Design of a Wireless Networks Detection and Management System Based on a Mobile Terminal

[1] Zhen-jiang Zhang, [2] *Mei-kui Zhang, [3] Lei Xia, [4] Hua-yu Shi
1, First Author Chinese PLA General Hospital, Beijing, China,
zzj@301hospital.com.cn
*2,Corresponding Author Chinese PLA General Hospital, Beijing, China,
zmk301@126.com
3,4 Chinese PLA General Hospital, Beijing, China

Abstract-In this paper, we present a wireless networks management system based on a mobile terminal detector. The system is designed on C/S architecture, consisting of client and server software, a centralized database and a data sharing in-sync mechanism. It helps to detect wireless access point devices automatically. The detailed information of wireless access point devices, such as precise location, will be stored in a shared centralized database. By using the data sharing in-sync mechanism, the data is consistent, even when multiple terminals access the database at the same time. The system makes wireless network safer, and network management work easier.

Keywords: Wireless Network; Mobile Terminal; Signal Detection; Information Security

1. Introduction

As we all know, wireless networks are widely used in almost every field in our lives. You can surf the Internet and do some shopping at home using a tablet computer, which is connected wirelessly to an APD (Access Point Device). You can transfer photos from one mobile phone to another one using a Bluetooth connection. Wireless technology is even used to avoid traffic accidents [1]. All of these are benefits of wireless technology. It's a fact that we are now living in a world full of unseen wireless signals.

Whilst wireless technology has brought us convenience and a new technological lifestyle, it has also brought us the risk of information loss and the problem of data security. A recent survey showed that the rate of security breaches on wireless networks is on an upward trend [2]. For example, a 104-bit WEP key can be broken in less than 60 seconds [3]. The Internet search engine results for "CRACK WEP" or "BREAK WEP" key words are extensive, and tools to break WEP passwords are widely available for download. Even a WPA2 password can be cracked in just a few minutes with the right software. The security of wireless networks is increasingly the focus of information and network security departments.

There are many kinds of wireless devices, which can be used to build wireless networks. All wireless devices work on an allocated frequency band. The most common public frequency band is 2.4GHz, implemented in a serial wireless protocol (IEEE 802.11b/g) [4,5]. Bluetooth (IEEE 802.15) technology also works at 2.4GHz [6]. The latest protocol, IEEE 802.11n operates on both the 2.4GHz and 5GHz bands [7]. This paper only focuses on 2.4GHz wireless signal detection and management, as this frequency band is the most common and widely used in current Wi-Fi devices.

The difficulties of wireless network management are due to the inherent characteristics of a wireless network itself. Wireless APDs are widely available and at low cost. They allow even novice users to configure their own wireless networks easily. That is to say, the implementation of a wireless network is so simple, and it can be managed easily. The administrator in charge of the network security needs to know the exact number of wireless network devices and the locations of them. However, as these devices are so easily available, it's very difficult to monitor this. This is a typical problem that network administrators in large corporations with extensive / complex computer networks face everyday.

Another problem introduced by wireless technology is the security of connections from an unauthorized network. Wireless access devices usually provide a DHCP (Dynamic Host Configuration Protocol) service, which allow any terminal wireless device to access the APD without configuring a static IP address. That means, the terminal wireless device may be able to connect to two different computer networks simultaneously. It's very dangerous if one of the networks is a secure network with access to sensitive or private information, and the other a public network connected to the Internet. In fact, the likelihood of such events happening is very high.

So the problem of wireless network management consists of two parts: one, locating the access points and two, how to get detailed information from wireless users and their devices.

2. Method

Invisible wireless signals are around us all the time. We can detect them using devices such as mobile phones, which can receive GSM (Global System for Mobile Communication) or CDMA (Code Division Multiple Access) signals. Similarly, we can detect the signals sent from a wireless access device at the frequency 2.4GHz using a special device. According to the intensity of signal detected, it is possible to accurately determine how far it is from the detection device and locate the wireless APD. After that, the network administrator can add a record containing detailed information about that particular wireless APD to the database, which can be accessed at any time it is needed. Therefore, a wireless network detection and management system consists of mobile detection terminal, management software, management information database and data sharing in-sync mechanism.

2.1. The Mobile Detection Terminal

The mobile detection terminal is also called the MTD(Mobile Terminal Detector). The wireless network detector has two basic functions: to receive the wireless signals and record their intensities. Generally, most mobile terminal devices have an integrated Wi-Fi module. However, they are not usually supplied with software tools or open class software libraries to develop additional functions relating to the Wi-Fi module. This is considered a security feature. Therefore, third party or private class libraries will be used to develop the management software and interface [8,9].

The relative intensity of a wireless signal perceived by the detector, is a function of the distance between the detector and wireless APD. The greater the distance, the weaker the wireless signal received. (See Figure 1 below). Using this feature, we can determine the location incrementally by moving closer to the APD.

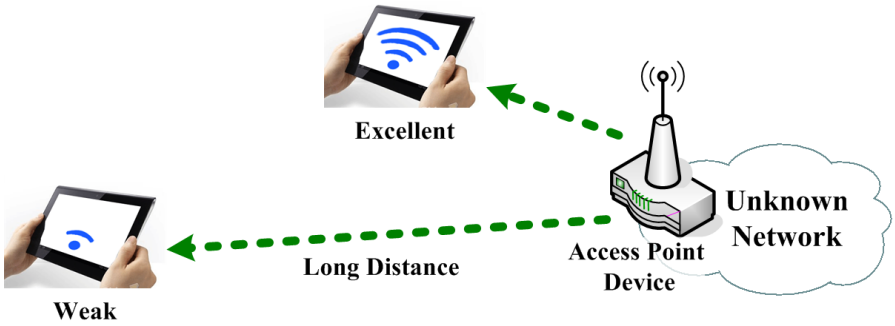

Figure 1. Signal Intensity Relative to Distance between APD and MTD

2.2. Management software

The management software has a client / server architecture, which consists of two parts: client software and server software. Client software has the function to collect the wireless signal information. Server software receives the information and manages it. The following is a detailed description.

2.2.1. Client Software

Client software runs on a mobile terminal device, which handles several functions.

The first function of client software is to perceive wireless signals. The mobile terminal device can track several wireless signals simultaneously and obtain their basic information, such as SSID (Service Set IDentifier), encryption method, and so on. But the mobile terminal device does not know from where the signals are being sent.

The second function is to analyze the intensity of the wireless signal. Although the device can detect several signals simultaneously, it can only interrogate one signal at a time. Generally, the user will select which signals are to be interrogated further. Based on the different signal intensity detected, the mobile terminal device user will know how far the wireless AP source is from the detector [10]. Therefore, it is completely possible to locate the AP source.

The third function is to make a new record for the selected wireless signal, and obtain detailed AP information. The mobile terminal device user needs to record information such as, building name, floor information, room number and so on. Even a snapshot of the wireless AP device taken from the mobile terminal device can be added in the record.

The last function is to determine the type of wireless network being used.

Figure 2 shows the identification process example.

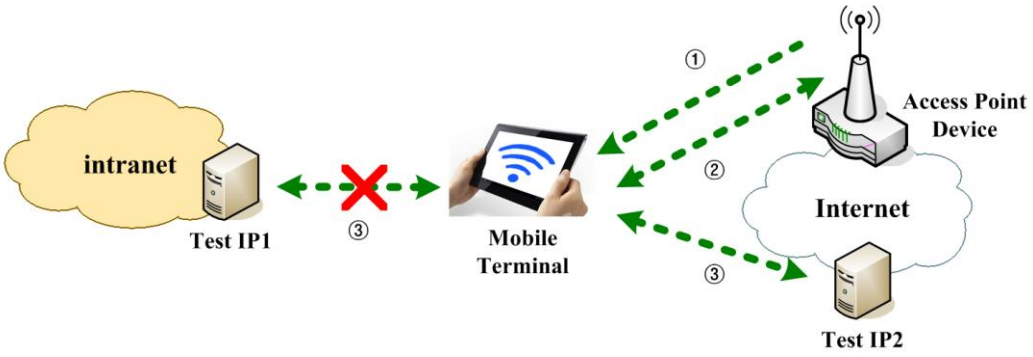

Figure 2. Network Type Identification Process (Step 1, the mobile terminal has detected an unknown wireless signal. Step 2, the mobile terminal accesses the wireless network. Step 3, the mobile terminal tests the IP address of each different network. As the figure shows, Test IP address 1 intranet test failed but Test IP address 2 was successful.)

2.2.2. Server Software

Server software is running on the server exchanges data with server software, such as the information collected by mobile terminal device. The detector not only uploads data to the server, but also downloads data from the server when necessary. We call this the Data Sharing Mechanism. The following section will discuss this in detail.

The Server is responsible for the operations with DBMS (Data Base Management Software). The operations include Insert, Delete, Query and Update. Additionally, the server also does some detection work. The difference of detection work between the server and client is that the server is not wireless, but wired. The main detection work is to test the status of the APDs. If some APDs are offline, the server will notice the status change immediately. From the perspective of the network administrator, this function is a benefit to network management.

2.3. Management Information Database

Both client and server software communicate with databases, transferring data between the client and server. That means there are at least two databases: one is on the client terminal device, the other is on the server. Client software has a lightweight database, storing and dealing with temporary data, such as the information relating to the wireless APD. The most commonly used format is XML database file. The definition of XML files is pre-designed as XSD files. As a result, one XML file stands only for one APD. The database deployed in the server is bigger, which is the master information center of wireless network access points. The fields of a complete record include the following: SSID; Encryption Method; Access Password (optional); Location; MAC Address; Status; User Name; User Contact; Network Type; Wireless Type; Snapshot Picture.

Some of the fields maybe null because the information fields are not available. 'Status' indicates whether the wireless network works normal. 'Network Type' includes at least two options: Internet or Intranet. 'Wireless Type' is distinguished by IEEE 802.11b/g/n or Blue-tooth protocols. All of these options are defined in menu lists, which are stored in the server database.

2.4. Data Sharing In-Sync Mechanism

In a real working environment, two or more mobile terminals could be operating in different places at the same time. All of the terminals upload or download data at any time, so a mechanism for keeping data consistent is needed.

The idea is to build up a data sharing in-sync mechanism, which will solve the data consistency problem mentioned above. In most cases, its function is to keep the data safe and up-to-date. Assuming that a terminal detector detects a wireless signal, the client software immediately retrieves the existing record by comparing the basic information, such as SSID, MAC Address etc. If some of the records are matched, any new information relating to the wireless APD will be refreshed on to the server database, allowing other terminal devices to download the latest data.

Based on the data sharing in-sync mechanism, the server software has an additional function. If the server database is updated by one client terminal software, the server will push a message to the other terminals to update the records. Message pushing is widely used in the applications of mobile phones, tablet computers and PCs (Personal Computer).

3. Results

3.1. Initiative Detection

The wireless APDs make the wireless application's implementation easier. However, other personal APDs will make the network management more difficult. It is hard to determine the location of an unauthorized APD. The activities of an unauthorized APD accessing the

network could result in a dangerous data security problem.

It is almost an impossible task to determine the number and location of all wireless APDs on the network, especially as there are so many unauthorized APDs. With a portable tool, the network manager can take the MTD anywhere and detect wireless signals and unauthorized access devices at any time. We call this 'Initiative Detection'.

In fact, the wireless networks detection and management system based on the mobile terminal is not only a management system, but also a check-up tool which is a good tool to detect unknown wireless signals and ascertain their senders' locations for the information and network security department.

3.2. Wireless APD Database

The wireless networks detection and management system builds up a central database for the wireless APDs. The database maintains a record set for all access devices, storing their latest information while the data sharing in-sync mechanism ensures the data consistent. The network manager can query the latest information at any time.

3.3. Client / Server Architecture

The system uses client / server architecture which supports multi-clients mode, so that several client terminal detectors can work at the same time. Although every client terminal has its own database to store information from wireless APDs, the master data center is stored in the server database. This design makes the data centralized and a wireless APDs information database is created. This architecture is better for wireless network management based on a mobile terminal.

3.4. Intuitive Operation

For network administrators, it's a brand-new experience to detect wireless signals using a MTD. Sometimes the device can automatically obtain information from the APD directly; however often manual data entry by the user will be required. The process of adding information from a detected wireless APD is easy and efficient because the system has defined many simple drop-down menu lists. The operator can select the appropriate option by a simple finger gesture on the touchscreen. As the menus are pre-defined, data entry is simple and intuitive, with less opportunity for mistakes or missed information fields [11].

4. Discussion

4.1. Benefits

The wireless networks detection and management system based on a mobile terminal is an efficient tool. By using the mobile detector, the number of wireless APDs, their information, exact locations and even the type of network the are connecting to can be identified and recorded. Further application may inform the network administrator which terminals are logged in on the wireless access point, including the Terminal Type, Hostname, MAC Address and so on.

4.2. Problems and Solutions

Actually accessing a particular detected wireless access point is difficult to accomplish because most of APDs will be configured with an encrypted password. That is to say, although we can detect the SSID of the APD, without the password (from the APD owner), it is not possible to access the device easily. One solution may be to use a tool such as a WEP password cracker, although these tools must be used under legal conditions.

Another typical case happens when the mobile terminal is unable to connect to the server wirelessly to update the database. The MTD stores data locally on its own XML database, but it cannot be uploaded via the network to the server database. The data sharing in-sync mechanism allows the user to upload data asynchronously. Therefore, when the network connection is re-established, or the terminal is connected to a computer by wire, the user can upload data immediately.

To locate the APD's location is not very easy in complicated environment. It depends on the sensitivity of the detector to wireless signal intensity. Although environmental factors such as obstacles and interference affect the sensitivity of the detector, it is reasonable to assume that the wireless signal is always within several meters of the wireless signal source. If the detector is not sensitive enough, it will not be able to determine the precise location of wireless APD.

Nowadays the scale of networks is becoming larger, and the application of wireless networks ever wider. Wireless networks management is increasingly difficult. Application of the wireless networks detection and management system based on a mobile terminal is not only very important, but also necessary.The system provides the network administrators with a tool to manage wireless networks from a new operational perspective. The initiative detection approach makes daily network management more efficient. The central database stores the most complete, latest wireless network and APDs information. If unauthorized APDs are detected, the administrator will cut the connection

between the device and the network. Furthermore, a blacklist can be created to prevent the illegal devices from re-connecting to the network again.

5. Conclusion

The wireless networks detection and management system based on a mobile terminal is a client / server architecture system. It realizes the management of wireless networks and wireless APDs. The client mobile terminal is in charge of detecting and analyzing the wireless signal, transferring information data to the server and keeping the data refreshed. The server maintains a centralized database and distributes the latest data to all mobile terminals. The system makes the management of wireless networks easier and more efficient.

Through a wireless networks detection and management system based on a mobile terminal, many of the features can also be integrated with the telemedicine system, so that patients could have completed care at home or at work just with a mobilephone[12]. In addition, mobile health is a new and advancing field in telehealth. It can be used to transfer patient biometrics, to provide reminders to patients about medications or scheduled medical appointments, and to empower patients by sending out information such as the nearest location to get help or an update on diabetes management. So, the wireless networks detection and management system based on a mobile terminal has practical significance and theory value and can be applied in every aspect of our life,.

6. Acknowledgement

This article supported by the funding of the National High Technology Research and Development Program (2009AA02Z412).

7. References

[1] Williams Thomas, Alves Paul, Lachapelle Gerard, Basnayake Chaminda, “Evaluation of GPS-based methods of relative positioning for automotive safety applications”, Transportation Research Part C-emerging Technologies, vol. 23, no. 8, pp. 98-108, 2012.

[2] Malekzadeh Mina, Ghani, Subramaniam Shamala, “A new security model to prevent denial-of-service attacks and violation of availability in wireless networks”, International Journal of Communication Systems, vol. 25, no. 7, pp. 903-925, 2012.

[3] Tews Erik, Weinmann Ralf-Philipp, Pyshkin Andrei, “Breaking 104 bit WEP in less than 60 seconds. Information Security Applications”, vol. 4867, pp. 188-202, 2007.

[4] IEEE Std 802.11b-1999 (R2003)

[5] IEEE Std 802.11g-2003

[6] Vallejos de Schatz Cecilia H., Medeiros Henry Ponti, Schneider Fabio K., Abatti Paulo J, “Wireless Medical Sensor Networks: Design Requirements and Enabling Technologies”, Telemedicine and E-health, vol. 18, no. 5, pp. 394-399, 2012.

[7] IEEE Std 802.11n-2009

[8] Fernamdes Chandra, Kok Yew Ng, Boon How Khoo, “Development of A Convenient Wireless Control of An Autonomous Vehicle Using Apple iOS SDK”, 2011 IEEE REGION 10 CONFERENCE TENCON 2011, pp. 1025-1029, 2011.

[9] Bainomugisha Engineer, Vallejos Jorge, Boix Elisa Gonzalez, Costanza Pascal, D’Hondt Theo, De Meuter Wolfgang, “Bring Scheme programming to the iPhoneuExperience. Software-Practice & Experience”, vol. 42, no. 3, pp. 331-356, 2012.

[10] Chan Eddie, Baciu George, Mak S. C, “Wireless Signal an information Tracking Using Fuzzy Logic. Studies in Computational Intelligence”, 1st international Joint Conference on Computational Intelligence, pp. 59-72, 2011.

[11] Hoggan Eve, Brewster Stehpen A, Johnston Jody, “Investigating the Effectiveness of Tactile Feedback for Mobile Touchscreens”, CHI 2008:26TH ANNUAL. CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEM VOLS 1 AND 2, pp. 1573-1582, 2008.

[12] Chung-Hsin Liu, Wen-Yen Tseng. Journal of Convergence Information Technology(JCIT) Vol.6, No.10, pp.106-114. 2011.