the existing method

When multiple users want to authenticate, this method easily produces queues because NFC supposes one to one communication. Furthermore users have to come close to communicable range within one meter. Considering these points, usability of this method becomes lower in a real environment.

III. Design Concept

A. Study approach

The objective of this study is to improve usability of public wireless LAN located at station yards for short-time usage. In order to realize it, this paper proposes the mutual authentication method that can automatically authenticate by receiving radio wave of BLE beacon.

B. Supposed environment

In this study, every user of public wireless LAN has installed an application for issuing authentication data in his or her terminal. It is also assumed that every user terminal can communicate with an authentication server and a public encryption key server via mobile network. Nowadays mobile users from abroad can easily get free SIM cards for a limited available time at most of international airports. System administrators can arbitrarily change SSIDs and passwords of public wireless LANs.

C. Names and roles of system elements

- BLE beacon: It is installed within communicable range with a specified access point. It periodically transmits a UUID corresponding to a specified access point, a Public Search ID corresponding to a public key and one-time password.

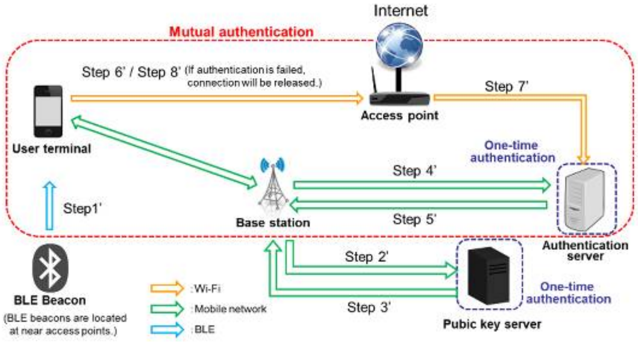

Fig. 1 System configuration of the proposed method

- ● <u>User terminal</u>: It receives radio wave of BLE beacon and communicates with both an authentication server and a public key server.
- ● <u>Public key server</u>: It carries out one-time authentication and manages public keys.
- ● <u>Authentication server</u>: It carries out mutual authentication by using both user information and authentication data, and manages access point data.
- ● <u>Access point</u>: They are access points of public wireless LANs. Security of them are protected by passwords that are arbitrarily changed by system managers.

IV. Proposed method

A. System overview

Novelty of the proposed method is both system configuration and its authentication procedure. System configuration is shown in Fig. 1 and authentication procedure is described as follows.

Step 1’: A BLE beacon periodically transmits a radio wave.
Step 2’: When a user terminal receives a radio wave of BLE beacon, it will send received data from the beacon to a public key server.
Step 3’: A public key server sends a public key that corresponds to an access point based on the result of one-time authentication, to a user terminal.
Step 4’: A user terminal sends an authentication request composed of received pubic key and its own user data to an authentication server.
Step 5’: An authentication server sends an encrypted authentication data that contains an SSID of an access point, to a user terminal.
Step 6’: A user terminal automatically connects with an access point by using authentication data received from an authentication server.
Step 7’: Both an authentication server and a user terminal validate correctness of authentication data.
Step 8’: If there is no problem in above validation, a user terminal can start accessing to the Internet via the access point.

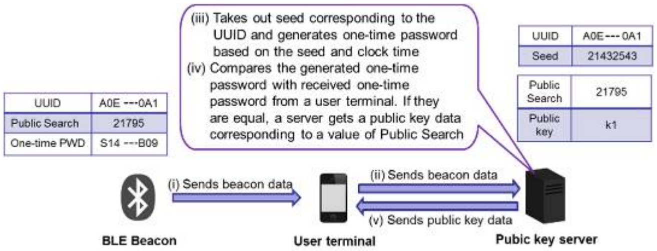
(iii) Takes out seed corresponding to the UUID and generates one-time password based on the seed and clock time
(iv) Compares the generated one-time password with received one-time password from a user terminal. If they are equal, a server gets a public key data corresponding to a value of Public Search
UUID A0E ---0A1
Public Search 21795
One-time PWD S14 ---B09
UUID A0E --- 0A1
Seed 21432543
Public Search 21795
Public key k1
(i) Sends beacon data
(ii) Sends beacon data
(v) Sends public key data
BLE Beacon
User terminal
Pubic key server

Fig. 2 One-time authentication in a public key server

B. One-time authentication

It is necessary for the proposed method to protect the system from a malicious user that accesses by using previous beacon data. This method generates one-time password by using both clock time and a seed or a random number generation key that has been set to each access point. Each access point corresponds to each BLE beacon or UUID. Pubic key server checks if the generated one-time password is equal to the received one-time password or not. As a result, it is validated that the terminal has the newest beacon data.

This one-time authentication is also used just before an authentication server registers user data.

C. Mutual authenticaiton

The proposed method carries out the mutual authentication composed of user authentication and server authentication in order to exclude an illegal user access or a connection with a malicious access point. The mutual authentication is realized by both user data in a user terminal and certificate in an authentication server. As a result, both a user terminal and an access point are validated.

An authentication server sends certificate, SSID of an access point and its encryption key to a user terminal. A user terminal sends user ID and his/her password that are arbitrarily defined by a user and one-time password that is received from a BLE beacon as user data, to an authentication server. One-time password is used for registering user ID, his/her password and certificate into an authentication server. Above data for mutual authentication is shared between a user terminal and an authentication server in advance. The sharing procedure of mutual authentication is shown in Fig. 3.

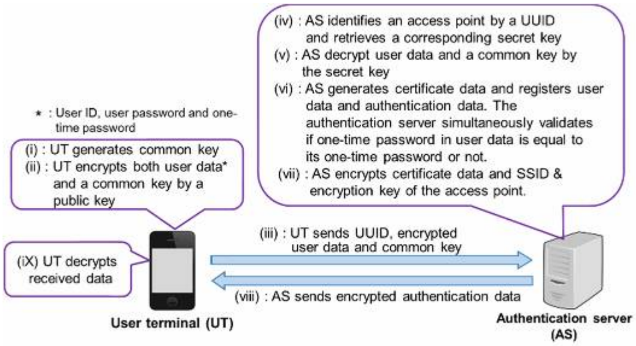
(iv) : AS identifies an access point by a UUID and retrieves a corresponding secret key
(v) : AS decrypt user data and a common key by the secret key
(vi) : AS generates certificate data and registers user data and authentication data. The authentication server simultaneously validates if one-time password in user data is equal to its one-time password or not.
(vii) : AS encrypts certificate data and SSID & encryption key of the access point.
* : User ID, user password and one-time password
(i) : UT generates common key
(ii) : UT encrypts both user data* and a common key by a public key
(iii) : UT sends UUID, encrypted user data and common key
(iX) UT decrypts received data
(viii) : AS sends encrypted authentication data
User terminal (UT)
Authentication server (AS)

Fig. 3 Sharing procedure of mutual authentication data

V. Evaluation

A. Experiments

In order to clarify effectiveness of the proposed method by comparing with existing method, trial system composed of Android terminals and PCs was created. Evaluation experiments were carried out on it.

In the proposed method, issuing frequency of authentication per minute is number of terminals that can receive beacon per minute, because it is possible for the system to issue authentication automatically without waiting for last authentication process. So the number depends on each station's incoming and outgoing passengers. Statistical passenger number data per minute for top three crowded stations in Tokyo is used for evaluating the number of issuing authentication [3].

In the existing method, the number of issuing authentication is obtained by the value that 60 seconds (one minute) is divided by sum of authentication time and operation time (about 2 seconds).

The existing method uses common key encryption system that is AES encryption scheme and its key length is 128 bits. Proposed method uses both public key encryption system and common key encryption system. RSA encryption scheme is applied to public key encryption system and its key length is 3,072 bits. Common key encryption system of the proposed system also uses AES encryption scheme and its key length is 128 bits. In security of both methods, they have the same security level because of equivalent security. So security of both methods do not need to be evaluated.

B. Evaluation items

- Average authentication time (msec)
  Time from start of processing to end of issuing authentication is measured.
- Possible issuing frequency of authentication (time/minute)

  (Proposed method)

  $$\frac{N\times\alpha\times\delta}{18\times60\ \text{(Available time of station)}}$$

  N: Average passengers per day at a major station of Japan [3]

  α : Average utility rate of ticket gates at a major station of Japan [3]

  δ : Average utility rate of public wireless LANs in Japan [4]

- Total communication amount (kB)
  Total communication amount for mobile network of the proposed method

C. Experimental results

For evaluation experiment results of the proposed method and the existing method, average authentication time is shown in Fig. 4 and possible issuing frequency of authentication is shown in Fig. 5. Total communication amount of the proposed method is 3.13 kB.

VI. Consideration

As Fig. 4 shows, authentication time of the existing method is shorter than that of the proposed method because of the number of procedures. However, the difference between both methods is 22 msec. So there is no problem in the case of using public wireless LAN.

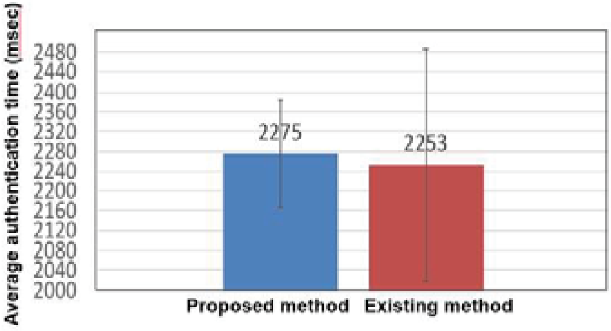

Fig. 4 Average authentication time

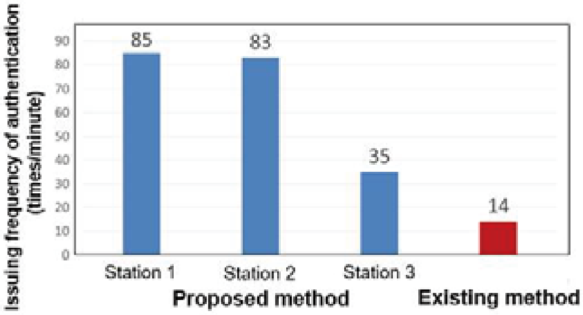

Fig. 5 Issuing frequency of authentication

As shown in Fig. 5, when the number of authentication is more than 14, the proposed method is more effective because the existing method needs to add on an authentication issuing device. Furthermore, the proposed method makes it possible to issue authentication automatically to a user terminal that receives a radio wave of BLE beacon. As a result, users do not need to come close to authentication issuing devices, because they can be installed at nearby ticket gates or escalators where a lot of passengers come and go.

VII. Conclution

The mutual authentication method by using BLE beacon was proposed and its effectiveness was clarified by evaluation experiments.

References

[1] Danny Neoh, "Corporate Wireless LAN: Know the Risks and Best Practices to Mitigate them", SANS Institute Reading Room, Mar. 2004.

[2] Y. Miyashita, S. Hashimoto, C. Fukui and M. Fujimura, "Construction of Connection Environment for Public Wireless LAN Using NFC ", IPSJ FIT2016, L-023, Sep. 2006.

[3] JR East Marketing and Communications, "Tokyo Metropolitan District Rout Groups and Total Number of Passengers/Average Travelling Time", May 2016.

[4] Ministry of Internal Affairs and Communications, Information Security Task Force, "Survey Results on Usage of Public Wireless LAN", Mar. 2015.