Ubiquitous System Technology

Oct. 1, 2003

Shiro Sakata, Ph. D.

NEC Laboratories

sakata@cd.jp.nec.com
Ⅰ Ubiquitous System Technology Trend

(1) What is Ubiquitous System?
(2) Key Technologies for Ubiquitous System
(3) Towards Ubiquitous System Era

Ⅱ Security Technology for Ubiquitous System

(1) Security Technology Overview
(2) Security Technology for Wireless LAN
(3) Mobility Control and Security
(4) Utilization and Protection of Privacy Information
(5) Interworking of IMT2000(3G) and Wireless LAN based on Security
Ubiquitous System Technology Trend

(1) What is Ubiquitous System?
   ① Origin of Ubiquitous Computing
   ② Internet Evolution
   ③ Ubiquitous System Definition

(2) Key Technologies for Ubiquitous System
   ① Network
   ② Terminal
   ③ Platform (Middleware)

(3) Towards Ubiquitous System Era
(1) What is Ubiquitous System?
Ubiquitous Computing

Mark Weiser (1952-99, Xerox PARC)

“Ubiquitous computing is the method of enhancing computer use by making many computers available throughout the physical environment, but making them effectively invisible to the user.”


② Internet Evolution
Waves toward Ubiquitous Information Society

- **1st Wave** (Mainframe Era)
  - ARPANET

- **2nd Wave** (PC Era)
  - Ethernet
  - WWW

- **3rd Wave** (Internet Era)
  - Digital broadcast
  - Mobile Internet
  - ITS
  - Secure & Robust
  - Broadband & Mobile

Market Size

Computer and Communication Integration and Device Tech. Growth
# Discussions for INET 2000

QoL: Quality of Life

| 1st Gen. (Research Network) | Early 1970s ~ 1995 | - Network for professionals (researchers and computer engineers)  
- Defense (ARPANET, ~ late 70s) →  
  Academia (CSNET/NSFNET, ~ late 80s) →  
  Commercial |
|----------------------------|-------------------|------------------------------------------------------------------|
| 2nd Gen. (WWW & QoS)       | 1995 ~ 2005       | - Information infrastructure for general individuals  
- Technical issues:  
  QoS control  
  Mobility control  
  Photonic Internet  
  Multicast  
  Security  
  Tera-bit router |
| 3rd Gen. (QoL)             | 2005 ~            | - Ultra broadband  
- **Ubiquitous computing**  
- Robust and secure |
## Technology Issues of Current Internet

<table>
<thead>
<tr>
<th>Technology Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadband</td>
<td>Photonic network, IP over WDM</td>
</tr>
<tr>
<td>High-performance Router</td>
<td>Tera-bit router</td>
</tr>
<tr>
<td>QoS Control</td>
<td>DiffServ, MPLS, Traffic engineering, Queue management, Bandwidth control</td>
</tr>
<tr>
<td>Multicast</td>
<td>QoS IP Multicast, Reliable multicast → Multicast using AP layer</td>
</tr>
<tr>
<td>Address-space Extension</td>
<td>IPv6 incl. security and QoS Control</td>
</tr>
<tr>
<td>Mobility Control</td>
<td>Mobile IP + Service continuity/Media handover</td>
</tr>
</tbody>
</table>
3rd Generation Internet

- Ultra broadband
  Peta-bit router

- Ubiquitous computing
  PAN(Personal Area Network)/HAN(Home Area Network)
  Seamless connectivity between heterogeneous networks and terminals
  Adaptively-customized/personalized services
  → Context awareness

- Robust and secure
  Autonomous network management at fault occurrence
  (Self-recovery, -resource alloc., -reconfiguration/plug&play)
  Protection against cyber attacks
Ubiquitous System Definition

Computers extremely more than persons

Pervasive Computing

Not Aware of Computers

- Calm, Invisible, Implicit, Proactive Computing

Sensing

- Sentient, Perceptual, Ambient Computing

Mobility Support

- Mobile, Nomadic Computing
Ubiquitous Computing

- **On the Street**: Convenience store, Station, Gas Station
  - Discount info.
  - Kiosk servers

- **On the Train**: Time table

- **On the Travel**: Sightseeing spot map/info.
  - Traffic condition info.

- **On the Car (ITS)**: Personal Area & Ad hoc Network
Mobile commerce driven by mobile internet (e.g. i-mode) has been expected to integrate TV commerce (e.g. digital broadcast) and convenience store commerce into channel-mix commerce in a ubiquitous computing environment.
Ubiquitous Network defined by Japan’s MPMHAPT(*)

‘Ubiquitous network’ consists of innumerable number of
- computing devices embedded in almost everything
  around us
- platforms and networks that interconnect them
- user devices that make use of and act on the available
  information

When fully implemented around 2010, ‘Ubiquitous
network’ will change our daily life by providing us with
the information and services we need less efforts.

(*) Ministry of Public Management, Home Affairs, Posts and Telecommunications, or Sohmusho
Future Life with Ubiquitous Networks

Urban areas
- Routing support to permit **seamless roaming** among networks and media types by maintaining active TCP/UDP connections.
- Provide **location-aware and personalized advice** for vehicle drivers

Public facilities
- Real-time congestion and weather information-based **traffic management** can increase road capacity.
- Monitoring secular change of road and building could **prevent accidents caused by incidents and natural disasters**.

Office
- Collaboration with other group within a company and with suppliers and customers can reduce cost from fluctuating supply and demand.
- Create new business from **real-time and location-based commerce**.

Home
- The home is constantly monitored using audio and video observation methods, and even monitors its **inhabitants’ medical conditions**.
- Support social connections of elderly people promoting peace of mind for the family.

Location-aware Personalized advice

Multimedia conference Automatic meeting minutes Searchable notes

Food recipe management On-line ordering Kitchen monitoring

Ubiquitous Network
RFID (Radio Frequency IDentification) Tags

RFID tags will play a vital role in ubiquitous networks
- Being very small, they can be embedded in numerous household goods around us, and can make them part of the network.
- Their communications capacity allow them to be managed and controlled from the network, thereby supporting human life.
Multimedia communication (Emergency aid)

Home network (Home security, Communication with appliances)

User profile server (incl. authentication and accounting)

AP server

Content server

Multimedia communication server

Music content download

Hotspot info. delivery
  Local content, streaming)

On the move

Doctors in hospital

Communication with doctors and family

Security

Home appliances remote control

Home network (Home security, Communication with appliances)

Mobile EC (Authentication, Transaction)
Ubiquitous Services over Diverse Networks & Terminals

- Electronic Ticketing
- Location/Presence Info. Service
- Content Delivery
- Bidirectional Communication (*)
- Home Control and Security (*)
- Storage Service

Servers → Diverse networks → Terminals

- Wired LAN
- Core Network
- FTTH
- ADSL
- MAN (Wide area Ether)
- Wireless LAN
- IMT 2000
- Wireless LAN

Terminals:
- Cellular phone
- PDA
- Note PC
- Wearable Terminal
- Home appliance
- Digital TV
- Home server
- Sensors
- Car terminal

(*) Indicates additional services
Bidirectional Communication

On the move

Office User

Home User

Public Wireless LAN
Home Control and Security

- Robot-type Home server
  - User controls robot from outside through the Internet
  - The robot controls home appliances with IrDA, RFID, etc.
  - The robot automatically acts in accordance with user’s presence

Example:
Outside home, e.g., on the way back home
- Confirmation of door locking
- Monitoring and taking care of pets, gardens, etc.
- Automatic video recording
- Warming bath when approaching the home
- Automatic light switch-on of when approaching the home

Internet

Maid robot

Light

HDTV and HD Video recorder

Door lock and door phone

Feeding

Warming bath

Lighting
(2) Key Technologies for Ubiquitous System
Key Technologies for Ubiquitous System

① Network

Wide-area cellular network (2/2.5G, 3G → 4G)
**Wireless LAN** (IEEE802.11a/b/g → 11n)
Home network
Short range/\textit{ad hoc network} (Bluetooth, IR, DSRC → UWB)
**Sensor network**

② Terminal

Note PC/PDA
Cellular phone
Home server and terminal/appliances
Robot
**Wearable terminal with various sensors**
Car terminal

③ **Server-terminal Middleware**
① Network

1) Sensor Network

Many kinds of sensors capture information somewhat in cooperation with each other through short range communication, and report the captured information to remote sites through the Internet.

Interconnectivity between sensor network and IP routing (Internet) is a key issue.

Sensed information:
location, speed/acceleration, pressure, direction, vibration, light, heat, sound, wind, bio (temperature, blood pressure, pulse stroke, ---), etc.
Current Sensor Application Examples

Remote monitoring and control
- Car theft detection using speed/acceleration sensors
- Vegetables and fruits cultivation in green houses using temperature, humidity and heat sensors
- Environment measurement of forests, urban areas, etc.
- Earthquake detection using vibration sensors
- Durability measurement of buildings
- Diagnose and health care using bio sensors

Some sort of games
Sensor Network Image

Forest

Green house

SN: Sensor Network
GW: Gateway

SN

SN

Urban environment

IPv6

Server

Internet
Technical Issues for Sensor Networks

**Scalable** Network Architecture and Protocol Stack

**Low-power** Media Access, Traffic Management and **Error Control**

**Robust/Reliable** Algorithm for Collaboration

**Secure** Communication and Authentication

**Naming**, Attribute-based **Addressing**, **Location** Management, **Routing**

Data **Compression, Retrieval, Discovery, Delivery**

Sensor-to-sensor **Association, Synchronization, Aggregation, Fusion**

New **Applications**
2) Ad hoc Network

- Sensor networks convey only captured data by sensors, \[\] and no mobility is assumed.

- Ad hoc networks:
  No fixed network infrastructure
  Frequent and dynamic network topology change
  → Wireless and mobile environment
  Multi-hop network

- Internet and cellular networks are not ad hoc networks, because they have fixed infrastructures.
Ad hoc Network Applications

- Personal Area Network (PAN) based inter-terminal communication, information delivery from local servers, etc.
- Rescue operation support in emergency: earthquake, flood, tornado, etc.
- Military use

Research on Ad hoc Network

- DARPA (US)
  Survivable Adaptive Networks (SURAN): 1983 - 1992

- IETF Mobile Ad hoc NETworks (MANET) WG since 1997 (RFC 2501).
Routing Protocols discussed in IETF MANET WG

- 4 protocols (**DSR, AODV, OLSR, TBRPF**) were selected as Experimental RFCs in 2003.

<table>
<thead>
<tr>
<th>Reactive</th>
<th>DSR (Dynamic Source Routing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Routing table is created</td>
<td><strong>AODV</strong> (Ad hoc On-demand Distance Vector algorithm)</td>
</tr>
<tr>
<td>when transmission is</td>
<td><strong>IERP</strong> (IntErzone Routing Protocol)</td>
</tr>
<tr>
<td>requested.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proactive</th>
<th>OLSR (Optimized Link State Routing protocol)</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Routing table is created</td>
<td><strong>TBRPF</strong> (Topology Broadcast based on Reverse Path Forwarding routing protocol)</td>
</tr>
<tr>
<td>prior to transmission</td>
<td>FSR (Fisheye State routing protocol)</td>
</tr>
<tr>
<td>request.</td>
<td>LAMAR (LANd MARk routing protocol)</td>
</tr>
<tr>
<td></td>
<td>IARP (IntrAzone Routing Protocol)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hybrid and others</th>
<th>ZRP (Zone Routing Protocol)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>BRP (Bordercast Resolution Protocol)</td>
</tr>
</tbody>
</table>
Flooding plays a vital role in routing control

**Flooding**: Each intermediate node broadcasts a packet to all neighboring nodes except a node from which the packet was received.

Advantages --- Simple mechanism, only data packet is transmitted and reliable
Disadvantages --- Heavy transmission overhead, low scalability and possible packet loss due to collision (e.g., $\diamond$ in 2)
### Examples of Reactive Protocols: DSR and AODV

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Details</th>
</tr>
</thead>
</table>
| **DSR**  | - Source node identifies the route to destination by flooding  
- Route information is inserted in packet header  
  (between IP and TCP/UDP)  
- Transmission efficiency is low  
- Effective when network topology change is not frequent |
| **AODV** | - Each intermediate node keeps the routing table  
  (correspondence between destination and the next hop node)  
- Effective when network topology change is frequent |
## 3) Mobile Internet

### Service

<table>
<thead>
<tr>
<th>Info. representation (incl. .HTML, XML)</th>
<th>Compression (MPEG4, etc)</th>
<th>Recognition/conversion (text voice)</th>
<th>User profile</th>
<th>User agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service platform</td>
<td>Location(GPS)</td>
<td>NMS</td>
<td>Security</td>
<td>Accounting</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Data sync. ...</td>
<td></td>
</tr>
<tr>
<td>Middleware</td>
<td>Wireless profiled TCP</td>
<td>(QoS control (Diffserv, MPLS, TE, ...))</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mobile IP</td>
<td>IPv6</td>
<td>IP Multicast</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anywhere</td>
<td>Any terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Any No. of terminals</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Infrastructure

- Low-speed and unstable
- 2G PDC, PHS, GSM
- More than 10 times high-speed packet trans.
- 3G IMT-2000
- 4G Wireless LAN
Protocol Stack for FOMA

- The World’s First Mobile Internet

Mobile terminal

- Language
  - Compact HTML
- Application Layer
  - HTTP 🔄 Push delivery
  - TLS (SSL)
- Transport Layer
  - Wireless Profiled TCP
- Network Layer
  - IP

Mobile gateway

Wireless access network (IMT-2000) 🔄 Internet

Web server

- Compact HTML
- HTTP 🔄 Push delivery
- TLS (SSL)
- TCP
- IP
### 4) Wireless LAN

<table>
<thead>
<tr>
<th>Standard</th>
<th>Maximum data rate</th>
<th>Transmission distance</th>
<th>Modulation/access method</th>
<th>Frequency, standardization, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE802.11b</td>
<td>11Mbps</td>
<td>30-100m</td>
<td>DS-SS CSMA/CA</td>
<td>1999.9, 2.4GHz</td>
</tr>
<tr>
<td>IEEE802.11a</td>
<td>54Mbps</td>
<td>30-100m</td>
<td>OFDM CSMA/CA</td>
<td>1999.9, 5.2GHz</td>
</tr>
<tr>
<td>IEEE802.11g</td>
<td>54Mbps</td>
<td>30-100m</td>
<td>OFDM CSMA/CA</td>
<td>2003.5, 2.4GHz</td>
</tr>
<tr>
<td>IEEE802.11n</td>
<td>100-200Mbps</td>
<td>30-100m</td>
<td>CSMA/CA</td>
<td>2006, 5.2GHz?</td>
</tr>
<tr>
<td>Zigbee (IEEE802.15.4)</td>
<td>250kbps</td>
<td>10~75m</td>
<td>Derived from HomeRF</td>
<td>2.4GHz, 2003 <strong>Home remote controller</strong></td>
</tr>
<tr>
<td>Bluetooth (IEEE802.15)</td>
<td>1Mbps</td>
<td>10m</td>
<td>FH-SS TDD</td>
<td>2001.2 (V1.1), 2.4GHz <strong>Wireless equivalent to USB</strong></td>
</tr>
<tr>
<td>UWB (IEEE802.15)</td>
<td>more than 100Mbps</td>
<td>10m</td>
<td></td>
<td>2003?, 3.1-10.6GHz <strong>Wireless equivalent to USB 2.0</strong></td>
</tr>
</tbody>
</table>

UWB: Ultra Wide Band    USB: Universal Serial Bus
Wireless LAN Standardization

[Standardization in US]
1990年 IEEE802.11 started wireless LAN standardization in US
1997年 IEEE802.11 wireless LAN with 2.4GHz, max. 1~2Mbps
1999年 IEEE802.11b wireless LAN with 2.4GHz, DH-SS, max. 11Mbps
2003年 IEEE802.11a wireless LAN with 5 GHz, OFDM, max. 54Mbps
2003年 IEEE802.11g wireless LAN with 2.4GHz, OFDM, max. 54Mbps

[Standardization and development in Europe and Japan in mid 90s - late 90s in Europe]
Europe - HIPERLAN/HIPERLAN2
Japan - HiSWAN(AWA/MMAC)

Market has been growing from IEEE802.11b, 11a to 11g, and 11n in the future.

In the investigation of interworking of 3G(IMT-2000) and wireless LAN which started in late 2001, target LANs are IEEE802.11b, a, g.
IEEE802 (= LAN) Committee [1980~]

802.1x (HILI Upper layer+Management)

802.2x (LLC)

802.18 (Radio Regulatory TAG)

802.19: Co-existence TAG
802.20: MBWA (Mobile Broadband Wireless Access)
IEEE802.11 (=Wireless LAN) [1990~]

PLCP (Physical Layer Convergence Protocol)

MAC (CSMA/CA) + 802.11e (QoS Control)

802.11f (Roaming)
802.11i (Security)
802.11h (5GHz Adaptation to EU Spec.)

802.11c (Bridge)
802.11d

2.4G DS 2.4G FH IR

802.11a 5GHz OFDM
802.11b 2.4GHz DS
802.11g 2.4GHz OFDM
802.11n 5GHz

(Adaptation to International Standards)
### Wireless LAN Standardization in IEEE802.11

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Wireless LAN (OFDM, 5GHz, Max. 54Mbps)</td>
</tr>
<tr>
<td>b</td>
<td>Wireless LAN (DS-SS, 2.4GHz, Max. 11Mbps)</td>
</tr>
<tr>
<td>c</td>
<td>Addition of wireless LAN’s MAC specification to MAC Bridge (802.1d)</td>
</tr>
<tr>
<td>d</td>
<td>MAC and physical layer spec. for areas where 2.4 or 5GHz cannot be used</td>
</tr>
<tr>
<td>e</td>
<td><strong>QoS control</strong> (Quality assurance and priority control for AV streaming, etc.)</td>
</tr>
<tr>
<td>f</td>
<td><strong>Roaming</strong></td>
</tr>
<tr>
<td>g</td>
<td>Wireless LAN (OFDM, 2.4GHz, Max. 54Mbps)</td>
</tr>
<tr>
<td>h</td>
<td>Addition of power-saving management and dynamic channel to 802.11a (Europe spec.)</td>
</tr>
<tr>
<td>i</td>
<td><strong>Security enhancement</strong></td>
</tr>
</tbody>
</table>

- **Pink**: Wireless LAN physical media
- **Blue**: Middleware
## Wireless LAN Standardization in IEEE802.11

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>j</td>
<td>Specifications for 4.9 – 5GHz utilization in Japan</td>
</tr>
<tr>
<td>k</td>
<td>Research on radio resource measurement</td>
</tr>
<tr>
<td>m</td>
<td>Specification revision of 802.11a and 802.11b</td>
</tr>
<tr>
<td>n</td>
<td><strong>- Next Generation wireless LAN</strong> (100 - 200Mbps, standardization target is 2006, and lower compatibility with 802.11a/b/g.)&lt;br&gt;- Has been discussed in HT SG (High Throughput Study Group).</td>
</tr>
</tbody>
</table>
Wireless LAN Hotspot System Image

Wireless LAN

Mobile terminal

Local server

Access point

Internet

Content server

AP server

ISP server

Service Provider with RADIUS authentication server

PDA/NotePC/Ubiquitous equipment

(Station, Airport, Train, Restaurant, Café, etc.)

incl. local content

‘Hotspot’
Market Size and No. of Hotspots in US

No. of Hotspots

$B

Year

2001 2002 2003 2004 2005 2006

10,000 20,000 30,000 40,000 50,000 60,000 70,000 80,000 90,000 100,000

0 10,000 20,000 30,000 40,000 50,000 60,000 70,000 80,000 90,000 100,000

2001 2002 2003 2004 2005 2006

0 10,000 20,000 30,000 40,000 50,000 60,000 70,000 80,000 90,000 100,000

2001 2002 2003 2004 2005 2006
Major Issues for Wireless LAN Solutions

High-speed Internet access ⇒
Value-added services supported by wireless ISP, ASP, Content providers

(a) Security [→□ ]
(b) Service Roaming □
(c) Business Method
(d) Killer Applications
(b) Roaming

In using multiple wireless LANs as a virtual wide-area network, service level roaming as well as connection level roaming is highly important, e.g., seamless telephoning, video streaming, interactive games, etc.

Technology standardization:
- **Mobile IP** provides key function for handover.
- Technology standardization in terms of both connection level and service level has been conducted in **802.11f**.
De facto or industry standardization
Brokerage for service level roaming such as wireless LAN-to-wireless LAN intermediation of user authentication and accounting in US.

- **WISPr (Wireless ISP Roaming):**
  Affiliated organization of Wi-Fi Alliance
  Roaming or interconnectivity authorization is named WiFi zone for 802.11b wireless LAN.
- Pass-One
- iPass
(c) Business Method

Costs
- Access point (AP) installation cost
- Communication cost for access networks (e.g., ADSL)
- Network management cost
- Customer management and support cost

Players
- Wireless LAN operator
- Local service provider (e.g., shop-owner)
- Wide area service provider (e.g., ISP, ASP, content provider)

Questionnaire on requested area for hotspot services in Japan:
1. Bullet train (Shin-kansen)
2. Cafe
3. Train
4. Airplane
5. Railway station
6. Airport
(d) Killer Applications

Multimedia services using broadband communication
- **IP phone** to IP TV phone and high-quality video streaming

Local positioning service
- Push-type personalized information services and advertising, etc. with highly accurate positioning

Issues in IP phone:
- Limited communication area
- Real-time/low delay handover
- Power consumption of a terminal
- Transmission quality
- Terminal interconnectivity (G.711, G.729 for voice compression, and H.323, MGCP/MEGACO, H.248 for signaling)

Infringement of Symbol Technologies’ patents?
Mobile Internet and Services

<table>
<thead>
<tr>
<th>Service</th>
<th>2001</th>
<th>2002</th>
<th>2003</th>
<th>2004</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Location-base service</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Content delivery</strong> (AV streaming, TV phone)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mobile EC</strong> (SSL, IC card, PKI, Cash card, …)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Infrastructure</th>
<th>3G (IMT-2000)</th>
<th>Wireless LAN</th>
<th>All IP</th>
<th>4G</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bluetooth</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>E911</strong> (Location function(GPS))</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related functions</th>
<th>BS</th>
<th>CS</th>
<th>Terrestrial</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Digital broadcast</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
QoS Control for Wireless LAN ◆ 802.11e

Two modes of QoS control, quality assurance and priority control, are available through HCF  
◆ Hybrid Coordination Function◆ .

(These modes correspond to RSVP and Diffserv, respectively. Though RSVP is not used due to poor scalability, no scalability issue occurs in wireless LAN.) ◆

- Quality Assurance using Parameterized QoS
- Priority Control using Prioritized QoS
HCF □ Hybrid Coordination Function □

CFP: Contention Free Period  CP: Contention Period

EDCF: Enhanced Distributed Coordination Function
Priority Control using Prioritized QoS

Mechanism of EDCF

- Priority Queue (8 levels)
- Parameters:
  - Queue length
  - Transmission interval
  - Contention window, etc.

Scheduler

Back-off

Contention with other terminals
Terminal

- Cellular phone (2G, 2.5G, 3G → 4G)
- Note PC/PDA
- Home appliances and terminals including AV equipment
- Home server with HDD storage, gateway and IP routing functions
- Car terminal for ITS (Intelligent Transport System)
- Robot
- Wearable terminal with various sensors

IPv6 will be essential
Wearable Computing

- Mobile computing terminal
  in a ubiquitous information environment -

- Ultimate Natural Human Interface
- Super-distributed Computing
- Pervasive Internet
Wearable Terminal

1. Ultimate Natural Human Interface
   - Collaboration between sensor-embedded physical agents and intelligent software agents
   - Terminal design with multi-modal natural user interface (NUI)

2. Super-distributed Computing
   - Terminal-to-terminal real-time info. exchange and sharing
   - Dynamic forming and dissolving of ad hoc communities (community computing)
   - Seamless connectivity between wired-to-wireless, tightly-to-loosely-coupled networks

3. Pervasive Internet
   - QoS control adapted to ‘context’
   - Personal profile and directory management
   - Information security and privacy protection
Versatile Types of Terminals
Wearable Computing

Head-Mount Display (HMD) for a single eye

Single-hand keyboard

Wearable computer

Positions where wearable computers can be attached

By courtesy of Nikkei BP Inc.
Wearable Computing System Architecture

Ultimate Natural Human Interface
- Intellectual
  - Info. capture, filtering, summarization, learning, context awareness

Multimedia
Multimodal

Super-distributed Computing
- Location-based ad hoc network
- Tightly-coupled distributed computing
- QoS control over mobile network

Info. processing, human interface
Network
Wearable Human Interface

**Portability**: small size and light weight  
**User friendly**: ease of use, less stress info. I/O, long-life battery  
**High-responsiveness**: real-time and on-demand interaction

### Interface examples

<table>
<thead>
<tr>
<th>Text/command input</th>
<th>New command input scheme for small panel, e.g., using a gradient of a terminal with acceleration sensors.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice input</td>
<td>Non-voice input and operation from a tiny microphone, e.g., automatic interpretation of intention through moving of user’s mouth.</td>
</tr>
<tr>
<td>Image/video input</td>
<td>Automatic understanding of external view and situation through a combined use of a tiny camera, transparent HMD, sensors and augmented reality.</td>
</tr>
<tr>
<td>Sound output</td>
<td>Creating a 3D sound space with a stereo speaker surrounding a user and adding a meaning for each different sound source.</td>
</tr>
<tr>
<td>Image/video output</td>
<td>HMD and VRD (Virtual Retinal Display, direct projection of external view to retina)</td>
</tr>
<tr>
<td>Feeler output</td>
<td>A vest which enables to recognize simple figures</td>
</tr>
</tbody>
</table>
## Wearable Computing Evolution

<table>
<thead>
<tr>
<th>Human-Computer Interaction</th>
<th>Personal</th>
<th>Intimate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HI</strong></td>
<td>MMI</td>
<td>NUI</td>
</tr>
<tr>
<td>(Multimedia &amp; Multi-modal)</td>
<td>(Natural)</td>
<td></td>
</tr>
<tr>
<td>Terminal</td>
<td>Function</td>
<td>External appearance or design</td>
</tr>
<tr>
<td>Communication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specific Applications</td>
<td></td>
<td>Daily and Usual Applications</td>
</tr>
<tr>
<td>□ Remote training, manufacturing, maintenance, diagnosis, etc. □</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Network-related Interface and Functions required to Terminals for 2005

<table>
<thead>
<tr>
<th>Middleware</th>
<th>Location detection by GPS, etc.</th>
<th>Terminal-to-server data synchronization</th>
<th>QoS-controlled high-quality streaming</th>
<th>SIP</th>
<th>Transport layer</th>
<th>Wireless-profiled TCP for IMT-2000</th>
<th>Network layer</th>
<th>IPv6, Mobile IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>AV Communication</td>
<td>MPEG4/H.264 (Video streaming), MPEG7</td>
<td>Multimedia info. retrieval</td>
<td>H.323M</td>
<td>V phone</td>
<td>MP3, AAC, MIDI (Music)</td>
<td>Terrestrial digital broadcast receiving (OFDM)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure</td>
<td>IMT-2000 (W-CDMA, cdma2000)</td>
<td>Bluetooth/IR (Ad hoc network)</td>
<td>IEEE802.11a/g/b</td>
<td>Wireless LAN</td>
<td>( UWB)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security, etc.</td>
<td>SIM card</td>
<td>IPsec, SSL/TLS, PKI/CA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Future Component Technologies

<table>
<thead>
<tr>
<th></th>
<th>~ 2010</th>
<th>~ 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portable PC</td>
<td>Ultra-thin sheet PC</td>
<td>Folding paper PC</td>
</tr>
<tr>
<td>Wearable terminal</td>
<td>Wrist-watch type</td>
<td>Embedded type</td>
</tr>
<tr>
<td>Storage capacity</td>
<td>100GB</td>
<td>300GB</td>
</tr>
<tr>
<td>Continuous usage</td>
<td>5 days</td>
<td>1 month</td>
</tr>
<tr>
<td>Battery</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Wearable Terminal Evolution

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information</strong></td>
<td>Article</td>
<td>Recording/Retrieving</td>
<td>Delivery/Distribution</td>
<td>Communication</td>
</tr>
<tr>
<td><strong>Application</strong></td>
<td>Services in limited areas, e.g., theme parks</td>
<td>Remote control</td>
<td>Careware/Lifeware</td>
<td></td>
</tr>
<tr>
<td><strong>Component technologies</strong></td>
<td>2000g, 600cc</td>
<td>300g, 200cc</td>
<td>100g, 50cc</td>
<td>10g, 10cc</td>
</tr>
<tr>
<td><strong>Weight, volume</strong></td>
<td>5 hours</td>
<td>15 hours</td>
<td>5 days</td>
<td>1 month</td>
</tr>
<tr>
<td><strong>Continuous usage</strong></td>
<td>50W</td>
<td>10W</td>
<td>7W</td>
<td>100mW</td>
</tr>
</tbody>
</table>
③ Server-Terminal Middleware

- Autonomous service discovery and information sharing
  - ⇒ P2P Computing

- Service binding and generation

- Context awareness (adaptation to location, preference, environment, situation, etc.)  ⇒ SIMPLE, Semantic Web

- Mobility support (terminal, user, service)  ⇒ Mobile IP
  - ⇒ IEEE802.11i/1x, AAA, P3P, OMA

- Plug & play  ⇒ UPnP
Context Awareness

Context:

- Context is the information about the situation or circumstances of a user.
  To provide the user with a service of his or her needs in the ubiquitous network, it is essential that the network has the knowledge of his or her context.

- Location, time and presence (on telephone connection or not, in PC use or not, etc.) are simple examples of context. Context includes user’s preferences, and various ambient or circumstantial information.
Context Awareness

User needs: Applications that are context aware and allow personalization based on his or her interest.

Context aware Applications: - can capture the context, - assign meaning to it, and - change behavior accordingly.

Business opportunities:
- Billing by location, time and user’s age
- Delivery of information on local restaurants, hotels, stations, etc. with a city map
- Geo-dependent advertising
- Multimedia navigation or tracking services
(3) Towards Ubiquitous System Era
Conditions for Ubiquitous System Penetration

Prediction
- 2007: 25% in mobile data communication will be over wireless LAN
- 2010: More than 35% in mobile data communication will be over wireless LAN

Conditions
- Interworking of cellular network (beyond 3G) and high-speed wireless LANs, and then covering the world \( \Rightarrow \) 4G
- Applications of RFID tag and sensor network to consumer market
  - Seamless interconnection between wired broadband (FTTH, metro Ether) and wireless LAN
- Penetration of non-PC terminals
- Ultra high-speed hotspot service using UWB
Wireless LAN and UWB

Application

- HD-TV
- Large volume file transfer
  (music 60min.= 360Mb
  TV 30min.= 691Mb)
- SD-TV DVD
  (4Mbps ~ 9Mbps)
- MPEG4/H.264 Video
  (384Kbps ~)
- AAC, MP3 Audio
  (nearly 100Kbps)
- Remote control

Data rate (bps)

- 2.4GHz
- 802.15.3
  QPSK
- 5GHz
  802.11a
- 2.4GHz
  802.11b
- 2.4GHz
  Bluetooth
  Medium/High Rate
- 2.4GHz
  Bluetooth
  1.1

Consumption power

- 100mW
- 1W

Dotted line: under technology assessment

ECHONET: Energy Conservation and Homecare network
UWB Application Examples

High-speed PAN
- Next generation Bluetooth)

Short distance link
- USB/USB2
- Wireless1394

Collision prevention

Short distance Radar
Security Technology for Ubiquitous System

(1) Security Technology Overview
(2) Security Technology for Wireless LAN
(3) Mobility Control and Security
(4) Utilization and Protection of Privacy Information
(5) Interworking of IMT2000 (3G) and Wireless LAN based on Security
(1) Security Technology Overview
# Mobile network Architecture

<table>
<thead>
<tr>
<th>Layer</th>
<th>Major Standardization Organization</th>
<th>Upper Layers</th>
<th>Physical Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>OMA</td>
<td>3GPP/3GPP2, ITU-R</td>
<td>3GPP/3GPP, ITU-R</td>
</tr>
<tr>
<td>Display</td>
<td>Compact HTML, HDML/WAP2.0. MML</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Middleware</td>
<td>Proprietary WAP1.1/1.2 (WTP, WSP, WAE)</td>
<td>Proprietary WTP</td>
<td></td>
</tr>
<tr>
<td>Transport</td>
<td>Proprietary WAP1.1/1.2 (WTP, WSP, WAE)</td>
<td>Proprietary WTP</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Proprietary WAP1.1/1.2 (WTP, WSP, WAE)</td>
<td>Proprietary WTP</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Layer</th>
<th>Upper Layers</th>
<th>Physical Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Major standardization organization</td>
<td>OMA</td>
<td>3GPP/3GPP2, ITU-R</td>
</tr>
<tr>
<td>Upper layers</td>
<td>IETF</td>
<td>IEEE802.11</td>
</tr>
<tr>
<td>Physical layer</td>
<td>IEEE802.15</td>
<td></td>
</tr>
</tbody>
</table>

- **2G/2.5G → 3G**
- **Wireless-profiled TCP**
- **TCP/UDP Authentication (802.1x)**
- **IP (MobileIP, IPv6)**
- **Roaming (802.11f)**
- **Security (802.11i)**
- **QoS Control (802.11e)**
- **IEEE802.11**
- **IEEE802.15**

- **Wide area cellular network**
- **Ad hoc network**
- **Wireless LAN**
## Security Technology for Ubiquitous System

<table>
<thead>
<tr>
<th>Function</th>
<th>Network</th>
<th>Technology &amp; Standardization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption,</td>
<td>Cellular Network (2G→3G)</td>
<td>- <strong>AAA</strong> (Authentication, Authorization &amp; Accounting) was discussed in IETF considering mobility support in late 1990s.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 3GPP started discussion on 3G-wireless LAN interworking in terms of authentication and accounting management in 2002.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- In actual communication, IPsec and SSL have begun to be used.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Secrecy has been assured using UIM/SIM in Europe.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Wireless LAN</td>
<td>- IEEE802.11 has been intensively discussing <strong>IEEE802.11i, 802.1x</strong> since 2001.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- IEEE802.11i (overall security) finalization of standardization is scheduled for the end of 2003.</td>
</tr>
<tr>
<td>Privacy protection</td>
<td></td>
<td>- W3C (World Wide Web Consortium) has been standardizing <strong>P3P</strong> (Platform for Privacy Preferences) which specifies framework, privacy information description and protocols independent from network infrastructure since late 1990.</td>
</tr>
</tbody>
</table>

---

**Notes:**
- **AAA** refers to Authentication, Authorization & Accounting.
- **IEEE802.11i, 802.1x** are standards for wireless network security.
- **PANA** is a protocol for carrying authentication for network access.
- **P3P** is the Platform for Privacy Preferences.
Security Technology for Ubiquitous System

Encryption, Authentication, Privacy protection

- Cellular Network (2G→3G) AAA (IETF→IRTF)
- Wireless LAN
- Internet AAA (IETF→IRTF)
- 3G-wireless LAN interworking (3GPP)
  - IEEE802.11i (IEEE802.11)
  - IEEE802.1x (IEEE802/802.11)
  - PANA (IETF)
  - P3P (W3C)

( ): Standardization organization
(2) Security Technology for Wireless LAN
Security Technology for Wireless LAN

- Basic security functions for wireless LAN:
  Encryption
  Authentication

- Technology assessment and standardization:
  Overall security issues → **IEEE802.11i**
    - standardized at the end of 2003
  Authentication → **IEEE802.1x**
    - originally port-based access control for wired network in 1990s
    - standardized at the end of 2001 for wireless LAN
History

IEEE802.11i had discussed security scheme called WEP (Wired Equivalent Privacy) which mainly targeted encryption scheme from 1998 to 2001.

WEP, however, was proven vulnerable in early 2001 and IEEE802.11i started to investigate a new highly-secure version. Full standardization of IEEE802.11i will be finalized at the end of 2003.

[WEP’s bottlenecks]
- Encryption key length is 40 or 104 bits.
- Encryption algorithm adopted in WEP is RC4 which is not so strong.
- All terminals in wireless LAN have the same encryption key.
- Check sum is CRC32 with no signature, etc.
802.11i’s major specifications were released in 2002 (draft v3).

**WPA** (Wi-Fi Protected Access, industrial standard) was released by Wi-Fi Alliance for promoting 802.11i.

1) **Encryption**

Protocol: **TKIP** (Temporal Key Integrity Protocol)
- Key change of each packet or constant time interval, and prevention of message tampering are available.

Algorithm: **AES (*)** (Advanced Encryption Standard)
- US decided to adopt as a standard replacing DES (Data Encryption Standard) in 2000.

2) **Authentication ← 802.1x**

Protocol: **EAP** (Extensible Authentication Protocol)
- Several authentication schemes have been proposed, each of which uses different protocols, such as EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-LEAP, etc.

**AES (*)**: called Rijndael algorithm which is a 128-bit block encryption scheme and was proposed by Belgian researchers, Joan Daemen and Vincent Rijmen.
# EAP

<table>
<thead>
<tr>
<th>Recommended</th>
<th>EAP-MD5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Client authentication based on user ID and password</td>
</tr>
<tr>
<td>EAP-TLS (IETF RFC2716)</td>
<td>- Client and server authentication based on PKI</td>
</tr>
<tr>
<td></td>
<td>- CA distributes certificate to clients and a client authentication server (RADIUS, etc.) prior to data transmission</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Optional</th>
<th>EAP-TTLS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Simplified protocol compared with EAP-TLS</td>
</tr>
<tr>
<td>EAP-PEAP</td>
<td>- Client and server authentication</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cellular phone use</th>
<th>EAP-AKA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- UMTS AKA and key distribution scheme are used. AKA has the compatibility with GSM.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>EAP-SIM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- SIM card-used authentication and key distribution</td>
</tr>
</tbody>
</table>

MD5: Message Digest algorithm 5  
TLS: Transport Layer Security  
TTLS: Tunneled TLS  
LEAP: Lightweight EAP  
PEAP: Protected EAP  
AKA: Authentication and key Agreement  
SIM: Subscriber Identification Module  
PKI: Public Key Infrastructure  
CA: Certificate Authority  
RADIUS: Remote Authentication Dial In User Service
Authentication Process using 802.1x

Client

Access point

Authentication server
(RADIUS server, etc.)

1. Access to network

2. Request user authentication

Authentication using EAP
(EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-LEAP)

3. Authentication result notification

Packets communicated by EAP
- Request
- Success
- Response
- Failure
# WPA and WPA v2 (= Full IEEE802.11i)

<table>
<thead>
<tr>
<th></th>
<th>WPA</th>
<th>WPA v2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification by Wi-Fi Alliance</td>
<td>Aug. 2002 ~</td>
<td>Feb. 2004 ~</td>
</tr>
<tr>
<td>Specifications</td>
<td>Part of IEEE802.11i draft v3</td>
<td>IEEE802.11i full specification</td>
</tr>
<tr>
<td>Encryption</td>
<td>TKIP</td>
<td>TKIP, CCMP, WRAP</td>
</tr>
<tr>
<td>User authentication</td>
<td></td>
<td>IEEE802.1x/EAP</td>
</tr>
<tr>
<td>Targeted user</td>
<td>Enterprises, consumers</td>
<td>Government, enterprise divisions which require particularly strong security</td>
</tr>
<tr>
<td>Version-up from existing system</td>
<td>Version-up by software</td>
<td>Hardware replacement is necessary for acquiring sufficient performance</td>
</tr>
<tr>
<td>Not supported usage mode</td>
<td>Ad hoc mode, handover</td>
<td>None</td>
</tr>
<tr>
<td>Other items</td>
<td>Lower compatibility with WEP Home mode in which IEEE802.1x is not used is available</td>
<td>AES is used as an encryption algorithm for CCMP and WRAP</td>
</tr>
</tbody>
</table>

CCMP: Counter mode with Cipher block chaining Message authentication code Protocol
WRAP: Wireless Robust Authenticated Protocol
(3) Mobility Control and Security
Mobility Control and Security

1. AAA
   Authentication, Authorization and Accounting

1) Standardization
   - Discussions were transferred to IRTF AAA Architecture Research Group in 2000 (http://aaaarch.org)
   - 3GPP2 adopts AAA in combination with Mobile IP

2) References
   - 4 RFCs were released in Dec. 2000.
     - RFC2903: Generic AAA Architecture
     - RFC2904: AAA Authorization Framework
     - RFC2905: AAA Authorization Application Examples
     - RFC2906: AAA Authorization Requirements
   - 1 RFC was added in Dec. 2002.
     - RFC3334: Policy based accounting
3) Standard protocol

- TACACS (Terminal Access Controller Access Control System) (*1)
- RADIUS (Remote Authentication Dial In User Service)
- DIAMETER (next generation AAA protocol)

  *1 TACACS+ is an extension by CISCO

4) Basic model

- AAA server calls and processes Application Specific Module (ASM) based on the policy in response to request.
DIAMETER

Though DIAMETER protocol uses different data unit from RADIUS protocol, it has a lower compatibility with RADIUS protocol.

DIAMETER’s Advantages
- Compatibility with current firewall: support for Keep/Alive messages
- Scalability: support for processing of many pending AAA requests
- Bidirectional architecture: support for both push and pull applications
  (RADIUS is unidirectional)
② PANA

(Protocol for carrying Authentication for Network Access)

Client authentication mechanism in IP layer in multi-network environment, such as 3G cellular network, Bluetooth, wired LAN, wireless LAN, etc.

BOF started in 50th IETF, Mar. 2001.

Advantages

- A client can be authenticated if layer 2 is connected regardless of the physical network, 802 or not (cellular network, etc.).

- Only a PAA (PANA Authentication Agent) is needed in a subnetwork. The PAA communicates with a remote authentication server (RADIUS, etc.). c.f, in IEEE802.1x, all access points and switches in a subnetwork must comply with IEEE802.1x.
PANA Authentication Model

Authentication server

Internet

Inquiry

Response

Connection

Direct port-open

PAA (PANA Authentication Agent)

Authentication request

Access point

Router

Base station

Hub

PANA client

Wireless LAN

Note PC

PDA

Cellular phone

PANA client
(4) Utilization and Protection of Privacy Information
Utilization and Protection of Privacy Information

P3P (Platform for Privacy Preferences) Standardization

• International standard for Web information utilization for personalized services and its privacy protection

• Major vendors have already supported.
  – NEC, Netscape, AOL, Microsoft, AT&T, IBM, HP, American Express, DoubleClick, Engage, etc.

• Government organizations in EU and Japan have already supported.

W3C: Standardization organization for XML, HTML, HTTP related specifications
0. Private information including its usage purpose is described in XML and is stored as P3P policy.

1. User accesses Web page

2. Web browser automatically accesses P3P policy

3. Web browser compares user preferences with P3P policy.

   - No difference
     - Web access is permitted.

   - Difference exists
     - Web browser warns user, and the user decides whether the private information is transferred or not.
P3P Web Browser ‘s Display Examole

- Icon changes and warns user in case of NG
- Display the difference portion between user preferences and P3P policy

P3P compliance may influence the total number of Web access.
How to make Web Server Comply with P3P?

• P3P policy creation from Web pages to which private information is collected.
  – Create XML using P3P policy editor
  – Make a link from these Web pages to P3P policy file

• Installation of necessary files at Web site
  – Install P3P policy and its link information into Web server

Only file creation and its installation are necessary. No special program and CGI are necessary.
(5) Interworking of IMT2000(3G) and Wireless LAN based on Security
Interworking Image of 3G and Wireless LAN

Communication area, Mobility, Portability

High speed, High quality

3G

Wireless LAN

ISP

Content Provider

ASPs

Enterprise Network

VPN

Internet Access

Content Delivery

User info., Authentication, Accounting

3G Service area

Hotspot
Integration Scenarios discussed in 3GPP

Key factors
- Authentication and Charging
- QoS
- Seamless Connectivity

Scenarios:
1. Common Billing and Customer Care
2. 3GPP system based Access Control and Charging
3. Access to 3GPP system PS based services
4. Service Continuity
5. Seamless Services
6. Access to 3GPP CS Services

Feasible solutions in a few years
# 3G - Wireless LAN Interworking Scenarios

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>- Security level of 3G and wireless LAN are independent.</td>
</tr>
<tr>
<td></td>
<td>- No new requirements on 3G specifications.</td>
</tr>
<tr>
<td>2</td>
<td>- <strong>AAA</strong> is provided by 3G system, e.g. <strong>EAP</strong> (EAP-AKA for GPRS/USIM and</td>
</tr>
<tr>
<td></td>
<td>EAP-SIM for GSM/SIM) is used for authenticating user by 3G server.</td>
</tr>
<tr>
<td></td>
<td>- Reuse 3G access control and charging principles (HSS/HLR, etc.) for the</td>
</tr>
<tr>
<td></td>
<td>benefit of 3G system operators and users.</td>
</tr>
<tr>
<td>3</td>
<td>- Operators grants access to 3G PS based services through wireless LAN.</td>
</tr>
<tr>
<td></td>
<td>- Service continuity between 3G and wireless LAN is not required.</td>
</tr>
<tr>
<td></td>
<td>- IMS based/location based/instant messaging/presence based services.</td>
</tr>
<tr>
<td>4</td>
<td>- Handover for specific services</td>
</tr>
<tr>
<td></td>
<td>- Change of service quality in mobility across 3G and wireless LAN</td>
</tr>
<tr>
<td></td>
<td>- Service continuities between 3G &amp; wireless LAN and between different</td>
</tr>
<tr>
<td></td>
<td>wireless LANs</td>
</tr>
<tr>
<td>5</td>
<td>- Seamless <strong>service continuity</strong> and <strong>handover</strong></td>
</tr>
<tr>
<td></td>
<td>- Non-real-time services: <strong>Mobile IP</strong></td>
</tr>
<tr>
<td></td>
<td>- Real-time services: fast <strong>Mobile IP</strong> protocols, <strong>Context Transfer</strong> protocol,</td>
</tr>
<tr>
<td></td>
<td>access router discovery schemes</td>
</tr>
<tr>
<td>6</td>
<td>- Grant access to 3G CS based services through CSed wireless LAN access</td>
</tr>
</tbody>
</table>
Thank you for your attention