

Design and Implementation of a WLAN/CDMA2000 Interworking Architecture

M. Buddhikot, G. Chandranmenon, S. Han, Y. W. Lee, S. Miller, L. Salgarelli

Bell Labs, Lucent Technologies, NJ USA

Abstract—The combination of 3G and WLAN wireless technologies offers the possibility of achieving anywhere, anytime Internet access, bringing benefits to both end-users and service providers. In this article, we discuss interworking architectures for providing integrated service capability across the widely deployed 3G CDMA2000-based and 802.11-based networks. Specifically, we present two design choices for integration, namely *tightly-coupled* and *loosely-coupled*, and recommend the latter as a preferred option. We describe in detail the implementation of the loosely-coupled integrated network, which provides two kinds of roaming services, the *Simple-IP* service, and the *Mobile-IP* service. We present in detail two new components used to build these services: a network element called *WLAN integration gateway* deployed in WLAN networks and a client software on the mobile device. For a mobile device with interfaces to both technologies, our system supports seamless handoff in presence of overlapping radio coverage.

I. INTRODUCTION

The Internet has emerged as an all-pervasive technology that continues to experience tremendous growth and popularity. Our ever increasing dependence on this technology has sparked the interest to make it truly ubiquitous – available *anywhere, any time*. Recent advances in wireless technologies will help realize this vision. To this end, there are two technologies that are gaining momentum. *Wireless local-area networks* (WLANs) based on the IEEE 802.11 standards [1], also known as Wi-Fi, are popular in enterprise networks, homes, and public hot-spots such as airports and hotels. WLAN enables wireless networks that support data rates of 1Mbps to 54Mbps over small areas of a few thousand square meters. *Wireless wide-area networks*, based on 3rd-generation (3G) standards such as CDMA2000 [2], on the other hand, support peak rates from 144Kbps to 2.4Mbps and offer connectivity over a wide area of the order of several square kilometers.

Given the complementary characteristics of WLAN (faster, short distance access) and CDMA2000 (slower, long range access), it is compelling to combine them to provide ubiquitous wireless access. Such integration can bring significant benefits to service providers and end-users. It will allow CDMA2000 service providers to economically offload data traffic from wide-area wireless spectrum to WLANs in indoor locations, hotspots and other areas with high density of users. Providing WLAN

hot-spot access as a value-added service can increase their customer base. For WLAN service providers, integration will bring them a larger user base from partner CDMA2000 networks, without having to win them through per-customer service contracts. Also, the customers will benefit from the enhanced performance in the form of greater coverage, higher data rate, and lower overall cost of such a combined service.

Figure 1 illustrates a conceptual view of the integrated public wireless networks that will offer such a service. End user devices, such as laptops, palmtops and phones that can access networks based on both technologies are already becoming available. A user of this integrated network would prefer to have exactly *one service subscription* with *one service provider* typically called its *home network provider*. When a user subscribes to such a service, credentials in the form of authentication information (such as shared secret keys), profile information (such as class of service, minimum bandwidth) and accounting information will be stored in a network based authentication, authorization and accounting server (AAA) called *home AAA*. This single account will enable the user to access the data and voice services anywhere, any time, receive exactly *one billing statement*, *roam* freely among all networks that the user's provider has agreements with, and get similar *quality of service*. Using a single account in this manner on different networks requires that the network providers be able to authenticate each other's users, and obtain their service profile parameters. This is enabled by roaming agreements established among service providers using the AAA protocols such as RADIUS[10] or DIAMETER [12] and AAA broker networks.

The emerging integrated public wireless networks will offer two roaming services: the Simple-IP service and the Mobile-IP service. The Simple-IP service offers integrated billing and subscriber profiles but does not guarantee session continuity across network boundaries. The Mobile-IP service additionally enables seamless handoffs between networks to preserve ongoing sessions.

The goal of this article is to first describe design options available to build an integrated network and then present details

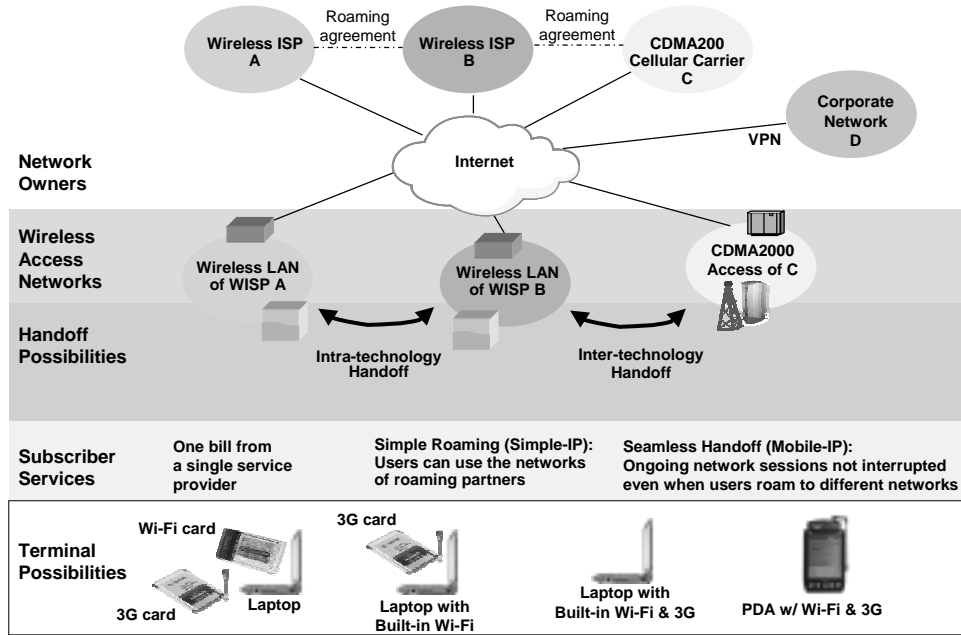


Fig. 1. CDMA2000/WLAN integration: The big picture

of design and implementation of the aforementioned two integrated services using the preferred approach. Specifically, we discuss two possible approaches, *tightly-coupled* and *loosely-coupled*, and advocate the latter as the preferred approach. We describe our implementation of the two services in the loosely-coupled architecture, which includes two new components: a network element called IOTA¹ gateway and a service access software on the mobile device. We primarily focus on integration of WLAN and 3GPP2 CDMA2000 networks. However, the loose integration architecture and design choices for the integration gateway and client software described here apply to integration of WLAN and 3GPP UMTS networks as well.

II. CDMA2000 AND WLAN BACKGROUND

In this section, we will provide a brief background on the architecture of CDMA2000 and 802.11 WLAN networks.

A. Overview of CDMA2000 Network

Figure 2a illustrates the basic architecture of 3G-1x, and 1xEV-DO CDMA2000 networks. The Radio Access Network (RAN) in CDMA2000 networks consists of multiple Base Stations (BS) each connected to a Radio Network Controller (RNC) by T1/T3 links. The RNC manages several concurrent Radio Link Protocol (RLP) layer-2 sessions with Mobile Nodes (MNs) and performs per-link bandwidth management functions. The 144Kbps per carrier throughput in 3G-1x is shared among multiple active MNs, though at any given instant, a single MN may

be allocated full data rate. When a MN moves from one RNC to the other, the on-going RLP session is torn down and a new session is established with the visited RNC.

The Packet Data Serving Node (PDSN) in the architecture aggregates data traffic from multiple RNCs and interfaces the RAN to a packet switched network. The PDSN terminates a Point-to-Point (PPP) connection (see Figure 2a) and maintains session state for each mobile node (MN) in its serving area. PPP header and payload compression can be negotiated between the PDSN and the MN. The hierarchical architecture and the radio access protocols of CDMA2000 enables mobility within the serving area of the PDSN, by keeping PPP connections alive.

The PDSN is required to support two modes of IP operation: Simple-IP and Mobile-IP. In Simple-IP mode, if the MN moves from one PDSN to another, the PPP connection must be re-established, and a new IP address is acquired. This requires the user to re-establish all their data sessions. In the Mobile-IP mode, the PDSN implements the Foreign Agent (FA) functionality defined in Mobile IP [9], allowing cross PDSN mobility.

From a data networking point of view, the 1xEV-DO architecture is similar to that of 3G-1x, in that it uses PPP between the MN and the PDSN, and provides mobility within the serving area of the PDSN. However, 1xEV-DO offers Data-Only service with up to 2.4Mbps downstream bandwidth, and relies solely on AAA server for authentication.

¹IOTA stands for "Integration Of Two Access technologies"

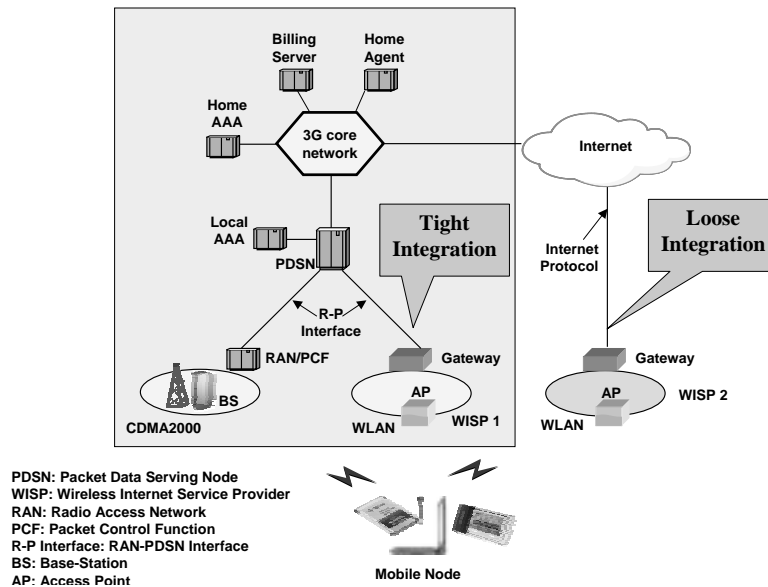


Fig. 3. 3G and WLAN integration: tightly-coupled vs. loosely-coupled architectures.

pendently operated WLAN islands could not be integrated with 3G networks without explicit physical connectivity to the 3G core network. Today's 3G networks are being deployed using carefully engineered network-planning tools, and the capacity and configuration of each network element is calculated using mechanisms which are very much specific to the technology utilized over the air interface. By injecting the WLAN traffic directly into the 3G core, the setup of the entire network, as well as the configuration and the design of network elements such as PDSNs have to be modified to sustain the increased load.

The configuration of the client devices also presents several issues with this approach. First, as described earlier, the WLAN cards would need to implement the 3G protocol stack. It would also mandate the use of 3G-specific authentication mechanisms for authentication on Wireless LANs, forcing WLAN providers to interconnect to the 3G carriers' SS7 network to perform authentication procedures. This would also imply the use of WLAN cards with built-in 3G credentials.

For the reasons described above, the complexity and the high cost of the reconfiguration of the 3G core networks and WLAN gateways would force operators that chose the tightly-coupled approach to become uncompetitive to WLAN-only ISPs.

B. Loosely-coupled Interworking

Like the previous architecture, the loosely-coupled approach calls for the introduction of a new element in the WLAN network, the WLAN gateway. However, in this design (WISP No.2 in Figure 3), the gateway connects to the Internet and does not have any direct link to 3G network elements such as PDSNs or 3G core network switches. The user population that accesses

services of the WLAN gateway may include users that have locally signed on, as well as mobile users visiting from other networks. We call this approach *loosely-coupled interworking* because it completely separates the data paths in WLAN and 3G networks. The high speed WLAN data traffic is never injected into the 3G core network but the end user still experience seamless access.

In this approach, different mechanisms and protocols can handle authentication, billing and mobility management in the 3G and WLAN portions of the network. However, for seamless operation to be possible, they have to interoperate. In the case of interoperation with CDMA2000, this requires that the WLAN gateway supports Mobile-IP functionalities to handle mobility across networks, as well as AAA services to interwork with the 3G's home network AAA servers. This will enable the 3G provider to collect the WLAN accounting records and generate a unified billing statement indicating usage and various price schemes for both (3G and WLAN) networks. At the same time, the use of compatible AAA services on the two networks would allow the WLAN gateway to dynamically obtain per-user service policies from their Home AAA servers, and to enforce and adapt such policies to the WLAN network.

There are several advantages to the loosely-coupled integration approach. First, it allows independent deployment and traffic engineering of WLAN and 3G networks. 3G carriers can benefit from other providers' WLAN deployments without extensive capital investments. At the same time, they can continue to deploy 3G networks using well-established engineering techniques and tools. Furthermore, while roaming agreements with many partners can result in widespread coverage, including key

hot-spot areas, subscribers benefit from having just one service provider for all network access. They no longer need to establish separate accounts with providers in different regions, or covering different access technologies. Finally, unlike the tightly-coupled approach, this architecture allows a WISP to provide its own public WLAN hot-spot, inter-operate through roaming agreements with public WLAN and 3G service providers, or manage a privately installed enterprise Wireless LAN.

It should be clear that the loosely-coupled approach offers several architectural advantages over the tightly-coupled approach, with virtually no drawbacks. Therefore, it has emerged as a preferred architecture for the integration of WLAN with 3G networks, and we will use it as a reference throughout the rest of the article.

IV. AUTHENTICATION AND PRIVACY

A WLAN gateway should provide Internet access to only legitimate users and therefore, must support user authentication at one or more protocol layers. In the WLAN link-layer, three authentication and/or access control methods are possible.

- *Static filtering based on MAC-address:* In this method, WLAN access points (AP) drop traffic of all hosts except those of certain pre-configured network devices. Typically filtering rules are specified using the layer-2 address (aka MAC or hardware address) of the network device.
- *WEP (Wired-Equivalence Privacy) of the 802.11b standard [1]:* In this method, WLAN APs verify that the end host knows a shared secret in the form of a 40 or 104-bit WEP key, which is used for all network devices accessing the same AP.
- *The 802.11i standard[4]:* 802.11i is a newer standard for access control that allows dynamic per-user, per-session authentication and encryption keys and stronger packet encryption.

The first two methods are not suitable for use in a public environment, whereas the third method is not backward compatible with legacy access points and mobile nodes that do not have 802.11i support.

In a public environment with dynamic user population, exhaustive and static configuration of all access points with a list of MAC-addresses is infeasible.

The main problem with WEP is that the same key is shared by all users using the same access point. In public environments, it is very difficult to securely distribute and revoke this key for a dynamic user population. Furthermore, since the same key is also used for encryption, all authenticated users can snoop on each other's traffic. Apart from this problem, there are well-known attacks on the flawed WEP encryption algorithm [7].

802.11i is considered a significant improvement for the public environment. It employs the IEEE 802.1x Port Access Control standard which specifies the use of EAP-over-LAN (EAPOL) protocol [3] between the MN and access point to perform per-session user authentication. The EAPOL protocol encapsulates Extensible Authentication (EAP) protocol packets, which access point can transfer to a service provider Home-AAA using RADIUS AAA protocol. This allows the use of any of the well known EAP-schemes such as EAP-TLS [5], EAP-SIM [13], EAP-AKA [6], EAP-SKE [11] to authenticate a MN. Additionally, individual per-user session keys, used for encryption and integrity protection, are derived and distributed during the authentication exchange with the Home-AAA server. This eliminates the need for any preconfiguration of keys and MAC addresses in WLAN access points, and only requires a security association between the user and its home service provider. The 802.11i standard also specifies a Temporal Key Integrity Protocol (TKIP) that defines a key-derivation procedure to derive encryption, authentication and integrity protection keys and a WEP-compatible encryption enhancement to fix known flaws in WEP. The TKIP specification improves WEP authentication and encryption to acceptable levels and provides a graceful migration of existing infrastructure and client devices. The 802.11i standard also describes an optional Wireless Robust Authentication Protocol (WRAP) that uses strong 128-bit AES encryption which is attractive in the long term.

Figure 4 illustrates the authentication model a WLAN integration gateway should implement to support authentication at layer-2, 3 and 7. The model relies on the dynamic packet filters that use information that includes MAC address, IP source and destination address, and TCP/UDP source and destination ports. The dynamic filters are updated based on the status of user authentication.

The authentication path and the corresponding dynamic packet filters used depend on the service mode. For Mobile-IP mode, the authentication is done as a part of the Mobile-IP registration, in which the mobile node (MN) registers through the Foreign Agent (FA) to the Home Agent (HA). During the registration, the MN presents to the FA an evidence that it knows the MN-AAA key, which is a shared secret between the MN and the Home AAA (H-AAA). Until the registration succeeds, FA inserts packet filters that block all other MN traffic.

For Simple-IP mode, the MN's authentication procedure is triggered by the first web access of the user. The HTTP access will be intercepted by the packet filter, and it will be redirected to a Web Authenticator in the gateway. The Authenticator presents

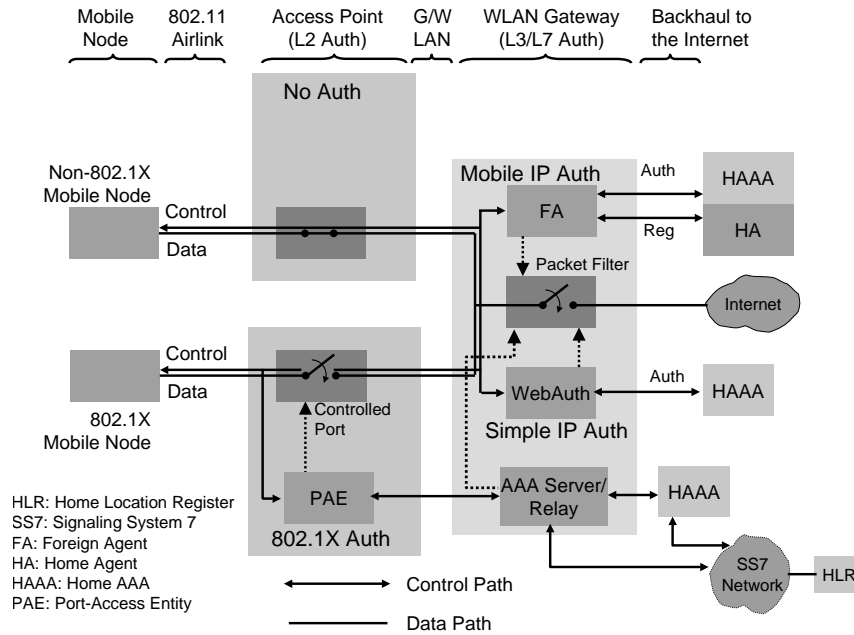


Fig. 4. Authentication model for WLAN gateway

to the user a secured login page over a HTTPS connection instead of the original web page that the user requested. The user enters her username and password to login. The Authenticator authenticates the user by consulting the Home AAA.

In our model, a non-802.11i mobile node can connect through the access point without any layer-2 authentication. However, it cannot connect to the Internet unless it has successfully authenticated with the gateway.

On the other hand, a 802.11i capable MN needs to authenticate with both the access point and the gateway for access to the Internet. Note that in Simple-IP mode, layer-3 authentication is redundant and can be eliminated to allow single-logon for user if the integration gateway monitors layer-2 authentication traffic and unblocks MN traffic upon successful authentication.

Note that certain EAP-schemes such as EAP-SIM, EAP-AKA rely on SIM/USIM cards on the MN and corresponding credentials stored at a Home Location Register (HLR) on a SS7 network. In this case, either the gateway or the H-AAA must interface to an SS7 network to communicate with the HLR.

One important final remark about the WLAN integration gateway is that it may support IPSEC or SSL VPNs and provide fast encryption to support privacy at layer-3 and above. This may be important if the 802.11 WLAN is operated without layer-2 encryption and authentication and only layer-3 or higher authentication is employed. Note that web authentication takes place over a HTTPS connection and therefore, the username and password information cannot be snooped by a malicious user in the WLAN network. Similarly, MIP registration has built in replay

protection. However, in both cases, lack of layer-2 encryption allows for MAC and IP address spoofing between successful authentications.

V. TWO INTEGRATED SERVICES

In this section, we describe the basic Simple-IP service and a more advanced Mobile-IP service.

A. Simple-IP Service

In case of 802.11i enabled deployments, the client first performs layer-2 authentication, and then requests IP address from the local WLAN integration gateway. If the authentication is successful, the gateway provides a private or public IP address through DHCP and configures appropriate features such as QoS guarantees, and Network-Address-Translation (NAT). Optionally, for non-802.11i deployments, web-based authentication can be used.

Note that in the event of mobility, the user acquires a new IP address and on-going sessions are lost. Therefore, the Simple-IP service is most appropriate for environments with limited mobility where layer-2 mobility mechanisms satisfy mobility needs. One key advantage of this service is that it does not need a specialized client software for service access.

B. Mobile IP service

The goal of Mobile-IP service is to preserve user sessions when a user roams among heterogenous networks of different providers with different access technologies. We employ two basic ideas to achieve this goal: (1) Use of Mobile IP in the

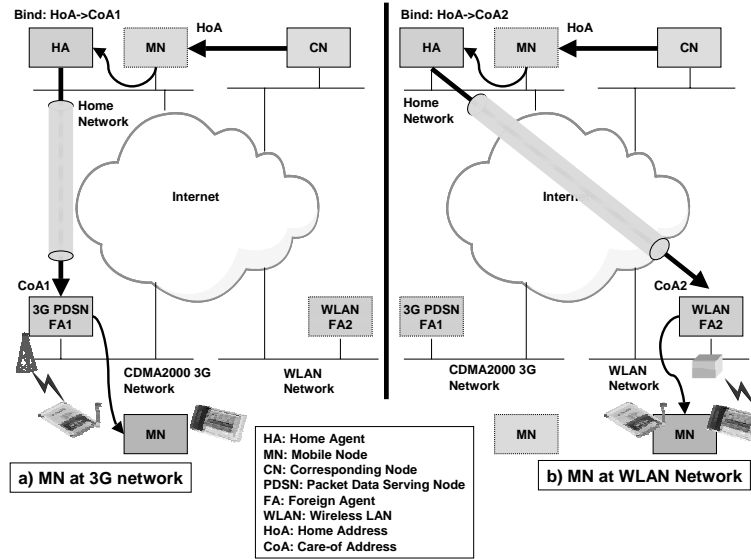


Fig. 5. Using Mobile-IP for inter-technology handoff

WLAN gateway and (2) Intelligent interface selection at the client in presence of overlapped coverage between CDMA2000 and WLAN networks. We elaborate on these ideas in detail below.

The Internet Protocol (IP) does not provide native support for mobility, i.e., when a host moves and attaches to a different physical network, its IP address must change, forcing all transport level sessions with any internet hosts to break. Mobile-IP [9], standardized in IETF, addresses this problem; it allows an internet host to keep a fixed address called *home address* (HoA). To deliver packets to the current point of attachment, Mobile IP employs two network elements: a home agent (HA) in the home network and a foreign agent (FA) in the visited network. When in the foreign network, MN discovers a local FA and registers the address of the FA as a “care-of-address” with its HA, creating the binding $B : HoA \rightarrow CoA$ (Figure 5(a)). The HA intercepts a packet from any correspondent host (CN) to the MN, encapsulates it in another IP packet, and tunnels it to the FA. The FA decapsulates and delivers the original packet to the MN. Since MN maintains its home address, all its transport protocol sessions are preserved.

The CDMA2000 standard incorporates Mobile-IP to achieve inter-PDSN handoff. The PDSN node in the CDMA2000 network implements the foreign-agent.

Therefore, a natural way to implement inter-technology handoff between CDMA2000 and WLAN networks is to implement Mobile-IP functionality in the WLAN gateway and in the Mobile Node. The scenario is depicted in Figure 5(b).

The MN performs session handoffs in two cases: when it loses signal on the wireless link currently in use or when it finds

a better wireless link that can provide better performance. For example, it will switch from 3G to WLAN when it acquires WLAN, and switch from WLAN to 3G when it loses WLAN signal. To avoid service disruption and packet loss during service handoff, the MN can exploit any overlapped 3G and WLAN coverage. It can keep both network interfaces active. While using the current network link (e.g. 3G), it can use the non-current network link (e.g. WLAN) to prepare a handoff in the background. Figure 6(a) depicts this scenario. Specifically, it shows the WLAN signal observed by the client over time. At t_1 , when the signal strength exceeds the threshold H , the client will attempt to use WLAN airlink. Similarly at time t_2 , when the signal strength drops below the threshold L , the client will revert to the 3G airlink. Two thresholds, H and L , are used to avoid unnecessary handoffs that can result in poor connection. Switching to a different airlink involves several steps: discovery of a local FA, Mobile-IP registration with FA over the new airlink, creation of new tunnels at the home agent, and setting up of packet filter in the gateway. If the client completes these steps before losing the signal on the current interface, the delays with these steps (indicated by Δ_1 and Δ_2 in the Figure 6) can be masked and handoff will appear instantaneous to the client application. For incoming traffic, packets that are in the network will continue to arrive at the old interface, which the mobile node still listens to. For outgoing traffic, the TCP/IP stack on the mobile node will start using the new airlink immediately after the atomic operation of airlink switching. As a result, packet loss due to handoff is minimized.

Of course, in the absence of overlapped coverage, there will be service interruption and packet loss. This is illustrated in

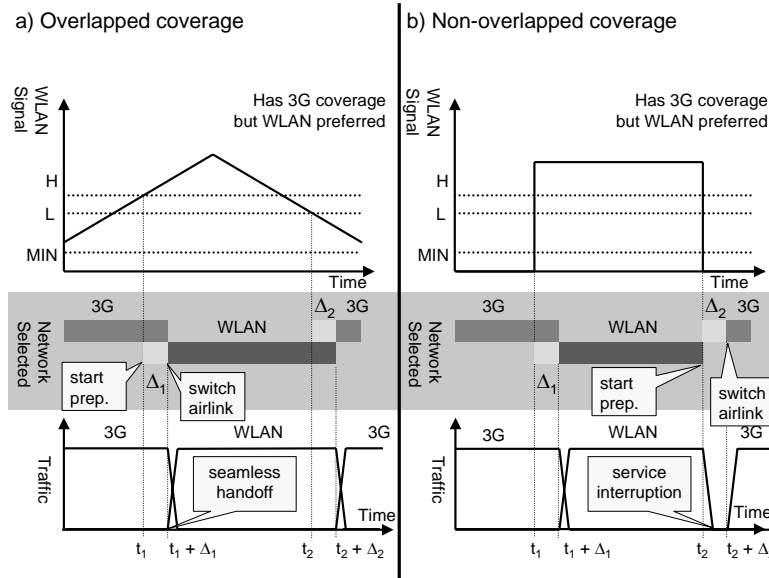


Fig. 6. Scenarios for overlapped and non-overlapped radio coverage

Figure 6(b), where the disruption occurs between t_2 and $t_2 + \Delta_2$. This incurred delay is determined by the performance of the gateway, the home agent, the home AAA, as well as the network latency among them. Typically, Δ_2 is of the order tens of milliseconds to hundreds of milliseconds [8].

Note that the use of Mobile IP can worsen the performance of web sessions in presence of webcache outside with the WLAN gateway. Figure 7(A) illustrates the case where requests from the client are transparently directed to a web cache.

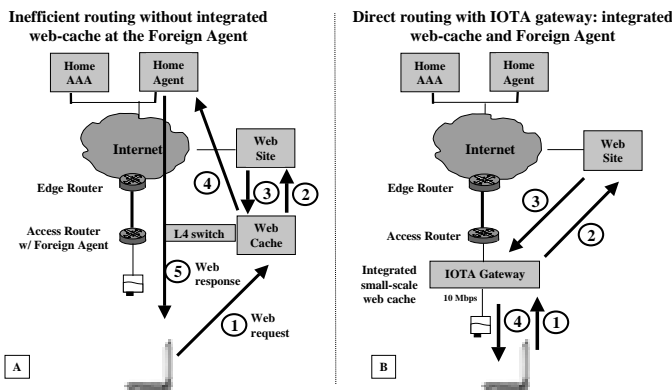


Fig. 7. The IOTA gateway integrates a web-cache, minimizing Mobile-IP overheads.

In the case of a cache-miss, the cache forwards the requests to the web-server and obtains a response. In the case of a cache-hit, the cache would already have the response in its own local disk. Either case, the cache would forward the response back to the users. In the case of Mobile-IP service, the requests coming from the users would appear to have come from their home addresses. Therefore, the cache would forward the response back to their home networks, where the home agent would tunnel the

response back to the gateway. As a result, while the cache was intended to reduce the traffic on the backhaul link, in this setup it would not eliminate any traffic even for cache-hits. In fact, the presence of the cache would double the traffic volume on the back-haul for cache-misses.

Figure 7(B) illustrates the scenario where the web-cache is an integral part of the WLAN gateway. Since the gateway is aware of the mobile node's presence and its use of Mobile IP service, it instructs the cache to forward the web response directly to the client.

VI. THE IOTA IMPLEMENTATION

Based on the loosely-coupled architecture described in Section III-B, we built a prototype system called IOTA with two primary components: the integration Gateway and the Multi-Interface Mobility Client. Another example implementation designed specifically for enterprise can be found in [14].

A. IOTA Gateway

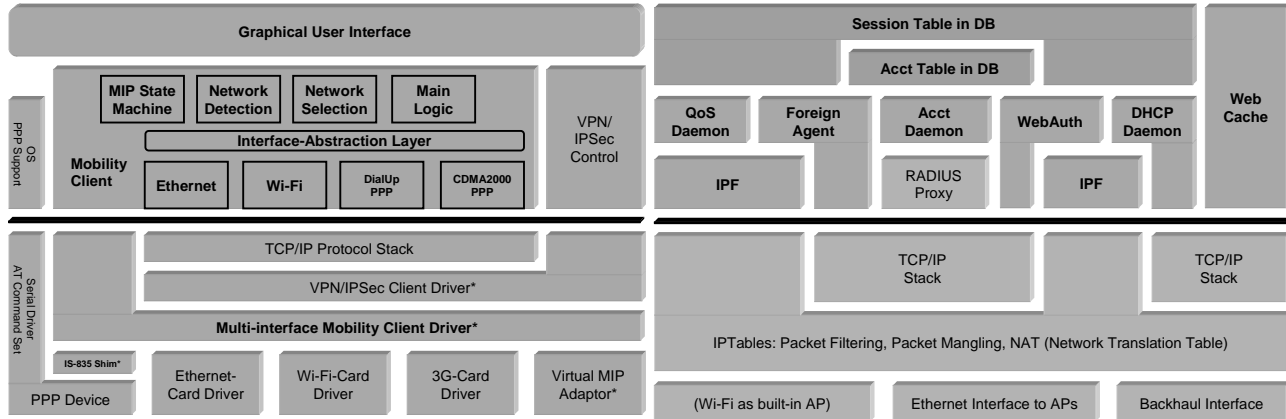
The IOTA gateway integrates a number of sub-systems, as shown in Figure 8d: RADIUS AAA proxy, Mobile-IP Foreign Agent (MIP FA), a DHCP server, a dynamic firewall, a QoS module, an integrated web cache, and an accounting module. These IOTA sub-systems rely on an on-disk database to store persistent information about each client's session and accounting records. Depends on different hardware configuration, the gateway box can have a built-in 802.11b access point, or it can connect to external 802.11b access point(s) through a gateway LAN.

The IOTA gateway uses the in-kernel Linux `iptables` ser-



a) IOTA Client GUI

b) IOTA Gateway



c) IOTA Client Architecture

d) IOTA Gateway Architecture

Fig. 8. IOTA implementation

vice to perform dynamic packet filtering, packet mangling, and NAT functions. User-space IOTA sub-systems use the IOTA Packet Filter (IPF) library to interact with iptables. Dynamic packet filtering is primarily used to achieve controlled access to the Internet for wireless clients, but it also implements certain firewall functions to prevent attacks from malicious users. Dynamic packet mangling redirects un-authenticated Simple-IP users' web request to the local Web Authenticator, but it also redirects some other traffic such as DNS lookup traffic. The NAT (Network Address Translation) function allows assignment of private IP addresses for wireless clients within the wireless LAN. These private IP addresses are not routable in the public Internet but they alleviate the demand on publicly routable IP addresses. When packets of these clients travel out to the Internet, the NAT function will translate these private IP addresses to public IP addresses.

The IOTA gateway software runs on off-the-shelf computers running the Linux operating system (Figure 8b).

B. Multi-Interface Mobility Client

Supporting the Mobile IP service across WLAN and CDMA2000 networks requires a client software that can per-

form Mobile-IP signaling with the Foreign Agent and Home Agent. Such a client must also intelligently select and sign the user onto the best access network depending on the network conditions. This latter feature is particularly useful in the Mobile-IP mode.

We implement the multi-interface client software for Linux and Windows 2000/XP. There are three components for the software: a GUI and a Mobility Client in the user space, and a Client Driver in the kernel space. Our current implementation supports 802.11b, CDMA2000, and Ethernet interfaces. The GUI and the software architecture for the client are shown in Figures 8a and 8c respectively.

The Mobility Client detects the presence of new networks and initiates link-level associations: PPP connections for CDMA2000 networks, and LAN associations for WLAN access points. It periodically scans all interfaces and measures observed signal strength. It uses an intelligent switching algorithm that accounts for signal strength and priority of different airlinks to avoid spurious network switching, often termed "bouncing". It handles the inter-technology handoff between different networks with minimal packet loss using mobile IP (Section V). The client also provides WLAN specific functionality, such as

supporting preferred network lists, WEP key configuration, and selection of WLAN access points based on signal strength. Our layering of IPsec over MobileIP enables users who are signed onto an enterprise VPN to maintain their sessions while moving through the integrated network. The client GUI allows the user to monitor the status of the physical interfaces and configure the mobile IP profiles and network interfaces.

The multi-interface mobility client driver is implemented in the kernel below the network protocol stack and offers the abstraction of a single virtual non-mobile interface to the OS protocol stack.

Using these three components together, the client software provides an illusion to networking applications on the mobile node that the node is always on the same network, even though the node may actually be moving across network boundaries of different access technologies.

VII. CONCLUSIONS

Integrated WLAN/CDMA2000 services will benefit both service provider and users. A loosely-coupled network architecture that allows independent deployment and growth of each network will emerge as the preferred way to implement such services. Using Mobile IP and AAA protocols, a service provider can support the two access technologies with a single home infrastructure for authentication and mobility management and allow inter-operator roaming.

A typical implementation for loosely-coupled architecture requires a WLAN integration gateway and mobility client software. The gateway supports Simple-IP and Mobile-IP services and implements an authentication model that allows various layer-2 and layer-3 authentication schemes preventing unauthorized users from accessing the public WLAN network. In the Mobile-IP mode of operation, the mobility client achieves seamless inter-technology handoffs without requiring user intervention.

We believe that the technologies described in this article may foster rapid deployment of integrated services and growth of ubiquitous high speed wireless data.

ACKNOWLEDGMENTS

We would like to thank Salim Virani, Dharani Vilwanathan and Jian Cai for their contributions to the IOTA project. We would also like to thank Peretz Feder, David Benenati, and Reuven Shapira from Lucent Technologies for frequent insightful discussions on this topic and their help in laboratory setup for our prototype testing.

REFERENCES

- [1] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. ANSI/IEEE Std 802.11: 1999 (E) Part 11, ISO/IEC 8802-11, 1999.
- [2] TIA/EIA/IS-835B - cdma2000 Wireless IP Network Standard. , Third Generation Partnership Program 2 (3GPP2), 2000.
- [3] Local and Metropolitan Area Networks: Standard for Port Based Network Access Control. Technical report, IEEE P802.1x, January 2001.
- [4] Part 11: Wireless MAC and physical layer specifications:Specification of Enhanced Security. Technical report, IEEE P802.11i, November 2002.
- [5] B. Aboba and D. Simon. PPP EAP TLS Authentication Protocol. RFC 2716, IETF, October 1999.
- [6] J. Arkko and H. Haverinen. EAP AKA Authentication. Work in progress - Internet Draft, IETF, February 2002. draft-arkko-pppext-eap-aka-03.txt.
- [7] N. Borisov, I. Goldberg, and D. Wagner. Intercepting mobile communications: The insecurity of 802.11. In *7th Annual International Conference on Mobile Computing and Networking*, July. 2001.
- [8] M. Buddhikot, G. Chandranmenon G., S. Han, Y. W. Lee, S. Miller S., and L. Salgarelli. Integration of 802.11 and third generation wireless data networks. In *IEEE INFOCOM 2003*, April. 2003.
- [9] C. Perkins (Editor). IP Mobility Support for IPv4. RFC 3344, IETF, August 2002.
- [10] C. Rigney et. al. Remote Authentication Dial In User Service (RADIUS). RFC 2865, IETF, June 2000.
- [11] L. Salgarelli et. al. EAP SKE authentication and key exchange protocol. Work in progress - Internet Draft, IETF, April 2002. draft-salgarelli-pppext-eap-ske-01.txt.
- [12] P. Calhoun et. al. Diameter Base Protocol. Work in progress - Internet Draft, IETF, April 2002. draft-ietf-aaa-diameter-10.txt.
- [13] H. Haverinen. EAP SIM Authentication. Work in progress - Internet Draft, IETF, February 2002. draft-haverinen-pppext-eap-sim-03.txt.
- [14] H. Luo, Z. Jiang, B. Kim, N. Shankamarayanan, and P. Henry. Integrating wireless lan and cellular data for enterprise. In *IEEE Internet Computing*, pages 25–33. IEEE Computer Society, March-April 2003.
- [15] A. Salkintzis, C. Fors, and R. Pazhyannur. WLAN-GPRS integration for next-generation mobile data networks. In *IEEE Wireless Communications*, October. 2002.