Loosely-Coupled Interworking of GSM/GPRS Mobile Networks and Wireless LANs

Toni Janevski[1], Aleksandar Tudzarov[2], Dusko Temkov[3], Perivoje Stojanovski[4]

***Abstract* – In this paper we propose a solution for interworking of cellular networks, such as GSM/GPRS networks, and Wireless LAN. Proposed interworking is based on so-called loosely-coupled architecture, where the integration is based on the Authentication, Authorization and Accounting i.e. AAA. The applicative solution for GSM/GPRS-WLAN integration includes development of several network nodes, such as WLAN Access Controller and WLAN AAA charging gateway. The proposed solution provides possibility for efficient deployment of WLAN network to existing GSM/GPRS system of the mobile operator.**

***Keywords* - AAA, Cellular, Internetworking, Mobile networks, Wireless LAN.**

I. INTRODUCTION

Wireless LAN (WLAN) is a complementary service offering for mobile operators. Mobile operators using GSM and GPRS already have infrastructure that covers wide-area. However, they lack the higher data rates for Internet services that are demanded by most of the users, which are accommodated to the wired Internet and expect similar offer in a wireless environment. WLAN may be deployed in Public, Corporate or Residential environments, where GSM/GPRS systems already are accommodated. In particular it is suitable for indoor public hot spots, hotels, exposition areas, and corporate business. Hence, with a little additional investment mobile operators can further expand the packet (i.e. Internet) service by adding throughput and capacity in hot spots by using WLAN.

General Packet Radio Service (GPRS) is a development of GSM that provides packet switched data communications. On the other side, Wireless LAN (WLAN) is a relatively cheap technology and provides many times higher bandwidth than GPRS for packet traffic, but with many times smaller cells (up to 50-100 meters).

[1] Toni Janevski is with Faculty of Electrical Engineering, University "Sv. Kiril i Metodij", Karpos 2 bb, Skopje, R.Macedonia, E-mail: tonij@etf.ukim.edu.mk
[2] Aleksandar.Tudzarov is graduate student at the Faculty of Electrical Engineering, Skopje, R.Macedonia,
E-mail: Aleksandar.Tudzarov@mobimak.com.mk
[3] Dusko Temkov is graduate student at the Faculty of Electrical Engineering, Skopje, R.Macedonia,
E-mail: Dusko.Temkov@mt.com.mk
[4] Perivoje Stojanovski is graduate student at the Faculty of Electrical Engineering, Skopje, R.Macedonia,
E-mail: pstojanovski@mt.net.mk

The most used WLAN standard today is IEEE 802.11b, which is relatively cheap and offers high data rate up to 11 Mbps. Wireless LANs IEEE 802.11b are already widely deployed in developed countries and also in some companies in Macedonia. Other currently available WLAN standard for interworking are 802.11a and 802.11g, which offer data rates up to 54 Mbps.

Due to interest for WLAN considering lower price than classical cellular infrastructure, large vendors on the telecommunication market have created different solutions for Wireless LAN operated by mobile operators. Some of these solutions are described in [1-51].

In this paper we propose and describe in details efficient and cost-effective system for unified Authentication, Authorization and Accounting (AAA) for loosely-coupled PLMN-WLAN internetworking, in particular, for the scenario where PLMN operator adds its own WLAN network to offer WLAN service.

The paper is organized as follows. In Section II we discuss architectures for PLMN-WLAN interworking. Proposed AAA solution is given in Section III. Finally, Section IV concludes the paper.

II. ARCHITECTURE FOR PLMN-WLAN INTERWORKING

Depending on the degree of inter-dependence that one is willing to introduce between the PLMN network and the 802.11 network, there are two different ways of integrating the two wireless technologies. They are usually defined as [16]:

- Loosely-coupled internetworking (loose coupling)
- Tightly-coupled internetworking (tight coupling).

There are several advantages to the loosely-coupled integration approach. First, it allows independent deployment and traffic engineering for PLMN and WLAN networks. Second, loosely-coupled solution has lower costs and complexity compared to tightly-coupled one. Furthermore, loosely-coupled internetworking provides easy access to WLAN services for all potential types of users, such as postpaid and prepaid users of the mobile operator, as well as provides possibility to use WLAN services to users that have no subscription made with the mobile operator by using WLAN vouchers. Also, tightly-coupled approach demands additional investments in end user equipment for WLAN access (besides traditional 802.11 network cards), while loosely-coupled solution does not.

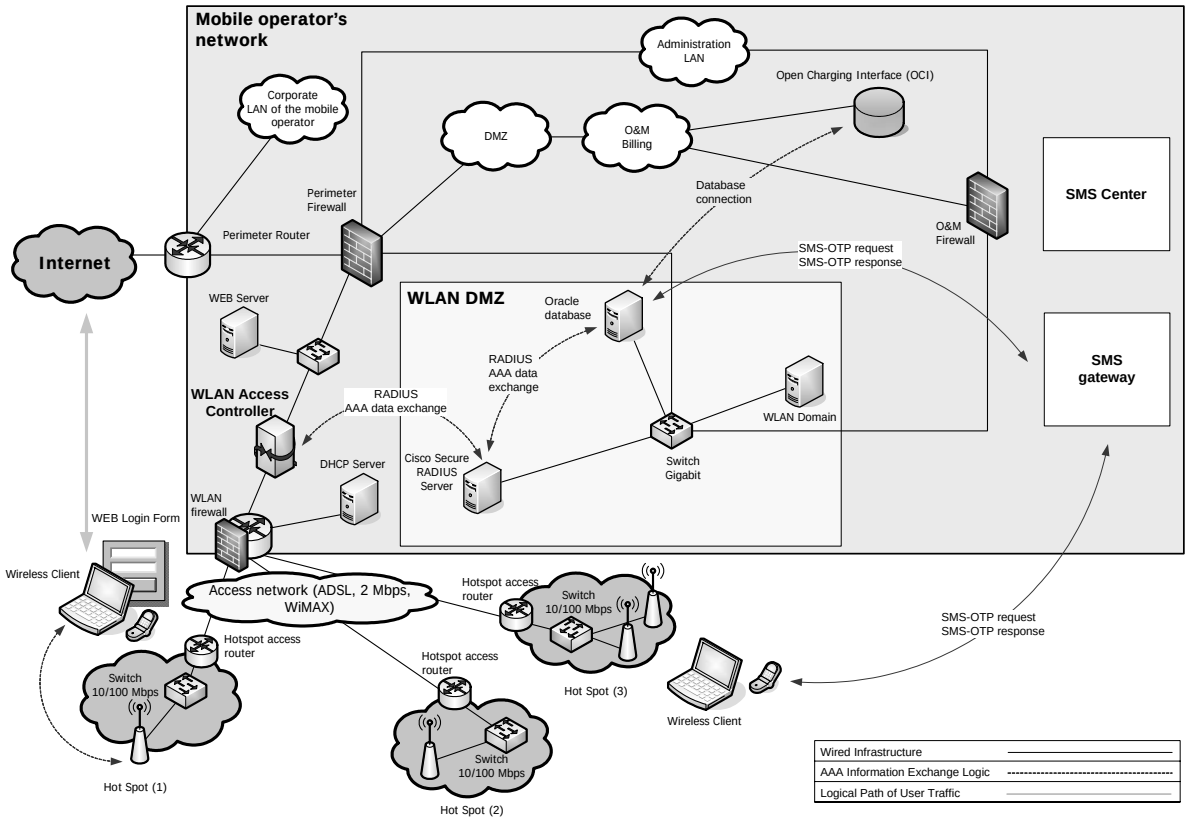

Fig. 1 Architecture for PLMN-WLAN interworking

From the discussion above it is clear that loosely-coupled solution offers several architectural advantages over the tightly-coupled approach, with no drawbacks. Furthermore, in loosely-coupled solution we may distinguish two main access methods:

- Universal Access Method – UAM, which is dominant today; and
- Secured access method, which should be implemented for users that care about the security

Because one WLAN access method is secured by using 802.1X and an encryption protocol, and other is not (i.e. UAM), we need to separate both types of access methods. Solution for this is to use Wireless Virtual LAN – WVLAN, which is based on 802.1Q standard [21]. In such approach, one Virtual WLAN will be used for UAM, and other (or others) will be used for secured WLAN access method.

Our PLMN-WLAN internetworking framework is based on loosely-coupled architecture (Fig. 1). Both, user data traffic and control traffic (e.g. AAA control signaling) aggregate at WLAN perimeter router. Traffic from hotspots (and vice versa) may aggregate in a switch (from the WLAN side of the network) that is plugged into the WLAN router.

III. Authorization, Authentication and Accounting for PLMN-WLAN

Security solution provided for a wireless LAN environment depends upon the purpose of the WLAN. In that sense, the solution differs for public WLAN network and corporate WLAN. While corporations give security a preference over easiness of use, an ordinary Internet user may prefer simplicity than security. There is always a balance that should be achieved between system security and user friendliness, especially in public WLAN access network.

The IEEE 802.11 standard defines two authentication mechanisms in the wireless interface, i.e. Open System and Shared Key, as well as a privacy method called Wired Equivalent Protocol (WEP). The standard mandates use of the authentication for the infrastructure BSS mode (it is optional for the ad-hoc mode), while WEP is optional in all cases.

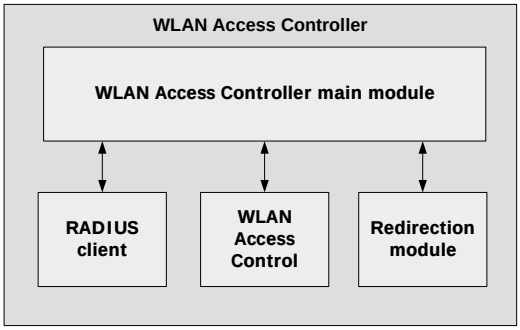

Fig. 2 WLAN Access Controller

Most common method for controlling Internet access for WLAN networks is to filter packets based on IP address and/or MAC address [43]. This method refers mainly to UAM, but it may be applied to the secured access as well. This method is based on limiting the user's access to only a set of designating destinations, which is usually web server with web-login page in the operator's WLAN backbone

network. This is referred to as browser redirection. However, the implementation of this access control is a proprietary solution, because there is no standardized one.

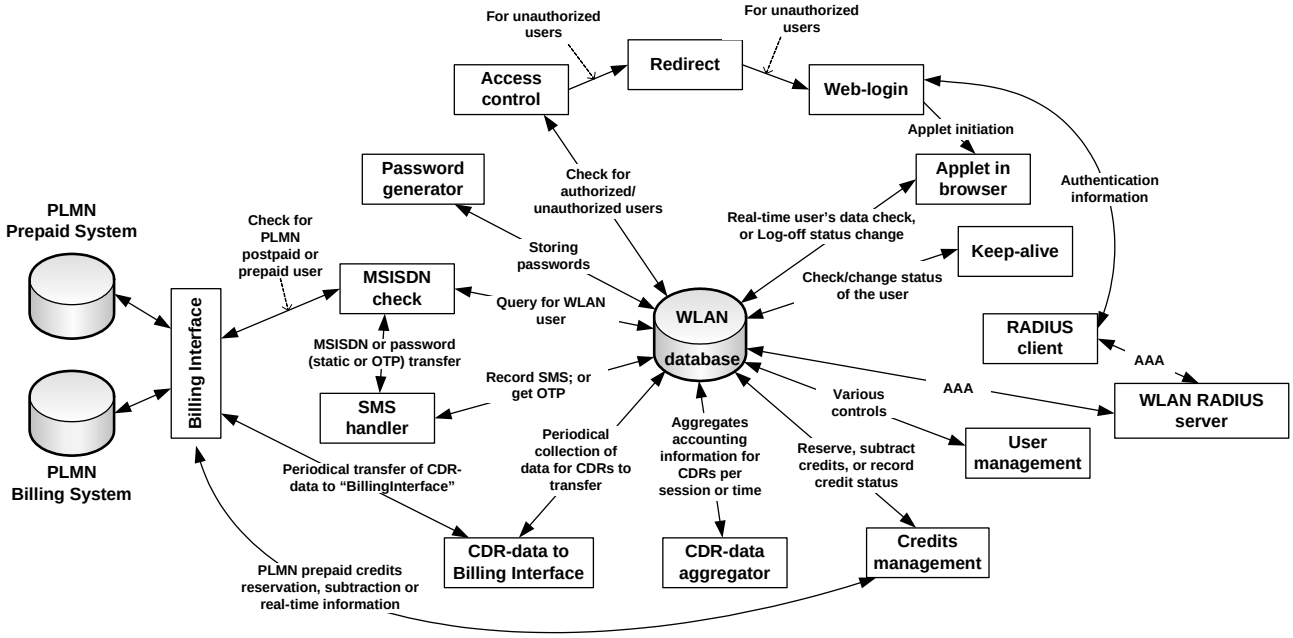

Fig. 3 Solution for PLMN-WLAN integration: software modules and interfaces

In the solution for mobile operator's WLAN network, we use dynamic packet filtering method for access control in the network access control server. The machine used for Access Control (i.e. gateway) has two Ethernet cards, one on the side of the WLAN access network, and the second out on the side to the external packet network (i.e. Internet). WLAN Access Controller is shown in Fig. 2. It is consisted of the following main modules:

- *RADIUS client* -for communication with RADIUS server
- *Access Control module* -for controlling the access of WLAN clients
- *Redirection module* -for redirection of unauthenticated users to the web-login server
- *WLAN web-login interface* -used as an user interface in the authentication process

The environment for the WLAN Access Controller is shown in Fig. 3.

When a user opens a browser his browser will be redirected to the web-login page of mobile operator's WLAN. There postpaid user will find information that he should send an SMS to a designated number to obtain access to the WLAN network (if he does not have such information in advance).

The SMS-Center of mobile operator receives the SMS and forwards it to a machine connected to IP backbone network of mobile operator by using the SMPP protocol for that purpose. An application receives that request for an OTP via SMS, and triggers check of the MSISDN number of the user (whether it is a mobile operator subscriber or not). The MSISDN check is necessary because there can be also roaming users from other operators. It is performed by an analysis of the number of the SMS sender.

After a positive check of the user's MSISDN, the application will trigger generation of OTP for that user. Then, the MSISDN and OTP are stored in the SQL database for WLAN users. Further, the OTP is sent to the user in a SMS via mobile operator's SMS-Center by using SMPP for communication between the application and the SMS-C (we refer to this OTP as Sent OTP i.e. S-OTP). The user receives the SMS-OTP and enters his MSISDN and the Received OTP (R-OTP) as his username and password. These credentials are sent to the WLAN RADIUS AAA server via the AP. Then, the Received OTP (R-OTP) is compared with Sent-OTP (S-OTP), which is in the WLAN users' database. After successful match of credentials given by the user and those recorded in the database, the user is granted access to the Internet, and accounting process starts. RADIUS server is also an accounting server and it receives all accounting messages (Accounting Start, Interim Accounting, Accounting Stop etc.). After session ends, RADIUS server records the accounting data into the SQL database. Also, all start, stop, and interim accounting messages are stored in the WLAN database.

Each accounting message triggers the WLAN database to send request to the mediation node i.e. PLMN charging mediation node (i.e. charging interface). From the accounting data recorded into the OCI database, an application periodically creates CDRs from the accounting data for completed sessions. All created CDRs are periodically sent to the Billing System of the mobile operator over FTP.

IV. CONCLUSIONS

In this paper we have described our solution for PLMN-WLAN interoperability based on loosely-coupled architecture. We have made a choice for loosely-coupled PLMN-WLAN integration as a dominant scenario today worldwide and we have justified its advantages over the tightly-coupled approach.

Further, we presented the developed WLAN Access Controller, which works as a gateway between WLAN segment and mobile operator's cellular network. Also, we have developed PLMN-WLAN AAA charging gateway, which is based on SQL database and carries all charging and billing functionalities for WLAN users.

The created solution is cost-effective and provides all needed functionalities for efficient charging and billing, as well as access control for WLAN. It is suited to be used for the scenario where PLMN operator adds WLAN as an additional service.

REFERENCES

[1] Alcatel, "Public Wireless LAN for Mobile Operators: WLAN beyond the enterprise", White paper, 2003.

[2] Flash Networks, "NettGain 1200 Flash Networks", www.adjungonet.com

[3] M. T. Bostrom, A. Norefors, "Ericsson Mobile Operator WLAN", Release 1 Technical Description, February 2002.

[4] M.Ritter, "Billing WLAN to macro-networks", White paper, Mobility Networks, www.mobilitynetworks.com, 2003.

[5] The Wireless Directory, "Hotspot Locations", http://www.hotspot-locations.com/modules.php?name=HotSpots, accessed June 2004.

[6] "Huawei to provide WLAN for China Mobile", http://www.ciol.com/content/news/repts/102112206.asp, accessed May 2004.

[7] WeRoam – WLAN and PLMN united, www.weroam.com, accessed June 2004.

[8] Swisscom-Eurospot, http://www.swisscom-eurospot.com, accessed June 2004.

[9] Telia HomeRun, http://www.homerun.telia.com, accessed June 2004.

[10] BT Openzone, http://www.btopenzone.com, accessed June 2004.

[11] T-Mobile International, http://www.t-mobile-international.com, accessed June 2004.

[12] T-Mobile US, http://www.t-mobile.com/hotspot/, accessed June 2004.

[13] "TDC Mobil" official WiFi/3G offer, www.tdcmobil.dk, accessed April 2004.

[14] VIPonline, https://airlink.vip.hr/hotspot/, accessed June 2004.

[15] Era Hot@Spot, http://www.erahotspot.pl, accessed June 2004.

[16] M. Buddhikot, G. Chandranmenon, S. Han, Y. W. Lee, S. Miller, L. Salgarelli, "Integration of 802.11 and Third-Generation Wireless Data Networks", Infocom 2003, San Francisco, USA, March 30 – April 3, 2002.

[17] Portal Software Inc., "Overcoming Wireless LAN Billing Challenges", 2003.

[18] Wi-Fi Alliance (2003) "Wi-Fi Alliance Wireless ISP Roaming Best Practices Document". http://www.Wi-Fialliance.org/opensection/

[19] Intel, "Wireless LAN (WLAN) End To End Guidelines for Enterprises and Public HotSpot Service Providers", Release 1.0, October 2002.

[20] IEEE 802.1X standard, "IEEE standard for local and metropolitan area networks – Port-Based Access Control", July 2001.

[21] IEEE 802.1Q standard, "IEEE standard for local and metropolitan area networks - Virtual Bridged Local Area Networks", May 7, 2002.

[22] C. Rigney, S. Willens, A. Rubens, W. Simpson, "Remote Dial-In User Authentication Service (RADIUS)", RFC 2865, June 2000.

[23] C. Rigney, "RADIUS Accounting", RFC 2866, June 2000.

[24] C. Rigney, W. Willats, P. Calhoun, "RADIUS Extensions", RFC 2869, June 2000.

[25] Cisco, "Single-User Network Access Security TACACS+", http://www.cisco.com/warp/public/614/7.html, accessed June 2003.

[26] P.Calhoun et al, "DIAMETER base protocol", IETF, RFC 3588, September 2003.

[27] C. Finseth, "An Access Control Sometimes Called TACACS", RFC 1492, July 1993.

[28] The Unofficial 802.11 Security Web Page, http://www.drizzle.com/~aboba/IEEE/, accessed June 2003.

[29] Wi-Fi Alliance, "Q&A Wi-Fi Protected Access", http://www.wi-fi.org/OpenSection/pdf/Wi-Fi_Protected_Access_QA.pdf , March 28, 2003.

[30] Frank Ohrtman, Konrad Roeder, "Wi-Fi Handbook: Building 802.11b Wireless Networks", McGraw-Hill, 2003.

[31] US Department of Commerce, "Advanced Encryption Standard (AES)", Federal Information Processing Standard (FIPS), Publication 197, November 2001.

[32] L.Blunk, J.Vollbrecht, "PPP Extensible Authentication Protocol", IETF, RFC 2284, March 1998.

[33] T. Dierks, C. Allen, "The TLS Protocol", RFC 2246, January 1999.

[34] T. Wu, "The SRP Authentication and Key Exchange System", RFC 2945, September 2000.

[35] IEEE 802.1X standard, "IEEE standard for local and metropolitan area networks – Port-Based Access Control", July 2001.

[36] W. Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)", August 1996.

[37] RFC 2716, "PPP EAP TLS Authentication Protocol", Internet Engineering Task Force (IETF), October 1999.

[38] J. Edney, W.A. Arbaugh, "Real 802.11 Security: Wi-Fi Protected Access and 802.11i", Addison Wesley, July 2003.

[39] J. Hammond et al., "Wireless Hotspot Deployment Guide", Intel in Communications, December 2003.

[40] Palekar, et al, "Protected EAP Protocol (PEAP) Version 2", draft-josefsson-pppext-eap-tls-eap-00, October 2003.

[41] N. Cam-Winget, D. McGrew, J. Salowey, H. Zhou, "EAP Flexible Authentication via Secure Tunnelling (EAP-FAST)", draft-cam-winget-eap-fast-00, February 2003.

[42] H.Haverinen, et al., "EAP SIM Authentication", draft-haverinen-pppext-eap-sim-13, April 5, 2003.

[43] P.Iyer at el, "Public WLAN Hotspot Deployment and Internetworking", Intel Technology Journal Vol. 7, August 19, 2003.

[44] Microsoft 802.1x Authentication Client, www.microsoft.com/windows2000/server/evaluation/news/bulletins/8021xclient.asp, December 13, 2002.

[45] Open Source Implementation of IEEE 802.1x, www.open1x.org/, accessed June 2003.

[46] IEEE 802.1Q standard, "IEEE standard for local and metropolitan area networks - Virtual Bridged Local Area Networks", May 7, 2003.

[47] SMPP Protocol Specification v4.0, http://www.smsforum.net/doc/public/Spec.

[48] ETSI TS 101 393 – Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (PLMN); PLMN Charging, 3GPP TS 12.15 version 7.7.0 Release 1998.

[49] Ericsson Radio System AB, "PLMN System Description", PLMN Customer Documentation, 1551-AXB 250 01/1 Uen, 1999.

[50] PLMN Association, "Services, Ease of Use, and Operator Considerations in Interworked WLAN-Cellular Systems", PRD SE. 27, May 28, 2003.