Available at
www.ElsevierComputerScience.com
POWERED BY SCIENCE DIRECT®

Computer Communications 27 (2004) 739–742

computer communications

www.elsevier.com/locate/comcom

GPRS-based WLAN authentication and auto-configuration

Phone Lin, Yi-Bing Lin*,[1], Vincent Feng, Yen-Cheng Lai

Department of Computer Science and Information Engineering, National Chiao Tung University, 1001 Ta Hsueh Road, Hsinchu 30050, Taiwan, ROC

Received 23 October 2003; accepted 24 October 2003

Abstract

This paper proposes an authentication and auto-configuration mechanism for wireless LAN (WLAN) based on short message service of mobile telecommunications network. Our approach automates the authentication and WLAN configuration setup procedure without involving the users.

Keywords: Authentication; General packet radio service; Short message service; Wireless LAN

1. Introduction

In the recent years, wireless Internet services have become one of the most important communications industrial trends and research directions. Two technologies are widely utilized to support wireless Internet services:

- Packet-switched based mobile telecommunications networks such as *General Packet Radio Service* (GPRS) or *Universal Mobile Telecommunication System* (UMTS) [4] have become a nature candidate for supporting wireless Internet services. The GPRS/UMTS networks have been widely deployed with large service coverages. However, the transmission rates are typically limited to no more than 40 kbps in most commercial GPRS networks. The UMTS networks support transmission rates up to 2 Mbps for each mobile user.
- Wireless LAN (WLAN) [3] was originally deployed for cable replacement. Recently, this technology has been enhanced with mobility support and is considered for business operations. Compared with the mobile telecommunications networks, WLAN systems can be easily deployed to support high-speed transmission. However, the spectrum of WLAN is not licensed, which may be interfered with other radio usage. Furthermore, WLAN service coverages are much smaller than that of mobile telecommunications networks.

Studies have been conducted [1] to investigate integration of WLAN and mobile telecommunications networks to take advantages of both technologies. That is, the system always connects a mobile user to WLAN whenever it is available (so that the user can enjoy high bandwidth transmission). If WLAN is not available, then the user is connected to GPRS/UMTS (so that access availability is always guaranteed). The models investigated by most studies focused on 'handover' between WLAN and mobile networks. On the other hand, integration of user identity and authentication for networks owned by various operators is an important issue in commercial operation, which has not been explicitly addressed in most previous studies [1]. In the existing business operations, a WLAN user must become a customer of various WLAN service operators to gain access to networks of these operators (which implies that a user must fill in many service subscription forms). To access WLAN networks of different operators, the user typically goes through various login procedures manually with different account/password formats. Furthermore, the user must remember WLAN card configuration setups for various WLAN networks. It is clear that such exercise is not user friendly. This paper proposes an approach to unify the WLAN user identity through GPRS/UMTS network, and automates

* Corresponding author. Tel.: +886-3-573-1842; fax: +886-3-572-4176.
E-mail address: liny@csie.nctu.edu.tw (Y.-B. Lin).
[1] Chair Professor of Providence University.

0140-3664/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2003.10.013

the authentication and WLAN configuration setup procedures without involving the users.

2. Authentication and auto-configuration

We consider an environment where the GPRS/UMTS network has full service coverage of a large area (e.g. the whole island of Taiwan) and the WLAN service coverages are limited to disjoint small zonal areas such as airports, shopping malls, and so on. These small service areas may be operated by various WLAN service providers. Fig. 1 illustrates the network architecture for the approach we proposed. In this architecture, a WLAN user utilizes a *Mobile Station* (MS) or *Mobile Terminal* (MT; Fig. 1(1)) to access the WLAN networks. An MT can be a notebook or PDA installed with a WLAN card and a GPRS/UMTS card. A notebook typically provides two PCMCIA slots that can accommodate both WLAN and GPRS cards. Also, WLAN and GPRS/UMTS dual-mode PCMCIA cards are now available [5]. We assume that the MT accesses *short message service* (SMS) through the GPRS/UMTS mobile network (Fig. 1(2)). By communicating with a WLAN access point (AP; Fig. 1(3)), the MT accesses Internet services through a gateway named *WLAN Gateway* (WGW; Fig. 1(4)).

Our approach utilizes standard GPRS/UMTS authentication mechanism to authenticate the MT. That is, the WLAN user is authenticated by GPRS/UMTS before he/she can access the WLAN services. The authentication procedure consists of two phases. In Phase I, the MT is authenticated by GPRS/UMTS to gain the SMS access. Then the MT triggers encrypted SMS to interact with the WLAN Location Register (WLR; Fig. 1(5)) to obtain a dynamically assigned password (to be used in Phase II authentication) and the configuration file of the WLAN network. The WLR is implemented on iSMS (Fig. 1(6)) [6], an SMS-based Internet application development platform to be elaborated in Section 3. In Phase II, the MT uses the configuration file obtained from the WLR to access the WLAN network, and is authenticated by the WGW using the password obtained from the WLR. The configuration file includes information such as the *Extended Service Set Identification*(ESS ID) [3] of the WLAN network, the *Wired Equivalent Privacy* (WEP) configuration (for encryption), the IP address of the WGW, and the assigned password.

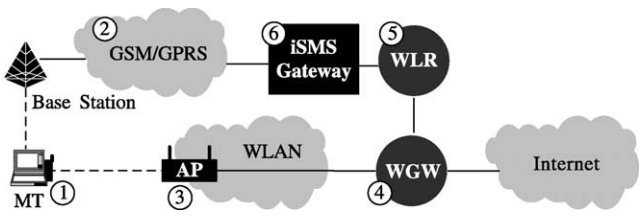

Fig. 1. The network architecture.

In Phase I, the MT is authenticated by GPRS/UMTS and then registers to the WLR as described in the following steps.

Step 1.
The MT first attaches to GPRS/UMTS (and therefore is authenticated by the standard GPRS/UMTS authentication procedure [4]). If the MT has been attached to GPRS/UMTS before Phase I authentication is executed, then this step is skipped.
Step 2.
The MT sends the WLAN Registration Request message to the WLR. Note that the WLR is assigned an MSISDN, and the MT-to-WLR communication is just like the standard GPRS/UMTS MT-to-MT communications. All messages exchanged between the MT and the WLR are implemented using encrypted SMS.
Step 3.
The WLR obtains the location of the MT and determines the target WLAN that will provide access service to the MT. Note that the WLANs in different locations may have different configuration setups. Therefore it is important to identify the WLAN network where the MT resides so that the parameters of the MTs WLAN card can be properly set up. We will elaborate on how to obtain the MTs location in Section 3.
Step 4.
The WLR issues the WLAN Information Request to the target WGW. All messages exchanged between the WLR and the WGW are implemented on IP. In commercial operations, the WGW and the WLR are connected by dedicated links. If the WGW and the WLR are located in different networks, then the exchanged messages can be protected by IPsec.
Step 5.
The target WGW creates a WLAN user record for this incoming visitor. Then the WGW dynamically generates a password. This password is stored in the WLAN user record and is then sent back to the WLR together with the WLAN configuration file through the WLAN Information Response message.
Step 6.
The WLR forwards the password and the configuration file to the MT through the WLAN Registration Response message.
Step 7.
The MT sets up the WLAN card using the received configuration file. If the setup is successful, the MT replies the Registration Complete message to the WLR and Phase I authentication is complete.

The round trip elapsed time T_D of SMS deliveries in Phase I is shown in Fig. 2. In most cases, T_D are limited within 20 s. In Phase II, the MT exercises the authentication procedure with the WGW to gain access to the WLAN network. Since the MT has configured the WLAN card at Step 7, the first contact from the MT to the target WLAN

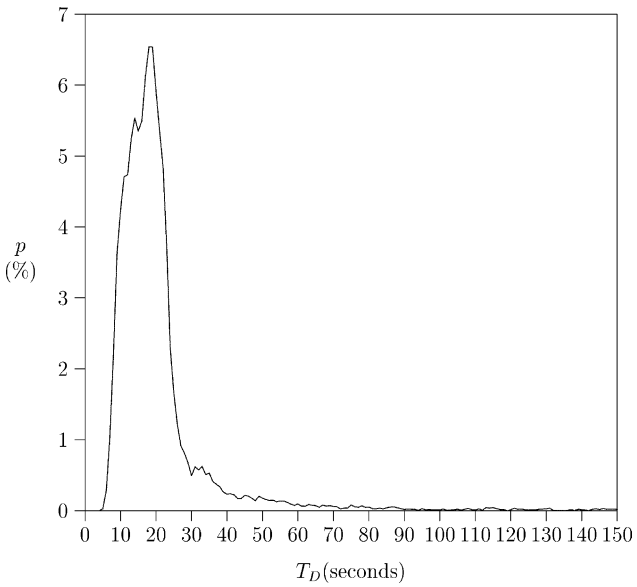

Fig. 2. The round trip elapsed time distribution for Phase I.

network can be protected with WEP encryption. We note that WEP is acknowledged to have serious problems, which will be addressed in Section 4.

In most existing approaches, before an MT can access the WLAN Internet services, it requires manually off-line configuring of the MTs WLAN card or the MT must communicate with the WLAN AP to obtain configuration parameters without WEP protection. The advantage of our approach is that only legal MTs can automatically and safely configure the WLAN cards before accessing the WLAN network. Any MT without correct configuration setting will not be able to access the target WLAN network.

Step 8.
The MT connects to the WGW through the WLAN. The MT sends the WLAN Authentication Request message with the password to the WGW. All messages exchanged between the MT and the WGW are implemented on IP.
Step 9.
The WGW searches the corresponding WLAN user record. The password stored in the record is retrieved to compare with the received password. If the comparison is successful, the WGW will allow the MTs IP address to pass through the firewall.
Step 10.
The WGW replies the MT the WLAN Authentication Ack message. At this point, the WLAN user can access the Internet through the WGW.

The user can explicitly terminate the WLAN access by a logout procedure exercised between the MT and the WGW through the WLAN connection. In some situations, the WLAN connection may be implicitly disconnected (for example, the user moves out of the WLAN coverage). In this case, the MT will detect the situation and sends a short message to WLR/WGW through GPRS/UMTS to terminate the WLAN connection.

3. Implementation of WLR

This section discusses the implementation of WLR and location detection of the WLAN users.

In our approach, the WLR is implemented using the iSMS gateway [6]. iSMS is an operator-independent platform that integrates the IP network with the SMS in mobile telephone systems. Through iSMS, an IP host in the external data network can offer Internet services to an MT. Specifically, messages are created by an iSMS application agent (WLR in our example; see Fig. 3(1)) implemented on the IP host, and then sent to the iSMS gateway (Fig. 3(2)). The iSMS gateway consists of a server (Fig. 3(3)) connecting to a GPRS/UMTS modem (Fig. 3(4)) that delivers the messages to the MT through the SMS. In the iSMS platform, no components in GPRS/UMTS are modified. The iSMS gateway can be implemented by an off-the-shelf high-reliability PC or workstation connected to a GPRS/UMTS handset.

The location of a WLAN user can be identified at Step 3 in two approaches:

WLAN-Based Location Detection. If the APs of the WLAN networks in different locations use different ESSIDs, then the WLAN networks can be distinguished by their ESSIDs. In this case, the WLAN user should obtain the ESSID of the target WLAN before executing Step 2 in Phase I authentication, and then sends the ESSID to the WLR at Step 2. The WLR then identifies the target WLAN using the received ESSID. In this approach, the ESSID of an WLAN network is broadcast by the APs, which may be accessed by illegal users. Another restriction of this approach is that different WLAN networks must be configured with different ESSIDs.

UMTS-Based Location Detection. The existing GPRS/UMTS location tracking mechanism is utilized to identify the MTs location. This approach can be implemented in either the *core network layer* or the *application* layer. In the core network layer approach,

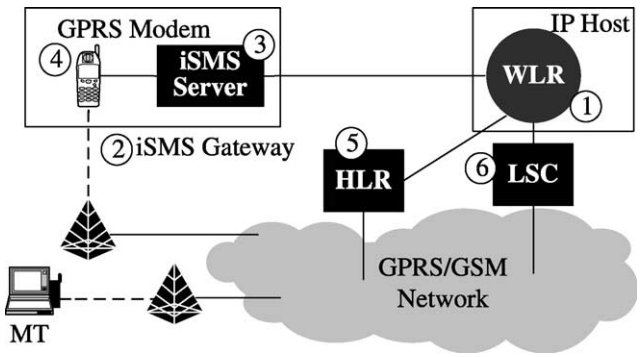

Fig. 3. WLR, iSMS Gateway, HLR, and LSC.

the WLR is equipped with the GPRS/UMTS *Mobile Application Part* (MAP) protocol to query the *Home Location Register* (HLR; see Fig. 3(5)) at Step 2. The HLR will return the routing area (RA) of the user to the WLR. In this case, every RA area accommodates exactly one WLAN network.

If location service is offered by the GPRS/UMTS network, then location tracking at the WLR can be implemented in the application layer. That is, the WLR will query the *Location Service Center* (LSC; see Fig. 3(6)) for location information of the WLAN user. Details of the location service can be found in Ref. [2].

Compared with the existing WLAN operations, our dynamic password assignment and WLAN protection approach offers better security and is more convenient to the WLAN users. The auto-configuration mechanism provides integrated access services over WLAN networks with different configuration setups, which provides more flexible business model than the existing solutions [1]. Consider the scenario where several WLAN service providers operate WLAN networks in many zonal areas. A third party *A* who owns the WLR and WGWs may negotiate roaming agreement with several WLAN service providers. Therefore, with the authentication and auto-configuration mechanisms described in the previous section, the customers of *A* can access WLAN services without involving in tedious authentication and configuration setup procedures when roaming among different WLAN networks.

4. Conclusions

This paper proposed an authentication and auto-configuration mechanism for WLAN based on short message service of mobile telecommunications network. Our approach automates the authentication and WLAN configuration setup procedure without involving the users.

An issue not clearly discussed in this paper is 'WLAN security'. It is well known that WLAN based on IEEE 802.11b is not secured. For a determined attack, WEP only makes a WLAN network more difficult for the attacker to intrude. While WEP has serious problems, WEP2's sliding window algorithm makes breeching more difficult for attackers. WEP2's improvements include 128-bit encryption keys and better encryption algorithms. But since WEP2 is based on the same RC4 encryption and key system as WEP, it is still vulnerable to the same attacks.

The IEEE 802.11 Task Group I is investigating the current 802.11 MAC security. The group settled on making Kerberos authentication mandatory and left open the possibility of requiring new and additional authentication methods (such as RADIUS). In the near term it is foreseen that authentication approaches such as RADIUS will be necessary to track metered public access usage, which many installations and APs already support, thereby offloading the authentication from APs altogether. Such systems will still remain fairly open. In the enterprise environment, however, VPNs and WEP (along with RADIUS and other authentication systems) are going to become the mandated norm in short order [7]. The implementations of WGW and WLR can be found in http://pcs.csie.ntu.edu.tw/gwlan/.

References

[1] 3GPP, Third Generation Partnership Project, Technical Specification Group Service and System Aspects, Feasibility Study on 3GPP System to Wireless Local Area Network (WLAN) Inter-working (Release 6), Technical Report 3G TR 22.934 Version 6.0.0, September 2002.

[2] 3GPP, Third Generation Partnership Project, Technical Specification Services and System Aspects, Location Services (LCS), Service Description, Stage 1 (Release 5), Technical Report 3G TS 22.071 Version 5.1.1, March 2002.

[3] ANSI/IEEE, Std. 802.11 Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Technical Report, IEEE, 1999.

[4] Y.-B. Lin, I. Chlamtac, Wireless and Mobile Network Architectures, Wiley, New York, 2001.

[5] Nokia, The Nokia D211, A Multi-mode Radio Card for Compatible Portable Computer Enabling Network Access Through GPRS, HSCSD, or WLAN Environment, http://www.nokia.com/phones/productsupport/d211/guides.html

[6] C.-H. Rao, D.-F. Chang, Y.-B. Lin, iSMS: an integration platform for short message service and IP networks, IEEE Network 15 (2) (2001) 48–55.

[7] R. Santalesa, TheWar over 802.11x Security, http://zdnet.com.com/2100-1107-503897.html