Sichere WLAN-Netze für Campus-Anwendungen und für öffentliche HotSpots

Gerhard Kadel, Dieter Busch, Heiko Knospe

T-Systems, Technologiezentrum Am Kavalleriesand 3 64295 Darmstadt
gerhard.kadel@t-systems.com

Zusammenfassung: Auf der Basis von WLAN-Technologien lassen sich in lokal begrenzten Bereichen flexible und kostengünstige drahtlose Breitband-Zugangsmöglichkeiten zum Internet realisieren. Der Beitrag gibt einen Überblick über den Stand der Technik und die Zukunftsperspektiven der WLAN-Technologie. Für Office-, Campus- und HotSpot-Szenarien werden unterschiedliche Architekturalternativen vorgestellt und Anforderungen hinsichtlich Authentisierung, Billing und Roaming diskutiert. Es wird ausführlich auf Sicherheitsanforderungen und Sicherheitslösungen eingegangen. Abschließend werden innovative integrierte WLAN-basierte Lösungen präsentiert, die komplexe Anforderungen wie beispielsweise „Internet in Bahn und Bus“ realisieren.

1 Einleitung

Das Internet prägt zunehmend alle Bereiche des privaten und geschäftlichen Lebens. Immer mehr Prozesse stützen sich auf das Internet ab, so dass ein „ubiquitous access“ zum Internet bzw. zu Firmen-Intranets von zunehmender Bedeutung ist.

Drahtlose Zugänge zum Internet und zu Intranets von Institutionen und Unternehmen eröffnen neue Möglichkeiten der Kommunikation und der Erreichbarkeit – unabhängig vom Ort des Nutzers und ohne die Notwendigkeit eines festen Netzwerkzugangs. Dadurch ist ein vernetztes Arbeiten sowie eine Flexibilisierung und Effizienzsteigerung von Arbeitsprozessen möglich.

Auf der Basis von WLAN (Wireless Local Area Networks)-Technologien lassen sich in lokal begrenzten Bereichen schnelle und kostengünstige drahtlose Zugangsmöglichkeiten zum Internet realisieren. Neben der privaten Anwendung als drahtlose Erweiterung von DSL-Anschlüssen innerhalb eines Hauses oder einer Wohnung sind einerseits Anwendungen in Unternehmen und Institutionen sehr attraktiv (z.B. Büro- und Campus-Szenarien, Produktions- und Fertigungsumgebungen), andererseits werden auf der Basis der WLAN-Technologie zunehmend auch in öffentlichen „HotSpots“ (z.B. Flughäfen, Hotels, Konferenzzentren, Messen, ...) schnelle drahtlose Zugangsmöglichkeiten zum Internet angeboten.

2 Stand der Technik und Zukunftsperspektiven der WLAN-Technologie

Ein WLAN ist ein „Wireless Ethernet“, das als Erweiterung oder Ersatz von drahtgebundenen Ethernets zum Einsatz kommt. Auf der Netzwerkseite steuert ein Zugangspunkt

(Access Point, AP) den Datenaustausch. Er bildet das Gateway für das drahtlos arbeitende Endgerät (z.B. Notebook oder PDA mit WLAN-Schnittstelle). Aus dem ursprünglichen WLAN-Standard IEEE 802.11 [802.11], der eine Datenrate bis 2 Mbit/s auf der Luftschnittstelle unterstützte, hat sich inzwischen eine leistungsfähige Standardfamilie entwickelt.

2.1 WLAN nach IEEE 802.11b

Der bislang erfolgreichste WLAN-Standard mit einer derzeit sehr dynamischen Entwicklung am Markt ist der Standard IEEE 802.11b, der im Jahre 1999 fertiggestellt wurde. Geräte nach diesem Standard arbeiten auf der Luftschnittstelle mit Datenraten bis 11 Mbit/s. Auf der Applikationsebene werden Datenraten bis ca. 6,5 Mbit/s erreicht. Die tatsächliche erreichbare Nutzerdatenrate ist von der Entfernung des Endgeräts zum Access Point und von der Größe der übertragenen Datenpakete, aber auch vom Hersteller und den verwendeten Treibern abhängig.

Die Technologie von 802.11b ist so ausgelegt, dass sie bei ansteigender Bitfehlerrate automatisch auf ein robusteres Modulationsverfahren zurückschaltet. Gründe für das Ansteigen der Bitfehlerrate können sinkende Empfangspegel, zunehmende Intersymbolinterferenz (Mehrwegeausbreitung) oder ansteigende Interferenz durch andere Funkzellen sein. Da das verwendete 2,4-GHz-ISM-Band unlizenziert auch durch andere (medizinische, wissenschaftliche und kommerzielle) Anwendungen genutzt werden darf, können zusätzliche Störungen durch andere Systeme auftreten und den möglichen Datendurchsatz verringern. Unter Berücksichtigung des automatischen „fallback“ können die in Tabelle 1 aufgezeigten Entfernungen als Richtwerte für die Funkreichweiten betrachtet werden.

	11 Mbit/s	**5,5 Mbit/s**	**2 Mbit/s**	**1 Mbit/s**
offene Umgebung bis	150 m	250 m	300 m	400 m
geschl. Umgebung[1] bis	30 m	35 m	40 m	50 m

Tabelle 1: Datenraten von WLAN nach 802.11b auf der Luftschnittstelle in Abhängigkeit der Entfernung zwischen Access Point und Endgerät.

2.2 Neue IEEE WLAN-Standards

Inzwischen sind eine Reihe von Erweiterungen zu 802.11b standardisiert oder in der Standardisierung. Die neuen Standards sollen die Leistungsfähigkeit weiter verbessern, die Anwendungsmöglichkeiten erweitern und zutage getretene Schwachstellen beseitigen. Tabelle 2 gibt eine Übersicht über die verschiedenen 802.11 Standards, die sich bzgl. der Luftschnittstellen unterscheiden.

[1] Bei den Entfernungen handelt es sich um mittlere Werte, sie sind stark von der spezifischen Gebäudestruktur abhängig.

Standard	**IEEE 802.11b**	**IEEE 802.11g**	**IEEE 802.11a**	**IEEE 802.11h**	
Verfügbarkeit des Standards	seit 1999	Erwartet bis Q3/2003	Seit 1999	Erwartet bis Q4/2003	
Verfügbarkeit von Produkten	seit 2000	Erwartet Ende 2003	Erste Produkte verfügbar	Erwartet Anfang 2004	
Max. User-Datenrate (1 User, 1500 Byte Datenpakete)[1]	5 - 6 Mbit/s	32 Mbit/s	32 Mbit/s	Standard ist Erweiterung von 802.11a um Dynamic Frequency Selection (DFS) und Transmit Power Control (TPC)	
Frequenzbereich[2]	2,4 GHz	2,4 GHz	5150 - 5250 MHz	5150 - 5350 MHz	5470 - 5725 MHz
Anzahl nicht überlappender Frequenzkanäle	3	3	3	8	11
Max. Sendeleistung[3]	100 mW	100 mW	30 mW (60 mW)	200 mW	1 W

[1] Gilt für kleine Abstände, bei größeren Abständen reduzieren sich die Datenraten
[2] Regulatorische Situation in Deutschland
[3] Leistung, die regulatorisch zugelassen ist – manche Produkte haben geringere Leistungen; (Klammer bei 802.11a: zul. Leistung mit TPC – Regelbereich > 6dB)

Tabelle 2: Übersicht über IEEE 802.11 Standards mit unterschiedlichen Luftschnittstellen.

Außerdem gibt es noch folgende Standard-Erweiterungen:

8802.11e: Quality-of-Service Verbesserungen des MAC-Layers, z.B. zur Unterstützung von Voice oder Video over IP over WLAN

802.11i: Security-Verbesserungen (siehe Abschnitt 4)

802.11f: Inter Access Point Protokoll (IAPP), ermöglich Roaming zwischen Access Points verschiedener Hersteller; Roaming wird in der Regel auch bei den heutigen Produkten schon unterstützt, allerdings mit proprietären Protokollen.

3 Office, Campus und HotSpot Szenarien

WLAN-Lösungen für Office, Campus und HotSpot Szenarien unterscheiden sich hinsichtlich verschiedener Merkmale wie Netzarchitekturen, Performanceanforderungen, Sicherheit, Authentisierung und Billing. Während in Office- und Campusbereichen naturgemäß nur eine eingeschränkte Nutzergruppe Zugang zum WLAN-Netz erhält, müssen öffentliche HotSpots prinzipiell für alle möglichen Nutzer offen sein. Semi-öffentliche HotSpots, beispielsweise zur Ermöglichung des Internet-Zugangs für Besucher auf Firmengeländen, erfordern wiederum andere Maßnahmen für Zugangskontrolle und Sicherheit. In allen Szenarien sind jedoch Authentisierung und Autorisierung des Nutzers notwendig.

3.1 Dezentrale und zentrale Architekturen

Ein wesentliches Unterscheidungsmerkmal verschiedener WLAN Netzarchitekturen ist die Lenkung des Datenverkehrs. Man unterscheidet grundsätzlich zwischen zentralen und dezentralen Architekturen.

Zentrale Architekturen leiten den gesamten Verkehr über einen zentralen Servicebereich. Neben zentralisierter Authentisierung, Autorisierung und Accounting wird auch der Datenverkehr über diesen zentralen Bereich geführt. Die Weiterleitung ins Internet oder in Firmenintranet erfolgt an einem Übergabepunkt in der Service Area. Die Lokationen werden durch verschlüsselte Layer 2 Tunnel mit dem zentralen Servicebereich verbunden. Die Layer 2 Tunnel ermöglichen, dass das IP-Adressmanagement im zentralen Servicebereich integriert werden kann.

Eine zentrale Architektur bietet Vorteile hinsichtlich der Bedienerfreundlichkeit, da an allen Lokationen die gleiche Konfiguration genutzt werden kann. Weiterhin wird die Sicherheit des gesamten Netzes an einer Stelle administriert. Dies vereinfacht im Allgemeinen die Erkennung von Angriffen, da kompetentes Personal nur am zentralen Knotenpunkt des Systems beschäftigt sein muss.

Neben den Sicherheitsdiensten werden im zentralen Servicebereiche auch andere, personalisierte Dienste bereitgestellt werden. Personifizierte Internetportale oder lokationsabhängige „Walled Garden“ Bereiche, d.h. Teile des Internets, die ohne Anmeldung erreichbar sind, sind solche Möglichkeiten.

Dezentrale Architekturen unterscheiden sich von zentralen in erster Linie dadurch, dass der Internet- bzw. Firmennetzzugang lokal vor Ort erfolgt. Dezentrale Architekturen sind insbesondere für kleinere und mittlere Lokationen geeignet, für die aus Aufwands- und Komplexitätsgründen eine zentrale Architektur nicht in Frage kommt. Außerdem eignen sich dezentrale HotSpot-Lösungen für temporäre Installationen, z.B. während einer Konferenz für die Bereitstellung von Internetzugängen und konferenzspezifischen Informationen für die Konferenzbesucher.

Es stehen spezielle WLAN-Access Points für dezentrale HotSpots zur Verfügung, die spezifische Funktionalitäten für Authentisierung, Autorisierung und Accounting (AAA) zur Verfügung stellen. Es sind jedoch auch bei dezentralen Architekturen Zugriffe auf zentrale Datenbanken möglich, z.B. um eine zentral verwaltete Anmeldung über einen RADIUS-Server vorzunehmen.

Auch für dezentrale WLAN-Architekturen können in Verbindung mit einem HotSpot-Controllern und einem Web-Server lokations-spezifisch kostenfreie Inhalte (z.B. Flugpläne, ÖPNV-Verbindungen oder Shop-Angebote auf einem Flughafen) sowie „Walled Garden“ Bereiche (s.o.) eingerichtet werden.

3.2 Billing und Roaming für öffentliche WLAN HotSpots

Derzeit steigt die Anzahl der WLAN HotSpots in Europa sehr schnell an. Fast ebenso schnell steigt auch die Zahl der Betreiber solcher HotSpots. An vielen Stellen entstehen

kleine, flexible Betreiber, so genannte Wireless ISPs (WISPs). Die Billingprozeduren sehen in der Fläche noch häufig den Kauf von Vouchern (Gutscheinen) mit Zeit- oder Volumenguthaben vor. Die überwiegende Anzahl heute aktiver HotSpots ist in dezentraler Architektur aufgebaut. In den meisten Fällen kann der Nutzer Voucher kaufen, um sich eine Zugangskennung zu erwerben. Weiterhin existieren auch Ansätze für Kundenabonnements, diese sind jedoch in den USA weit mehr verbreitet als in Europa.

Der Kauf von Vouchern ist für den Kunden jedoch teilweise unbefriedigend, da erworbene Guthaben verfallen und ein zusätzlicher Zeitaufwand für den Kauf des Vouchers entsteht. Auch für Netzbetreiber ist ein Abonnementskunde „wertvoller“ als ein Prepaid Kunde. Problematisch ist dabei derzeit, dass durch die Zersplitterung des Marktes in viele kleine HotSpot-Betreiber kein Betreiber eine hinreichende flächendeckung mit HotSpots für seine Kunden bieten kann, Aus diesem Grund ist die Implementierung von funktionierenden Roaming Abkommen zwischen HotSpot-Betreibern notwendig.

Für den HotSpot Bereich kommen folgende Roaming-Szenarien in Betracht:

- Bilaterales Roaming: Roaming-Abkommen werden zwischen jeweils zwei beteiligten HotSpot-Betreibern geschlossen. Vorbild ist hier das Roaming im GSM Bereich. Bei HotSpots ist jedoch eine Vielzahl von Betreibern am Markt, anders als bei GSM. Die Anzahl der zu betreuenden Abkommen wird damit für einen einzelnen Betreiber unübersichtlich und kostenintensiv. Bilaterales Roaming in HotSpots ist ein Modell, dass nur bei einer erheblich reduzierten Anzahl an Anbietern funktionieren wird.
- Roaming-Plattform: Ein Roaming-Plattform-Betreiber steht als Bindeglied zwischen einzelnen HotSpot-Betreibern. Jeder Betreiber hat ein Abkommen mit dem Plattform-Betreiber; dieser bietet die Möglichkeit, zwischen den HotSpots der unterschiedlichen Betreiber zu roamen. Die notwendige Billing-Infrastruktur und Clearinghouse-Funktionalitäten sind in der Plattform abgebildet.
- Lokations-Roaming: Lokations-Roaming kommt nur für sehr große HotSpots in Frage. Hierbei besitzt der Lokationsbesitzer die Infrastruktur und bietet HotSpot-Betreibern die Möglichkeit, sich direkt an seine Infrastruktur anzubinden. Dadurch können in seiner Lokation befindliche Kunden von HotSpot Betreibern einen Zugang bei ihrem Provider erhalten.
- Hardware-Roaming: Hardware-Roaming wird für Hard- und Softwarelieferanten für HotSpot-Lösungen angeboten. Dabei werden HotSpot-Betreiber, die die Hardware des Lieferanten nutzen, auf einer Plattform zusammengefasst, die das Roaming ermöglicht.

3.3 Differenzierung verschiedener Nutzergruppen

Die Kapitel 3.1 und 3.2 zeigen in erster Linie Lösungen für öffentlich betriebene HotSpots auf. Für semi-öffentliche HotSpots, z.B. auf einem Unternehmenscampus, wird ein weiteres Unterscheidungsmerkmal benötigt. Neben den öffentlichen Nutzern muss ein gesicherter privater Bereich für die firmeninternen Nutzer geschaffen werden. Dies kann durch die Nutzung unterschiedlicher VLAN (Virtual LAN) für diese Bereiche realisiert werden, die alle auf der gleichen physikalischen Infrastruktur geführt werden.

Moderne Access Points ermöglichen den Betrieb unterschiedlicher VLAN auch über die Luftschnittstelle. Dies wird durch die Abbildung mehrerer Service Set Identifier realisiert. Dadurch ist es möglich, dass am selben Access Point beispielsweise Rechner mit und ohne Verschlüsselung arbeiten können, die anschließend in unterschiedliche VLAN geroutet werden.

4 Sicherheitsanforderungen und Sicherheitslösungen für WLAN-Netze

Wichtige grundsätzliche Sicherheitsanforderungen an Kommunikationssysteme sind:

- Authentifikation der Kommunikationspartner
- Vertraulichkeit der übertragenen Daten
- Authentizität und Integrität der Daten
- Verbindlichkeit, Nicht-Abstreitbarbkeit der Kommunikation
- Wirksamkeit der Zugangs- bzw. Zugriffskontrolle
- Verfügbarkeit des Kommunikationssystems

Bei drahtlosen Systemen sind diese Sicherheitsziele in besonderer Weise gefährdet und moderne mobile Kommunikationstechnologien wie GSM, UMTS, Bluetooth oder WLAN verfügen daher über eigene Sicherheitsmechanismen. Wireless LAN Netzwerke sind dabei in einem Umkreis von bis zu einigen Hundert Metern Entfernung vom Access Point angreifbar. Sogenannte „War-Driver“ suchen mit frei verfügbaren WLAN Network Analysern (und teilweise mit GPS Empfängern) nach Netzwerken. Das Spektrum der Bedrohungen reicht hier von bloßer Erfassung der Netzwerke, Abhören der Kommunikation bis zu aktiven Angriffen gegen die Wireless LAN Komponenten oder sogar gegen die angeschlossenen Netzwerke.

Ein WLAN Netzwerk sollte daher zunächst als grundsätzlich unsicher eingestuft werden. Die Authentisierung der Benutzer und die Absicherung der Datenkommunikation ist daher ebenso erforderlich wie der Schutz der angeschlossenen Systeme durch entsprechenden Barrieren (Firewall). Die Anforderungen hierfür variieren je nach Nutzergruppe und Architektur.

4.1 Integration von Sicherheitsdiensten in den einzelnen Schichten

Die Integration der gewünschten Sicherheitsdienste kann in verschiedenen Schichten erfolgen (siehe Abbildung 1). Zu beachten ist aber, dass bei Integration in den unteren Schichten (Layer 1 und 2) die Reichweite geringer ist und die Abhängigkeit von der Hardware bzw. Technologie größer ist als bei den höheren Schichten.

Die im WLAN Standard IEEE 802.11 vorgesehenen Sicherheitsmechanismen sind auf der Datensicherungsschicht (Link Layer) implementiert; Details dazu werden im nächsten Abschnitt erläutert. Da die Sicherheitsbeziehung am Access Point endet, sind die weiteren (leitungsgebundenen) Verbindungen in das Zielnetzwerk a priori ungesichert, wenn nicht

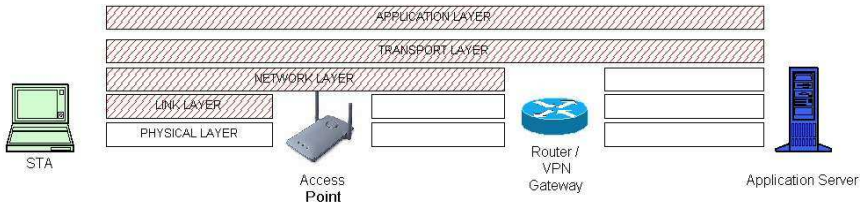

Abbildung 1: Sicherheitsdienste in verschiedenen Schichten

weitere Schutzmaßnahmen zum Einsatz kommen. Dies ist z.B. bei Hotspot- oder Campuslösungen wichtig, weil bei einer großen Zahl von in der Fläche verteilten Access Points die Übernahme einzelner Geräte durch Angreifer nicht ausgeschlossen werden kann.

Ein weiterer Ansatz ist die Verwendung von Sicherheitsdiensten der Netzwerkschicht auf der Grundlage von VPN Technologie. Diese Vorgehensweise wird im Abschnitt 4.3 besprochen. Ein Vorteil hierbei ist, dass sich die Sicherheitsbeziehung bis zu einem VPN Gateway erstreckt, das sich üblicherweise im Netzwerk des Zugangsproviders oder der jeweiligen Firma befindet.

Außerdem kommt die Verwendung von Sicherheitsdiensten der Transportschicht (z.B. Transport Layer Security mit SSL/TLS nach [TLS]) oder der Anwendungsschicht (z.B. Mailsicherheit mit S/MIME oder PGP) in Frage. Diese Protokolle sind aber in der Regel für spezielle Anwendungen konzipiert und daher nicht generisch einsetzbar, bieten aber „Ende-zu-Ende“ Sicherheit zwischen den Kommunikationssystemen. Das SSL/TLS Protokoll kann z.B. zum Schutz von http basierten Anmeldedialogen bei WLAN Hotspots verwendet werden.

4.2 Sicherheitsmechanismen von IEEE 802.11

Der Wireless LAN Standard IEEE 802.11 definiert mit WEP (Wired Equivalent Privacy) verschiedene Sicherheitsfunktionen auf Schicht 2:

- Authentisierung der Instanzen
- Verschlüsselung der Daten-Frames
- Integritätssicherung der Daten-Frames

Die Sicherheitsfunktionen basieren auf gemeinsamen geheimen Schlüsseln (40 oder 104 Bit), die vorab konfiguriert werden müssen. Der Einsatz von WEP ist daher bei öffentlichen Hotspots oder bei größeren Unternehmen wegen der Verteilung und Geheimhaltung der Schlüssel de facto nicht möglich. In diesen Szenarien sind Benutzer-spezifische Schlüssel erforderlich. Es wurden außerdem wesentliche Schwächen von WEP aufgedeckt ([Flu], [Bor]), für die inzwischen auch „Exploits“ existieren:

- Die WEP Authentisierung ist durch Abhören einer einzigen erfolgreichen Anmeldung zu brechen
- Der geheime WEP Schlüssel kann (statistisch) mit +/- 1 Millionen Paketen ermittelt werden

- Die Wiederholung von Initialisierungsvektoren der RC4 Stromchiffre, die WEP zugrunde liegt, kann Informationen über den Klartext liefern.
- Nachrichten können unbemerkt manipuliert werden

Von der IEEE Task Group I wird daher z.Z. ein neuer Sicherheitsstandard **IEEE 802.11i** erarbeitet, der die Probleme des aktuellen Standards beheben soll. Ein öffentlicher Entwurf ist gegenwärtig (Mai 2003) noch nicht verfügbar. Es wird aber davon ausgegangen, dass die folgenden Protokolle verwendet werden sollen:

- IEEE 802.1X (Port-Based Network Access Control [802.1X]) und EAP (Extensible Authentication Protocol [EAP]) für Zugangskontrolle, Authentifikation und Schlüsselerzeugung
- TKIP (Temporal Key Integrity Protocol, [WPA]) mit einem verbesserten Einsatz der RC4 Stromchiffre, Rekeying Funktionen und einer sicheren Nachrichtenauthentisierung
- Verschlüsselung und Integritätssicherung mit AES (Advanced Encryption Standard) Varianten

IEEE 802.1X ist heute bereits verfügbar und kann für die Zugangskontrolle und zur Authentifikation eingesetzt werden. Als Protokoll kommt dabei EAP zum Einsatz, das wiederum lediglich eine Umgebung für die eigentliche Authentisierungsmethode bereitstellt. Diese kann z.B. Passwort-basiert erfolgen (z.B. EAP-LEAP, EAP-MD5), mit Hilfe von Zertifikaten und einem SSL/TLS Handshake auf beiden Seiten (EAP-TLS) oder sogar mittels einer SIM Karte und den GSM bzw. UMTS Authentifikations- und Schlüsselerzeugungsverfahren (EAP-SIM, EAP-AKA). Die Einzelheiten werden durch die jeweilige EAP Methode definiert, wobei die EAP Protokollnachrichten vom Access Point (Authenticator) an einen AAA (Radius-)Server weitergereicht werden (vgl. Abbildung 2).

4.3 Einsatz der VPN Technologie für Wireless LAN

Beim Einsatz der Virtual Private Network (VPN) Technologie wird die Kommunikation zwischen der WLAN Station über den Access Point und ggf. weitere lokale Infrastruktur hinweg bis zu einem VPN Gateway gesichert. Die Sicherung erfolgt auf der Netzwerkschicht, wobei die Möglichkeit des IP Tunneling besteht (z.B. durch das Internet in ein privates Netz).

Als VPN Protokolle stehen im wesentlich der Internet Standard IPsec (RFCs 2401-2412), das Microsoft Point-to-Point Tunneling Protocol (PPTP) und andere Layer 2 Tunneling Protokolle zur Verfügung. Insbesondere IPsec gilt dabei als etabliertes Sicherheitsprotokoll, das die folgenden Sicherheitsdienste bietet:

- Authentisierung der Kommunikationspartner
- Schutz der Vertraulichkeit der Pakete
- Nachrichtenauthentisierung und Datenintegrität, Schutz vor Wiedereinspielen von Nachrichten
- Sicherheitsrichtlinien und Zugangskontrolle

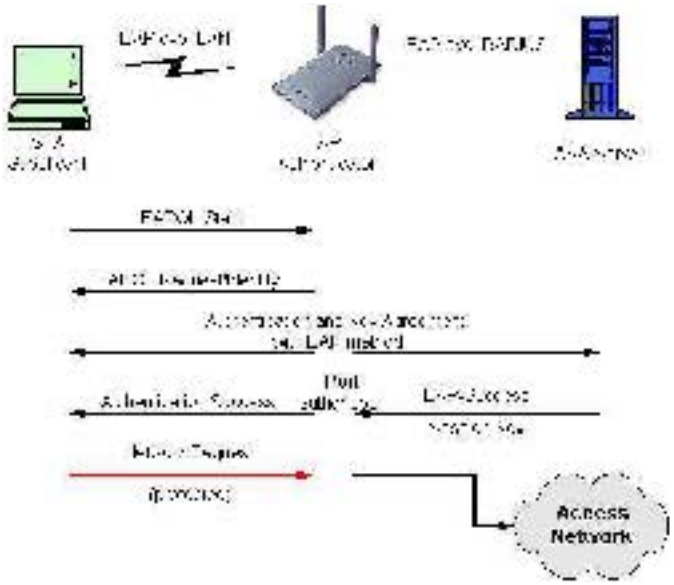

Abbildung 2: Zugangskontrolle und Authentisierung mit IEEE 802.1X und EAP

Der Schutz der Daten erfolgt dabei mit ESP (Encapsulated Payload Protocol, [ESP]), die Nachrichtenauthentisierung wahlweise mit ESP oder AH (Authentication Header, [AH]). Die Authentisierung der Teilnehmer und die Aushandlung der Schlüssel ist Aufgabe des IKE Protokolls (Internet Key Exchange, [IKE]).

Bei der praktischen Implementierung insbesondere in mobilen Umgebungen stellt sich das IKE Protokoll aber als wenig flexibel heraus. IKE sieht hier nur shared secrets zwischen Client und IPsec Gateway vor (unpraktikabel bei größeren Umgebungen) sowie Public Key basierte Verfahren. Die häufig gewünschten Username/Passwort-gestützten Methoden zur Client-Authentisierung können nur mit bestimmten Erweiterungen des IKE Protokolls realisiert werden. Dies wiederum gefährdet die Interoperabilität zwischen IPsec Clients und Gateways unterschiedlicher Hersteller. Der IKE Nachfolger [IKEv2] wird einige Mängel von IKE beheben und durch die Verwendung von EAP Methoden mehr Flexibilität bieten.

5 Fast Internet in Bahn und Bus, ein Realisierungsbeispiel für eine innovative integrierte Kommunikationsplattform

Der wachsende Bedarf nach flexiblen Hochgeschwindigkeitszugängen zum Internet besteht nicht nur in den beschriebenen Office, Campus und HotSpot-Szenarien, sondern auch für Menschen „on the move“, z.B. für Reisende in öffentlichen Verkehrsmitteln. Abbildung 3 zeigt ein Lösungskonzept, das diese Anforderungen erfüllt. Das Konzept hat folgende wesentliche Merkmale:

- Im Fahrzeug erfolgt ein drahtloser schneller Zugriff auf Dienste eines intelligenten Fahrzeug-Servers über Endgeräte (Notebook, PDA, ...) mit Hochgeschwindigkeits-

Funkschnittstellen (WLAN und Bluetooth). Es ist ein breites Spektrum an Diensten möglich, u.a. E-Mail, Internet- oder Intranet-Access, Zugriff auf Fahrplandaten, News, Information, Entertainment, Games, e-Commerce.

- An ausgewählten Punkten (z.B. Bahnhöfen) erfolgt eine schnelle Anbindung des Fahrzeugservers über eine dedizierte Funkverbindung (WLAN-Bridges). Diese Anbindung wird benutzt zur Aktualisierung der Server-Inhalte, zum „Be- und Entladen“ des Servers mit E-Mails und auch zur schnellen Kommunikation mit dem Internet.
- Der entscheidende Vorteil der WLAN-Bridges besteht darin, dass keine Übertragungskosten anfallen und dass wesentlich höhere Datenraten als in Mobilfunknetzen möglich sind.
- Zur Anbindung des Fahrzeugs an das Internet wird eine adaptive und dynamische Online-Anbindung über unterschiedliche Kommunikationsnetze (z.B. WLAN, GSM/GPRS, UMTS, DAB oder DVB) realisiert. Es wird automatisch die jeweils günstigste Verbindung ausgewählt, ggf. erfolgt die Kommunikation gleichzeitig über verschiedene Funknetze. Durch die Verwendung des Internet-Protokolls „Mobile IP“ erfolgt das Umschalten zwischen den verschiedenen Netzen für die Anwendung unterbrechungsfrei. Es ist keine Neuanmeldung beim Übergang zwischen den beiden Netzen notwendig, die laufenden Anwendungen, z.B. Download aus dem Internet oder einem Intranet, bleiben beim Netzwechsel erhalten.

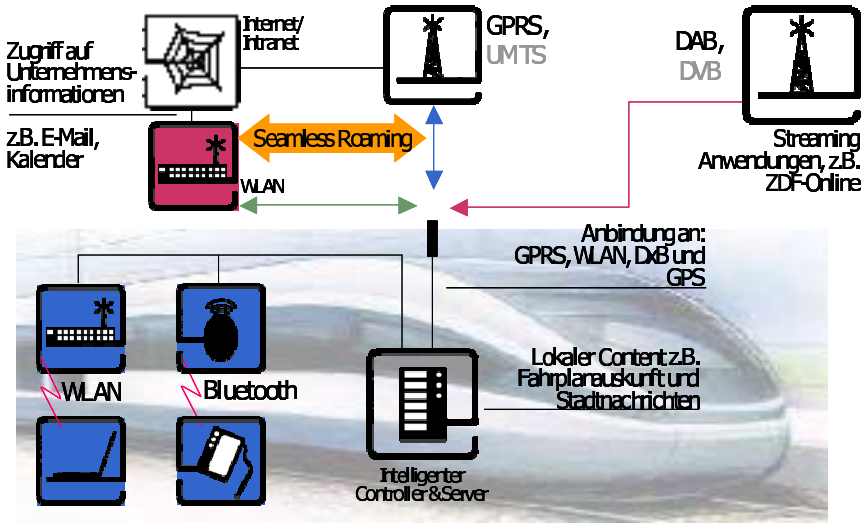

Abbildung 3: Lösungskonzept „Fast Internet in Bahn und Bus“

6 Zusammenfassung und Ausblick

Es wurde dargestellt, wie auf der Basis der WLAN-Technologie in privaten, semi-öffentlichen und öffentlichen Bereichen flexibler Breitband-Internetzugänge realisiert werden

können. Neue WLAN-Standards werden eine weitere Verbesserung der Leistungsfähigkeit und Sicherheit von WLAN-Lösungen ermöglichen. In Kombination mit anderen drahtlosen Zugangstechnologien aus dem Bereich des Mobilunks oder des digitalen Rundfunks lassen sich leistungsfähige integrierte Gesamtlösungen realisieren. Als Beispiel wurde das Lösungskonzept „Fast Internet in Bahn und Bus“ vorgestellt.

Literatur

[802.11] Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications (PHY). ANSI/IEEE Standard 802.11, 1999.

[802.1X] Port-Based Network Access Control. IEEE Standard 802.1X-2001

[AH] Kent, S.; Atkinson, R.: IP Authentication Header. Internet Standard RFC 2402

[Bor] Borisov, N.; Goldberg, I.; Wagner, D.: Intercepting Mobile Communications: The insecurity of 802.11. In Proceedings of MOBICOM 2001, http://citeseer.nj.nec.com/article/borisov01intercepting.html

[EAP] Blunk, L.; Vollbrecht, J.: PPP Extensible Authentication Protocol (EAP). Internet Standard RFC 2284.

[ESP] Kent, S.; Atkinson, R.: IP Encapsulating Security Payload (ESP). Internet Standard RFC 2406

[Flu] Fluhrer, S; Mantin, I; Shamir, A: Weaknesses in the Key Scheduling Algorithm of RC4. Lecture Notes in Computer Science 2259, 1-24

[IKE] Harkins, D; Carrel, D.: The Internet Key Exchange (IKE). Internet Standard RFC 2409

[IKEv2] Kaufman, C: Internet Key Exchange (IKEv2) Protocol, Internet Draft <draft-ietf-ipsec-ikev2-06.txt>

[TLS] Dierks, T.; Allen, C.: The TLS Protocol Version 1.0, Internet Standard RFC 2246.

[WPA] Wi-Fi Protected Access. The Wi-Fi Alliance, http://www.weca.net/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf