THE KEY PROVIDING SYSTEM FOR WIRELESS LAN USING VISIBLE LIGHT COMMUNICATION

Kuniyoshi Okuda[1], Takuya Yamamoto[2], Tomoo Nakamura[1] and Wataru Uemura[1]

[1]Department of Electronics Informatics, Ryukoku University, Shiga, Japan
[2]Graduate School for Creative Cities, Osaka City University, Osaka, Japan

ABSTRACT

Public wireless LAN services have been increasing recently. These are convenient services for carrier companies particularly. And carrier companies and the user can disperse traffic. However in order to improve the convenience, the services do not often use the encryption key or do not change the encryption key that has already been set. Therefore, the services have a problem in safety. This paper solves this problem using the visible light communication.

The visible light communication sends a signal by blinking the light. One of the visible light communication features is that we can see the transmission area. The visible light communication can use lighting equipments as the transmitter unlike infrared or conventional radio communications. Further, visible light communication can separate to clarify the transmission range by using light.

We propose the distribution of the encryption key and the SSID using visible light communication. Visible light communication can easily prepare a small network, such as a partition or per a room basis. For malicious users connecting to the network is necessary to enter in the service provided area. Thus the administrator is able to easily manage legitimate users. In addition, it is possible to update the SSID and the encryption key by visible light communication easily for an administrator. Thus if malicious users get the SSID and the encryption key, they cannot use the SSID and the encryption key immediately. Normal users may only need to run the shell script for receiving information from the receiver. Therefore, convenience is good.

In order to confirm the improved convenience, we measured the time it takes for a user to connect to the network. Conventional methods are methods that use or do not use the encryption key. As a result, users can connect to the network in a short time compared with the conventional methods. The system becomes stronger than conventional methods because it is possible to update the encryption key and SSID automatically in the security aspect.

KEYWORDS

Wireless LAN, SSID, encryption key, visible light communication

1. INTRODUCTION

Recently, a network environment has become familiar. Now we can connect to the network anywhere. Such a condition is called ubiquitous. The ubiquitous means interface, environment, and technology. It may benefit at any time anyone everywhere. And a ubiquitous mobile communication is especially important. The traffic is increasing all the time. Carrier companies have strengthened the network to support the traffic. However it is not enough. So the wireless LAN has drawn attention. Wireless LAN is a communication system for a small area. Wireless LAN does not require a line. The user can connect to the network by simply setting the terminal.

DOI : 10.5121/ijasuc.2014.5302

Communication speed of wireless LAN is faster than the line of mobile phones. It is supported by a wired communication. And the communication speed becomes faster year by year. Effective speed of the current is approximately 1Gbps or more. Communication speed is reduced by the user increases. However, it is much faster as compared to the line of mobile phones. Therefore we can expect high-speed communication in a specific area in the wireless LAN. Therefore carrier companies have supported the traffic by providing wireless LAN services. This service can be enjoyed by people who are only contracted with the carrier company basically. And rather than covering a wide range in a single access point, it is better to cover the specific range of the access point some better network efficiency [1]. Recently a public wireless LAN service becomes also popular (Figure 1). The services are provided at the place where many people gather. These are airports, restaurants and stations. The public wireless LAN service is an important service to foreigners, because communication of complicated content is the burden for foreigners. In addition, in some cases network of career companies are not required when the stay is short like transit. The public wireless LAN service is particularly effective in such case. There is a fee or free in the public wireless LAN services. This paper focuses on the free wireless LAN service that anyone can use.

Figure 1: public wireless LAN services

2. PROBLEM OF WIRELESS LAN SERVICES

Some methods are required in order to connect the wireless LAN service. They depend on the method of service. We describe three procedures.

The first method is the method that does not use the encryption key. It can be connected by anyone. The procedure of the connection is easy. Users can connect the network by selecting a SSID (Service Set Identifier).

The second method is the first method with some options. The options require a license agreement or show them advertising for users. The service requires the same procedure again after a certain interval time. Convenience of these services is the better than other methods. However these methods have some problems. Malicious users can easily access to public wireless LAN, because anyone can connect to the wireless LAN. In addition, this system does not use an encryption method. Therefore persons who have some techniques can see another person's communication contents.

The third method is the methods that an administrator gives both the SSID and the encryption key to users. The SSID and the encryption key are told in the poster for bulletin board. The user can connect to the network using them. This method is often used at the hotel. The SSID and the

encryption key are posted in the private room and lobby. Convenience of this method is worse than the first method, however security is better. This method essentially does not change the SSID and the encryption key. If malicious users know the SSID and the encryption key even once, they can connect to the network easily.

In addition to these methods there is an option that requires a users' authentication. It is necessary to pre-register for users. Users select the SSID to connect to the network. Then, they are guided to the top page through the browser. And they will enter a username and a password. The convenience is bad and the security is good, and to connect the network is difficult for malicious users. However, if the administrator does not use an encryption key, there is a possibility that the communication contents are analyzed.

In addition to users authentication, to change the encryption key frequently is effective for malicious users. Changing the encryption key is not performed basically in the public wireless LAN service, because the convenience is reduced. However, using network and analysis of communication content for malicious users is difficult by changing the encryption key frequently. We show the relationship between the convenience and the encryption key and the security in Table 1.

Table 1. The relationship between convenience and encryption key and security

	Convenience	Security
Without encryption key	Good	Bad
With checking the license agreement or showed ads	Good	Bad
With encryption key	Bad	Good

In the conventional method, the second method uses the encryption key. By the second method to change the encryption key frequently, it is possible to achieve both security and convenience. In this case, the burden of administrators and users must not be small when changing the encryption key. In addition if the area of transmitted encryption key is minimum, the availability of the encryption key is difficult to malicious users, because the administrator can easily monitor user. Therefore, to deliver a new encryption key periodically in limiting the service providing area is required. There are methods using radio waves, infrared and visible light communication [2-4] (shown in Figure 2) in the information delivery. The communication area of infrared and radio waves is unclear, because we cannot see the infrared and radio waves. That is, it is impossible for the administrator to understand the transmission range of the encryption key. It is a benefit to a malicious user. Therefore, with the use of a visible light communication, it is possible to lower the potential to provide an encryption key to the malicious user. Visible light communication transmits a signal by blinking the visible light. Characteristic of visible light communication is to look for human eyes. The communication range is illuminated by the transmitter. The administrator is able to recognize the transmission range easily. Further, the visible light communication can use the lighting equipment as a transmitter. Recently the lighting equipment using LEDs has been increasing. A response speed of LEDs is faster than that of the conventional illumination as incandescent lamps or fluorescent lamps. When the encryption key is delivered by the visible light communication by the lighting equipment, users in lighting area may be able to enjoy the service. If this system can send the encryption key, sending SSID is easily. The selection of SSID is the procedure for connecting to the network.

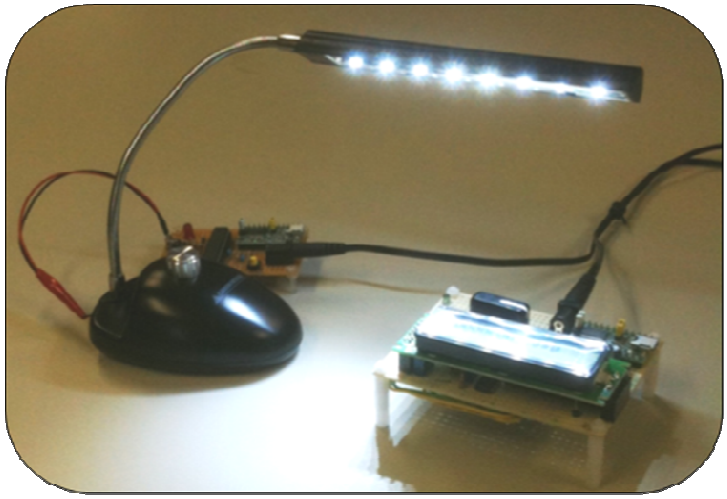

Figure 2: Visible light communication

3. THE KEY PROVIDING SYSTEM FOR WIRELESS LAN USING VISIBLE LIGHT COMMUNICATION

We propose the distribution system of the SSID and the encryption key using visible light communication. We show the system overview in Figure 3. The proposed system uses the lighting equipment as a transmitter. In order to use the illumination device as the transmitter, the brightness should be constant. Therefore, the proposed system uses the PPM (pulse position modulation) [5-6].

At first the router transmits the SSID and the encryption key to the lighting equipment. The transmitter distributes the SSID and the encryption key by visible light communication [7]. Therefore users only in the lighting area can get the signal using a receiver of visible light communication. The receiver gets the signal by the visible light communication and decodes the signal. In this way users can know the SSID and the encryption key. And the router changes the SSID and encryption key on a regular basis. In that case, the proposed system repeats from the first step.

Traditional public wireless LAN services do not use the encryption key, or they continue to use the encryption key determined once more. Because changing the encryption key is the burden for the administrator and users. The proposed system can change the encryption key easily, because the proposed system can change the encryption key without the burden of the administrator and users. In addition, it is easy for us to set an SSID to each room, because we can block the visible light communication by providing a partition or a wall easily. The proposed system by preparing a plurality of small-scale network is expected to be high-speed communication. The proposed system can be expected to improve convenience and security. And the proposed method can make multiple small network.

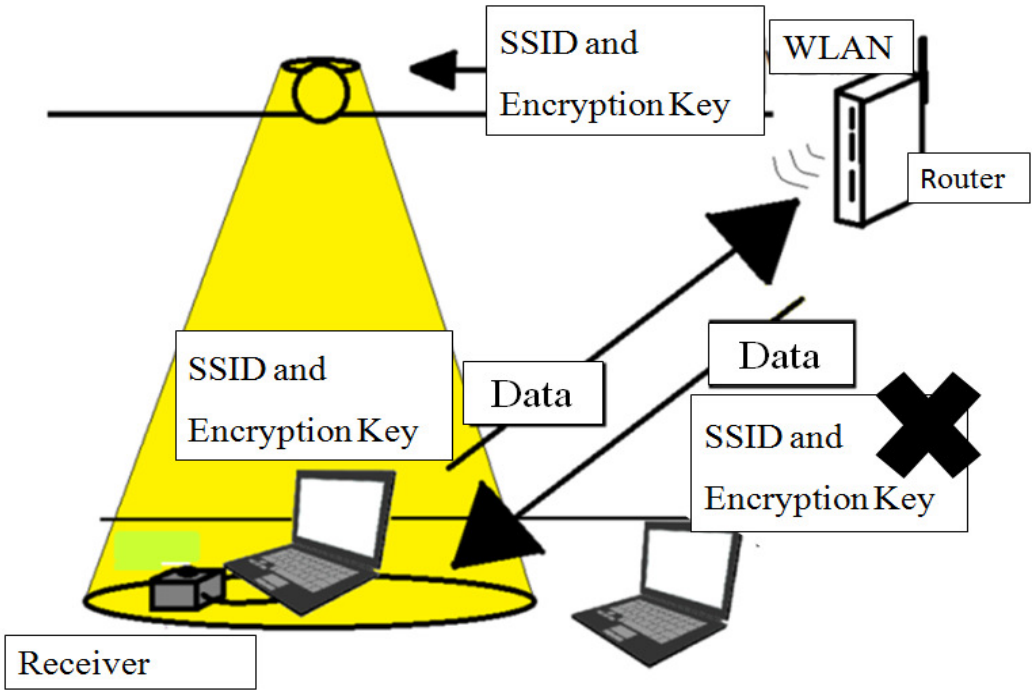

Figure 3: Overview of proposed system

4. EXPERIMENT

We show whether the proposed system can provide and change the encryption key without the burden for the administrator and users. We compare the time it takes to connect the network of proposed method and the two methods in the conventional methods. The first method in the conventional method is the type that does not use the encryption key. The second method in the conventional method is the type that uses the encryption key. Last method is our proposed method. We use fabricated the transmitter and the receiver in the experiment (Figure 4, 5). We make a shell script that receives the SSID and the encryption key from the receiver. The subjects are 5 men who are 20 years old are accustomed to the operation of the smart phone and computer.

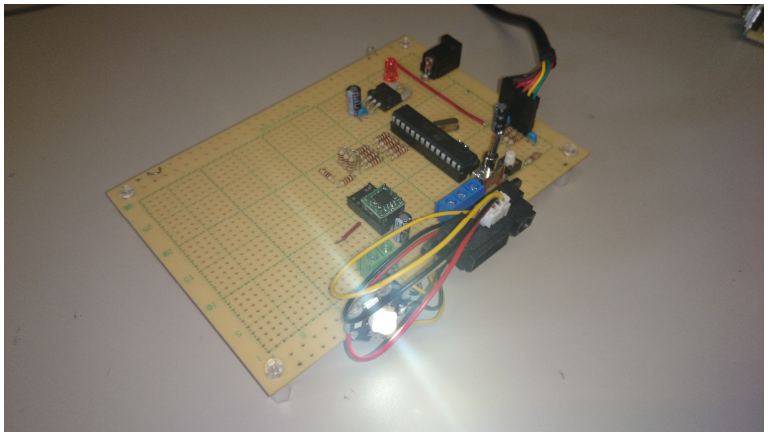

Figure 4: Visible light transmitter

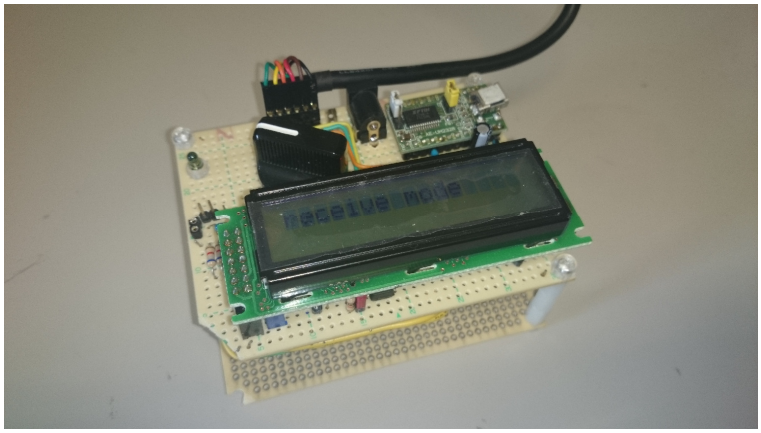

Figure 5: Visible light receiver

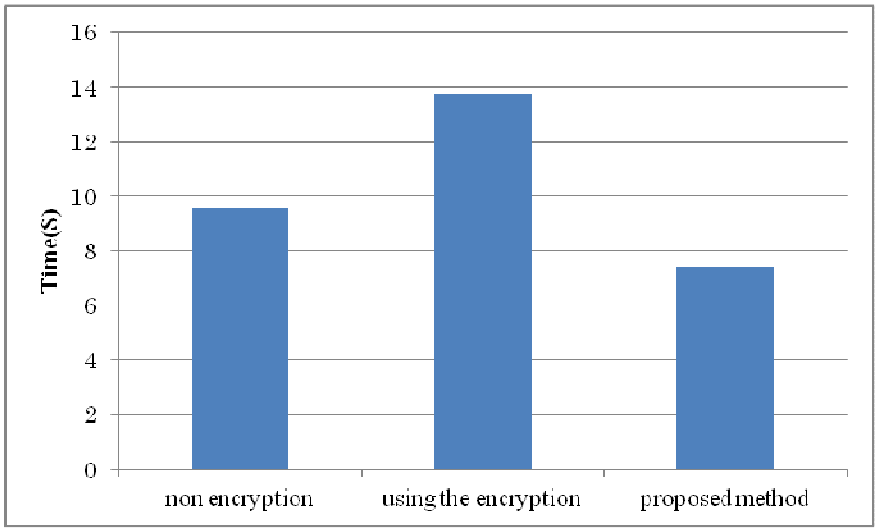

Figure 6: Experimental result

We show the experimental results in Figure 6. The vertical axis represents the time it took to connect the network. The method of shortest time to connect the network was our proposed method. Time of the method of longest time to connect the network was the method of using the encryption key. Because this is the labor required for the connection's associated with time. At the proposed method the computer get the SSID and the encryption key using the shell script from the receiver connected by USB. The effort of the users is only to connect the receiver and run the shell script. Time of users touching the keyboard is short. Therefore the time that takes for the connection is short. Users need only to select the SSID in the method that does not use an encryption key. However it is necessary to launch a network manager and select the SSID. In addition to it, the method that uses the encryption key requires the input of the encryption key. Thus, if time to touch the keyboard is short, we can reduce the time to require for connection.

In addition, the proposed method changes the SSID and the encryption key automatically. We switched the SSID and the encryption key every 60 seconds in this experiment. WPA2 which is one of the encryption methods encrypt the information by using the SSID and the encryption key. If the encryption key and SSID are immutable, WPA2 was weak for attack to prepare a dictionary in advance. However for changing the SSID and the encryption, the proposed system is strong for

such attacks. By using the proposed system and the conventional encryption, we can construct a secure and convenient network.

5. CONCLUSION

We proposed the distribution of encryption key and SSID using visible light communication. The public wireless LAN service has been increasing recently. It is a convenient service for short stay travelers particularly. However in order to improve the convenience, the services do not often use the encryption key or do not change the encryption key that has already been set. Therefore, the service has a problem in safety. We solve the problem using the visible light communication.

The visible light communication sends the signal by blinking the light. The visible light communication sends the signal by blinking the light. The visible light communication can use lighting equipments as the transmitter unlike infrared or radio communications conventional. Further, visible light communication can separate to clarify the transmission range by using light.

We proposed the distribution of encryption key and SSID using visible light communication. Visible light communication can easily prepare a small network, such as the partition or per room basis. For malicious users to connect the network is necessary to enter in the service provider area. Thus the administrator is able to easily manage users. In addition, it is possible to update the SSID and the encryption key by visible light communication easily for the proposed system. Thus if malicious users get the SSID and the encryption key, they cannot use the SSID and the encryption key immediately. Normal users may only need to run the shell script. Therefore, convenience is a good.

We fabricated the transmitter and the receiver in the experiment. In order to confirm the improved convenience, we measured the time it takes for a user to connect to the network. Comparison methods are methods that use or do not use the encryption key. As a result, users can to connect to the network in a short time compared with the conventional method. The system became very strong because it is possible to update the encryption key and SSID automatically in the security aspect.

REFERENCES

[1] Mostafa Azami, “Increasing the Network life Time by Simulated Annealing Algorithm in WSN with Point ", IJASUC Vol.4, No.2, 2013.

[2] S. Haruyama,"Visible light communication", Journal of IEICE, 94(12), D, pp. 1055-1059, 2011.

[3] Rajan Sagotra, "Visible Light Communication", International Journal of Computer Trends and Technology (IJCTT) volume4 Issue4, pp. 906-910, 2013.

[4] Dominic C. O'Brien, "Visible Light Communications: challenges and possibilities", PIMRC 2008. IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, pp.15-18, 2008.

[5] T. Saito, "A Study for flicker on Visible Light Communication", Technical Report of IEICE CS, vol. 106, No. 450, pp. 31-35, 2007.

[6] I. Shouichi, "Reduction of Flicker by Coding and Modulation for Visible-Light Communication" Technical Report of IEICE OCS, vol. 108, No. 39, pp. 1-4, 2008.

[7]Xin Lin, "Development of Visible-Light Wireless LAN Accesspoint with Illumination Fuction" IEICE Technical Report 109(245), pp.63-68, 2009.

AUTHORS

Kuniyoshi Okuda (b.1986) is a student of Ryukoku University in Japan. After studying Electronics and Informatics at Ryukoku University, he completed his Master of Engineering at Osaka City University. Now he is a doctor course student at Ryukoku University.

Takuya Yamamoto received B.E, M.E. and D.E. degrees from Ryukoku University and Osaka City University, in 2010 and 2012, respectively.

Tomoo Nakamura was born in 1948, and received B.E, M.E. and D.E. degrees from Kyoto University, in 1970, 1972, and 1988. He is a professor of Ryukoku University in Shiga, Japan.

Wataru Uemura was born in 1977, and received B.E, M.E. and D.E. degrees from Osaka City University, in 2000, 2002, and 2005. He is an associate professor of the Department of Electronics and Informatics, Faculty of Engineering Science, Ryukoku University in Shiga, Japan. He is a member of IEEE, RoboCup and others.