ROOT INC.

高速シームレスモバイル通信

Hiroshi MANO (ROOT Inc.)
Hmano@root-hq.com

ROOT INC.

Agenda

- **MISP protocol (Basic seamless hand over)**
  - Introduce our MIS Protocol (MISP)
  - Comparison with IEEE802.11 and IEEE802.1x from the point of view of handover latency
  - Comparison with IEEE802.11 and IEEE802.1x from the point of view of security
- **PDMA (Make before break hand over)**
  - Handover latency
  - Packet Division Multiple Access (PDMA)
  - Laboratory experiment
  - Field experiment
- **Media hand over (Wireless LAN & PHS)**

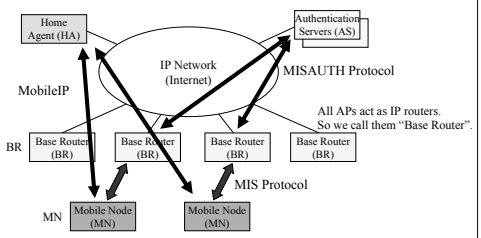
ROOT INC.

Introduction of MISP (Basic seamless hand over)

- **The combination of Wireless LAN and mobile IP is a fast and low-cost mobile communication method.**
- **But there are some issues.**
  - Security Weakness
  - Handover Latency
- **So we developed a new link layer protocol, MISP.**

ROOT INC.

MIS System Architecture



ROOT INC.

MISP Overview

- **MIS protocol is a layer 2 protocol designed for public mobile internet services.**
- **IPv4 is mainly targeted as upper layer.**
- **Lower layer is IEEE802.3 or part of IEEE802.11.**
- **Features**
  - Mutual authentication, session key exchange and network layer setup between BR and MN by ONE ROUNDTRIP PACKET EXCHANGE

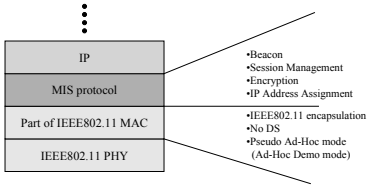
    ⇩

    Effective for fast handover
  - Encryption between AP and STA with periodic key update
  - Authentication of every frame
  - Multiple Service Providers support
- **It can be used with MISAUTH protocol (MISAUTHP) which enables remote authentication over IP.**

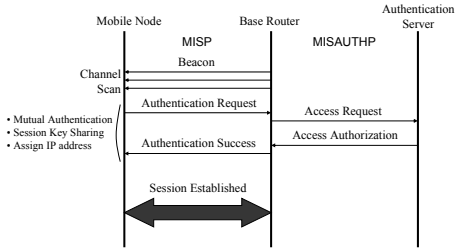
ROOT INC.

Layer

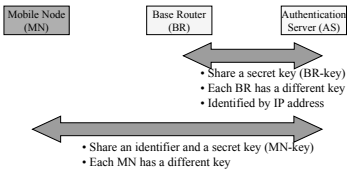
In case of using IEEE802.11 as lower layer



MISP and MISAUTHP Sequence



Pre-shared Secret Key



- **No pre-shared information between MN and BR**

MIS Protocol Frame Format

- MIS Protocol Control Frame

IEEE802.11 Header	IEEE802.2 Header	MISP Control Message

- MIS Protocol Data Frame (transferring network layer packet)

IEEE802.11 Header	IEEE802.2 Header	MISP Header	IP Header	••••

Encrypted by MISP

- Ethernet number 0x8893 is assigned for MISP by IEEE.

MIS Protocol Control Message Format

MISP Header

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1		
Code	Flags	Length

Control Message

Code	Message
0x00	Data
0x01	Beacon
0x03	Authentication Request
0x04	Authentication Success
0x08	Authentication Fail
0x09	Finish Session

- Followed by some “objects”

Format of an Object

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1		
Type	Length	Value…

Objects

Type	Length	Name	Beacon	Auth. Req.	Auth. Suc.	Auth. Fail
0x00	1	Padding	Optional	Optional	Optional	Optional
0x02	10	Beacon Timestamp	Required	Required	Required	Required
0x03	6	IPv4 Local Address		Optional	Optional	
0x04	6	IPv4 Remote Address			Optional	
0x05	Variable	ICV (Integrity Check Value)		Required	Required	
0x06	Variable	NAI (Network Access Identifier)		Required		
0x08	Variable	Session Key Derivery Data		Required		
0x09	14	Geographical Information	Optional			
0x0a	3	IPv4 available address number	Optional			
0x0b	3	IPv4 Source Address Filter	Optional			
0x0d	4	Error Reason				Required
0x0e	2+4n	BR Group	Required			
0x0f	4	Session Key Valid Time			Required	
0x10	4	Serial Number	Required			
0x11	4	Beacon Interval	Required			
0x12	2+2n	Security Type	Required	Required		
0x13	8	Uplink Speed	Optional			
0x14	3	Channel	Optional			
0x15	2+2n	Network Layer Type	Required	Required	Required	

Security Types Supported by MISP

- **Null (Optional)**
  - No security
- **HMAC-MD5/HMAC-MD5/HMAC-MD5-128bit (Optional)**
  - HMAC-MD5 is used for authentication.
  - HMAC-MD5 is used for delivery of session key.
  - HMAC-MD5 is used for authentication of frame.
- **HMAC-MD5/HMAC-MD5/AES-CBC-128bit (Mandatory)**
  - HMAC-MD5 is used for authentication.
  - HMAC-MD5 is used for delivery of session key.
  - AES-CBC-128bit is used for data encryption

Beacon

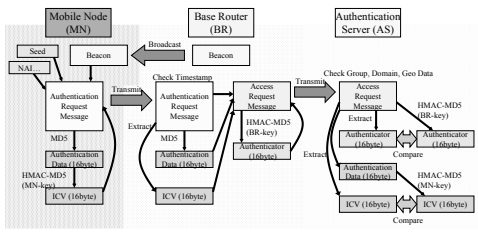
- **Beacons are transmitted in 30ms interval.**
- **Each beacon includes the following information.**
  - Timestamp
  - Serial number
  - Beacon interval
  - Group (like SSID)
  - Supported Network layer type
  - Remaining IPv4 addresses
  - Channel
  - Etc…

Behavior of MN

1. **An MN makes a list of BRs by scanning channels and receiving beacons. The BRs in the list have corresponding "group (like SSID)".**
2. **The BR list is sorted by the signal strength of the beacon.**
3. **The MN try to authenticate to the top of the list of BRs.**
4. **If the authentication fails, the MN try to authenticate to the next BR in the list until the end of the list.**
5. **After the authentication succeed, the MN can communicate to the network.**
6. **The MN makes a registration to the HA.**
7. **The MN watches the beacon of connected BR. If the MR cannot receive the beacons of the BR for a certain period or the beacon strength becomes less than the threshold, the MN closes the session and return to 1.**

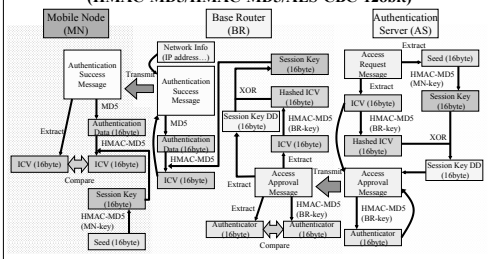
Authentication

(HMAC-MD5/HMAC-MD5/AES-CBC-128bit)



Authentication (Cont.)

(HMAC-MD5/HMAC-MD5/AES-CBC-128bit)

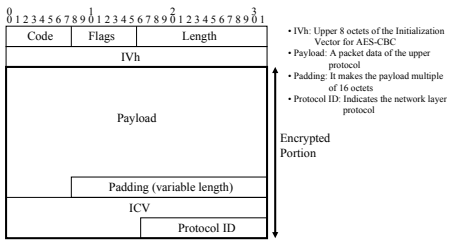


Network Layer Setup

- **IPv4 Configuration**
  - Assign IP address and gateway
  - DNS server, SMTP server, etc. are not assigned because it is premised on mobile IP. In case of using mobile IP, it is enough that fixed servers are installed near the home agent.
  - But it is easy to expand to assign them for non mobile IP users by defining new objects.
- **Other network layer such as IPv6 support is also easy by defining new objects.**

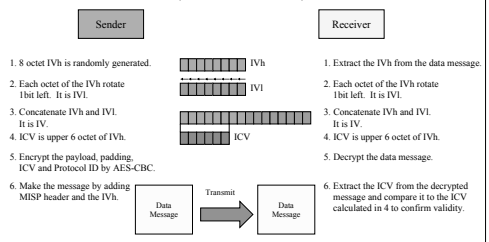
Data Message Format

(HMAC-MD5/HMAC-MD5/AES-CBC-128bit)



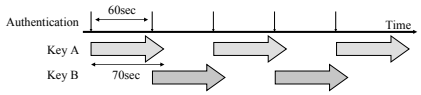
ROOT INC.

Encryption, Decryption and Message Authentication (AES-CBC-128bit)



ROOT INC.

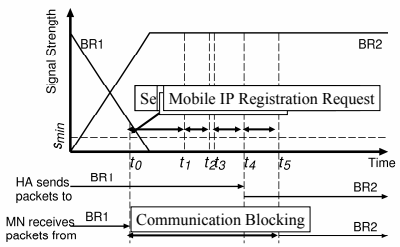
Session Key Updating



• The session key is identified by the flag in the MISP header.

ROOT INC.

Communication Blocking in Handover



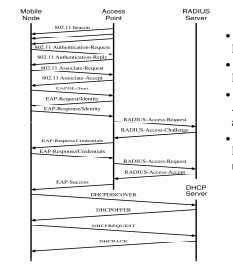
ROOT INC.

Factors of Communication Blocking

- **Channel Scan**
- **Link Layer Set up**
- **IP Layer Set up**
- **Mobile IP registration**

ROOT INC.

IEEE802.11+IEEE802.1x Session Establishment



- 2 roundtrip packet exchanges between MN and AP for association
- 3 roundtrip packet exchanges between MN and AP for authentication.
- 2 roundtrip packet exchanges between AP and RADIUS server for authentication.
- 2 roundtrip packet exchanges between MN and DHCP server for IP layer set up.

ROOT INC.

Handover Comparison with IEEE802.11+IEEE802.1x

- **If the authentication server is far away from BR(AP), the time needed to establish session is significantly affected by the number of packet exchanges.**
- **And DHCP needs more time to set up IP layer.**
- **So MISP has advantage to fast handover because it needs only ONE roundtrip packet exchange between MN and BR, and BR and AS to establish session including IP layer set up.**

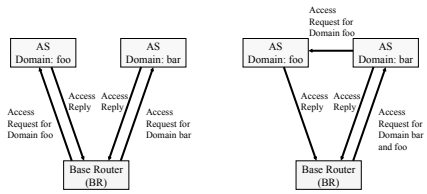
ROOT INC.

Security Comparison with IEEE802.11+IEEE802.1x

	IEEE802.11+IEEE802.1x	MISP+MISAUTHP
Man-in-the-middle attack	Available by fake EAP success message	Unavailable (avoided by mutual auth.)
Fake access points	Available	Unavailable (avoided by mutual auth.)
DoS attack by fake management frame	Available	Depends on implementation
Session Hijack	Available by MAC address hijacking	Unavailable (avoided by packet auth.)

ROOT INC.

Multiple Service Providers Support



(a) By BR configuration (b) By AS proxy

ROOT INC.

Field experience

- Net meeting over UDP
- Video streaming over TCP/IP

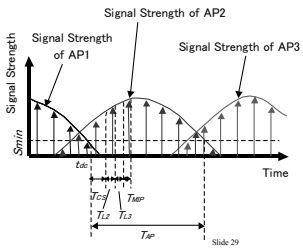
ROOT INC.

PDMA (make before break)

- We developed a new link layer protocol MISP and a new multiplexing method PDMA.

ROOT INC.

Ordinary Handover Latency



- Channel Scan (T_{CS})
- L2 Setup (T_{L2})
- L3 Setup (T_{L3})
- Mobile IP (T_{MIP})

Communication Blocking

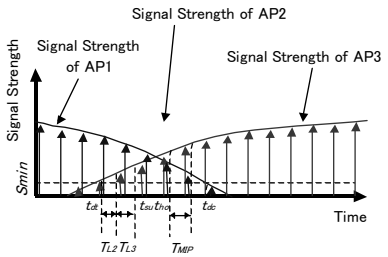
ROOT INC.

Packet Division Multiple Access (PDMA)

- All cells uses same channel.
- All packets share the bandwidth by CSMA/CA fully dynamically and automatically.
- Mobile nodes don't need to scan channels.

ROOT INC.

Handover Timing of PDMA



Slide 31

ROOT INC.

Implementation

- **We implemented MISP, PDMA and mobile IP on a mobile router ROOT RMR2400G.**
  - CPU: Intel Celeron 400MHz
  - Wireless I/F: Atheros AR5212 (IEEE802.11a/b/g)
  - OS: NetBSD 2.99.10 (-current in Oct. 2004)

Slide 32

ROOT INC.

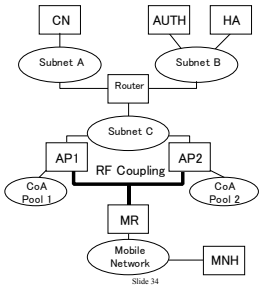
Laboratory Experiment

- **Wireless Interface: 5GHz, OFDM54**
- **1200byte UDP packet at 20Mbps**
- **Observe packet losses and latency at handover**
  - No packet losses were observed
  - No significant latency was observed

Slide 33

ROOT INC.

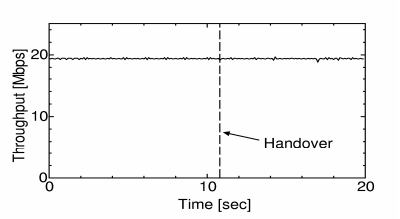
Laboratory Experiment Network



Slide 34

ROOT INC.

Throughput in Handover



Slide 35

ROOT INC.

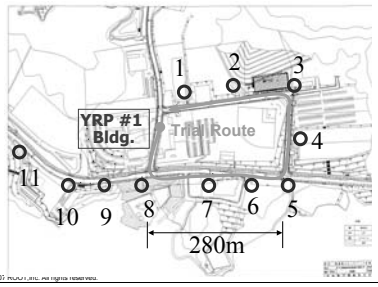
Field Experiment

- **Wireless Interface: 5GHz, 108Mbps (Turbo mode)**
- **11 APs are installed along the road**
  - 70-150m interval
- **MR, PC and camera are installed in a car**
  - The car was driven at 30km/h
- **Observe signal strength, packet losses and 802.11 retry**
  - 58byte UDP packet at 1000packets/sec (1Mbps)
- **DVTS (video streaming), Skype (VoIP)**

Slide 36

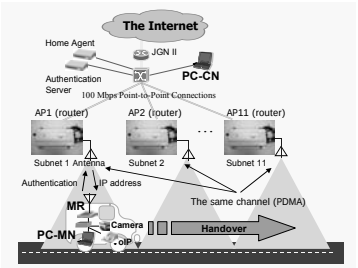
ROOT INC.

AP Location



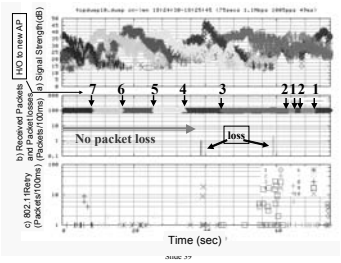
ROOT INC.

Field Experiment Network



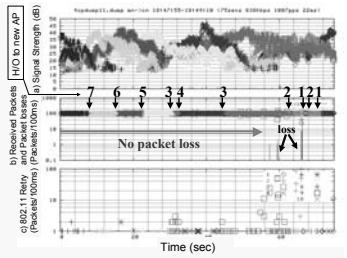
ROOT INC.

Signal strength, Packet losses and IEEE802.11 retry (from PC-CN to PC-MN)



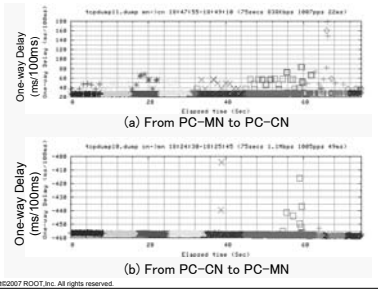
ROOT INC.

Signal strength, Packet losses and IEEE802.11 retry (from PC-MN to PC-CN)



ROOT INC.

One-way Delay



ROOT INC.

Field experience

ROOT INC.

Media hand over

Media	Data rate	Service cost OPEX	Infrastructure CAPEX	Services area
Cellular	<Mbps	Packet charge High	Operator's property High	Nation wide
PHS	<100kbps	Fixed charge Low	Operator's property High	Nation wide
Wireless Lan	<54Mbps	Free	Low	Limited area

The hybrid system of PHS and Wireless LAN can makes large service area by low OPEX & CAPEX.

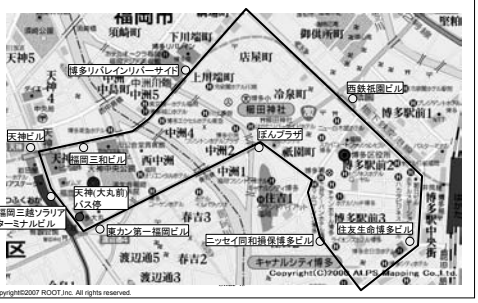
ROOT INC.

Field Trial

- **Dates 2006/2/15-2006/3/31**
- **Area: Shuttle bus around Hakata area.**
  - Hakata ST→ Gofukumachi →Tenjin →Canal city→Hakata ST
  - Length : 5.4km
  - Round trip time: 30 to 60 min (depends on traffic condition)
- **Number of Mobile (bus): 10**
- **Number of Warless LAN AP (2.4GHz, OFDM6) : 9**
- **Service Contents:**
  - Operating information (Estimate Arrival time)
  - News（Text、Video）
  - Advertisement（Picture、Video）
  - Emergency information

ROOT INC.

Filed Trial Area



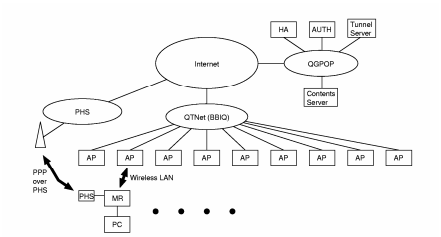
ROOT INC.

Wireless LAN anteena

Cardioids Antenna
（140°、6 dBi）

ROOT INC.

Network shematics



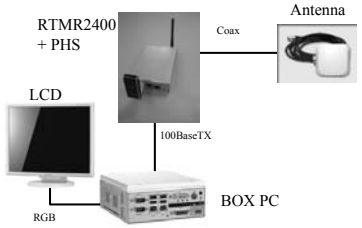
ROOT INC.

Mobile Router（RTMR2400）

- **CPU: Intel IXP425**
- **OS：NetBSD**
- **Interface**
  - IEEE802.11a/b/g
  - 100BaseTX ×2
  - USB ×2
- **Size：95mm×139.5mm×33mm**
- **Weight: 500g**

ROOT INC.

Mobile system schematics



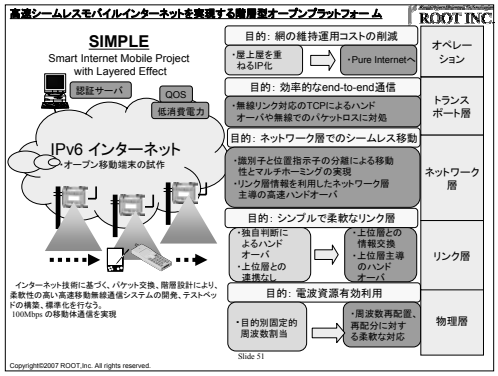
Slide 49

ROOT INC.

Slide 50

高速シームレスモバイルインターネットを実現する階層型オープンプラットフォーム

ROOT INC.



Slide 51

ROOT INC.

Conclusion

- **We implemented MISP, PDMA and mobile IP**
- **We did laboratory experiment and field experiment**
- **The combination of MISP and PDMA minimize handover latency without packet losses.**
- **We deployed media hand over between PHS and Wireless LAN. This hybrid systems makes huge service area immediately with low CAPEX and OPEX.**
- **All technologies should be optimized by module architecture.**

Slide 52