病院情報システム端末からの安全なインターネット接続に関する検討

田中 勝弥[1)] 山本 隆一[2)] 大江 和彦[3)]
東京大学医学部附属病院[1)] 東京大学大学院情報学環[2)] 東京大学大学院医学系研究科[3)]

A Study for Safe Internet Access from Hospital Information System Terminals

TANAKA KATSUYA[1)] YAMAMOTO RYUICHI[2)] OHE KAZUHIKO[3)]
The University of Tokyo Hospital[1)]
Interfaculty Initiative In Information Studies, Graduate School of The University of Tokyo[2)]
Graduate School of Medicine and Faculty of Medicine, The University of Tokyo[3)]

This paper describes a study on safe direct access to the Internet from a hospital information terminal. In the guidelines, published by the Ministry of Health, Labour and Welfare, direct connections to the Internet from a hospital are not inhibited, but they suggests close supersivion should be required for the safe use. Therefore, many hospitals have no Internet connection though the demand is growing. This study has an aim to describe requirements and concrete examples for a safe Internet connection from a hospital. For the purpose of grasping the current usage of the Internet, we carried out statistical investigation about the real traffic of the Internet in 2 university hospitals, that already has a direct access to the Internet.

Keywords: Network Security, The Internet, Hospital Information System

1. はじめに

医療機関の大部分は何らかの情報システムを導入し、レセプトオンライン、緊急安全性情報へのアクセス、診療ガイドラインへのアクセスなど外部ネットワークへのアクセスに対する医療機関側からの要求は増大してきている。厚生労働省による「医療情報システムの安全管理に関するガイドライン」では、インターネットへの接続を禁止はしていないが、厳重な対策を求めており、一般の医療機関が安易に接続できる状況ではない。

政府でも、「新たな情報通信技術戦略」の実現[2)]と並行して、「国民を守る情報セキュリティ戦略」において、情報セキュリティへの政策として、サイバー攻撃・情報漏えいやデバイス・技術の多様化などを焦点として、政府関連組織のセキュリティ基盤強化や利用者への普及・啓蒙活動、人材育成に対する取り組みを行っている[3-6)]

とくに経済産業省では、民間企業を対象として、これまでにコンピュータウィルスや不正アクセスを対象とした情報システムの基本的な安全管理基準にくわえ、Webを含むソフトウェアの脆弱性に対する基準やフィッシング対策ガイドラインの作成なども行っており[7-9)]、情報セキュリティに対して専門の人材確保が行えない中小企業への支援も重点とされている。

こうした状況において、医療機関においてインターネットに直接接続する場合に考えられるリスクとしては、

1) マルウェア等の混入により、診療情報システムに予期せぬ障害がもたらされること
2) 通信先が適切に認証されない状況での利用により、なりすまし等による情報漏洩が起こること
3) 通信内容が適切に秘匿されず、患者・医療者に関する機微な情報の漏洩が起こること
4) 利用者による公序良俗に反した利用がなされること

などが挙げられる。ブロードバンドの普及と上記のような啓蒙活動により一般市民のITリテラシーは向上してきてはいるが、中小企業の場合と同様に専門人員の確保が困難な医療機関が、こうしたリスクに対する自らの情報資産の安全を確保した上で診療に必要なインターネット通信を行える状態を促進するためには、リスク分析および対応要件を詳細に定義し、接続の程度に応じた現実的に可能な方法や具体例を示す必要がある。

本稿では、要件定義のための検討材料の一つとして、すでにインターネット接続を行っている大学病院における利用状況の分析を行った。

2. 方法

現在の利用状況の把握のため、パケット解析装置を用い、2つの大学病院においてインターネット利用状況の調査を行った。双方の大学病院ともに施設内からのインターネット接続を行っているが、A大学病院は診療端末からのインターネットアクセスは禁止されており、個人ないしは診療科の端末からアクセスができる。一方で、B大学病院はそれらに加えて、診療端末からのインターネットアクセスが可能である。

調査期間は平日の1週間程度とし、プロトコル・宛先サイトの分類・利用帯域・セッション数などの統計情報を採取した。パケット解析装置として、Cisco Systems社製のService Control Engineを使用した。

3. 結果

3.1 サービス別の利用帯域

どちらの大学病院でも、インターネット利用のうち大部分がHTTPやHTTPSといったブラウザ系の通信で帯域が使用されている(図1～2)。また、メールの受信、IM、VoIP通信、FacebookやTwitterによる専用プロトコルなども観測される。

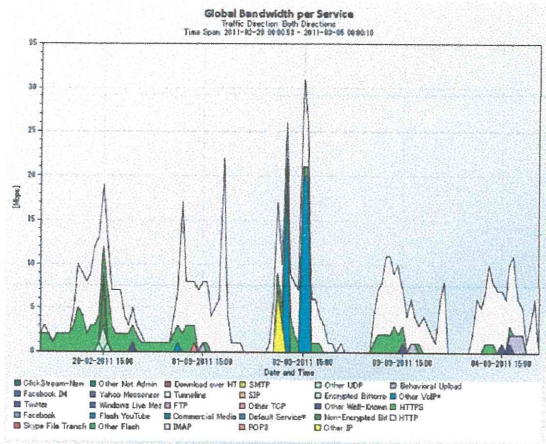

図1 サービス別通信流量(A大学病院)

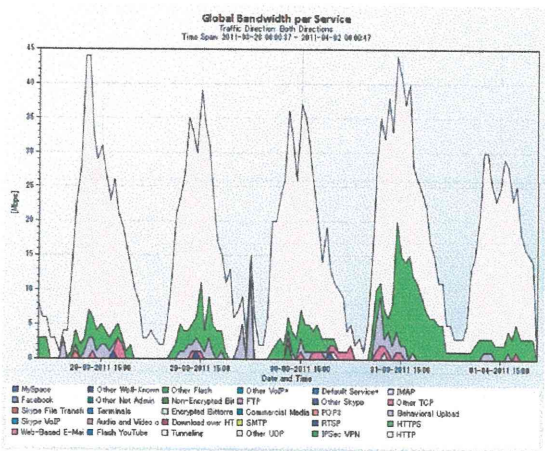

図2 サービス別通信流量(B大学病院)

3.2 Webサイト利用

利用形態として帯域の大半をしめるWeb系の通信について、アクセス先サイトの内訳は、図3～4のとおりとなる。アクセスページ数として多いのは、情報検索目的と思われる検索エンジンやtwitter・facebookなどの利用のほか、文献検索サイトへのアクセスも上位に観測された。また、OSやウィルス対策ソフトウェアのアップデートによるアクセス数も上位に観測された。

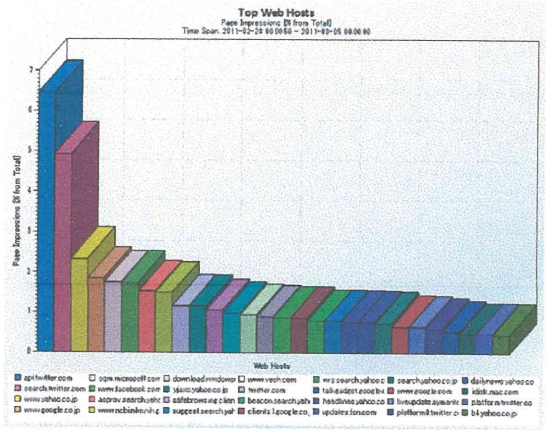

図3 Webサイトのアクセス状況(A大学病院)

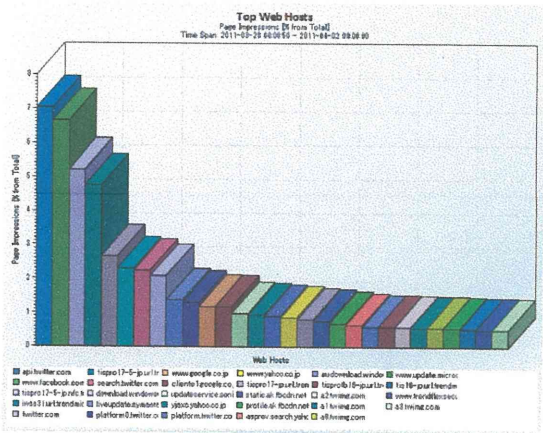

図4 Webサイトのアクセス状況(B大学病院)

3.3 外部からのアタック

外部からの不正アクセスとして、Webサーバへの攻撃と見られる80番ポートへのアクセスが多く観測された(図5)。また、データベース接続やリモートアクセス用のサービスへのアクセスが検出されている。

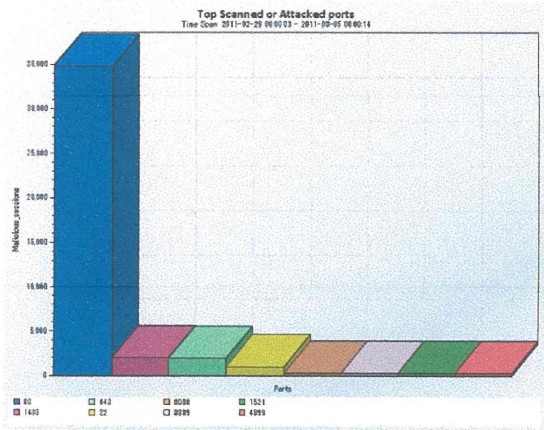

図5 ポート別不正アクセス検出数(A大学病院)

4. 考察

4.1 利用状況

本稿の調査では、とくにWebを利用した情報検索エンジンの利用が圧倒的なアクセス数を有し、その他に、電子メールの送受信を含めると大半の利用数がカバーされる。利用者へのヒアリングでは、情報検索対象として、医薬品・診療ガイドライン・副作用・略語・学術文献・他医療機関やその担当医師名の情報などが挙げられた。したがって、Web・メールとに対する安全性の確保とこれら以外の通信を区別・制限できるか、といったことが大きな課題になると考えられる。Webアクセスに対するリスク軽減策の一つとして、不特定のサイトアクセスを回避するために、事前登録制によりアクセス先を限定することも考えられるが、維持管理にかかる人的負担は大きい。たとえば、外来診療システム端末からのWebによるアクセスサイト数は約14000サイトにのぼる(B大学病院、2011年6月分)。

4.2 リスクと対策

厚生労働省「医療情報システムの安全管理に関するガイドライン 第4.1版」に記載されているように、不正ソフトウェア対策、不正アクセスに対する技術的対策は行う必要がある。利用状況の調査にも見られる多くのWebアクセスやメールの受信など外部コンテンツを取得する場合には、個々の情報システム端末上でマルウェア対策ソフトを導入するのが効果的であると考えられる。

たとえば、2011年8月の一か月間で、B大学病院では、全429件(Web経由:1件、USB経由:4件、その他は受信メール経由)のウィルス検出があり、いずれも対策ソフトにより駆除あるいは隔離されている。

一方で、こうした対策ソフトは、定義ファイルを常に最新のものに維持しておかなければ、新しいマルウェアに対応できないため、業務システムとしても対策ソフトの最新化を行える機能が求められる。同様に、こうしたマルウェアが標的とする基本OSの脆弱性についても個々の情報システム端末で常に最新化されること、業務システムが基本OSの最新化に対応していることが求められる。逆に、特殊な検査機器など、こうした技術的な対策が取れない機器は、医療機関内部でネットワークとしても区別される必要がある。

また、インターネット接続することにより、医療機関側のネットワーク機器やサーバコンピュータが外部からの攻撃対象となりうるため、ネットワーク機器・サーバコンピュータにおいても同様に基本OSやアプリケーションの脆弱性対策を行うことが求められる。大規模病院では多くの場合、外部からのアタックは対策がされており、ファイアウォール等により効果的にブロックされているが、特にアプリケーションサーバごとの脆弱性への対応[10]など、情報収集段階から人的努力に依存する部分が大きい場合もあり、どのようなサイトにも期待できるとは限らない。

このような技術的な対策で一定の防御が可能なリスクのほかに、Webやメールによる人為的な情報漏洩もリスクとして考えられる。これに対しては、継続的な運用ルールの周知やセキュリティ教育などを実施するといった人的対策が必要と考えられる。

4.3 接続形態

現状で病院情報システム端末としては、インターネット接続を禁止しているケース、アクセス可能な端末を別に設置するケース、直接アクセスが可能なケースがある。今回調査を行った大学病院のような大規模機関では、自身でインターネット接続を行い、一定の専門知識を持った管理要員が情報システムを管理している場合がほとんどであり、先に述べた技術的対策は自身で行っている。これに対し、一定の専門知識のある管理要員を確保できないケースでは、上述のような技術的対策を、外部サービス利用により実現することも考えられる。多くの商用サービスプロバイダでも、メール・Web利用時のウィルススキャンやP2P通信対策などのサービスが提供されてきている。インターネット接続を行う際に、情報システム端末上での対策とあわせて、こうしたサービスを利用することにより、一定の安全性を確保できると考えられるが、公的機関等による接続サービスの運営も考慮し、さらに詳細に検討する必要がある。

5. おわりに

医療機関からのインターネット接続の要求は今後ますます増加すると考えられ、施設規模に応じていくつかの接続形態が想定される。今後、接続形態による実装例を挙げながら、さらにリスクおよび対策について詳細な検討を行う。

なお本研究は平成22年度厚生労働科学研究費補助金(地域医療基盤開発推研究事業)「病院情報システム端末からの安全なインターネット直接接続に関する研究(H22ー医療ー一般ー030)」において実施した。

参考文献

[1] 厚生労働省:医療情報システムの安全管理に関するガイドライン 第4.1版(平成22年2月).http://www.mhlw.go.jp/shingi/2010/02/s0202-4.html.
[2] 高度情報通信ネットワーク社会推進戦略本部(IT戦略本部).http://www.kantei.go.jp/jp/singi/it2/index.html.
[3] 内閣官房情報セキュリティセンター.http://www.nisc.go.jp/index.html.

[4] 国民を守る情報セキュリティサイト.http://www.nisc.go.jp/security-site/index.html.
[5] 警察庁　サイバー犯罪対策.http://www.npa.go.jp/cyber/.
[6] 国民のための情報セキュリティサイト.http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm.
[7] 経済産業省 情報セキュリティ政策ポータル.http://www.meti.go.jp/policy/netsecurity/.
[8] インターネット安全教室｜経済産業省 JNSA.http://www.net-anzen.go.jp/.
[9] フィッシング対策協議会　Council of Anti-Phishing Japan.http://www.antiphishing.jp/antiphishing_guide.pdf.
[10] Japan Vulnerability Notes.https://jvn.jp/.

Wireless LAN Security Management with Location Detection Capability in Hospitals

K. Tanaka[1]; H. Atarashi[1]; I. Yamaguchi[1]; H. Watanabe[1]; R. Yamamoto[2]; K. Ohe[3]
[1]Department of Planning, Information and Management, The University of Tokyo Hospital, Tokyo, Japan;
[2]Interfaculty Initiative in Information Studies, The University of Tokyo, Tokyo, Japan;
[3]Graduate 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 consider the radio signal strength as both an index of likelihood at the detection location and an index for the level of risk.

Conclusions: We determined the location of wireless devices with high accuracy by filtering the detection results on the basis of 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.

Correspondence to:
Katsuya Tanaka
Department of Planning, Information and Management
The University of Tokyo Hospital
7-3-1, Hongo, Bunkyo-ku
Tokyo 113-8655
Japan
E-mail: katsuya@hcc.h.u-tokyo.ac.jp

Methods Inf Med 2012; 51: 221–228
doi: 10.3414/ME10-01-0002
received: January 12, 2011
accepted: February 15, 2011
prepublished: March 21, 2011

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

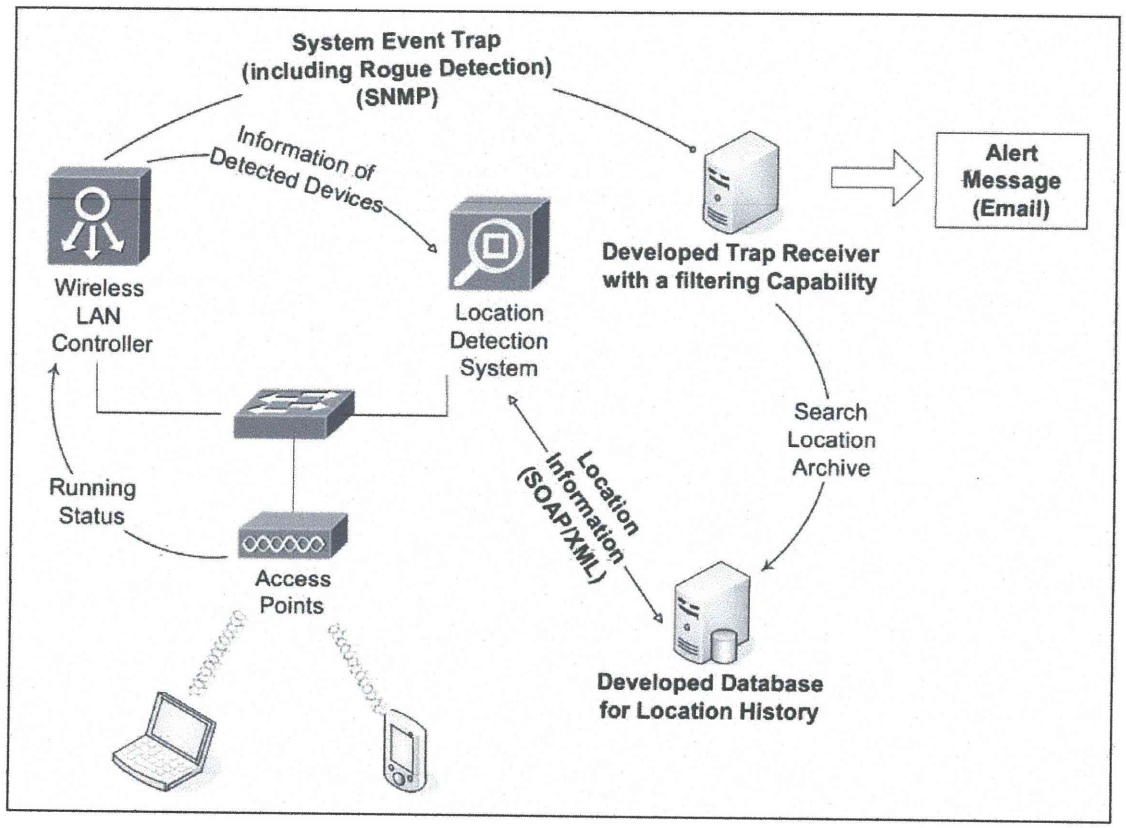

Fig. 1 Overview of wireless LAN system with location detection system

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-

tect 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.

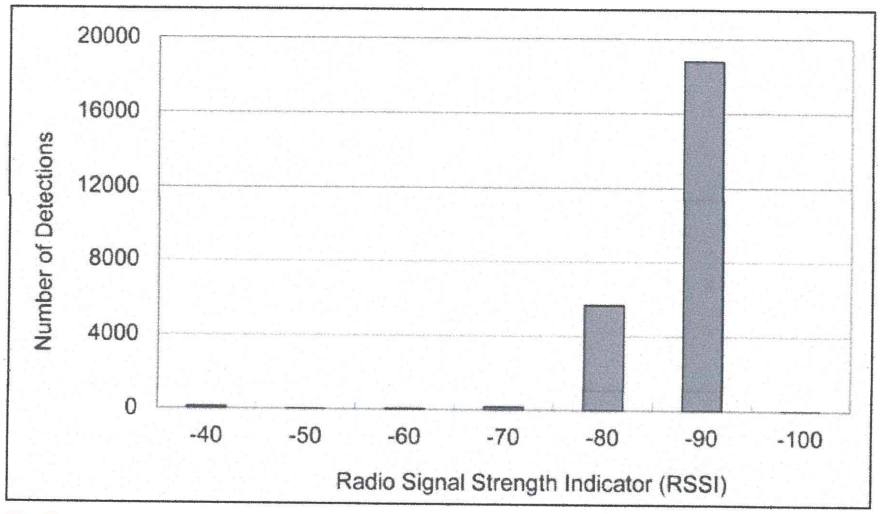

Fig. 2 Number of unauthorized device detections and their signal strength

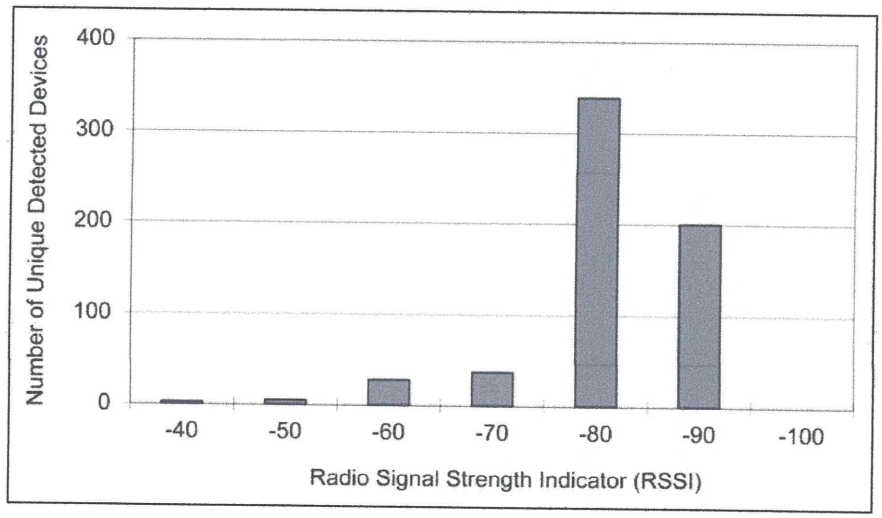

Fig. 3 Number of unique unauthorized devices detected and their signal strength

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.

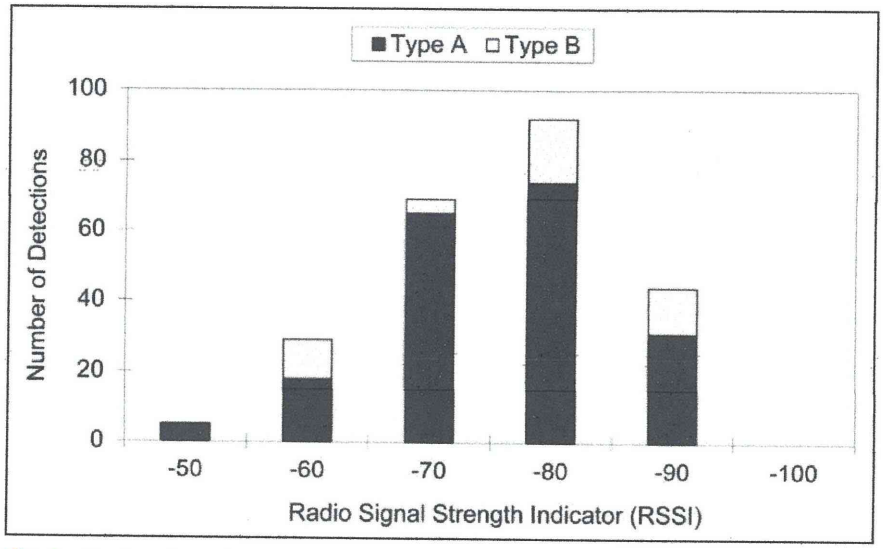

Fig. 4 Number of portable game machine detections and their signal strength

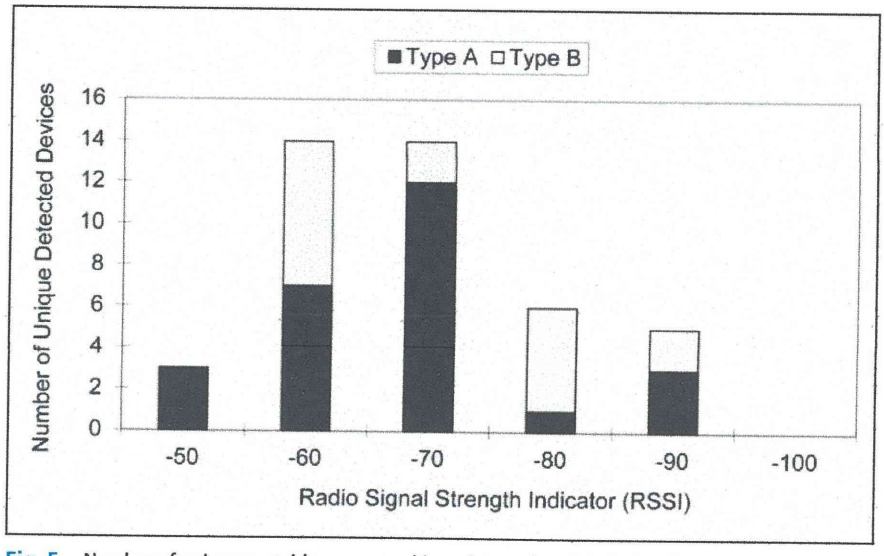

Fig. 5 Number of unique portable game machines detected and their signal strength

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 continuance 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:

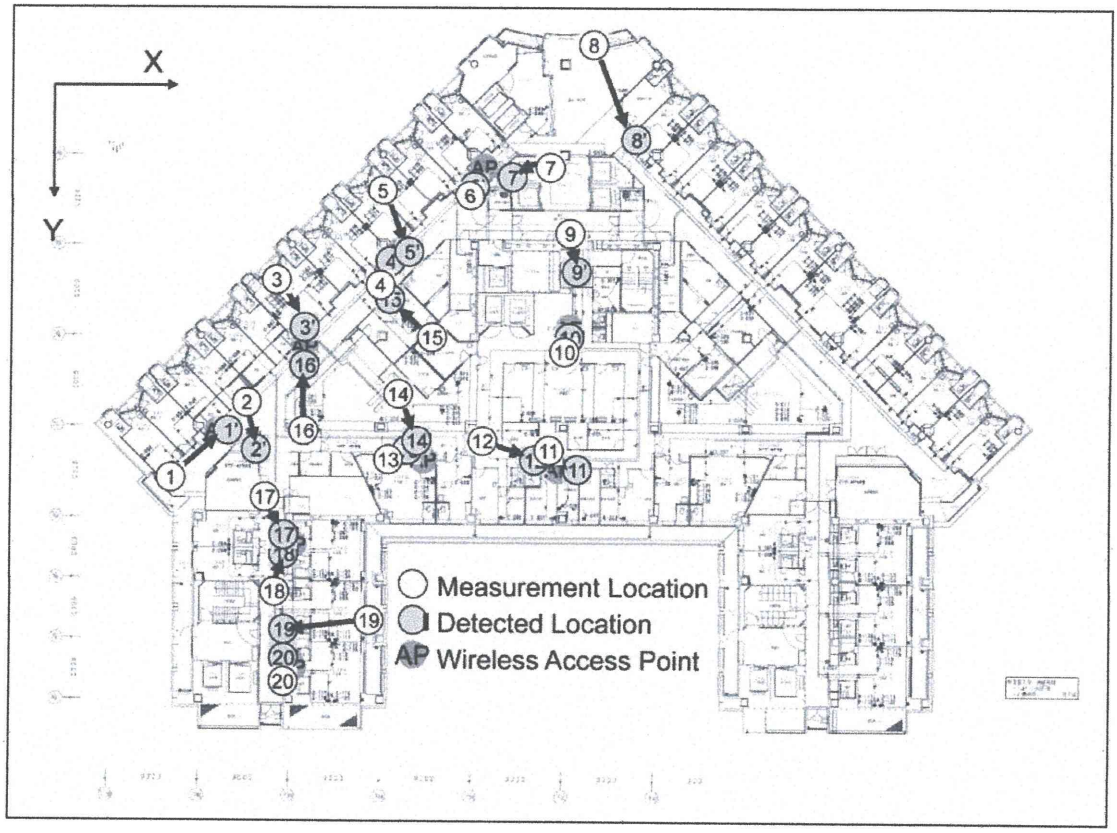

Fig. 6 Overview of measurement location and error margin in a ward

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.

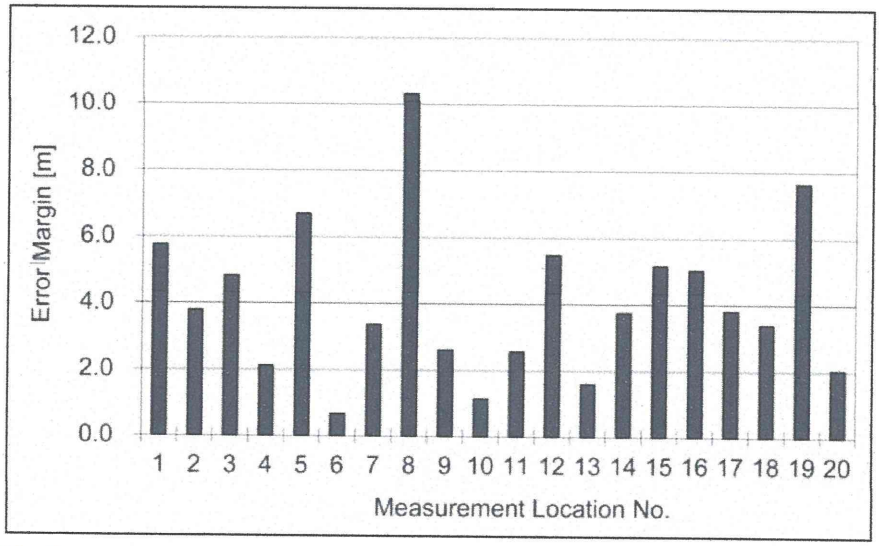

Fig. 7 Error margin at each measurement location (location no. is same as that in Fig. 6)

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-

Time [min]	X [feet]	Y [feet]	Delta X [feet]	Delta Y [feet]	
0	222.98	121.85	0	0	move start
3	208.88	155.73	–14.1	33.88	
8	202.2	175.18	–6.68	19.45	
13	200.41	182.55	–1.79	7.37	
18	200.3	185.68	–0.11	3.13	
23	201.6	187.58	1.3	1.9	convergent

Table 1 Example of transition at time of detection location

Table 2 Misdetection rate at each measurement location

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

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 continuance of 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

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.

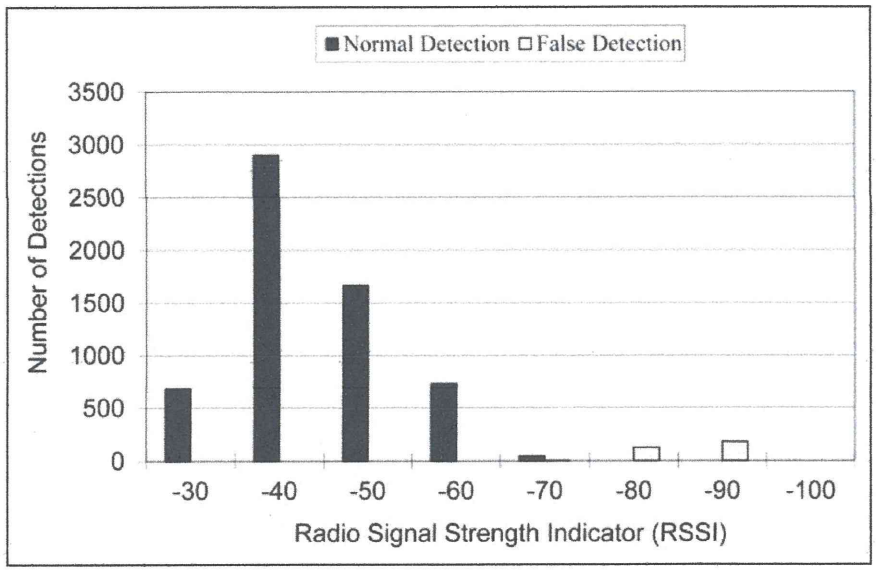

Fig. 8 Distribution of signal strength when normal and when misdetected

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

1. Chen Y, Chiu H, Tsai M, Chang H, Chong C. Development of a personal digital assistant-based wireless application in clinical practice. Computer Methods Programs Biomed 2007; 85 (2): 181–184.
2. Hauser ES, Demner-Fushman D, Jacobs LJ, Humphrey MS, Ford G, Thoma RG. Using wireless handheld computers to seek information at the point of care: an evaluation by clinicians. J Am Med Inform Assoc 2007; 14 (6): 807–815.
3. Triantafyllidis A, Koutkias V, Chouvarda I, Maglaveras N. An open and reconfigurable wireless sensor network for pervasive health monitoring. Methods Inf Med 2008; 47 (3): 229–334.
4. Struzik ZR, Yoshiuchi K, Sone M, Ishikawa T, Kikuchi H, Kumano H, et al. "Mobile Nurse" Platform for Ubiquitous Medicine. Methods Inf Med 2007; 46 (2): 130–134.
5. Ministry of Health, Labor and Welfare (Japan). Guidelines for the Security Management of Health Information Systems. Available at http://www.mhlw.go.jp/shingi/2010/02/s0202–4.html. Unofficial English translation is available at http://rylab.hcc.h.u-tokyo.ac.jp/guidelines.html.
6. Samani R. When networks collide. Information Security Technical Report 2007; 12 (2): 98–110.
7. Wan Z, Deng HR, Bao F, Ananda LA. Access control protocols with two-layer architecture for wireless networks. Computer Networks 2007; 51 (3): 655–670.
8. Solms B, Marais E. From secure wired networks to secure wireless networks? what are the extra risks? Computers & Security 2004; 23 (8): 633–637.
9. Furnell S, Ghita B. Usability pitfalls in wireless LAN security. Network Security 2006; 2006 (3): 4–8.
10. Katos V, Adams C. Modelling corporate wireless security and privacy. J Strategic Inform Systems 2005; 14 (3): 307–321.
11. Badra M, Urien P, Hajjeh I. Flexible and fast security solution for wireless LAN. Pervasive Mob Comput 2007; 3 (1): 1–14.
12. Mahanti A, Williamson C, Arlitt M. Remote analysis of a distributed WLAN using passive wireless-side measurement. Performance Evaluation 2007; 64 (9–12): 909–932.
13. Sobh ST. Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art. Computer Standards & Interfaces 2006; 28(6): 670–694.
14. Potter B. Rogue access points? threat to enterprise security. Network Security 2003; 2003 (4): 4–5.
15. Liao I, Kao K. Enhancing the accuracy of WLAN-based location determination systems using predicted orientation information. Inf Sci 2008; 178 (4): 1049–1068.
16. Kao K, Liao I, Li Y. Detecting rogue access points using client-side bottleneck bandwidth analysis. Computers & Security 2009; 28 (3–4): 144–152.
17. Curtis WD, Pino JE, Bailey MJ, Shih IE, Waterman J, Vinterbo AS, et al. SMART–an integrated wireless system for monitoring unattended patients. J Am Med Inform Assoc 2008; 15 (1): 44–53.