4 Wireless Security Technologies

4-1 Mobile Ethernet and its Security Toward Ubiquitous Network

MIYAMOTO Goh and KURODA Masahiro

The ubiquitous environment is a seamless integration of radio systems, such as the 3 G, WLAN and wireless MANs, and is expected popular in near future combined with small RF devices. The Mobile Ethernet is an architecture to integrate different types of radio systems and provide transparent network access anytime anywhere. We explain the Mobile Ethernet architecture for future ubiquitous environment from the viewpoint of 3 GPP and IEEE802 LMSC. We, then, talk the Mobile Ethernet Security which is the security framework to accommodate both application and network authentications. We, then, discuss wireless security issues. One is to have a common mechanism to keep confidentiality among radio systems. The other is to provide functions to maintain availability. The wireless security discussion is still on the way and we need to investigate privacy issues for security of future ubiquitous network.

Keywords
Security, Mobility, DoS attack, Ubiquitous wireless network, Wireless security

1 Introduction

The ubiquitous environment is expected to be always connected to network. The next generation wireless network, called the Beyond 3 G, that integrates various radio systems, such as 3 G, WLAN and wireless MANs, is a candidate for the environment. It provides an all IP wireless solution to IP services, taking advantage of each radio system.

There are activities to integrate wireless networks into all IP network using IP technologies[1]-[3]. The main idea is to localize radio dependent functions as much as possible and to have a common IP layer to support mobility, authentication and signaling control. The IP network infrastructure is prevailing as metropolitan network in conjunction with the IEEE802 wireless technologies and expected to accommodate the 3 G system.

The IP network based on 3 G is gradually extending as wireless networks, whereas the network works on IEEE802.11 is dramatically expanding its deployment because of the cost efficiency. In the 3rd Generation Partnership Project (3 GPP), there are discussions to enhance the mobility and handover management in the radio access network (RAN) between radio systems under the IP layer for the Beyond 3 G[4]. The IEEE802 LMSC[5] is also working on the integration of radio systems. The IEEE802.16[6] Working Group is developing a specification for Fixed Broadband Wireless Access Systems for combined fixed and mobile operation in wireless MAN environment and the IEEE802.21[7] Working Group is defining a seamless handover interface among wireless technologies, such as IEEE802.11, 802.16 and 3 G. The IEEE802 LMSC based wireless systems are becoming key components of the ubiquitous environment and are expected to converge to a common IEEE802 MAC layer in conjunction with software radio technologies[8] with MIMO systems. The common IEEE802 MAC convergence does not expect complex IP packet forwarding and inefficient reauthentication in place.

There are two types of mobility management. One is macro mobility which requires lossless but not real-time feature. The other is micro mobility to keep response time for real-time applications, such as VoIP and Video conference over IP. The macro mobility is managed by Mobile IP[9] in integrated wireless systems. In the Mobile IP enhancements, efficient route optimization, fast handover[10] and control packet reduction using hierarchical network management[11] are raised. These enhancements need capsulations and many message exchanges, such as Binding Update, at terminal movements between access routers and Return Routability to check the validation of the binding update information. The capsulation increases process load and these messages exchanges increase signaling load for frequent handovers in metropolitan areas. This approach is suitable for the macro handover between two different service networks. The micro mobility, on the other hand, requires seamless wireless integration for real-time applications. A packet loss in voice communication causes noise and some disconnection. The Ubiquitous environment expects both macro and micro mobility following standards for public use.

The security management for ubiquitous environment has different aspects. There are network access authentications, wireless access security, and wireless privacy. In the integrated wireless network, when a mobile device handovers from one radio system to the other, the network verifies the wireless access whether it is allowed by inquiring an authentication server in the network. A network access authentication which is independent of radio systems is expected. The network also needs to have safe wireless access not to be attacked. Once the wireless system is attacked by Denial of Services (DoS) by utilizing context information which is in air, the network will not function properly. Untraceability using context information are required to escape from DoS attacks besides wireless jamming, wireless session hijacking, and wireless association flooding.

In this paper, we introduce the Mobile Ethernet and its security targeted for ubiquitous network. The section **2** explains the Mobile Ethernet architecture, a Beyond 3 G, and its micro mobility solution. The section **3** introduces a framework of the network access authentication which is consistently used with application level authentication and discusses the handover authentication. The section **4** discusses wireless security. It introduces a security key management utilizing location information of a mobile device that is independent of radio systems. We discuss functions to protect the wireless interface of the Mobile Ethernet from Denial of Server (DoS) attacks. We, then, conclude with future works in the section **5**.

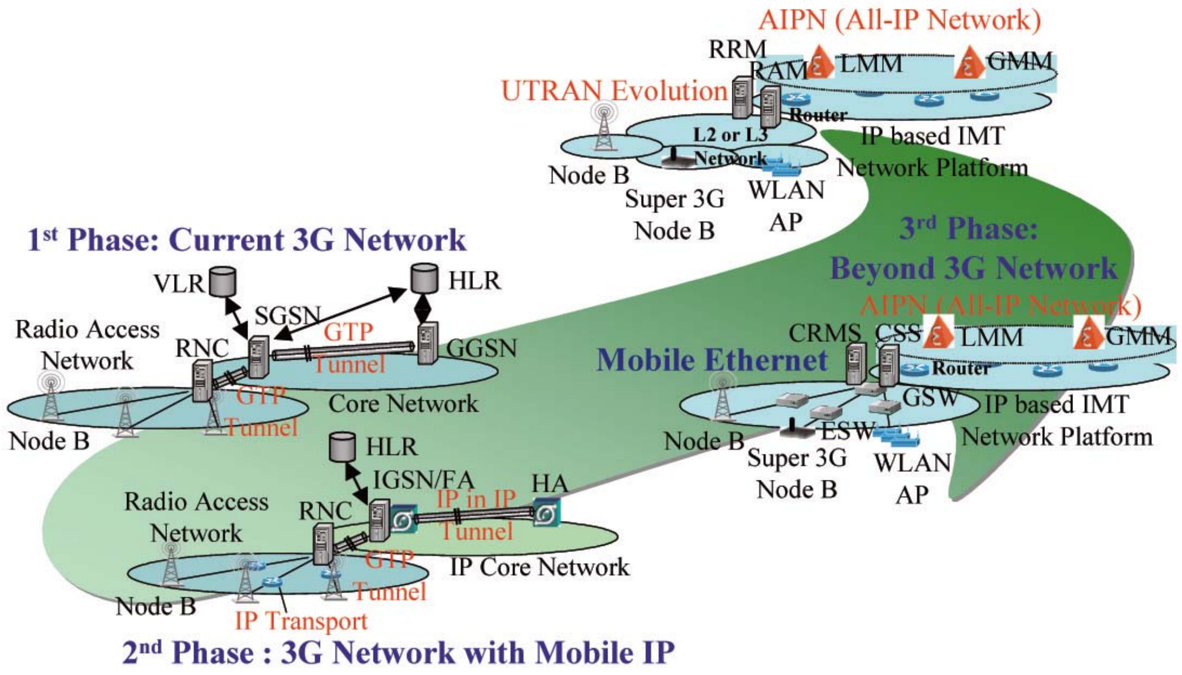
2 Ubiquitous network: Mobile Ethernet

The ubiquitous network expects seamless integration of networks and radio systems. The Mobile Ethernet with Mobile IP solutions provides both macro and micro mobility. In this section we explain the current Mobile Ethernet and its future network.

2.1 Mobile Ethernet in 3 GPP evolution

There are discussions of the 3 G direction. Figure 1 presents the 3 G evolution discussed in the 3 GPP.

The 1st phase shows the current 3 G cellular network service in Japan. The 2nd phase is an attempt to enhance the mobility management by introducing IETF Mobile IP into core network, but it is not proved as future 3 G. The architecture combines GSM with Mobile IP mobility handling[12]. The 3rd phase aims at the enhancement of mobility management



GTP: GPRS Tunneling Protocol (GPRS: General Packet Radio Service), RNC: Radio Network Control, HLR: Home Location Register, VLR: Visitor Location Register, SGSN: Serving GPRS Support Node, GGSN: Gateway GPRS Support Node, IGSN: Internet GPRS Support Node, HA: Home Agent, FA: Foreign Agent, UTRAN: UMTS Terrestrial Radio Access Network (UMTS: Universal Mobile Telecommunications System), GMM: Global Mobility Manager, LMM: Local Mobility Manage, RAM: Radio Access Manager, CRMS: Common Resource Management Server, CSS: Common Signaling Server, GSW: Gateway Switch, ESW: Edge Switch

Fig.1 *3 GPP Evolution*

in the core network as an advanced router network[13]. The UTRAN evolution is also discussed to optimize dynamic resource allocation and scheduling. There are talks for traffic/mobility control and MAC interface enhancement to allow efficient handover between various types of radio systems[14]. The Mobile Ethernet is a candidate RAN technology for the UTRAN evolution.

2.2 Mobile Ethernet architecture

The Mobile Ethernet is a metropolitan area Layer 2 based network that accommodates different types of radio systems satisfying a common interface for both data and signaling. The Mobile Ethernet can extend a support area using other technologies, such as Provider Bridge[15] and also connect to the Internet via a router as shown in Fig. 2.

In the Mobile Ethernet, every message is virtually broadcasted on the core network shared with proper MAC addresses and allows to plug-in various radio systems, such as 3 G, WLAN, wireless MANs, and 4 G, following a common MAC interface. To achieve scalability, Layer 2 switches with path-learning caches are deployed in the network. A path to a destination MAC address is learned at all switches on the path and unnecessary broadcast is suppressed, once the path is learned[16][17].

The Mobile Ethernet provides a real-time handover mechanism based on Layer 2 switch architecture and a prediction mechanism of seamless handover for real-time applications. It also provides a signaling mechanism to update path-learning caches on the switches dynamically, and needs suppressing broadcast signaling traffic.

The Mobile Ethernet consists of Layer 2 switches, the Common Signaling Server (CSS) and Buffering Server. There are three types of Layer 2 switches called the Gateway Switch (GSW), the Branch Switch (BSW), and the Edge Switch (ESW). The GSW has the basic mobility functions, such as MAC address learning with exchanging Layer 2

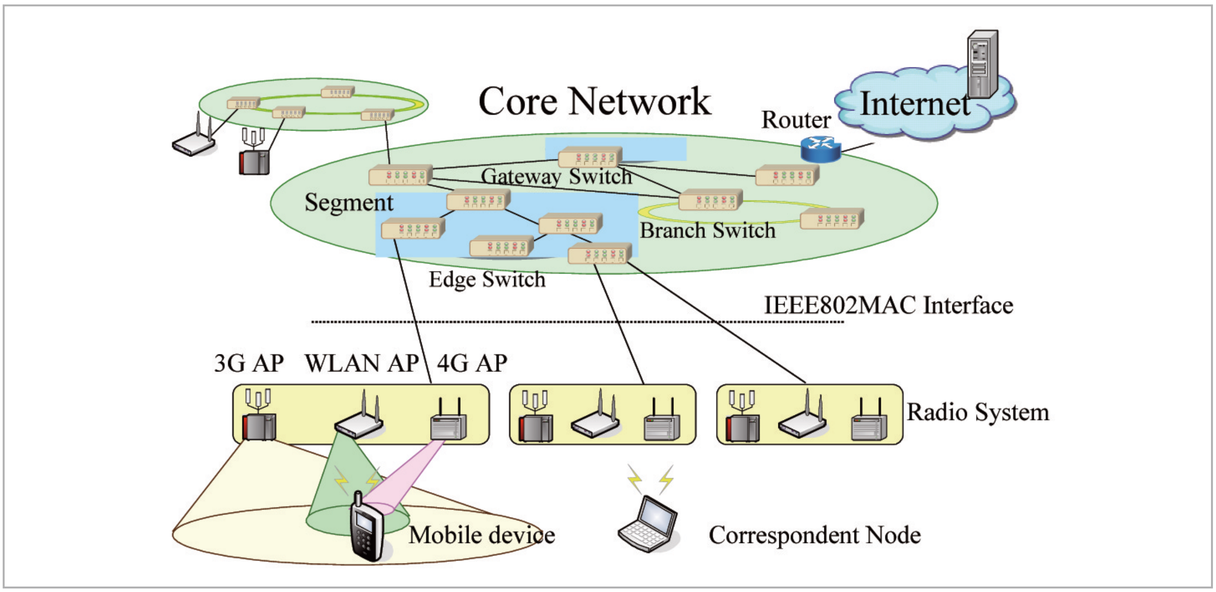


Fig.2 Mobile Ethernet

mobility management frames and IPv6 multicast traffic control without flooding, and interfaces for MAC address replacement and MAC address table setup to the Common Signaling Server. A BSW is the intermediate switch between a GSW and an ESW and has the basic mobility functions in it. An ESW manages MAC frame transfers, such as relaying common radio signaling messages between a mobile device and the CSS besides the basic functions.

The CSS manages messages to control mobile devices and radio systems. The server informs to a mobile device adjacent APs list for the network access point detection and mobility management instruction such as a handover request[18]. The mobile device, on the other hand, informs various common radio signaling messages, such as the Location Area Update message for mobility management in dormant mode[19] and measured received-signal strength information used for triggering in network initiated handover[20]. The Buffering Server keeps user data frames for paging mobile devices. The components and interfaces are shown in Fig. 3.

2.3 Future Mobile Ethernet

The Mobile Ethernet architecture described in the previous section defines all the components and specifications. Our experimental Mobile Ethernet system[21] consisting of different types radio systems, W-CDMA(3 G) and IEEE802.11b, verifies the common MAC interface and components for lossless and real-time handover.

The future Mobile Ethernet expects a Mobile Ethernet switch which is used as a GSW, a BSW, or an ESW and a CSS/Buffering server integrated somewhere in the network, once the specification and interface of each component is verified and standardized. The network also expects any access points at any location and provides wireless access to users anytime. The future Mobile Ethernet is expected to provide a ubiquitous wireless network independent of radio systems showed in Fig. 4.

In near future, a mobile device can configure its radio adjusting to available radio systems and services at a user location. The mobile device changes its radio from one to the other seamlessly and expects a unique address, such as IP address for efficient service continuity. The Mobile Ethernet has the feature not to change an IP address to access any radio systems.

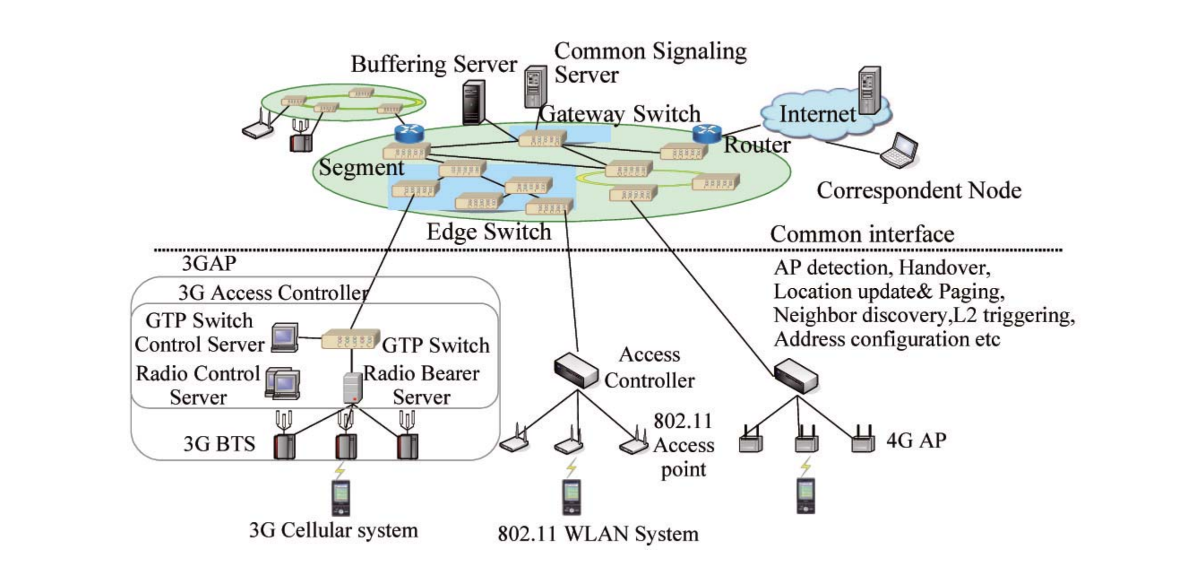


Fig.3 Components and Interfaces

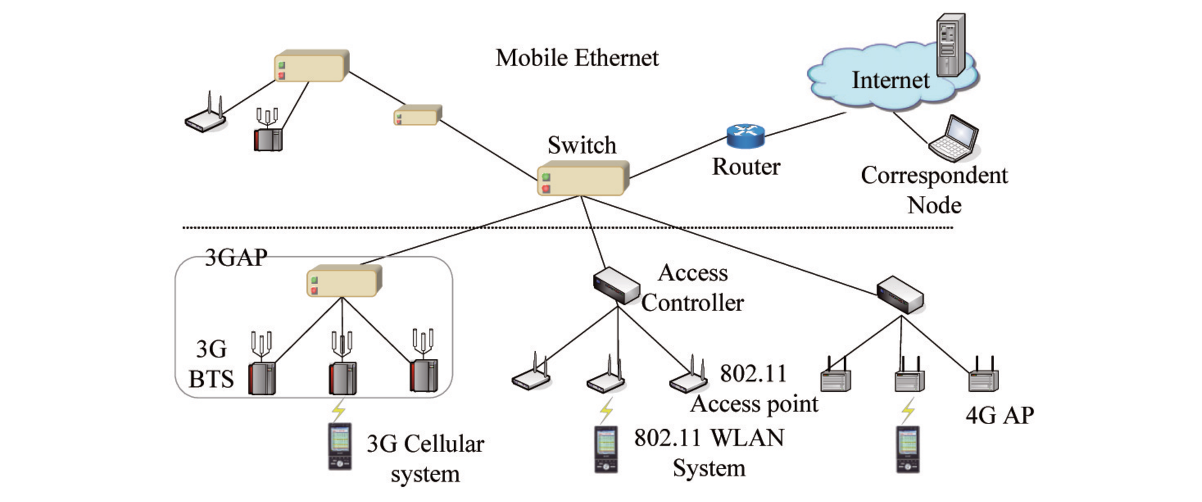


Fig.4 Future Mobile Ethernet

3 Mobile Ethernet security

The Mobile Ethernet allows a user to seamlessly handover from one radio system to the other along with the user movement. The user expects service continuation with no interruption, even in the case of real-time applications. Following section describes a framework for network access authentication which is consistently used with application level authentication and, then, discusses the vertical handover authentication.

3.1 Framework for network access authentication

We proposed the security framework for the Mobile Ethernet consisting of application level authentication, network access authentication, and the security link between the two authentications[22]. The framework expects that a user device is divided into two components, a personal identity card (PIC) securely storing any kind of certificates, such as wireless access/ISP certificates, and a mobile device holding the delegated certificates used for network access/application level authentications. It defines mutual authentication between the PIC and the mobile device with certificate activation in the PIC using biometrics or another method.

The application level authentication is mutual authentication between a mobile device having the delegated certificate and service providers, such as ISP. The network access authentication is also mutual authentication between the mobile device and wireless networks. The device authenticates a wireless network when it connects to it. The network also checks whether the device has the right to access it.

Figure 5 shows the framework to accommodate both application level and network access authentications.

3.2 Handover authentication and AAA

When a mobile device moves to a different radio system in the same segment (intra-segment handover), the device sends an Update Entry Request (UER) to the AP and goes up the hierarchy until the UER reaches the AAA server shown in Fig. 6. The network access

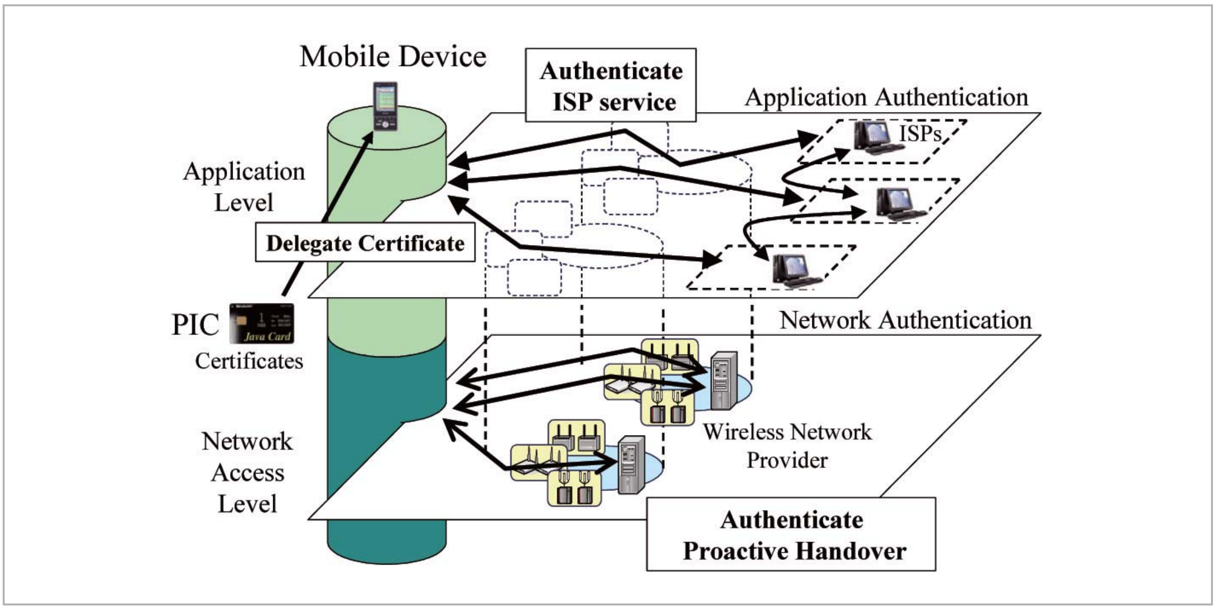


Fig.5 Application and Network Authentication Framework

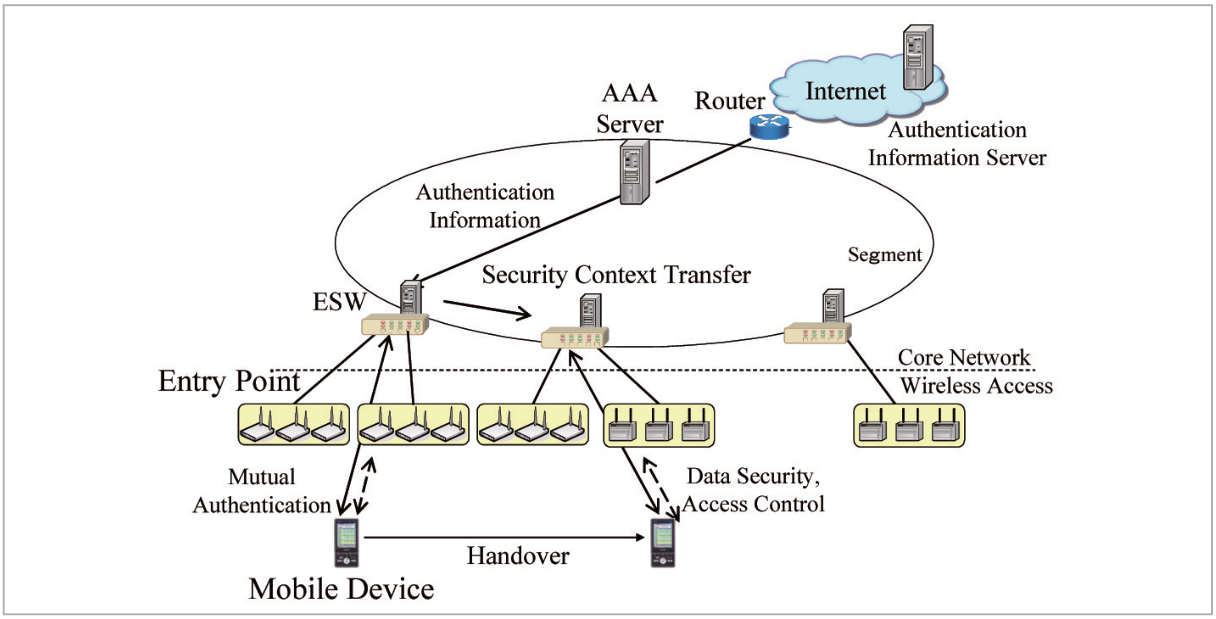


Fig.6 Proactive Network Access Authentication

authentication is done by a twoway handshake between the device and the AAA server. When the mobile device moves to a radio system in another segment, it goes up to the AAA server in the hierarchy.

In the case of handover, a real-time application expects authentication on the fly. The Mobile Ethernet expects proactive authentication taking advantage of the network initiated handover. The network knows which radio system is to be used when a mobile device moves out of current communication area. The network transfers the security context from the ESW where the mobile device in located to the new ESW and authenticate beforehand without sending a request in the future.

The authentication framework assumes many service providers, such as application and wireless access, and many users. In such system, if users authenticate by sharing a secret every time they moves, it requires heavy computation for users to do beforehand. It is preferable to employ a ticketgranting service and register each provider with each AAA server in a segment. The ticket-granting authentication is applied to ubiquitous environment assuming a PIC for each user for any services.

4 Wireless security toward ubiquitous network

There are two discussions in wireless security. One is to have a common mechanism to keep confidentiality among radio systems. The other is to provide functions to maintain availability.

The Mobile Ethernet expects to integrate various radio systems. Each radio system has its own authentication mechanism on it and some mechanisms are not consistent with others. We introduce a security key management utilizing location information of a mobile device[23] that is independent of radio systems. We, then, discuss functions to protect the wireless interface of the Mobile Ethernet from Denial of Server (DoS) attacks.

4.1 Radio independent authentication

In this section we describe a radio independent wireless security using location information that provides a lightweight authentication between a mobile device and the network[24].

(1) Location information as key material

In the mobile environment, location information is a candidate for authentication. The authentication uses the list of location of a mobile device as a shared context between a mobile device and the AP. The location of a mobile device changes in accordance with the user movement. The location is shared between the device and the AP when the user starts communication[25]-[27]. The list of location information, which is a kind of trail of the mobile device, is considered as a shared context between the two entities.

An AP of the network, whereas, compute the location of a mobile device by the signal strength[28] from the device. These locations are shared by transmitting between the device and the AP. Although it is coarser than that of the Global Positioning System (GPS), a unique ID of an AP at which the device is connecting is also seemed to be location of the mobile device. The location information shared between a mobile device and a network is utilized as a seed to generate a symmetric key between the mobile device and the AP that performs mutual authentication.

(2) Track: Shared location information

A track is a list of location information of a mobile device. The location information, for instance, is the ID of a radio system. Once a track is created, the list is updated separately on the mobile device and network, and kept consistent. The latest location, then, is inserted at the top of the list and the oldest one at the bottom is removed to keep the length required.

The track is used as a shared context for mutual authentication between a mobile device and the AP to solve the following issues: a) Eavesdropping and Prediction, b) Compromise and c) Confliction.

a) Eavesdropping and prediction

If there is an eavesdropper who sniffs any traffic of a mobile device at any place, an attacker can have the location information of the device. The attacker, however, hardly predict the entire track of the device from the location information which the eavesdropper has. If the strong enough key variation is 2128, the estimated minimum length of the track is greater than 40 and looks practical computation when implementing on a mobile device.

b) Compromise

The compromise of the track caused by its long-term use never happens because it is frequently changed along with the move of a mobile device. It is assumed that the mobile device is so robust that the track will not be disclosed by any physical attacks.

c) Confliction

There is a confliction in tracks such that a track of a mobile device is equivalent to that of the other devices The network avoids by detecting the likelihood of the confliction. It enables that, for instance, a user carries two mobile devices whose tracks don't conflict.

4.2 Untraceability

Wireless security is treated as the extension to the wired network security and focuses on access control and confidentiality, but the core feature of wireless network is availability. We expect security threats in its wireless part of the Mobile Ethernet that come from the openness of Ethernet frames in air. Contents in air are protected by the established cryptography, but contexts including headers are open in air. A malicious person can trace the MAC address of a mobile device and attack it. Untraceability of a mobile device becomes an important requirement for Denial of Service attacks, besides wireless jamming, wireless session hijacking, and wireless association flooding.

We have proposed the Transient MAC Address (TMAC) scheme which allows a mobile device to dynamically change its MAC addresses to escape from the tracing[29][30]. Only a mobile device and the AP to which the device is connecting can remember the transition of the MAC address, as the TMAC is updated by means of a one-way keyed hash function. An attacker, who does not acquire the TMAC key, cannot predict the next TMAC from the current TMAC.

5 Conclusion and future work

We explained the Mobile Ethernet architecture and its future direction from the viewpoint of 3 GPP and IEEE802 LMSC. We, also, described the Mobile Ethernet Security. We explained the security framework to accommodate both application and network authentications. We, then, talked about wireless security considerations. One is to have a common mechanism to keep confidentiality among radio systems. The other is to provide functions to maintain availability.

The wireless security discussion is still on the way and we need to study privacy issues for future ubiquitous wireless network.

Acknowledgements

We present special thanks to people of Mitsubishi Electric Corporation who supported the Mobile Ethernet development and to Prof. Wade Trappe who discussed the wireless DoS attack targeted for next generation wireless network.

References

1 H. Lach, C. Janneteau, and A. Petrescu, “Network Mobility in Beyond-3 G Systems”, IEEE Communication Magazine, pp.52-57, Jul. 2003.

2 H. Yumiba, K. Imai, and M. Yabusaki, “IP-Based IMT Network Platform”, IEEE Personal Communication Magazine, Vol.8, No.5, pp.18-23, Oct. 2001.

3 T. Otsu, I. Okajima, N. Umeda, and Y. Yamao, “Network Architecture for Mobile Communication Systems Beyond IMT-2000”, IEEE Personal Communication Magazine, Vol.8, No.5, pp.31-37, Oct. 2001.

4 http://www.3gpp.org/specs/specs.htm

5 http://www.ieee802.org/

6 http://www.ieee802.org/16/

7 http://www.ieee802.org/21/

8 H. Harada and R. Prasad, “Simulation and Software Radio for Mobile Communications”, Artech House, 2002.

9 D. Johnson, C. Perkins, and J. Arkko, “Mobility Support in IPv6”, Internet-Draft, draft-ietf-mobileip-ipv6-24.txt, Jun. 2003.

10 R. Koodli, “Fast Handovers for Mobile IPv6”,
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-fastmipv6-06.txt, Internet-Draft, Mar. 2003.

11 Hesham Soliman, Claude Castelluccia, Karim El-Malki, and Ludovic Bellier, “Hierarchical Mobile IPv6 mobility management (HMIPv6)”, Internet-Draft, draft-ietf-mipshophmipv6-00.txt, Jun. 2003.

12 “Combined GSM and Mobile IP Mobility Handling in UMTS IP CN”, 3 GPP TR23.923 V3.0.0

13 “All-IP Network (AIPN) feasibility study”, 3 GPP TR22.978 V7.0.0

14 Compendium of Abstract, 3 GPP TSG RAN Future Evolution Work Shop, 2-3 Nov. 2004, Toronto, Canada.

15 “Virtual Bridge Local Area Networks – Amendment 4: Provider Bridge”, IEEE P802.1ad/D2.0 Dec. 2003.

16 M. Kuroda, M. Inoue, A. Okubo, T. Sakakura, K. Shimizu, and F. Adachi, “Scalable Mobile Ethernet and Fast Vertical Handover”, IEEE Wireless Communications and Networking Conference (WCNC) 2004, Mar. 2004.

17 A. Okubo, M. Tsuzuki, Y. Hirano, K. Shimizu, and M. Kuroda, “Evaluation of Mobile Ethernet Switch on Network Processor”, Workshop on High Performance Switching and Routing (HPSR) 2004, Mar. 2004.

18 M. Kuroda, K. Ishizu, Y. Saito, and G. Miyamoto, “Empirical Evaluation of Real-Time Vertical Handover for Beyond 3 G Wireless Network”, WPMC’05, Sep. 2005.

19 Z. Lan and M. Kuroda, “A Load Balancing Proposal for Beyond 3 G Wireless Network”, WPMC’05, Sep. 2005.

20 Y. Saito, K. Ishizu, M. Kuroda, and T. Mizuno, “A Study of Media Independent Paging Mechanism for Beyond 3 G Wireless Network”, WPMC’05, Sep. 2005.

21 K. Ishizu, Y. Saito, and M. Kuroda, “Design of Media Independent Handover Interface for Beyond3 G Terminal”, WPMC’05, Sep. 2005.

22 M. Kuroda, M. Yoshida, and R. Ono, “Double Stuff Security for the Beyond 3 G Wireless Network”, WPMC’03, Oct. 2003.

23 R. Nomura, M. Kuroda, and D. Inoue, “Location-based Key Management for Ubiquitous Wireless Network”, WPMC’05, Sep. 2005.

24 M. Kuroda and R. Nomura, “Radio-independent Mobile Authentication Protocol for Ubiquitous Network”, WPMC’05, Sep. 2005.

25 I. F. Akyildiz, J. S.M. Ho, and Y. Lin, “Movement-Based Location Update and Selective Paging for PCS networks”, IEEE Personal Communication Magazine, Vol.8, No.5, pp.18-23, 2001.

26 J. Li, Y. Pan, and X. Jia, “Analysis of Dynamic Location Management for PCS Networks”, IEEE Trans. on Vehicular Technology, Vol.51, No.5, pp.1109-1119, 2002.

27 Y. Lin, “Reducing Location Update Cost in a PCS Network”, IEEE/ACM Trans. on Networking, 1997.

28 T. Aono, S. Tawara, T. Ohira, B. Komiyama, A. Kitaura, H. Mori, and H. Sasaoka., “Secret Common Key Generation Method Exploiting the Fluctuation of Communication Channels Using an Espar Antenna”, Proc. of the 2004 IEICE General Conference, 2004.

29 D. Inoue, R. Nomura, and M. Kuroda, “Transient MAC Address Scheme for Untraceability and DoS Attack Resiliency on Wireless Network”, WTS2004, Apr. 2004.

30 D. Inoue, M. Kuroda, and K. Ishizu, “FAST Transient MAC Address Scheme Based on Prearranged Update”, WPMC’05, Sep. 2005.

MIYAMOTO Goh

Researcher, Ubiquitous Mobile Communication Group, New Generation Wireless Communications Research Center

Wireless Communication

***KURODA Masahiro**, Ph.D.*

Senior Researcher, Ubiquitous Mobile Communication Group, New Generation Wireless Communications Research Center

Ubiquitous Mobile Network and its Wireless Security