AAA System for PLMN-WLAN Internetworking

Toni Janevski

Abstract: **Integration of mobile networks and Internet has started with 2.5 generation of mobile cellular networks. Internet traffic is today dominant traffic type worldwide. The hanger for higher data rates needed for data traffic and new IP based services is essential in the development of future wireless networks. In such situation, even 3G with up to 2 Mbit/s has not provided data rates that are used by Internet users with fixed broadband dial-up or through wired local area networks. The solution to provide higher bit rates in wireless access network has been found in wireless LAN although initially it has been developed to extend wired LAN into wireless domain. In this paper, we propose and describe a solution created for interoperability between mobile cellular network and WLAN. The integration between two networks, cellular and WLAN, is performed on the authentication, authorization, and accounting, i.e., AAA side. For that purpose we developed WLAN access controller and WLAN AAA gateway, which provide gateway-type access control as well as charging and billing functionalities for the WLAN service. In the development process of these elements, we have considered current development stadium of all needed network entities and protocols. The provided solution provides cost-effective and easy-to-deploy PLMN-WLAN Internetworking scenario.**

Index Terms: **AAA, billing, cellular, Internetworking, mobile, wireless LAN.**

I. INTRODUCTION - WHY A MOBILE OPERATOR NEEDS PLMN-WLAN INTEROPERABILITY?

Wireless services have grown rapidly in the last decade. The evolution started with second generation (2G) mobile networks, such as PLMN in 90-es, and it continued by introducing IP (Internet protocol) based services besides the traditional voice.

On the other side, IEEE standardized 802.11 wireless local area network—WLAN technology, which was primarily seen as a supplement to the wired Ethernet for enterprises. It did not take long for 802.11s standards to enter into public areas besides the enterprises. Today, the wireless LANs are placed in hotspots, where a hotspot is by a definition place with high user density (airports, hotels, and cafes, etc.). In the following several years, such public WLAN access networks are expected to become more and more common and to attract more users. Some predictions say that until the end of this decade number of WLAN users will be more than a double of the number of 2.5G and 3G mobile users, while in the following couple of years PLMN users will dominate in number over WLAN [1].

Wireless access networks can be classified into two main groups: Wireless networks that provide high data rates and have limited coverage from a given access point, such as 802.11 WLAN, and wireless networks that have wide coverage from a given base station and limited bandwidth, such as GPRS, EDGE, and UMTS (as well as CDMA2000 in America). Hence, the WLAN standard will never be able to provide large-scale coverage due to limited propagation. However, the WLAN systems are a good complement to the widespread 2.5G systems as well as 3G systems. 2.5G and 3G offer lower data rates compared to WLANs. One may expect 2.5G or 3G to be the dominating large-scale coverage data transfer wireless system for some years to come and due to this, the combination of WLAN and public land mobile network (PLMN) technology will use the best features of the both systems.

To make an integrated PLMN/WLAN system popular, it is necessary to have a shared system for billing the users. Without such shared system, someone using different networks could receive many bills from small WLAN operators. High bandwidth WLANs are used for data transfer where they are available and PLMN is used where WLAN coverage is lacking. In other words, WLAN and PLMN should be able to complement each other and will probably not compete for the same users. The price for usage of WLAN should be smaller than price for usage of the same services (e.g., transferred data volume) over PLMN, thus forcing subscribers to use WLAN where it is available, and to use PLMN where WLAN is not available. Of course, such scenario is an excellent choice for mobile operators to additionally offer WLAN service, besides PLMN.

Due to interest for WLAN considering lower price than classical cellular infrastructure, ease of use, and higher bandwidth than PLMN, either 2.5G or 3G (e.g., UMTS) mobile networks, large vendors on the telecommunication market have created different solutions for wireless LAN operated by mobile operators. Some of these solutions provided by some of the world largest vendors in wireless communications market are implemented [1]–[15].

In this paper, we propose and describe in details efficient and cost-effective system for unified authentication, authorization, and accounting (AAA) for PLMN-WLAN Internetworking, in particular, for the scenario where PLMN operator adds its own WLAN network to offer WLAN service.

This paper is organized as follows. In next section, we discuss architectures for PLMN-WLAN Internetworking. In Section III, we propose authentication, authorization, and accounting (AAA) mechanisms for PLMN-WLAN interoperability. Unified billing solution for PLMN-WLAN is given in Section IV. Finally, Section V concludes the paper.

II. ARCHITECTURE FOR PLMN-WLAN INTERNETWORKING

Integration of PLMN and WLAN is to some extent dependent upon their integration framework. There are differences in the two technologies, namely PLMN and WLAN. PLMN is based on detailed standards published by 3GPP (or 3GPP2), while WLAN can be often designed in various ways. Although

Manuscript received January 11, 2005.

Toni Janevski is with the Faculty of Electrical Engineering, University Sv. Kiril i Metodij, Skopje, R. Macedonia, email: tonij@etf.ukim.edu.mk.

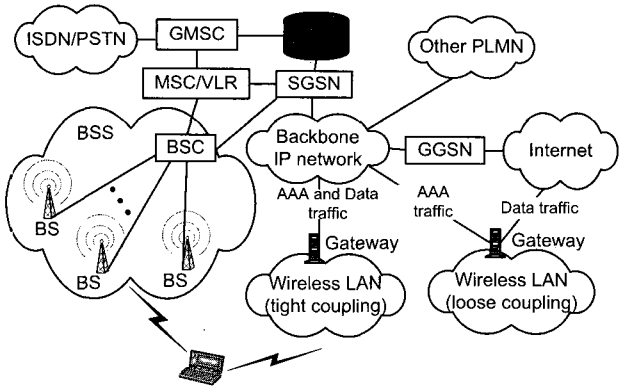


Fig. 1. PLMN-WLAN logical architectures: Tightly coupled vs. loosely coupled architecture.

802.11 WLAN and its versions are standardized by IEEE, the standard refers only to physical and data-link layers (the first two from the bottom of the OSI layering model). Hence, there can be different solutions applied on a network layer for practical implementation of a WLAN, and it is usually dependent upon the users' type (e.g., corporate users, or users at public hotspots, etc.).

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] (Fig. 1).

- Loosely-coupled Internetworking (loose coupling) and
- tightly-coupled Internetworking (tight coupling).

A. Loose Coupling

For loose coupling, the network PLMN-WLAN Internetworking is based on the sharing of certain client specific information for AAA purposes. A loosely coupled WLAN network uses information about the PLMN mobile subscribers, as well as the mobile operator's billing system functionality in order to transfer charging information.

In loose-coupling scenario, as described in [17], the WLAN uses the Internet as the transport network to transport both control traffic as well as user traffic.

Here we will also have a WLAN gateway between the WLAN and PLMN networks. But, in this case the gateway directly connects to the Internet and routes the user data traffic to and from Internet not affecting the PLMN core network. There are two main different approaches for this solution.

1. Only the user data traffic is routed to/from Internet. The AAA server of the WLAN is directly connected to PLMN network for the purpose of authentication, authorization, and accounting.
2. Data traffic and AAA are injected directly to the Internet. But, this approach cannot provide unified billing for WLAN and PLMN services, and needs additional security measures for AAA traffic that passes through Internet.

In loose-coupling scenario, the user population that accesses Internet services via WLAN may include users that have signed-on with the operator (i.e., postpaid users), as well as mobile users visiting from other networks. Also, in this approach the high speed data traffic from 802.11 WLAN will never be injected into PLMN backbone network.

In this approach, we can use different mechanisms and protocols to handle authentication and billing in PLMN and 802.11 networks. However, to have unified approach we need to provide Internetworking considering the AAA process.

B. Tight Coupling

In tight coupling scenario, WLAN appears to PLMN as another PLMN access network. In this case, the WLAN should emulate the functions that are native in PLMN access networks using a WLAN gateway that should implement all PLMN protocols (mobility management, authentication, etc.) required in PLMN access network. So, in a tightly coupled scenario WLAN and PLMN networks share many more functionalities. In other words, in a tightly-coupled scenario WLAN must emulate PLMN functionality and should behave as a PLMN node. In such case, the WLAN network will use layer two (according to OSI model) connectivity to interface the PLMN network transport backbone. All signalling and control traffic (e.g., AAA traffic) as well as all data traffic from WLAN users will pass through PLMN backbone network and use existing interfaces towards external packet network (e.g., Internet).

In this scenario, mobile nodes (e.g., lap-top computers) are required to implement the corresponding PLMN protocol stack on top of their WLAN network cards (i.e., PCMCIA, PCI, or integrated 802.11 cards).

However, this approach has several drawbacks. First, by injecting the WLAN traffic directly into the PLMN core network, the setup of the entire network as well as the configuration and the design of network elements such as SGSN and GGSN have to be modified to sustain the increased traffic load, and the obtained network behaviour will be uncertain. Second, as we mentioned above, the 802.11 cards will have to implement PLMN protocol stack. Furthermore, it will demand to use PLMN specific authentication mechanisms based on SIM card, thus limiting opportunity to attract users that are not PLMN subscribers. That will also imply the use of 802.11 network cards with built-in SIM slots or external cards into the mobile devices. However, when there will be widespread dual-mode PLMN/WLAN terminals on the market, it will be reasonable to provide SIM-based authentication for WLAN service as well.

For all the reasons described above, using the tightly-coupled scenario will increase complexity and cost of such solution, and at the same time will limit the number of potential users due to demands on the end-user mobile devices, that it will be uncompetitive to a wireless Internet service provider (WISP).

C. Choice of PLMN-WLAN Internetworking Architecture

First, we have to make a choice between the two architectures: Loose-coupling and 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 to users that are not subscribers of the PLMN 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.

>From the discussion above, it is clear that loosely-coupled solution offers several architectural advantages over the tightly-coupled approach, with no drawbacks. Therefore, we decide for the loosely-coupled architecture as the preferred architecture for PLMN-WLAN Internetworking.

D. The State of the WLAN Deployment Today and Tomorrow

The most common method today for Internetworking of WLAN and mobile operator's network (e.g., 2.5G or 3G PLMN operator) is referred to as the universal access method (UAM) [18]. In such approach, we have loosely-coupled cellular-WLAN network, where user's web-browser at a WLAN hotspot is intercepted and redirected to a web-page for UAM login with aim to enter username and password. However, UAM approach has minimal requirements on mobile clients, i.e., they do not have to install any software on their mobile devices (e.g., lap-tops) or to make specific settings for WLAN access. The mobile client needs only a web-browser to be able to access the WLAN. Seamless access to the WLAN by the users is the major strength of the universal access method [19].

While the simplicity for users is the major advantage of the UAM method, it has several drawbacks. The most important disadvantage of such WLAN access is the security issue. Most of the UAM implementations do not have security protection for user's credentials, such as username and password. Also, user's data traffic may be exposed to others that listen on the same radio interface. These disadvantages of the UAM can be dealt with using the Wi-Fi secured access method. For user data we can provide encryption of the data. Disadvantage for the secured access method is more complexity that is added on the side of the mobile clients (e.g., a user has to make certain settings on the lap-top's software, or should download and install certain software to be able to use the secured access).

>From the discussion above, we may distinguish between two main access methods.

- Universal access method—UAM, which is dominant today.
- Secured access method, which should be implemented for users that care about the security.

However, one may expect broad range of users and user types in the WLAN. We may have users with low-level computer skills which, for an example, want to use WLAN hotspots to surf the web or check email. On the other side, we may also have business users (and other users as well) that want to use secured access to Internet via WLAN for their needs. Generally, the conclusion is that the WLAN architecture and design should support both types for network access with aim to make the network attractive to different types of users.

E. PLMN-WLAN Architecture for Mobile Operator

Considering the network security on the WLAN side, in our proposal we decided to use both types of architectures, i.e., universal access method—UAM, and secured access method. Justification for such decision is the broad range of potential users for WLAN service.

Our PLMN-WLAN Internetworking framework for mobile operator's network is shown in Fig. 2. We have decided to use loosely-coupled architecture. 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 WLAN router.

Current layout of mobile operator's IP backbone networks is given in Fig. 2 as well. Servers' farm of the current IP backbone is placed between two firewalls in so-called de-militarized zone (DMZ). The billing system for PLMN network is also placed in the DMZ of the mobile operator. This DMZ network is connected to Internet via a gateway router. Additionally, on this router can be also connected mobile operator's corporate LAN. New servers for the WLAN networks as well as WLAN users data base is planned to be placed in so-called WLAN DMZ, which will be connected to the existing firewalls in mobile operator's IP backbone, i.e., firewalls will be reused for the WLAN as well. This approach will save costs for securing WLAN servers by reusing the existing firewalls.

Furthermore, we define the two architectures that will coexist in parallel. Each of the architectures will use the same hotspots, i.e., the same access points placed in public places or in companies. Also, both architectures will use the same data base for WLAN users as well as the same AAA servers. However, there will be also some differences.

Main difference between the two access approaches (i.e., UAM and secured access method) is the users login and access control procedures.

The proposed architecture for PLMN-WLAN Internetworking for a mobile operator should provide both access methods on different wireless VLANs [20], i.e., UAM and secured access, as shown in Fig. 2.

Hotspots are connected to the WLAN access controller via IP-routed network. There are different possibilities to connect with hotspot locations, such as WiMAX (i.e., 802.16) backbone network, leased 2 Mbps lines, or ADSL. In near future, WiMAX may replace WLAN, which is dependent upon the distribution of WiMAX cards in wireless client devices. In such case, the UAM architecture can be used for WiMAX clients as well.

III. AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING (AAA) FOR PLMN-WLAN INTERNETWORKING

AAA stands for authentication, authorization, and accounting. Shortly, authentication is created for identification of a user, authorization manage what a user is allowed to do, and accounting measures the used resources by the user with aim to bill the user for their usage. There are several systems that are capable to do AAA functions, such as remote dial-in remote access service (RADIUS) [21]–[23], terminal access controller access control system plus (TACACS+) [24], [25], and DIAMETER [26].

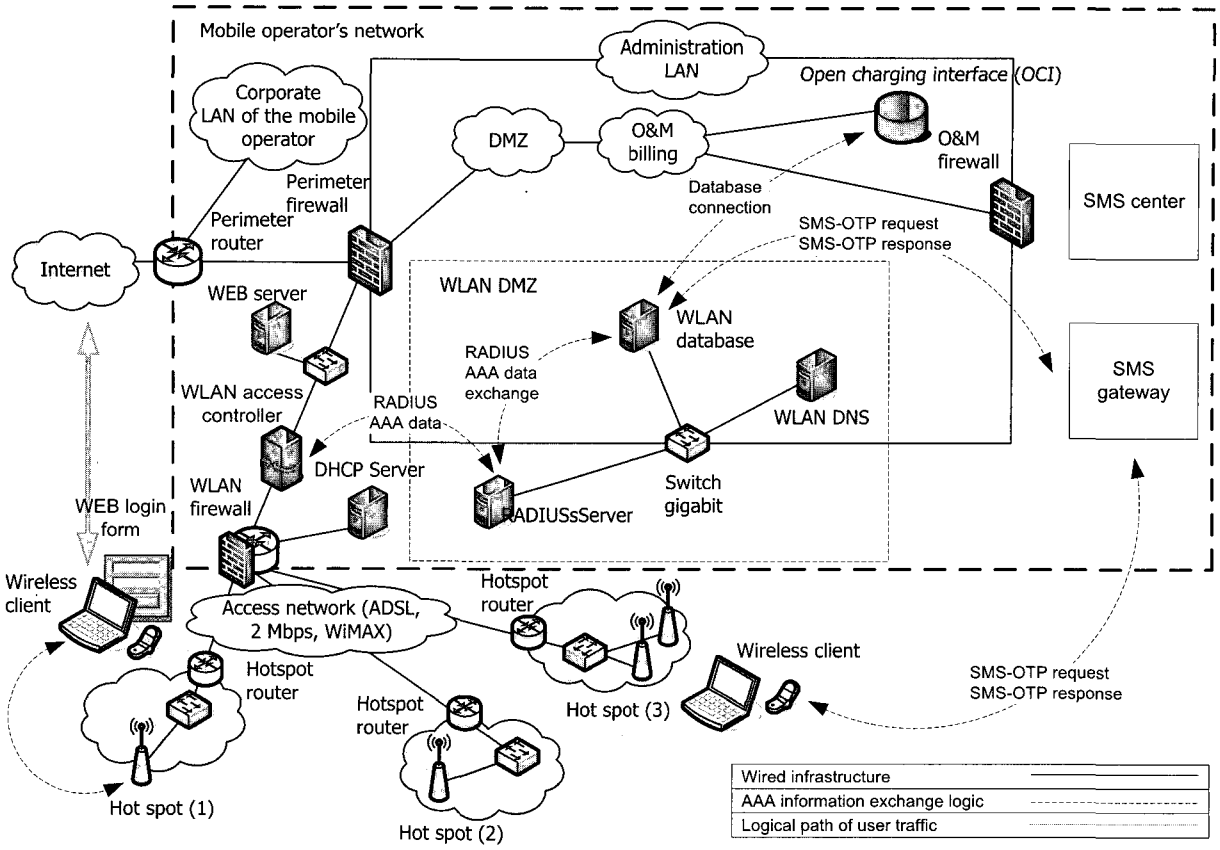


Fig. 2. Architecture for PLMN-WLAN Internetworking.

A. Choice of AAA Protocol

One of the differences between TACACS+ and RADIUS is the network transport protocol that each uses. The RADIUS protocol uses UDP, whereas TACACS+ uses TCP. However, both protocols are created to use a specific transport protocol, so one cannot say that TCP or UDP is better choice.

Further, the RADIUS protocol combines the processes of authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain all the authorization information, making separation of the authentication, and authorization functions difficult. The use of RADIUS is most appropriate when simple, single-step authentication and authorization is required, and it is the case with most service provider networks. While RADIUS supports both time-based and usage-based accounting, the drawback of TACACS+ is lack of the support for usage-based accounting, which is essential. Hence, from the above discussion is straightforward to decide for RADIUS protocol (when the options are TACACS+ or RADIUS).

Our next step is to make a choice between RADIUS and DIAMETER protocols for AAA. While DIAMETER is created as a successor of the RADIUS protocol for the same job, it does not have support from hardware vendors, whereas RADIUS is uniformly supported. Today RADIUS is the de-facto standard for remote authentication. It is very prevalent in both new and legacy systems. Although RADIUS was not designed for wireless networks, it is today standard AAA protocol in WLANs as well as cellular packet networks (e.g., PLMN). Therefore, we choose the RADIUS as a protocol for AAA functionalities in PLMN-WLAN environment. RADIUS is also suggested as AAA protocol by 3GPP [27], and 3GPP2 documents [28].

Table 1. Security protocols on different OSI layers.

OSI layer	Security protocols
Layer 7 - application layer	Firewalls, virus scanning
Layer 6 - presentation layer	
Layer 5 - session layer	
Layer 4 - transport layer	
Layer 3 - network layer	IPsec (VPN)
Layer 2 - data link layer	802.1X, WPA, WEP
Layer 1 - physical layer	Physical location based user-access policies

B. Security Solutions in 802.11 Wireless LAN

Every network should have some level of security to prevent attacks. This is especially a case with wireless LAN because radio interface is exposed to many users and makes thighs more complex than in wired networks. In Table 1, are shown security protocols for WLAN on different OSI layers. In following sections, we describe each of the security solutions in more details.

Security in access networks should be transparent to applications. Hence, security can be placed in layers up to layer 5 (session layer) since presentation layer (layer 6) is rarely used.

Security in the link layer is provided on a hop-by-hop basis (because it deals with medium access control—MAC addresses of the hardware), while security in the network layer is provided in an end-to-end basis.

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 over security. There is always a balance that should be achieved between system security and user friendliness, especially in public WLAN access network.

Security in 802.11 WLAN refers to security provisions in IEEE 802.11 standards. Because these standards deal only with physical layer and data link layer, the WLAN security specified in IEEE standards is provided only in these two layers. Hence, in 802.11 standards security provisions are made in access points as well as in WLAN user's cards (e.g., PCMCIA). Therefore, they can provide security only in the wireless part of the 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.

Open system: In this case, anybody with appropriate WLAN card can connect to an AP, and use the network resources. In this case, there is no security at all.

Public access: Public access security methods are the current favorite one for hotspots and wireless Internet service providers (WISP). In this case, the authentication process protects the networks by verifying the access credentials (i.e., username and password). Also, users can be billed for network resources usage. However, the data is send over the wireless link as clear text. Users must provide their own protection (in the case they need one) against breaches of confidentiality such as using a VPN tunnel (e.g., with IPsec protocol) to their enterprise network. It is important to stress that this is the usual way for public access to WLAN today (either they are operated by a mobile operator or by a WISP).

Limited Security with WEP: Besides the open authentication, the 802.11 standard specifies a shared key authentication as well, which is based on a secret key shared between the AP and mobile clients. In this case, all clients connected to the AP share the same secret key, which is never transmitted as clear text over the air. However, secret key authentication requires using the wired equivalent privacy (WEP) mechanism.

WEP authentication is not suitable for public WLAN because most of the WLAN cards and APs rely on manual key distribution. Therefore, WEP is usually used in company's WLAN, not in public access WLAN implementations.

Wi-Fi protected access (WPA) for basic 802.11 security: Wi-Fi protected access (WPA) is created by the Wi-Fi alliance [29] to offer better security than WEP. This way, by providing WPA functionality in the AP and software upgrades for WLAN cards, the vendors were trying to fill the gap between low-security WEP and a recent standard IEEE 802.11i. So, WPA is not an IEEE standard.

WPA uses temporal key integrity protocol (TKIP), which is a stronger encryption scheme than WEP. TKIP uses key hashing (key mix) and nonlinear message integrity check (MIC). WPA may work in two different modes [30].

- *Without authentication servers* - for SOHO users, WPA technology works in so-called pre-shared key mode, where a user simply enters a network key to gain access.
- *Managed mode* (with authentication servers, such as RADIUS [29]) - in this case WPA requires support of 802.1X [31] and EAP, where 802.1X and EAP enable a mobile client to communicate with the authentication server using securely encrypted transaction to exchange session keys.

However, every device (mobile client or an AP) must be upgraded (if do not has software module for WPA) in order WPA to work.

The recent standard 802.11i offers advanced encryption Standard (AES) [32] as a replacement for RC4. There are also additional features that are provided with 802.11i, such as secure de-association and de-authentication etc. The products with 802.11i standard are labeled as Wi-Fi WPA2 [30].

802.1X and EAP for 802.11 advanced security: Advanced security solution in WLANs is provided by using 802.1X and EAP. 802.1X gives an authentication framework for a WLAN, enabling a user to be authenticated by a central authority. The actual algorithm for authentication that uses 802.1X is left open and there multiple algorithms are possible. For example, there are

- *Certificate-based* solutions, such as EAP—Transport layer security [EAP-TLS],
- *Password-based* solutions, such as EAP-one time password [EAP-OTP] and EAP-message digest 5 [EAP-MD5],
- *Smart-card-based* solutions, such as EAP—Subscriber identification module [EAP-SIM],
- *Hybrid* solutions, such as EAP-tunnelled TLS authentication protocol [EAP-TTLS] that use both certificates and passwords,
- *Proprietary EAP* solutions, such as lightweight EAP (LEAP).

In this advanced security, 802.1X uses EAP a protocol [33] that works on both wired LAN (i.e., Ethernet) and wireless LAN, for message exchange during the authentication process.

IEEE 802.1X can be used for key derivation with aim to provide per-packet authentication, authorization, integrity, and confidentiality. But, 802.1X does not provide encryption by itself. Therefore, a ciphering algorithm (e.g., WEP, 3DES, or AES) is needed for encryption. Encryption algorithms are used with key derivation algorithm such as TLS [34] or SRP [35].

802.1X defines three components to the authentication conversation, which are shown in Fig. 3. The supplicant is the end user machine that seeks access to network resources. Network access is controlled by the authenticator; it serves the same role as the network access server in a traditional dial-up network. Both the supplicant and the authenticator are referred to as Port authentication erntities (PAEs) [36]. The authenticator terminates only the link-layer authentication. It does not maintain any user information. Any incoming requests are passed to an authentication server, such as a RADIUS server, for processing.

Table 2. Security options for 802.11 WLAN.

Security level	Configuration	What is secured?	Applications
Open system	Network with no security configuration	Nothing	Many users operate their equipment in this mode
Public access	User authentication via credentials supplied through the Internet	Network access	Hot spots, coffee shops, hotels, airports, etc.
Limited security	40- or 128-bit WEP	Some network access and data privacy	Home and small-office-home-office (SOHO)
Basic security	Wi-Fi protected access - WPA or 802.11i standard	Network access and data privacy	Home, SOHO, and small enterprise
Advanced security	802.1X/EAP-X and RADIUS	Network access and data privacy	Enterprise
End-to-end security	VPNs such as the point-to-point tunneling protocol (PPTP), PPTPv2, layer 2 tunneling protocol (L2TP), kerberos, and IP security (IPSec)	Network access and data privacy	Special applications, business travelers, business to business, and enterprise with outside users

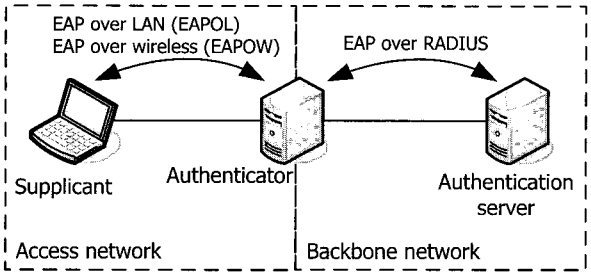


Fig. 3. 802.1X architecture.

802.1X is not a single authentication method, but rather it utilizes EAP as its authentication framework. This means that 802.1X enabled APs and switches can support a wide variety of authentication methods.

EAP was initially developed for use with point-to-point protocol (PPP) [33]. EAP is a peer-to-peer authentication protocol used between a supplicant and a back-end authentication server. It can run over any link layer, such as PPP and 802.11 (refer to Fig. 4). EAP has been defined as a generic authentication protocol, which for instance may be executed over RADIUS protocol. In such case, the authenticator (i.e., the AP) may only understand RADIUS specific protocol commands. In general, the EAP protocol provides various authentication types, such as EAP-MD5 [37], EAP-TLS [38], EAP-TTLS [39], LEAP, PEAP [40], EAP-FAST [41], and EAP-SIM [42]. One should note that there are also other EAP types, but those shown in Fig. 4 are the most known.

End-to-end security: For end-to-end security solution we have virtual private networks—VPN. A VPN enables a specific group of users (e.g., corporate users) to access private network data and resources over the Internet and other networks. VPNs provide tunneling, encryption, authentication, and secured access control over a public network.

VPN creates virtual point-to-point connection using a technique called tunneling. Tunneling acts like a pipe that bores through a network cloud to connect two points. It is typically started by a remote user. The tunneling process encapsulates data and encrypts it into standard TCP/IP packets, which can then securely travel across the Internet to a VPN server on the other side where they are decrypted and de-encapsulated onto the private LAN network.

To be able to provide VPN on 802.11 WLAN, VPN client software application must be deployed on all mobile clients that will use a WLAN. Almost all VPN solutions today are proprietary (not an IETF standard) in some form or another and they are generally not interoperable. Thus, VPNs are impractical for securing a public access WLAN.

However, that does not mean that VPN tunnels shall not pass through a public WLAN. It should be expected that business users will exploit the use of VPN to connect to the enterprise networks via a public access WLAN. In such case, the business user will have already installed proprietary VPN client when he is out of the office, and will use it to connect to the enterprise network from public access networks, such as WLAN.

To provide possibility for transparent VPN access of users via the public WLAN, we need to provide tunneling for different VPN protocols, because different users may use different VPN clients. This can be achieved by preventing from blocking the array of IP ports and protocols that VPN are using.

Most used VPN protocols are point-to-point tunneling protocol (PPTP), PPTPv2, layer 2 tunneling protocol (L2TP), kerberos, and IP security (IPSec), where IPsec VPNs are nearly accepted as the de-facto standard for securing IP transmission over shared public data access networks.

C. Choice of Security Solution for Mobile Operator's WLAN

In this section, we make a choice for an optimal security solution. However, such choice is mutually dependent with the WLAN architecture, which was proposed and discussed in Section II.

Choice of a security level for mobile operator's WLAN: In Table 2, we presented six different security solutions and we described each of them.

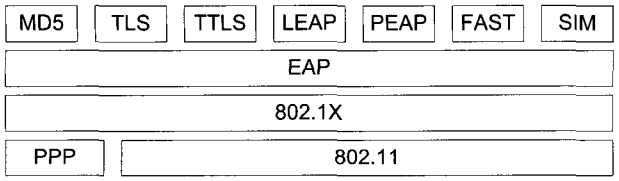


Fig. 4. 802.1X/EAP protocol stack.

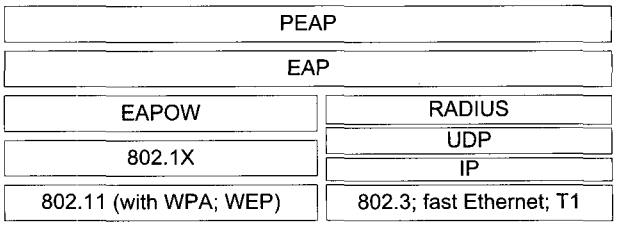


Fig. 5. Protocol stack for 802.1X with PEAP solution.

The open system solution has no security at all. In many public WLAN, hotspots is allowed open access to local web-servers with some local information or marketing messages.

Public access solution is in fact the UAM, when users are redirected by an access control node to web-login page. This security solution is de-facto standard today in public WLANs, because there is no specific requirements on the client side (i.e., wireless user) [43]. Hence, public WLAN of a mobile operator must incorporate public access security solution for the ordinary users (the UAM).

Limited security (with WEP) and basic security (with WPA) are primarily targeted to enterprise WLAN solutions.

To provide higher level of security, there are two alternatives. One is using the VPN. However, this requires VPN clients in wireless devices and a VPN network infrastructure. These are non-trivial requirements that will be required from subscribers in a public access WLAN.

The advanced security (according to the Table 2) is the other alternative, which is capable to provide mutual authentication between the mobile client and the AP by using the 802.1X and EAP.

The supplicant for 802.1X/EAP is included by default in recent operating systems as well as in older ones [44]. No changes in the hardware are required. 802.1X supplicants are available for different operating systems [45]. The authenticators for 802.1X/EAP are already widely deployed in all commercial APs from major vendors.

Considering the above discussion the choice for a security solution of mobile operator's WLAN is providing infrastructure for parallel existence of

- Public access security (with web-login, that is universal access method),
- Advanced security (with 802.1X/EAP and RADIUS as an authentication server).
- There is only one choice left here, that is the type of EAP authentication protocol to be used with advanced security solution with 802.1X/EAP. Protocol stack for this solution is shown in Fig. 4.
- Choice of an EAP method for 802.1X/EAP authentication EAP is a generic authentication framework, so it does not require any particular authentication method. The next task is to decide on the type of authentication for wireless users.

EAP-MD5 is widely supported, but it is vulnerable to dictionary attacks and does not support dynamic WEP keys.

EAP-TLS is attractive because it enables mutual authentication and protects against rogue access points, but it requires that the RADIUS server supports EAP-TLS. Use of the EAP-TLS also requires certificate authority to be deployed. However, certificate-based EAP method is not practical for public WLANs. It was the reason for creation of TTLS and PEAP, which can perform authentication based on a username and a password. This is appropriate since web-login (i.e., UAM) authentication is also based on username/password credentials. Between TTLS and PEAP, PEAP is supported by worldwide largest vendors for supplicants and authenticators. Due to this reason mainly, the choice between TTLS and PEAP gives PEAP as a choice.

Considering the proprietary solutions such as LEAP, it is a good solution for an enterprise. But, in a public WLAN, even in the case when we use APs from one vendor, we must offer a possibility to users to choose the vendor for WLAN card. Therefore, proprietary solutions are not good for a public WLAN. LEAP is additionally proven to be vulnerable [46]. On the other side EAP-FAST [41] solves disadvantages of the LEAP, but it is very recent and not widely deployed, and there is a possibility to get similar position as LEAP on the market, especially because all its features are also implemented in PEAPv2 [47].

EAP methods such as EAP-SIM are lacking support in WLAN equipment (such as WLAN cards), and at this point are not suitable for a public WLAN. However, this can be favorite authentication method if a mobile operator decides to offer dual-mode PLMN/WLAN terminals. In such case, SIM-based authentication will be used for WLAN service in addition to WLAN specific methods, as specified in [27].

According to the above discussion the choice of an EAP method to be used for secured access in a public WLAN is PEAP [43]. So, for secured access in the public WLAN currently the best solution is usage of 802.1X/EAP with PEAP (encryption can be either WEP or WPA, where WPA should have priority in the implementation). The protocol stack for the 802.1X with PEAP solution is shown in Fig. 5.

D. Virtual LAN (VLAN) Solution for a Mobile Operator for Coexistence of UAM and 802.11/EAP Access Methods

So far we have decided to implement at the same time two security solutions, i.e., UAM (public access solution with web-login) and 802.1X/EAP with RADIUS as an advanced security solution. To be able to provide the same infrastructure for both solutions (to reduce costs for network resources as well as networks administration and maintenance), the solution is to use Virtual LAN (defined by IEEE 802.1Q standard [48]).

Virtual LAN technology can provide additional flexibility to the deployment of WLANs, because it can be used to provide logical isolation of traffic sent through WLAN APs. This can be used to separate private WLAN connections from public access traffic.

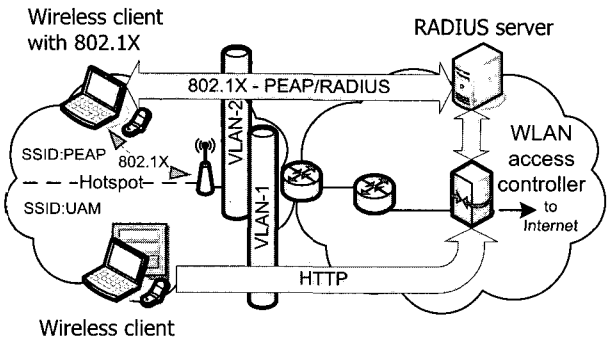


Fig. 6. Solution for coexistence of UAM and 802.1X/EAPfor a mobile operator.

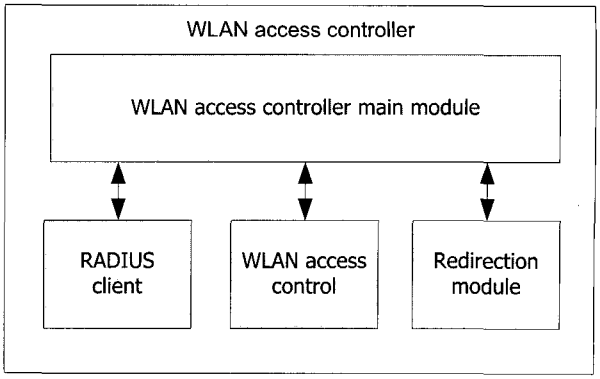


Fig. 7. WLAN access controller.

Solution for coexistence of UAM and 802.1X/EAP access methods is shown in Fig. 6. For that purpose we need to have VLAN support in all APs of the WLAN network. When using different VLANs we are capable to offer UAM and Secured access via the same APs. To support both 802.1X and UAM, the access point needs two different service sets IDentifiers (SSID), where one is corresponding to 802.1X, and the other to UAM.

With current AP hardware only one of these two SSIDs can be broadcasted in the air and seen by WLAN clients, but the other can be also discovered via the 802.11 probe request/response mechanism.

Considering the type of users that will use WLAN, it is better to broadcast the SSID of the UAM VLAN, which uses browser redirection by using IP address filtering mechanism in the WLAN access controller node. When SSID of the UAM VLAN is broadcasted then an authenticated user will be redirected to the web-login page for WLAN whatever he enters for URL. On the web-login page will be provided option for UAM access and secured access (with 802.1X). Additionally, on the web-page should be given links to necessary settings for users that want to start to use the 802.1X secured access to WLAN (some supplicants can be put on the web site for downloading). Also, some information can be offered free to all users that are associated with the WLAN (not authenticated) The SSID of the 802.1X VLAN will be given on the UAM web-login page, so the users that want secured access will use secured SSID with 802.11 probe.

The open SSID (that will be used for UAM) will not require any security on the link layer, but the access controller will limit a user to access only the local web-server until the user obtains authorization to use the network.

Due to single network architecture for both access methods (UAM and 802.1X), we will have the access controller on the path of 802.1X traffic as well.

E. WLAN Access Controller Solution for UAM

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.

In our solution for mobile operator's WLAN network, we will use dynamic packet filtering method for access control in the network access control server. The machine used for access control will have two Ethernet cards, one on the side of the WLAN access network, and the second on the side to the external packet network (i.e., Internet). WLAN access controller is shown in Fig. 7. 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 user interface in the authentication process.

The environment for the WLAN access controller is shown in Fig. 8. In the following sections are described components shown in the Fig. 8.

Web-login solution for UAM: The universal access method—UAM should be as simple as possible for WLAN users. It is worldwide practice to use web-login for the UAM. All HTTP requests of all unauthenticated users will be redirected to the web-login server.

The web-login server will get the original HTTP request, and will log the original URL. Since the requested URL will not be available at the local web-server, default web-login page will be sent to the user.

The user will be requested to enter username and password on the web-login page. After a successful authentication, new rules are added in the WLAN access controller for that user. These rules will remove the redirection and the user will have open access to the Internet.

At the moment when user is logged into WLAN, an applet will start in the user's browser. This applet will contain a logout button. By pressing the logout button the user will be able to log out of the network.

Also, an operator should be able to force a user connection to terminate for some reason (e.g., no credit on WLAN prepaid account). For that purpose we will have an application that should

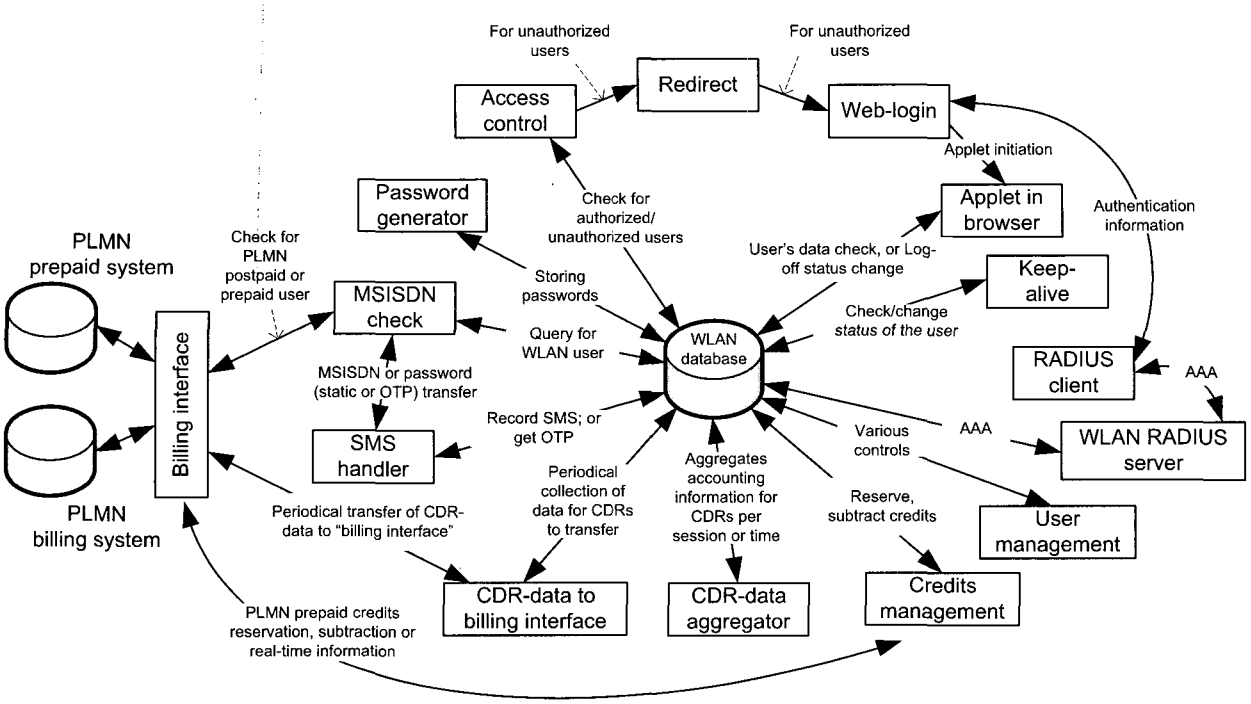


Fig. 8. Solution for PLMN-WLAN integration: Software modules and interfaces.

cut the connection of the user by adding rules at the access controller for user redirection to the initial web-login page.

User's credentials (username and password): This section has to decide what should be used as user credentials for different types of users that may exist, such as PLMN/WLAN postpaid, PLMN/WLAN prepaid, and WLAN prepaid.

For the WLAN prepaid users we will use vouchers with username and password, similarly to prepaid vouchers of Internet service providers. WLAN prepaid cards should not be associated with existing subscribers of the mobile operator. Any user, either mobile operator's subscriber or not, should be able to purchase a WLAN voucher and use it to access the WLAN network. In this case, users' credentials (usernames and passwords) can be generated as random strings with appropriate level of security (e.g., they should have certain length).

For the PLMN postpaid users that will want to have WLAN service charged on their monthly bill, as well as for PLMN prepaid users that will want to have WLAN service charged to their prepaid account, we have a different solution for user credentials than the one for WLAN prepaid users. For authorization purposes of postpaid and PLMN prepaid users of the mobile operator, we use a solution with SMS-OTP as further described. In this case, it is convenient to the MSISDN number of the subscriber as his username. Password will be sent to the user over SMS (as SMS-OTP). When the user will receive the SMS with the OTP, he will be able to access the WLAN, using the MSISDN as his username and SMS-OTP as his password.

Keep-alive solution: Once the user has logged in and started to use the service, accounting has to start. Accounting is done by using RADIUS accounting messages. However, user should not be billed more than his real usage of the network resources. The system has to be created to stop creating accounting records for that user whenever user stops using them.

For that reason, we provide the logout button in Internet browser after the successful login. For time-based charging, whenever the user pushes the logout button he is assured by the system that his session has finished and further no resources are available to him, and no more usage will be charged to him.

However, there is a possibility that the user eventually closes the web-browser without logging out or runs out of battery, so the applet for logout will be killed. In that case, the user losses the feedback module provided in his browser via the applet (which will be java-applet).

There is a security risk associated with the above actions. For example, if a user leaves without closing the session, an attacker may steal the session while the firewall at the access controller is still open for that user. Therefore, the system should be able to detect that the user left the hotspot in order to solve the problems mentioned above. There are several possibilities to perform such control.

- Traffic sent to access controller have to be checked, and whenever a user has not sent traffic for fixed amount of time (e.g., 5 minutes) one may consider that the user has left the network.
- The system could continuously probe the user by using ICMP echo request (i.e., "ping" command) to check if it still available. To avoid unsuccessful checks due to bad coverage, the user should not be logged out at the first unsuccessful ping. However, several unsuccessful probes will lead to user logout.
- Periodical communication between the applet installed in the user's browser at the login phase and a daemon installed at the access controller.

The first solution is the most favorite one, because we do not need to communicate with the user all the time while there is an ongoing session from that user. Hence, we propose and we have

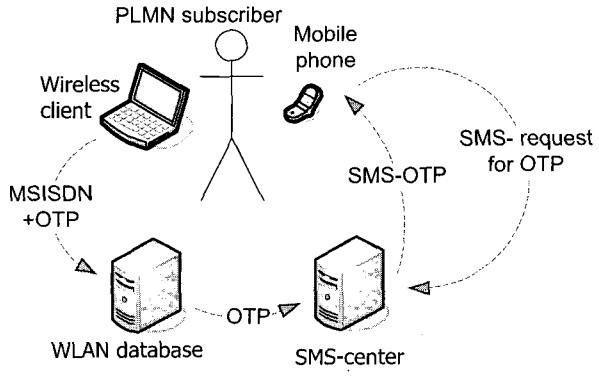


Fig. 9. SMS-OTP flow for authentication of PLMN subscribers for WLAN service.

used the first solution.

SMS-OTP solution: Short message service-one time password (SMS-OTP) is a practical way of authorization of existing PLMN users for additional services, such as WLAN public access at hotspots. If for example, a PLMN subscriber of the mobile operator enters a WLAN hotspot, he should have the possibility to use the WLAN network while still receiving the bill on his monthly PLMN invoice. Using the method of sending password with limited validity we ensure that we will bill the user that owns that subscription, because the OTP will be sent at the process of authentication and authorization to his cellular phone (which is identified by his SIM card). For this purpose, the one time password (OTP) over SMS functionality was set to be mandatory for all PLMN postpaid or prepaid users when they attempt to use public access WLAN of the mobile operator. The OTP over SMS is a feature that will generate a password with a limited validity time and send it to the user's cell phone.

The flow of SMS-OTP is shown in Fig. 9. When a PLMN postpaid or prepaid user is redirected to the web-login page (in UAM) or receives popup window (in 802.1X-PEAP method), he enters his MSISDN number as a username, and a password. If a user requires OTP, he should request one by sending SMS to a designated number (of the mobile operator) for that purpose. WLAN database triggers at the OTP request event and generates one time password (OTP), referred here to as sent-OTP (S-OTP), and sends the S-OTP over SMS using SMS handler application. The SMS handler application receives the S-OTP from RADIUS server together with the MSISDN number of the subscriber, and then sends MSISDN and SMS message content (containing S-OTP) to SMS-center (SMS-C) via an SMS gateway. From SMS-C the message with S-OTP is transferred to the user mobile phone. When the user receives the SMS (shortly after), he enters the MSISDN as his username and received OTP (R-OTP) from the SMS as his password on the web-login page (or popup window for 802.1X). The RADIUS server receives the OTP, referred here to as R-OTP, and compares it with the S-OTP. If the result of matching is positive the user is authenticated and authorized to use the WLAN service.

OTP generation: We propose using the OTP consisted of several randomly generated digits (e.g., 8 or 10 digits). The OTP has a limited time of validity. After expiration of validity time the password is removed from database.

SMS handler: For SMS handling there are existing different applications. Most appropriate protocol for sending/receiving messages to/from SMS-C from the same LAN network as SMS-C is SMPP protocol [49]. There are also other protocols, such as CIMD or simplewire (SMS over the Internet), that are interesting in cases when WLAN is not owned by a mobile operator (which usually has an SMS-C). Hence, in our case SMS-OTP should be send with application that uses SMPP.

PLMN coverage issue for SMS-OTP: The SMS-OTP can not be sent to a user if he is at a place without PLMN coverage. However, PLMN usually has wide coverage, including rural as well as dense populated areas. On the other side, WLAN will be placed in hotspots, where the user population is very dense and certainly will be available PLMN coverage.

IV. SOLUTION FOR UNIFIED BILLING IN THE PLMN-WLAN INTEGRATED NETWORK

In an integrated PLMN-WLAN network, the main objective for an operator is to bill subscribers for the service. Hence, billing of the WLAN users is an essential issue.

In Section II, we defined the architecture for PLMN-WLAN Internetworking. The main integration between the two systems, i.e., PLMN and WLAN is the billing system. Since a mobile operator has already a robust billing system the intention is to use the same system for billing the users for WLAN service.

The billing process is directly related to accounting handling, that is collecting information about usage of the network resources from users, and then sending this information to the billing system with aim to include it in the bill for that user. However, this scenario suits the best for postpaid PLMN subscribers. We may have different requirements for the case of the PLMN prepaid (there is no monthly bill for these users). Additionally, we have already specified that public WLAN network should also include prepaid WLAN users.

To summarize, in a WLAN network operated by a mobile operator, the following types of users are foreseen.

- *PLMN/WLAN postpaid* - these are existing PLMN postpaid users that will subscribe to WLAN service as well.
- *PLMN/WLAN prepaid* - these are existing PLMN prepaid users that will want to use WLAN service and to be charged from their prepaid account.
- *WLAN prepaid* - these are WLAN users that will use WLAN prepaid vouchers (this category includes all, those that are not prepaid or postpaid subscribers of the mobile operator, as well as those that are subscribers of the mobile operator and want to use WLAN vouchers).

A. PLMN/WLAN Postpaid

Billing the PLMN users for WLAN services is related to how to handle accounting, i.e., the process of gathering charging information about the user, processing it, and transferring the bill to the user. To be able to provide a solution for billing WLAN usage to postpaid users, we briefly explain the PLMN accounting in the continuing section.

PLMN-WLAN integrated accounting for postpaid users: A mobile operator already posses a robust billing system for

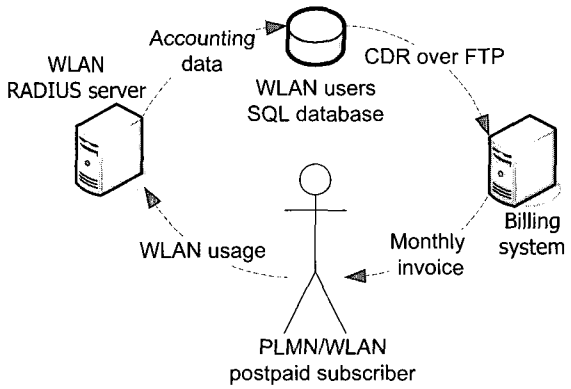


Fig. 10. WLAN postpaid accounting deployment solution.

billing PLMN services to its postpaid users. By adding WLAN service as additional service for the existing postpaid users, the solution is to integrate WLAN accounting into PLMN charging. This way, the existing billing system will be reused for WLAN postpaid subscriptions, and each user will get a single bill considering the WLAN usage as well as PLMN usage.

For integration of WLAN accounting into the PLMN system, it is required that WLAN accounting entity follows the concept of CDRs [50] for correct communication against PLMN entities (e.g., SGSN and GGSN). To be able to reuse the billing system for charging for WLAN usage, we need to provide to WLAN system capability to generate CDRs and to send them periodically to the PLMN billing system.

This scenario is very similar to those of PLMN networks. WLAN CDRs are generated by the WLAN network and sent to the billing system. Generally, there are two options for sending CDRs from WLAN segment to the billing system.

- Option 1: Through PLMN network's CGF, where the PLMN CGF handles the WLAN CDRs just as if they originated from a PLMN specific node. The actual structure of the WLAN-CDR should look like a G-CDR (CDR generated from GGSN) or an S-CDR (that is a CDR generated from SGSN) for the CGF in order for it to process the information without any further modifications to the CGF software and/or PLMN platform in the billing system.
- Option 2: Directly to the billing system, where collection and processing of WLAN-CDRs is done by WLAN AAA server. In this case, CDRs from WLAN will be formatted in ASN.1 format and sent to the billing system over FTP.

In our solution, we choose to use the first option, Option 1, where all charging information is processed at the WLAN AAA server (i.e., RADIUS), and sent to the mediation node, i.e., charging gateway. Further, CDRs are created according to ASN.1 format and sent to the billing system using the FTP over TCP/IP. This way, we exclude any possible problem that may occur due to compatibility. However, the Option 2 is also possible.

In PLMN-WLAN integration, both networks PLMN and WLAN have the same IP backbone. Hence, there will be no problem for communication between the WLAN RADIUS accounting server and the PLMN billing system. The framework for WLAN postpaid AAA flow is shown in Fig. 10.

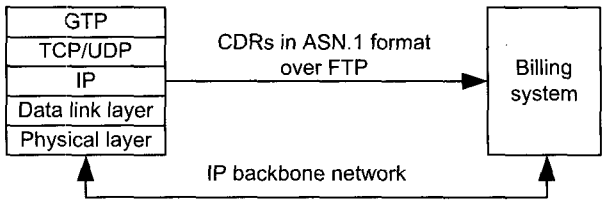


Fig. 11. Transfer of CDRs from WLAN to the billing system of the mobile operator.

Call detail records for WLAN postpaid users: When a PLMN client logs in or logs out from WLAN network RADIUS client always generates accounting start and accounting stop records which are sent to an AAA server (i.e., RADIUS server). These records are collected by the WLAN access controller. The accounting information is then stored in an SQL database. The SQL database contains all the necessary information needed for the mediation node to generate proper CDRs that can be transferred to the billing system. The generation of CDRs does not need to be performed in real-time, but it should be done periodically. For example, CDRs may be created each hour or once a day. However, there are certain factors that should be taken into consideration about the storage and transmission of the CDRs.

As we discussed above, the choice for the CDRs should follow ASN.1 format [51], as shown in Fig. 11. This is the most commonly used record format for charging information in PLMN networks.

Roaming issue for WLAN postpaid: A mobile operator has roaming agreements with PLMN mobile operators worldwide. The roaming provides possibility for a user from other operator than home operator to use given mobile network, and vice versa.

Because in the case of PLMN-WLAN integration, WLAN network will be owned by the mobile operator, which already has roaming agreements for PLMN services, the best solution for WLAN roaming is to exploit the existing roaming agreements. In that sense, the roaming will be mainly possible for PLMN-WLAN postpaid and prepaid users.

The created CDRs from the roaming WLAN users should be sent over TAP or TAP3 to a clearing house. The clearing house may reformat and forward the billing information to the correct mobile operator's billing system. In such case, it is up to a clearing house to keep track of different billing formats, while the WLAN uses the format which was agreed between the clearing house and mobile operator for WLAN service. This practice for PLMN operators that run WLAN networks is also suggested by the GSMA [52].

Another way of roaming between WLANs is by using RADIUS proxy. In such case, a user adds to his username a realm of his home network when roaming (e.g., username@realm).

PLMN to non-PLMN roaming for WLAN, however, proves to be a complex issue with respect to authentication and settlement, since the authentication mechanisms adopted by WISPs are typically username/password which would require Internetworking between PLMN mechanisms and Internet mechanisms. Additionally WISPs will tend to use the AAA which will require some effort to integrate with PLMN TAP procedures. Operators may still have a competitive advantage in this area be-

cause the operators have pre-existing roaming agreements and arrangements and it is probably easier and quicker to negotiate and integrate than to build from beginning.

Accounting information for WLAN postpaid users: Because RADIUS AAA server performs the authentication, authorization, and accounting functionalities, there is minimum information about PLMN/WLAN postpaid user that should be available to the RADIUS server. Such information would be used in order to define the unique identity of the mobile user that is necessary to make sure that correct mobile subscriber is billed for the WLAN usage. In that sense, to be able to use such information, the WLAN part of the network should have capabilities to store such information about the WLAN users somewhere in the network.

The authentication server needs to store certain information about the WLAN subscribers. Relevant information about a WLAN postpaid subscriber is

- MSISDN/IMSI number of the mobile user,
- One-time-password (the current one), and
- Accounting data.

The above information should be stored in such a way that authentication server (i.e., RADIUS server) can connect to the WLAN database and then get the relevant information from the database. This is done over SQL.

Accounting data needed for generation of the CDR will include the following details: MSISDN number of the user, IP address, number of sent and received octets (i.e., bytes) by WLAN user, session identifier, session duration time, session start time, and authentication method (UAM or 802.1X-PEAP).

All accounting details listed above are already included in the RADIUS protocol. One should note that MSISDN information refers to accounting data for PLMN/WLAN postpaid or prepaid users (not for WLAN prepaid).

WLAN postpaid AAA flow: In Fig. 12, we show the complete flow of AAA information between different network nodes. Here, we will summarize our solution for authentication and billing of PLMN/WLAN postpaid subscribers. However, due to the usage of the mediation node that handles requests towards postpaid billing system and prepaid billing system, this diagram can be also applied for charging WLAN service to PLMN prepaid users.

When a user enters a hotspot with WLAN coverage, he needs to perform authentication to be able to access the global Internet. As we defined in Section III, we will have two types of authentication: UAM and 802.1X-PEAP. Regardless of the type of the authentication, we unify the accounting and billing process for the WLAN postpaid users.

For both authentication methods, the user should enter (in the web login page for UAM, or in the popup window for 802.1X-PEAP) his MSISDN number as a username, and a password. The password is one-time-password (OTP), which will have limited time validity (e.g., a few hours). To be able to obtain OTP the user will be required to send an SMS message to a designated number for that purpose.

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 found also roaming users from other operators.

After a positive check of the user's MSISDN, an application will trigger generation of OTP for that user (refer to Section III). 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, and accounting stop). RADIUS server stores every accounting message into WLAN database.

Each accounting message triggers the database to send request to the mediation node, i.e., PLMN open charging interface—OCI (Fig. 12). From the accounting data recorded into the OCI database, an application periodically creates CDRs for completed sessions. All created CDRs are periodically sent to the billing systems of the mobile operator over FTP.

B. PLMN/WLAN Prepaid

In PLMN-WLAN network, there are possible two types of prepaid users: One with PLMN prepaid cards and the other with WLAN prepaid cards. In this section, we refer to the first one.

In PLMN, there is existing solution for handling prepaid users. Each user purchases voucher (scratch-card), which has certain value and limited time validity (e.g., three months, six months, etc.). When a mobile user runs out of credits, or validity of his voucher expires, he is barred from using the network resources.

PLMN/WLAN prepaid users are prepaid users of mobile operator that also use WLAN service. Main problem here is how to handle credits in real-time. Handling of prepaid users considering the billing is very much different than postpaid users.

While postpaid users get all the charging for WLAN usage in their monthly bill, PLMN/WLAN prepaid users have credits that are used for all their services including PLMN services and WLAN.

The flow of accounting and billing information for PLMN/WLAN prepaid users (as described above) is shown in Fig. 12, and is the same as for PLMN/WLAN postpaid users. The difference between PLMN postpaid and prepaid users is made in the open charging interface—OCI. For PLMN prepaid users the OCI request credits in advance for WLAN usage, either for a time period (e.g., one minute) or for a given amount of data (in bytes). However, different pricing factors (e.g., different tariffs) are agreed between WLAN database and the OCI prior to their interconnection.

C. WLAN Prepaid

WLAN prepaid refers to prepaid users that are using WLAN vouchers. This category includes WLAN users that are not PLMN subscribers, but it may also include PLMN subscribers that want to use WLAN prepaid vouchers to access WLAN network. In general, there is simply no limitation about who can be a WLAN prepaid user, i.e., everybody with purchased and activated WLAN voucher will be WLAN prepaid user of the mobile

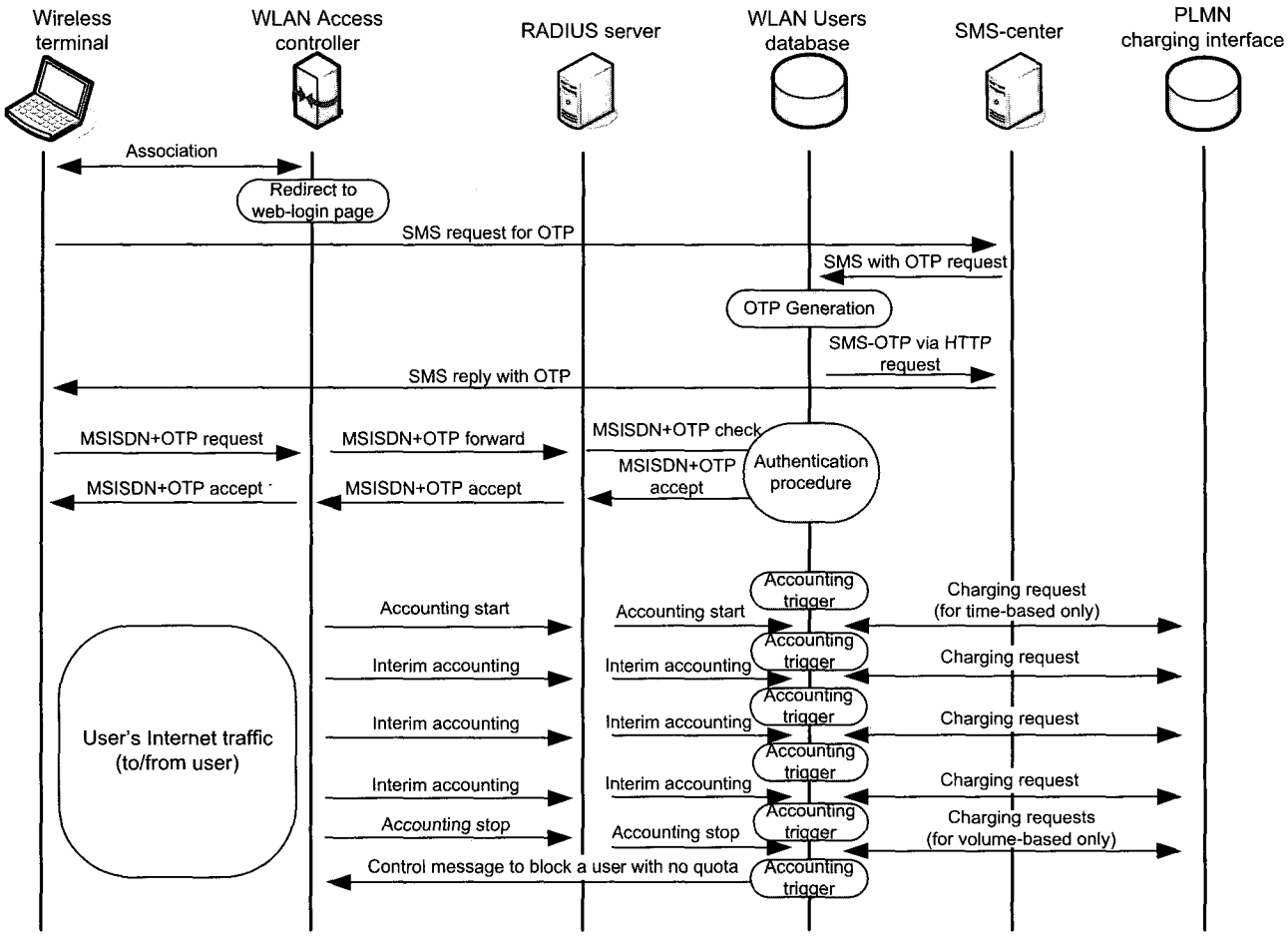


Fig. 12. Accounting and billing flow for PLMN postpaid and prepaid users that use WLAN service.

operator.

In the case of WLAN prepaid users, there is no intercommunication between nodes in PLMN network and nodes in WLAN segment. However, WLAN prepaid users share the same Internet access as PLMN/WLAN postpaid and PLMN/WLAN prepaid users.

The accounting flow for WLAN prepaid users is shown in Fig. 13. First major difference between WLAN prepaid and the PLMN/WLAN postpaid or PLMN/WLAN prepaid is the type of credentials. While in the previous two cases username was MSISDN number of the PLMN subscriber, in the WLAN prepaid case the credentials will be given on the WLAN voucher. There can be username and password given on the voucher, or just one credential (i.e., unique number of the voucher).

As usual with prepaid vouchers, all voucher numbers or username/password pairs of the vouchers will be recorded into WLAN database prior to their selling. When subscriber buys a voucher at the first login he should enter credential(s) from the prepaid card into web-login page (for UAM access) or in popup window (for 802.1X-PEAP access). Then, system compares the entered credentials from the user with those in WLAN database, and if a match is found, WLAN prepaid account is created with a certain amount of credits (dependent upon the voucher type).

After a successful authentication, user is granted access to the Internet. During the active session user balance is periodically checked (i.e., every minute) and number of credits is updated according to the usage of resources. At each balance check quota is allocated until the next balance check. For example, for time-based charging, with balance check on every minute, the user will be granted further usage only when he has at least credits for another minute of usage. It is similar for volume-based charging of the prepaid WLAN users. When next quota can not be allocated to the user during a session (or at the authentication phase) his access to the Internet will be terminated by WLAN access controller and his browser will be redirected to the web-login page where the user will be offered to activate another voucher.

D. Billing and Pricing for WLAN Usage

Billing and charging management in the WLAN network operated by a mobile operator is process of integrating the WLAN billing functions into the overall customer billing system [52]. In particular, the billing for WLAN can be based on

- Resource usage (e.g., amount of data transferred in bytes, or time duration of a session) or fixed fee and
- Location of the user (i.e., hotspot location) and discounts.

In our solution for each user will be collected parameters for the WLAN resources usage as well as location information. The duration of a session is the time between the login and logout (which happens when user pushes the logout button or when

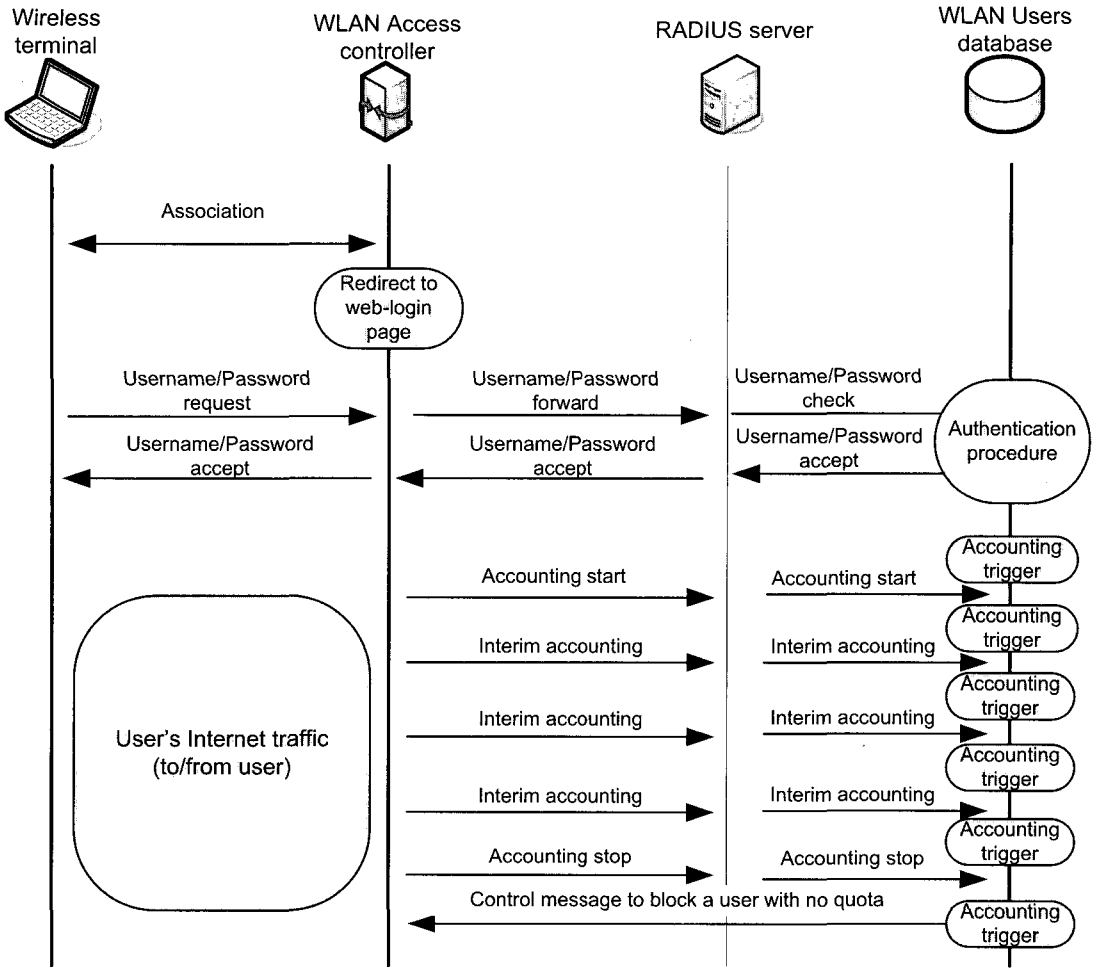


Fig. 13. Accounting and billing flow for WLAN prepaid users.

session ends due to session or idle timeout).

The collected information about connection duration and transferred bytes can be used for different pricing schemes [53]. Table 3 provides pricing basis as well as pricing factors that influence the type of pricing.

Hence, besides billing on basis of resource usage there can be flat fee (or fixed fee) pricing. The fixed fee pricing can be on hourly, daily, weekly, or even monthly basis. In some cases, it is useful to provide access to some services for free (e.g., to obtain local information at the airport, or to obtain information about local shops, events, etc.).

Also, there are some pricing factors that influence the price for resource usage. One pricing factor is location, that is same amount of time or bytes can be charged differently in different areas (i.e., the cost may be higher in a hotel, and lower in a coffee shop, or vice-versa). Another pricing factor is discount, such as time of day (e.g., in current cellular networks different tariffs are usually applied during the day and the night hours). Other pricing factor is usage intensity, i.e., users with higher usage may be offered lower prices per minute or byte. Also, there can be given different prices for group usage (e.g., corporate subscriptions), etc.

However, pricing for the WLAN usage is dependent upon the mobile operator.

Table 3. Pricing basis and factors.

Pricing basis		Pricing factors	
Usage	Fixed fee	Location	Discount
Per minute	Free	Home area	Time of day
Per bytes	Hourly	Roaming area	Usage
	Daily	Premium	Loyalty
	Weekly	hotspots	Group
	Monthly		

V. CONCLUSION

Public WLANs provide an important complement to mobile networks, enabling broadband Internet access in selected hot spots and offering additional capacity to the PLMN networks. Public WLANs can be deployed today with a simple and cost effective solution based on existing equipment.

In this paper, we have described our solution for PLMN-WLAN interoperability. First, we have made a choice for loosely-coupled PLMN-WLAN integration, which is a dominant scenario today worldwide and has advantages over the tightly-coupled approach. Furthermore, we have decided to provide both types of access methods, unsecured or universal access

method, which is dominant in wireless ISPs today, and secured access, which offers higher protection of user's information, but requires certain settings in mobile clients.

We have chosen AAA server type as well as protocols for secured WLAN access. Further, we have developed WLAN access controller, which works as a gateway towards Internet and PLMN. Also, we have developed PLMN-WLAN AAA gateway, including PLMN/WLAN postpaid and prepaid users as well as WLAN prepaid users. The created solution is cost-effective and provides all needed functionalities for efficient charging and billing, as well as secured and non-secured access to Internet via WLAN.

REFERENCES

[1] Pyramid Research, "US Wi-Fi users (paid and free) vs. 2.5G/3G data users (paid)," 2004.

[2] Alcatel, "Public wireless LAN for mobile operators: WLAN beyond the enterprise," White paper, 2003.

[3] Flash Networks, "NettGain 1200 flash networks," available at http://www.adjungonet.com.

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

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

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

[7] WeRoam – WLAN and PLMN united, availabe at http://www.weroam.com, accessed June 2004.

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

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

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

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

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

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

[14] VIPonline, availabe at http://airlink.vip.hr/hotspot/, accessed June 2004.

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

[16] M. Buddhikot *et al.*, "Integration of 802.11 and third-generation wireless data networks," in *Proc. INFOCOM 2003,* San Francisco, USA, Mar.–Apr., 2002.

[17] M. T. Bostrom and A. Norefors, "Ericsson mobile operator WLAN," Release 1 Technical Description, Feb. 2002.

[18] Wi-Fi Alliance (2003), "Wi-Fi alliance wireless ISP roaming best practices document," availabe at 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, Oct. 2002.

[20] IEEE 802.1Q standard, "IEEE standard for local and metropolitan area networks - virtual bridged local area networks," May 7, 2002.

[21] C. Rigney *et al.*, "Remote dial-in user authentication service (RADIUS)," RFC 2865, June 2000.

[22] C. Rigney, "RADIUS accounting," RFC 2866, June 2000.

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

[24] Cisco, "Single-user network access security TACACS+," availabe at http://www.cisco.com/warp/public/614/7.html, accessed June 2003.

[25] C. Finseth, "An access control sometimes called TACACS," RFC 1492, July 1993.

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

[27] 3GPP TS 23.234, "3GPP system to wireless local area network (WLAN) interworking; system description (Release 6)," v6.4.0, Mar. 2005.

[28] T. Janevski, *Traffic Analysis and Design of Wireless IP Networks*, Boston, MA: Artech House, 2003.

[29] Wi-Fi Alliance, "Q&A Wi-Fi protected access," availabe at http://www.wi-fi.org/OpenSection/pdf/Wi-Fi_Protected_Access_QA.pdf, Mar. 2003.

[30] F. Ohrtman and K. Roeder, *Wi-Fi Handbook: Building 802.11b Wireless Networks*, McGraw-Hill, 2003.

[31] IEEE 802.1X standard, "IEEE standard for local and metropolitan area networks - port-based access control," July 2001.

[32] US Department of Commerce, "Advanced encryption standard (AES)," Federal Information Processing Standard (FIPS), Publication 197, Nov. 2001.

[33] L. Blunk and J. Vollbrecht, "PPP extensible authentication protocol," IETF, RFC 2284, Mar. 1998.

[34] T. Dierks and C. Allen, "The TLS Protocol," RFC 2246, Jan. 1999.

[35] T. Wu, "The SRP authentication and key exchange system," RFC 2945, Sept. 2000.

[36] IEEE 802.1X standard, "IEEE standard for local and metropolitan area networks - port-based access control," July 2001.

[37] W. Simpson, "PPP challenge handshake authentication protocol (CHAP)," Aug. 1996.

[38] RFC 2716, "PPP EAP TLS authentication protocol," Internet Engineering Task Force (IETF), Oct. 1999.

[39] J. Hammond *et al.*, "Wireless hotspot deployment guide," Intel Commun., Dec. 2003.

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

[41] N. Cam-Winget *et al.*, "EAP flexible authentication via secure tunnelling (EAP-FAST)," draft-cam-winget-eap-fast-00, Feb. 2003.

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

[43] P. Iyer *et al.*, "Public WLAN hotspot deployment and Internetworking," *Intel Technol. J.* vol. 7, Aug. 19, 2003.

[44] Microsoft 802.1x Authentication Client, availabe at http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/, Dec. 13, 2002.

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

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

[47] Palekar *et al.*, "Protected EAP Protocol (PEAP) version 2," draft-josefsson-pppext-eap-tls-eap-00, Oct. 2003.

[48] IEEE 802.1Q standard, "IEEE standard for local and metropolitan area networks - virtual bridged local area networks," May 7, 2003.

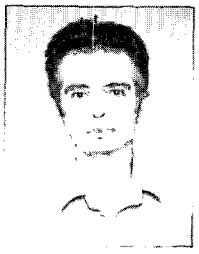
[49] SMPP Protocol Specification v4.0, availabe at http://www.smsforum.net/doc/public/.

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

[51] 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.

[52] PLMN Association, "Services, ease of use, and operator considerations in Interworked WLAN-cellular systems," PRD SE. 27, May 28, 2003.

[53] Portal Software Inc., "Overcoming wireless LAN billing challenges," 2003.



Toni Janevski was born in Skopje, Republic of Macedonia, on October 15, 1972. He received the B.Sc. degree in Electrical Engineering and the M.Sc. and the D.Sc. degrees in Electrical Engineering from the University Sv. Kiril i Metodij, Skopje, R. Macedonia, in 1996, 1999, and 2001, respectively. From 1996 to 1999, he was with Mobimak GSM mobile operator in R. Macedonia. From October 1999, he is with Faculty of Electrical Engineering in Skopje. From July 2001 to November 2001, he was at IBM T. J. Watson Research Center, New York, USA. He has written the book *Traffic Analysis and Design of wireless IP Networks*, published by Artech House Inc. in 2003. He is Assistant Professor at the Faculty of Electrical Engineering, University Sv. Kiril i Metodij, Skopje. His research interests are in wireless and mobile networks, Quality of Service, network planning and dimensioning, traffic theory, and Internetworking. He is Senior Member of IEEE.