Wireless LAN Security Management with Location Detection Capability in Hospitals

K. Tanaka1; H. Atarashi1; I. Yamaguchi1; H. Watanabe1; R. Yamamoto2; K. Ohe3

1Department of Planning, Information and Management, The University of Tokyo Hospital, Tokyo, Japan;
2Interfaculty Initiative in Information Studies, The University of Tokyo, Tokyo, Japan;
3Graduate School of Medicine and Faculty of Medicine, The University of Tokyo, Tokyo, Japan

Keywords
Wireless LAN, security management, location detection

Summary
Objectives: In medical institutions, unauthorized access points and terminals obstruct the stable operation of a large-scale wireless local area network (LAN) system. By establishing a real-time monitoring method to detect such unauthorized wireless devices, we can improve the efficiency of security management. Methods: We detected unauthorized wireless devices by using a centralized wireless LAN system and a location detection system at 370 access points at the University of Tokyo Hospital. By storing the detected radio signal strength and location information in a database, we evaluated the risk level from the detection history. We also evaluated the location detection performance in our hospital ward using Wi-Fi tags.

Results: The presence of electric waves outside the hospital and those emitted from portable game machines with wireless communication capability was confirmed from the detection result. The location detection performance showed an error margin of approximately 4 m in detection accuracy and approximately 5% in false detection. Therefore, it was effective to use the developed location database containing radio signal strength and detection history. Results of this study showed that it would be effective to use the developed location database containing radio signal strength and detection history for security management of wireless LAN systems and more general-purpose location detection applications.

1. Introduction

A wireless local area network (LAN) system is an important component of the medical information network in numerous hospitals. Notebook computers are often used at bedsides throughout wards[1,2], to refer to laboratory results, and to execute order entry and management systems for treatment and injections. Moreover, various research on bioinstrumentation has been actively conducted using the wireless LAN system [3,4]. For stable operation of these systems, it is indispensable to secure availability of the wireless LAN environment. The fourth edition of the “Guidelines for the Security Management of Health Information Systems,” released in March 2009 [5] by the Japanese Ministry of Health, Labor and Welfare, provides details on security management issues. There exist several threats to the safe use of wireless LAN, including tapping, unauthorized access, and electric wave interference. Risks such as illegal invasion and falsification against information systems exist in the cases of both the cable LAN and the wireless LAN [6–8]; however, in the case of wireless LAN, the guidelines suggest certain measures against unauthorized computer access, such as “stealth mode,” “ANY connection refusal,” “use of SSID,” “MAC address restriction”, and “WPA2/AES.” By using such technical measures, we can safeguard information systems against these risks to a certain extent [9–11].

On the other hand, such technical measures alone are not sufficient to manage the threat of carried-in equipment. Patients may bring in their handheld devices with wireless communication capability. In some cases, medical staff set up unauthorized wireless equipment. This equipment can cause interference in the radio wave environment of medical institutions which is often difficult to detect the devices causing interference because of the building construction. When such equipment is considered a high risk factor to the stable operation of the wireless network systems, we need to establish systematic security measures [12] such as operation regulations. In fact, confirmations of the appropriate setting of the wireless LAN access points and explanations of the security rules to the staffs and in-patients are necessary as a basic operation management by human beings. In particular, it is difficult to keep stable operation of a wireless LAN system in a large-scale organization only by strictly enforcing operation regulations; therefore, it is necessary to
perform periodical or real-time status monitoring and provide feedback to relevant patients or staffs.

This research aims at the security management of a wireless LAN using a centralized controlled wireless LAN system at a large hospital with several wards. We developed an effective method with location detection capability for monitoring and filtering unauthorized devices and applied it to our hospital environment. Moreover, the developed location detection database of Wi-Fi equipment for security management can not only detect the existence of illegal equipment but also locate all the detected Wi-Fi equipment. This database enables us to acquire the location information of the object equipment, if necessary. The basic performance of this database was evaluated with the objective of applying it to the future use of location-based applications in hospitals.

2. Methods

2.1 Detection of Unauthorized Wireless Devices

The operation of a centralized controlled wireless LAN system began at our hospital in August 2006. Presently, approximately 500 wireless terminals operate daily on 40 floors, using 370 wireless access points. The main advantage of using the centralized controlled wireless LAN system is that the technical measures, such as "stealth mode", "ANY connection refusal", "use of SSID", "MAC address restriction", and "encryption method", can be uniformly managed. During system operation, the settings of the wireless access points can be changed, unlike in the case of an autonomous access point. Therefore, it is easy to change the settings of the whole wireless LAN system rapidly when a vulnerability is found. Moreover, the "MAC address restriction" on each floor was carried out in the past, and when the standalone access points were shifted to the centralized controlled ones, it was found that this policy gave the desired results at our hospital. The floor location of a terminal is identified by its VLAN ID (network segment), and this information helps to determine the terminal location and the surrounding situation, particularly when a problem arises. In our case, when a terminal attempts to connect with a network on an unauthorized floor, an authorization error occurs, the connection is denied, and the terminal becomes an unauthorized one.

The method of monitoring unauthorized computer access in wireless LAN for security management involves the following steps:

- Audit of connected record and error [13]
- Existence confirmation of unauthorized electric wave equipment [14, 15]

The existence of an unauthorized terminal can be confirmed by the former step; the latter step is carried out by the detection of carried-in equipment.

It is also possible to check the connections by the log confirmation of the authentication server (RADIUS) and to de-
Protect unauthorized connections in real time by the SNMP notification function built into the wireless LAN system. In the latter case, the purpose is to avoid the electric wave disturbance caused by unauthorized terminals and access points. However, it is often not easy to detect unauthorized access points, and it takes a considerable amount of time to investigate the location because the disturbance is temporary in many cases.

In this study, the location of Wi-Fi devices was detected by using a location detection system synchronized with a centralized controlled wireless LAN system. Figure 1 shows the entire system configuration. The wireless LAN system is composed of wireless access points and centralized controllers (Cisco Systems Inc., Wireless LAN Controller). Eight centralized controllers are set up in our hospital, where the main management controller is allocated according to the building and the floor. The location detection system (Cisco Systems Inc., Location Appliance) periodically acquires detected radio signal strength data from all controllers, calculates the location information of Wi-Fi devices, and maintains the calculated data inside the device.

The location detection system also has a SOAP/XML communication interface; therefore, we can extract the location information of the detected equipment with the radio signal strength (Received Signal Strength Indicator: RSSI) in real time by using a special API. In this study, we built an external database that contains the numerical data of calculation time, the detected floor, the position on the floor, and RSSI, which is extracted from the location detection system by using the API. From this database, we can obtain the historical location information of the detected devices.

Here, the SNMP alert function of the wireless LAN system and the location search function were combined by MAC address as key information. The cycle for monitoring and anomaly detection was shortened for daily operation; it improved the efficiency of security management monitoring.

Moreover, because many portable game machines with built-in wireless function, which have particularly found widespread use in recent years, were detected, impact evaluation was unified. Since this evaluation was essentially a qualitative evaluation, the state of communication, including packet loss, and the response of the Web browser were investigated under the wireless use of such game machines in all cases.

### 2.2 Location Detection Accuracy and Location Database

In this study, the detection accuracy at fixed positions and the performance against a moving object were verified by using Wi-Fi tags (AeroScout Inc.). The detection accuracy was evaluated by measuring the error margin between the detection result and the installed position at 20 arbitrary places on a ward floor. The developed positional history database was used for this measurement evaluation.

### 3. Results

#### 3.1 Detection of Unauthorized Access Points

The detection result of unauthorized access points for one week (2009/03/19 to 2009/03/25) is shown in Figures 2 and 3.
The number of detections increases rapidly when the RSSI value is less than –80. It is thought that the electric waves are emitted by devices placed outside the hospital, and these detections are made at higher elevations in a building. The number of detections of equipment whose RSSI value is greater than –80 is approximately 70. According to technical support information of Cisco Systems Inc., in the case of electric waves whose RSSI value is greater than –70, there is a possibility of achieving an excellent connection under IEEE 802.11b/g. Because such a rogue access point may cause electric wave interference with the neighbor access points and communication deterioration in the case of management terminals, it requires special attention.

The location detection system obtains the position information of each Wi-Fi device at 5-min intervals by communicating with the wireless LAN controllers. By periodically moving this data to an external database, we could identify the detected continuity time and the detected position history; this information is necessary for site investigation in the case of communication problems.

When a rogue access point is present in the operation environment, it can cause communication problems in the environment. Therefore, we must take immediate measures to deal with such an access point. In this examination, 36 rogue access points were detected in one week; during the investigation, 9 unauthorized access points with RSSI value greater than –70 were continuously detected. By evaluating the detected radio signal strength and continuance of the rogue access points, we can investigate and correspond with a certain priority against the investigated object and area range.

### 3.2 Detection of Portable Game Machines

The detection frequency of portable game machines was high in the above investigation. Figures 4 and 5 show the detection frequency and the number of unique detection devices. About 50% of these game machines were detected in the pediatric ward.

An electric wave having an RSSI value greater than –70 was detected, and 17 devices of above-mentioned 36 ones were portable game machines. This is considered a large value for the detection ratio. Although the detection frequency was low for a brief period, it could lead to communication failures. Therefore, further investigation was carried out using the game machine of two well-known manufactures, and it was observed that the detection status of both these machines on the wireless LAN system was different.

The game machine of Nintendo Co., Ltd. (Type A) was recognized as an ad hoc access point (host machine) or an ad hoc terminal (guest machine), and the ESSID was not confirmed.

The game machine of Sony Corporation (Type B) was recognized as an ad hoc terminal, and the ESSID of a peculiar pattern and the BSSID in the private range address were confirmed.

In both cases, game machines were recognized as IEEE-802.11b-standard-based equipment. Moreover, to measure their influence on a neighborhood terminal in the same segment as that of the game machine, the following two evaluations were carried out:

![Fig. 4 Number of portable game machine detections and their signal strength](image1)

![Fig. 5 Number of unique portable game machines detected and their signal strength](image2)
1. ICMP ping command (one packet/second)
2. Transfer rate of the packet (ttcp command/Windows XP)

The following results were obtained when the game machine was in use:
1. The response performance worsened (from 5 ms to 60 ms); however, a packet fall rarely occurred.
2. The transfer rate decreased from 16 Mbps to 5.6 Mbps.

The frame drop phenomenon of animation in streaming reproduction was confirmed, although the phenomenon of the Web-based application’s time-out was not observed in the verification.

### 3.3 Detection Performance

#### 3.3.1 Detection Accuracy

The outline of the measurement points and the detection results is shown in Figure 6, and the detection error margin in each measurement point is shown in Figure 7.

The value of the X-Y coordinates and a straight line distance between the mean detected location and the measurement location, where the detection result of five times acquisition at 5-min intervals was used, were measured by using Adobe Photoshop 5.5 on a drawing file. On an average of 20 places in the measurement part, the result of avg. 4.1 m (Max.: 10.3 m, Min.: 0.7 m) was obtained. The detection error margin was small in the center of the ward where the access points were closely set up, and it increased in the outer part where patient rooms were located. More-
over, the detection of the Wi-Fi tag on another floor and in another building was confirmed during the verification.

### 3.3.2 Follow-up Performance

The calculation position is smoothed by the wireless location detection system with the previously calculated position of the device. In the investigation, the weighting factor was 25% for the newly detected position and 75% for the previously detected position. As a result, when a large movement of a Wi-Fi tag occurs, the detection position catches up with the real position after approximately 20 min, which corresponds to four calculation times, as in the case of the example listed Table 1.

### 3.3.3 Misdetection of Floor and Building

While the previously mentioned positional accuracy was verified, misdetections were identified for a floor and a building, i.e., it was different from the actual installation position. Therefore, a follow-up survey was separately carried out by obtaining a continuous detection position for 24 h. Table 2 summarizes the results of this survey. Although there is a difference in the misdetection rate at each measurement location, it is observed that the misdetection rate increases when the measurement location is away from the access point. Moreover, the distribution of RSSI in the examination is shown in Figure 8. When the floor was misdetected, we confirmed that the RSSI value often becomes less than −70. Therefore, we believe that it is useful to consider RSSI as an index for the likelihood of the detection result. Further, because considerable detection on the floor under the control of a different centralized controller was confirmed when the floor was misdetected, we believe that a possible cause for failure of the data acquisition of a specific centralized controller was its own overload or a network connection failure.

### 4. Discussion

#### 4.1 Security Management of Wireless LAN System

When a wireless LAN system is operated in medical institutions, the appropriate management of wireless access points and connected terminals is an important task for maintenance of safety. In general, a feasible solution has been obtained for prevention of the use of illegal equipment, by techniques such as SSID in the IEEE 802.11 standard, WPA encryption, and the PKI authentication mechanism. On the other hand, it is difficult for the network administrators to manage an external electric wave and carried-in equipment.

In this paper, a monitoring technique that involves detection by a centralized controlled wireless LAN system and location information archive is described. It was possible to reduce the load related to monitoring by assigning priority to detected devices with filtering on the basis of radio signal strength and examining a considerable number of notifications using several indicators. Moreover, the continuing risk was recognized by referring to the detected location archive and the detection frequency using the developed location information database. Further, it was possible to use this database for prior correspondence.

In addition, the existence of portable game machines that used the same frequency band and standard of electric wave could be recognized on this system. It was confirmed that the communication performance could possibly deteriorate because the use of these game machines could become a noise source against the operation environment. It was believed that the error rate could easily increase because of the existence of turbulent electric waves during a real-time process such as reproduction of a burst transfer and animation to generate a time-out by the process of resending of the packet and to ensure the failure of the communication packet. The actual measurement value decreased to approximately 1/3 the transmission rate. The influence on the operational environment of this electric wave disturbance is believed to be closely related to the time-out value of

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>222.98</td>
<td>121.85</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>208.88</td>
<td>155.73</td>
<td>−14.1</td>
<td>33.88</td>
</tr>
<tr>
<td>8</td>
<td>202.2</td>
<td>175.18</td>
<td>−6.68</td>
<td>19.45</td>
</tr>
<tr>
<td>13</td>
<td>200.41</td>
<td>182.55</td>
<td>−1.79</td>
<td>7.37</td>
</tr>
<tr>
<td>18</td>
<td>200.3</td>
<td>185.68</td>
<td>−0.11</td>
<td>3.13</td>
</tr>
<tr>
<td>23</td>
<td>201.6</td>
<td>187.58</td>
<td>1.3</td>
<td>1.9</td>
</tr>
</tbody>
</table>

Table 1 Example of transition at time of detection location

<table>
<thead>
<tr>
<th>Location no.</th>
<th>Number of measurements</th>
<th>Misdetection rate [%]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>288</td>
<td>2.4</td>
</tr>
<tr>
<td>2</td>
<td>288</td>
<td>1.7</td>
</tr>
<tr>
<td>3</td>
<td>288</td>
<td>1.0</td>
</tr>
<tr>
<td>4</td>
<td>288</td>
<td>0.3</td>
</tr>
<tr>
<td>5</td>
<td>288</td>
<td>1.7</td>
</tr>
<tr>
<td>6</td>
<td>288</td>
<td>6.3</td>
</tr>
<tr>
<td>7</td>
<td>288</td>
<td>29.9</td>
</tr>
<tr>
<td>8</td>
<td>288</td>
<td>0.0</td>
</tr>
<tr>
<td>9</td>
<td>288</td>
<td>19.4</td>
</tr>
<tr>
<td>10</td>
<td>288</td>
<td>2.8</td>
</tr>
<tr>
<td>11</td>
<td>288</td>
<td>0.0</td>
</tr>
<tr>
<td>12</td>
<td>288</td>
<td>3.5</td>
</tr>
<tr>
<td>13</td>
<td>288</td>
<td>1.4</td>
</tr>
<tr>
<td>14</td>
<td>288</td>
<td>0.7</td>
</tr>
<tr>
<td>15</td>
<td>288</td>
<td>14.6</td>
</tr>
<tr>
<td>16</td>
<td>288</td>
<td>0.3</td>
</tr>
<tr>
<td>17</td>
<td>288</td>
<td>1.0</td>
</tr>
<tr>
<td>18</td>
<td>288</td>
<td>0.0</td>
</tr>
<tr>
<td>19</td>
<td>288</td>
<td>20.1</td>
</tr>
<tr>
<td>20</td>
<td>288</td>
<td>6.9</td>
</tr>
<tr>
<td>Total</td>
<td>5760</td>
<td>5.7</td>
</tr>
</tbody>
</table>

Table 2 Misdetection rate at each measurement location
the real-time application used; this time-out value was derived from the communication procedure. Therefore, according to the setting of the time-out value between the server and client communication used in running applications, the possibility of causing unavailability of the application is unable to disregard. It is necessary to continue observing the failure that originates in the packet fall to the response needed as an application and the increase in the communication error rate continuously.

4.2 Location Detection System and Its Capability

In recent years, several location detection systems connected by the wireless LAN in an organization have been researched [16, 17]; and a similar system is used in this study. However, because the necessary space and time resolution performance is different in each application, a prior site survey is necessary. Wireless mobile PCs conform to the Wi-Fi standard and can be used when they are connected to the access points on the floor. The location information of these PCs can be calculated by detecting the radio signals related to the transmission and reception of data of the OS and the application. In contrast, radio signals and calculated positions of rogue access points are often transient; therefore, the accuracy of calculated positions is thought to be dependent on the installation situation of the access points and the detection situation. In addition, in order to detect the location of medical staff or medical equipment using Wi-Fi tags, it is necessary to verify the detection accuracy in a similar manner.

In this study, it was confirmed that there was a restriction in the follow-up performance of the portable device and the detection error margin at a regular position as a result of evaluating the detection performance by using the location detection system and Wi-Fi tags. For the cyclic calculation and the smoothing process, about 20 min settling time was necessary; therefore, although it may be difficult to apply the location detection system for tracking objects with high time resolution that move around a hospital ward, we can use the detected location information for tracking objects that remain for long enough. However, it is necessary to develop a location management application, considering the detection error margin and false detection.

The detection error margin was several meters long. Considering the calculation method of triangulation that uses radio signal strength, we need to install additional access points at a location with sparse wireless access points for precision enhancement, if necessary. In our hospital, the access point arrangement was mainly determined considering the coverage area; therefore, the detection accuracy in the patient rooms located toward the end of floors was not as good as expected. However, we can confirm the existence of a target device with a certain accuracy using the location detection system.

The misdetection of floor and building in the investigation is thought to be mainly caused by the failure of the data collection by the concerned wireless LAN controller. As a result, a calculation might be performed with insufficient data and resulted in a misdetection. Moreover, misdetections to a close floor were often made, though there were less frequent cases of building misdetection in the false detection results. Appropriate logic is necessary to evade these misdetections, while referring to not only newly calculated location information but also the detected radio signal strength and a past detection history. For such a purpose, the use of the developed location database is effective in the development of a judgment logic referring to the historical location and the radio signal strength for improvement of the location detection accuracy.

5. Conclusion

This paper describes the detection of unauthorized wireless access points using a centralized controlled wireless LAN system, the positional confirmation technique, and the investigation results. By filtering detected results with radio signal strength and duration, we could obtain accurate location information of unauthorized devices. Moreover, we evaluated the impact of detected portable game machines with wireless functions and confirmed a danger of performance deterioration depending on the communication technique of the operation application. Finally, we verified the basic performance of location detection system. The detection accuracy could be secured by including detected radio signal strength and the location history as evaluation factors, using the developed archive database. This database may be applicable to other location-based applications, such as location management of medical equipment in hospital wards.
References


