IPSJ Journal Vol. 52 No. 3 953–967 (Mar. 2011)

Regular Paper

Radio-Free Mutual Authentication for Cognitive Radio Network

Ritsu Nomura,[†1] Masahiro Kuroda[†2] and Tadanori Mizuno[†3]

Cognitive radio (CR) technology has been offered to improve efficiency in bandwidth use and the quality of service (QoS) of heterogeneous wireless networks with varied types of radio systems. As the CR network system grows, network security has been raised as an area of concern. The topic has yet to be fully considered and no suitable authentication methods have been identified. In this paper, we propose a radio-free mutual authentication protocol for the CR network. The protocol, named EAP-CRP, adopts the location information of a mobile terminal as a shared secret for authentication. EAP-CRP has been designed to satisfy the requirements of wireless network security, confidentiality, integrity and availability, and is realized as a lightweight and quick-responding mutual authentication protocol.

1. Introduction

Cognitive radio (CR) technology has been developed as a solution to low usage of the radio spectrum. It is the key technology that enables flexible, efficient and reliable spectrum use by adapting the radio's operating characteristics to the real-time conditions of the environment. It can utilize the large amount of unused spectrum in an intelligent way while not interfering with other devices in frequency bands already licensed for specific uses.

IEEE 802.22 [1),2)] is a standard based on CR technology for the Wireless Regional Area Network (WRAN) using white spaces in the TV frequency spectrum for wireless broadband access in rural areas.

IEEE 1900.4 [3)] is a standard of CR network architecture. It was established to improve the overall, composite capacity and quality of service of wireless systems in a multiple radio access technologies environment. It also enables CR networks containing multiple network operators.

Figure 1 shows an architecture of CR for these standards [4)]. In order for CR technology to be successfully deployed and adopted, it is necessary to develop security solutions for cognitive radios that can address the following operations:

- Selection of the radio spectrum is promised by adaptive spectrum allocation policies even with the existence of malformed devices that conduct denial of service (DoS)/jamming attacks by monitoring the radio environment.
- CR components of a mobile terminal (MT) are correctly reconfigured by relying on the behavior of signal-processing units that monitor the environment and decisions based on spectrum allocation policies.
- Re-authentication is performed while the MT reconfigures itself to employ a different radio system when the MT moves from one radio access network (RAN) to another.

IEEE 802.22 prescribes a security sublayer with specifications inherited from the security sublayer of IEEE 802.16e [5)]. The sublayer provides a solution against DoS attacks by incorporating a message authentication scheme to prevent the existence of rogue MTs. IEEE 802.22 has a network-managed CR architecture with no negotiation or coordination between MTs and BSs. The architecture expects a scenario such that each BS controls the MTs it is serving, manages its use of spectra to avoid interference, and configures the modulation. Therefore there is no chance of illegal reconfiguration of CR components on MTs. The security manager of IEEE 802.22 incorporates an authentication scheme only between MT and a BS, but there is no feature for an authentication scheme between MT and BSs where the MT moves from one BS to another.

IEEE 1900.4 [3)] proposes a "network-managed and terminal helps" architecture that assumes the existence of network reconfiguration managers (NRMs) to decide the spectrum assignments and the terminal reconfiguration manager (TRM) to reconfigure the CR components of the MT in accordance with the decision of the NRM. Therefore, the solution for correct reconfiguration of CR components is provided if an authentication scheme between the TRM of an MT and the NRM has been prepared. There is no IEEE 1900.4-specific authentication

†1 Mitsubishi Electric Corporation
†2 National Institute of Information and Communications Technology
†3 Graduate School of Science & Technology, Shizuoka University

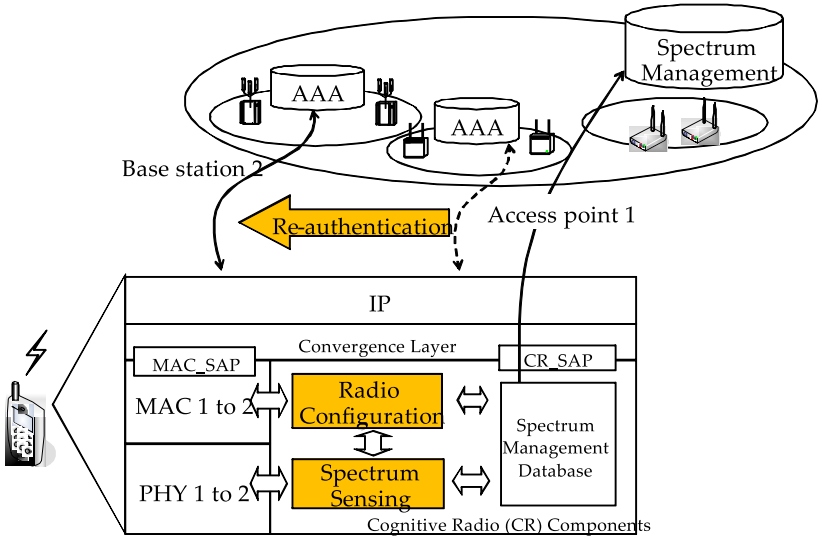

Fig. 1 Cognitive radio architecture.

scheme, so the IEEE 1900.4-based CR network system will apply some existing authentication schemes standardized for the existing radio systems incorporated in the CR network system.

The re-authentication process between an MT and a network in the CR system should be performed seamlessly to provide continuous communication, which is important for users. It will be even more critical in CR networks that are constructed with several types of RANs such as WiFi, WiMAX [6] and 3G because the authentication frameworks for various radio technologies, such as IEEE802.11 [7] and WiMAX [6]), substantially differ from one another. The heterogeneous authentication frameworks in a CR network make seamless communication difficult for users.

Almost all mutual authentication frameworks require any central AAA servers. This makes a long authentication process during re-configuration of the radio system because any queries are exchanged between an MT and the servers. These frameworks also incorporate a Public Key Infrastructure (PKI)-based authentication architecture. This requires a certificate verification and key exchange process that consumes the computing resources, such as CPU time, network traffic and electric power, of an MT. This causes not only communication delays but also shortens the lifetime of the MT's electric power.

Therefore a radio-free and lightweight authentication protocol for CR networks is required. This should be independent from several radio-specific authentication frameworks and should be a lightweight scheme to enable seamless communication and reduce use of the MT's computing resources.

This paper proposes the Carousel Rotating Protocol (CRP), a radio-free mutual authentication protocol for CR networks, and a re-authentication protocol based on it. These protocols are independent of the underlying radio protocols and can support EAP transport [8)–10)]. EAP-CRP, and EAP-CRP re-authentication, requires only a small amount of the MT's computing resources because it is based on pre-shared secret architecture. The re-keying protocol assumes user-specific information, such as location information, as a key seed. The keys for authentication and encryption are derived from the historical location registry, named a Trail, of an MT. The keys are frequently updated as mobile users' positions vary. Neither protocol assumes the existence of any central AAA servers.

The next section summarizes works concerning security issues of CR networks and authentication models for wireless networks. Section 3 shows the concept of the EAP-CRP and Section 4 describes the EAP-CRP and EAP-CRP re-authentication. Sections 5 and 6 explain the evaluations of the EAP-CRP, for which there are two main points. One is the evaluation of security requirements such as ensuring confidentiality, integrity and availability, shown in Section 5. The other is the performance evaluation of the EAP-CRP and EAP-CRP re-authentication, shown in Section 6.

2. Related Work

2.1 Security in CR Network

With a limited number of works, CR network security appears to be a relatively uncharted field.

The TRIESTE [11)] is a framework that provides assurance regarding the operation of a CR to protect against jamming from malformed MTs. It guarantees that a coalition of autonomous cognitive radios behaves according to acceptable com-

munal policies. It is composed of three tiers: a general-purpose cognitive radio layer, the Distributed Spectrum Authority (DSA) layer and the Spectrum Law Makers (SLM) layer. The SLM regulates the radio spectrum adaptive policies and the DSAs enforce regulation on the MTs.

Security vulnerabilities in IEEE 802.22 has been discussed [12], where several threats on CR, such as DoS, replay attack and so on were reported. Vulnerability is also described as being caused by the absence of protection of the channel among the BSs by which the CR system is constructed.

The Primary User Emulation (PUE) attack on CR networks has been discussed [13]. The PUE attack is that, an attacker may modify the air interface to transmit a signal in the licensed band emulating the primary user's real transmission. A transmitter verification scheme [14] is capable of detecting PUE attacks and pinpointing the attackers. CR components of an MT must be trusted to not provide incorrect sensing information/profiles and to avoid replacing with malformed components.

One solution for having a trusted platform is a concept lead by the Trusted Computing Group [15]. This group promotes enforcing the behavior of platforms in expected ways by loading the hardware with a unique encryption key inaccessible to the rest of the system.

2.2 Authentication Model for Wireless Network

This section describes several existing authentication models that serve as a basis for considering authentication frameworks for the CR network.

2.2.1 Pre-shared Secret Authentication

The 3G/GSM cellular system has its own security model based on a pre-shared secret key. The key is shared between a mobile device and the Home Location Register (HLR) [16]. The basic WLAN (IEEE802.11) [7] system also employs a shared-key authentication scheme. The pre-shared secret key framework requires less traffic in setting up secure communication between two entities than the server-centric model, described next, but it fails to require a mobile terminal to check whether the network is the right one to access. If the network expects protection from man-in-the-middle attacks, mutual authentication and heavy computation on the device is required.

EAP-SIM [17] is a pre-shared secret (contained on the SIM) authentication scheme that uses the EAP framework to achieve a SIM-based challenge/response authentication between an MT and an AAA server. EAP-AKA [18] can also be a pre-shared secret-based authentication scheme. It proposes a one-path challenge/response authentication between an MT and an authenticator.

Both EAP-SIM [17] and EAP-AKA [18] require an AAA server to protect the shared secret and respond with an authentication query from the MT via an access point (AP). It follows the long authentication process during re-configuration of the radio system because challenge/response messages are always exchanged between the MT and the server. When an MT moves from one network to the other, it re-configures the CR component and consults with the server to re-generate a key.

2.2.2 Server-centric Authentication

The server-centric model manages all authentication keys on a central authentication server. The IEEE802.11i [19] model does not assume there are any pre-shared keys. IEEE802.1X [20] accommodates various types of authentication via the operation of EAP with a central AAA server. EAP-TLS is a TLS-based extension of the EAP that requires a PKI-based certificate for both a mobile terminal and a network. The server-centric model provides authentication independent of a mobile terminal. However, it has drawbacks in terms of the amount of network traffic involved, as well as heavy computational requirements placed on mobile devices. CR-network traffic causes latency in the communications setup. PKI-based authentication requires heavy CPU usage on both the mobile device and the network.

WiMAX [6] also deploys a server-centric authentication mechanism that is also PKI-based authentication [21]. Mutual authentication is required to protect from attacks, but achieving such protection is expensive due to the use of a certificate on an MT.

2.2.3 EAP and its Key Hierarchy

The Extensible Authentication Protocol (EAP) started as a PPP extension and prevailed in many different scenarios, particularly in wireless network environments, where IP is not necessary over the access links. EAP is a powerful authentication framework that supports multiple and future authentication mechanisms, such as EAP-SIM, EAP-TLS and EAP-TTLS. EAP incorporates

a key hierarchy derived from a long-term credential shown in **Fig. 2**. EAP methods generate a Master Session Key (MSK). A Transient Session Key (TSK), derived from the MSK, is used for secure transmission between the MT and Authenticator (AU). The key hierarchy also contains an Extended Master Session Key (EMSK), which is generated at the same time as an MSK is created.

There is discussion on using the EMSK and the hierarchy based on the EMSK as a re-authentication key, named a Re-authentication Integrity Key (rIK), for handover [22]. The EAP-ER is proposed as the EAP efficient re-authentication protocol using the EMSK-based key hierarchy. However, it is difficult for the CR network, which requires a quick reconfiguration when an MT moves from one BS to another, to adopt the EAP-ER because the protocol needs a protocol overhead to acquire a re-authentication key (rRK) from the AAA server and the overhead lowers the QoS of the network.

3. Basic Concept

3.1 Location and Trail

Whenever an MT makes communication using a CR network system composed of several types of BSs, the MT connects to one of the BSs which its signal can reach. If there are several signal-reachable BSs, the connecting BS is chosen from the set of the signal-reachable ones by the assignment policies of the CR system.

The location of the MT is defined by the ID of the connecting BS. The location is changed due to the movement of the MT or the change of the connecting BSs by the assignment policies. Therefore the historical registry of the location chain, named a trail, is eventually updated according to the activity of the MT. The location and the trail can also be recorded by both the MT and the network system.

An MT's trail can be assumed to be different from that of any other MT. The trail, therefore, can be considered as a shared secret between the MT and the wireless network system.

3.2 Carousel and Its Synchronization

A carousel is a data structure that is a circular list of cells with each cell capable of containing location information regarding an MT's trail. A visual representation of a carousel (shared between two entities) is presented in **Fig. 3**, where the

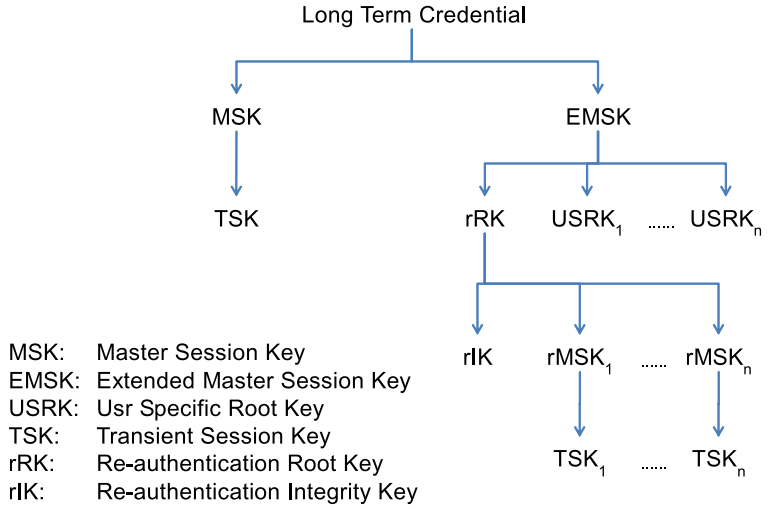

Fig. 2 EAP key hierarchy.

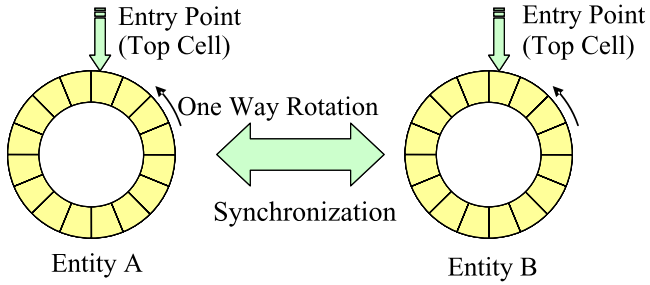

Fig. 3 Carousel and its synchronization.

"top" cell represents the entry point to the carousel. When new location information is entered into the carousel, it is placed into the entry point cell, and the carousel is rotated by a random number of cells. Any old location information stored in the entry point is overwritten by new information.

Both an MT and a wireless network system will share a carousel corresponding to the MT's trail. We use this carousel as a credential to establish a shared authentication key between the two entities. The key-generation function pro-

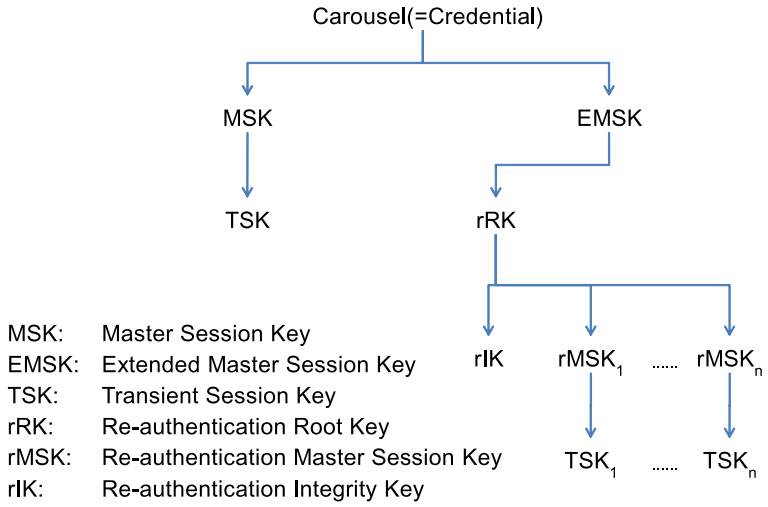

Fig. 4 EAP-CRP key hierarchy.

duces the same key independently of each carousel, as keys are created when new location information is placed in the carousel following the MT's movement.

Prior to establishing shared keys, the carousels need to be synchronized. Here, synchronization refers to arranging both carousels so their cells are in the same order. Clearly, as the MT's carousel rotates, and location information is written to the entry cell, the two carousels become unsynchronized, thus requiring resynchronization.

Resynchronization is a process by which the second entity rotates its carousel to the same configuration as the first entity. During resynchronization, the first entity generates an authentication key from the carousel and sends a challenge to the second. The second entity generates a key by rotating the carousel, attempts to decode the challenge, and continues to rotate until decoding is successful. Upon successful decoding, the second entity responds to the first. We note that keys derived from synchronized carousels will support mutual authentication. EAP-CRP is the protocol for the resynchronization of carousels between two entities.

3.3 Key Hierarchy of EAP-CRP

Figure 4 shows the EAP-CRP key hierarchy, which is based on that of the EAP shown in Fig. 2.

The MT carousel is adopted as the credential of the key hierarchy. However, the carousel does not appear be long-term because it has been periodically changed with the movement of the MT. The MSK is created after the synchronization of the carousel between the MT and the network system. The TSK is used for making the channel secure. The EMSK is a root of the hierarchy of keys for re-authentication between the MT and the authenticator.

4. Carousel Rotating Protocol

This section describes the EAP-based carousel rotating protocol (EAP-CRP) that uses the carousel for mutual authentication and the EAP-CRP re-authentication protocol that enables re-authentication without consulting an AAA server.

4.1 Initial Carousel Setup

The initial setup of a carousel between an MT and the network should be performed during an initial setting process when the MT subscribes to a network operator. The initial setting process should be performed via wired connection and by using several network security methods, which has been established as a secure means of protecting against adversaries.

4.2 Location-converting Function

Both an MT and the network system have a hash function for converting the location information to a value. The cells in the carousel store the hashed value L calculated by the function $L = HASH(Loc, R)$, where Loc is a location and R is a random value passed by the EAP-CRP. This function is useful for protecting against issues such as carousel disclosure, authenticating immobile devices and privacy of the mobile user.

4.3 EAP-CRP Protocol

This section describes EAP-CRP shown in **Fig. 5**. The BSn has the role of authenticator of the network system. There is a location registry (LR) to manage the carousel of an MT either by holding its data or by the link to an authenticator having the data. It is assumed that a secure communication path is established

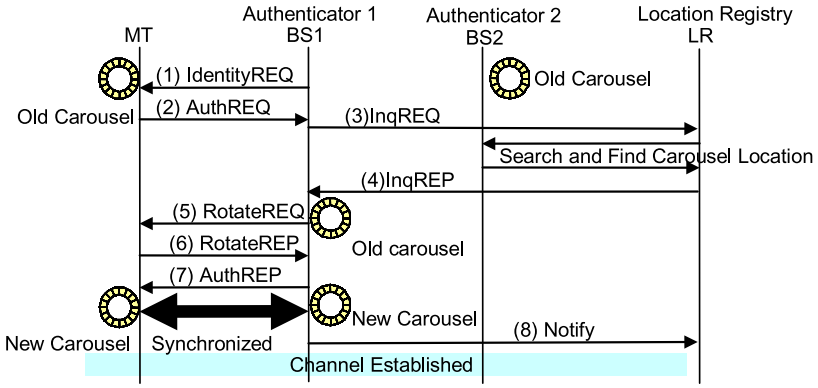

Fig. 5 EAP-CRP protocol.

between the nodes, such as BSn and LR.

The protocol between an MT and BS1 is as follows:

1) BS1 → MT: IdentityREQ()
   IdentityREQ() is sent from an BS1 to MT.
2) MT → BS1: AuthREQ (ID_{MT})
   MT responds to the identity request with its identity information (ID). It then triggers mutual authentication between MT and the network using carousels. BS1 → LR: InqREQ (ID_{MT})
3) BS1 asks for the carousel of MT with ID to the LR. LR acquires this from other authenticators if it does not have the carousel.
4) LR → BS1: InqREP (ID_{MT}, CR_{MT})
   LR responds to BS1 with the carousel.
5) BS1 → MT: RotateREQ($\{R_1||MAC_1\}_{K_N}$)
   BS1 generates an authentication key K_N from the carousel and sends a challenge to MT. R_1 is a random value and MAC_1 is a message authentication code derived from it.
   A) Undergoes a random carousel rotation
   B) Derives an authentication key K_N from the carousel
   C) Encrypts $\{R_1||MAC_1\}$ by K_N
6) MT → BS1: RotateREP($\{R_1||\ R_2||\ MAC_2\}_{K_M}$)
   MT decodes the cipher message by an authentication key generated by the carousel. If the decode fails, MT rotates the carousel once and decodes the message until it succeed. MT then replies back to BS1 with the corresponding cipher message encoded by the authentication key that is successfully decoded. MAC_2 is a message authentication code derived from R_2.
   A) Undergoes one-step carousel rotation
   B) Derives an authentication key from the carousel
   C) Decrypts the received cipher message by the key
   D) When the authentication by MAC_1 succeeds, MT obtains R_1 from the message and stores L = HASH (location, R_1) into the carousel entry.
   E) Derives an authentication key K_M' from the carousel
   F) Encrypt $\{R_1||R_2||MAC_2\}$ by K_M'
7) BS1 → MT: AuthREP($\{R_2||\ MAC_2\}K_N'$)
   BS1 decodes the received cipher message by inserting MT's new location information into the carousel, and then replies back to MT for authentication success. Mutual authentication succeeds by this message exchange.
   A) Stores L = HASH (location, R_1) in the carousel entry
   B) Derives an authentication key K_N' from the carousel and decrypts the received cipher message with key K_N'
   C) Encrypt $\{R_2||\ MAC_2\}$ by K_N'
8) BS1 → LR: Notify (ID_{MT}, location)
   BS1 notifies LR of the carousel location of MT.

MT and BS1 succeed in mutual authentication and each side generates MSK and EMSK from the carousel and uses the keys for communication across the secure channel.

4.4 EAP-CRP Re-authentication

The details for EAP-CRP re-authentication shown in **Fig. 6** are as follows:

9) BS2 → MT: IdentityREQ()
   IdentityREQ() is sent from BS2 to MT.
10) MT → BS2: ReAuthREQ($\{R_3||\ ID_{BS1}\}$rIK)
    MT triggers re-authentication to BS2 using a message containing the name of the re-authentication integrity key rIK which is created when the first

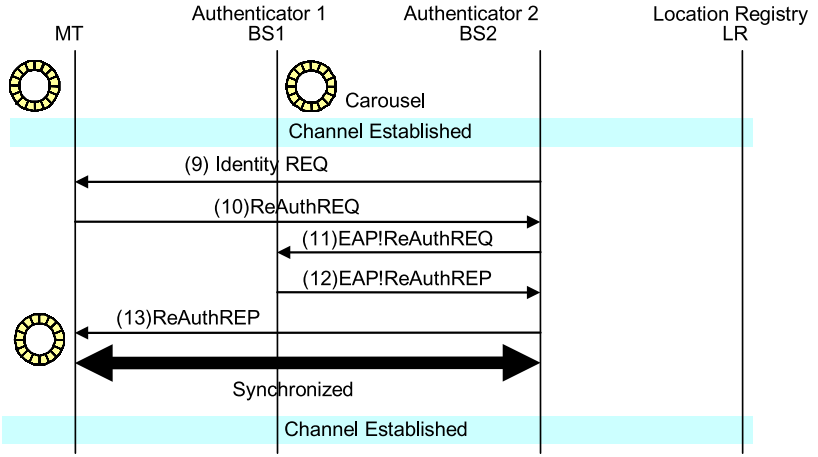

Fig. 6 EAP-CRP re-authentication protocol.

mutual authentication was established between MT and BS1. The rIK key is used for integrity protection.

11) BS2 → BS1: EAP!ReAuthREQ($\{R_3||\ ID_{BS1}\}$rIK)
BS2 follows the authentication protocol with BS1. BS2 sends a challenge to BS1.

12) BS1 → BS2: EAP!ReAuthREP($\{R_3||R_4\}$rIK, rMSK)
BS1 receives a re-authentication challenge and responds with the message $\{R_3||R_4\}$rIK and rMSK.

13) BS2 → MT: ReAuthREP($\{R_3||R_4\}$rIK)
BS2 sends the message $\{R_3||R_4\}$rIK to MT. After the protocol finishes, both the BS2 and MT have the same rMSK and the secure channel has been established by using rMSK.

5. Evaluation of Wireless Security Requirements of EAP-CRP

The NIST-SP 800-48 [23] shows the potential threats and attacks in wireless networks. It also shows that the prime objectives of the security practice are ensuring confidentiality, integrity and availability of the network system. This section describes how to ensure the requirements.

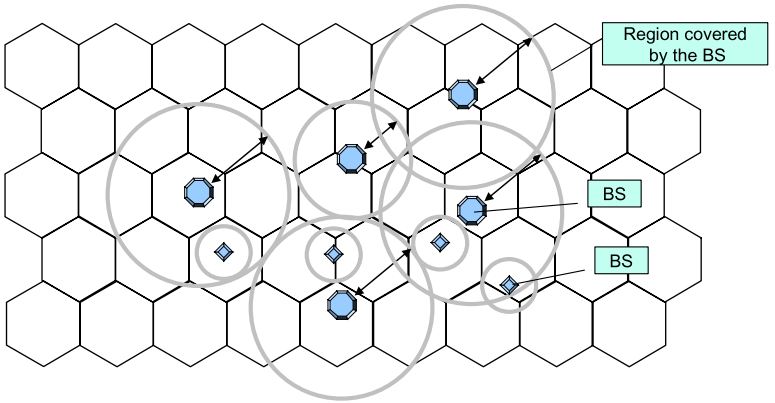

Fig. 7 Model of CR network area.

5.1 Confidentiality of EAP-CRP

Confidentiality is the property by which information is not made available or disclosed to unauthorized entities. The confidentiality of EAP-CRP is based on the difficulty that an adversary is faced with when attempting to reproduce an equivalent carousel. There are two steps for reproducing the carousel. First, an adversary tries to acquire a trail of a target MT by methods such as inferring the trail or tracing after the target MT to monitor the location. If the adversary succeeds in having the trail of the target MT, it tries to produce an equivalent carousel of the target from that trail.

The following sections describe the complexity of each of the steps.

5.1.1 Trail Complexity

This section describes the difficulty an adversary faces in inferring the trail of an MT.

1) Location Model

We assume a model of the area covered by a CR network system. The model is filled with hexagons, each of which has the same size. There are several types of BSs, such as 3G, WLAN and PAN, constructing the CR network system in the area, and each BS has its own signal-covering region whose size depends on the type of BS (**Fig. 7**). There may be several regions overlapped on a hexagon.

The RS(H) means a set of BSs whose region overlaps the hexagon H. The

density, noted as $Density(H)$, of the hexagon is defined as the number of BSs on which an MT can connect at hexagon H.

The trail of the MT is defined as:

$Trail_{\mathrm{MT}} \equiv rs_n \| rs_{n-1} \| \cdots \| rs_1 \qquad$ where $rs_i \in RS(H_i)$

The H_i is the hexagon where the MT makes communication using the CR network. When an adversary tries to infer the trail of the MT, it has to know the H_i where the MT was when the MT made the communication and the rs_i to which the MT was connected at that time. The difficulty in identifying the next H depends on the number of choices of hexagon where the MT makes communication, and depends on the activity of the MT owner. The difficulty in knowing the rsi depends on the density of H_i.

The next two sections discuss the arithmetic approach to quantifying both difficulties.

2) Choice of Hexagons

The choice of hexagon is the measurement of the number of hexagons where the next communication was made by an MT. This is derived from the relation of the speed of the user of the MT and the interval between two communications using the MT. The relation, named call-to-mobility-ratio ρ, is defined as:

$$\rho = \frac{\lambda_c}{\lambda_m}$$

where λ_c is the interval time between two communications and λ_m is the interval time between the first communication and the time when the user moves out of the hexagon.

The probability distribution function that an MT crosses the K hexagons between two communications is as follows [24]:

$$\propto (\mathrm{K}) \begin{cases} 1 - \dfrac{1 - f_m^*(\lambda_c)}{\rho} & \mathrm{K} = 0 \\ \dfrac{1}{\rho}[1 - f_m^*(\lambda_c)]^2 [f_m^*(\lambda_c)]^{\mathrm{K}-1} & \mathrm{K} > 0 \end{cases}$$

The fm described above is the density function of the period of the residence in a hexagon. Therefore, the expectation K' of the number of hexagons that the mobile device crosses between two communications is:

$$K' = \left\lceil \sum_{k=0}^{K} \alpha(k)\, k \right\rceil$$

Finally, the expectation of the choice of hexagons within the K' crossings is the number of hexagons where the user resides within K' steps. The number, which is the choice of hexagons, is defined as $N(K')$, such as:

$$N(K') = \sum_{i=1}^{K'} 6i + 1$$

3) Density of a hexagon

The density of a hexagon is the measurement of the number of BSs in a hexagon. A region S_i covered by a BS is as follows:

$S_i = \pi r_i^2 \qquad$ where r_i is a radius of an area $rs_i \in RS(H)$

The density of H is defined as follows:

$$Density(H) = \frac{1}{S}\sum_{i=1}^{n} S_i = \frac{1}{S}\sum_{i=1}^{n} \pi r_i^2 \qquad \text{where } n = |RS(H)|$$

The real $RS(H)$ is affected by the physical layout of BSs. In this paper, therefore, we suppose the mean of the density of all hexagons, such that:

$$E(H) = \frac{1}{n}\sum_{i=1}^{n} Density(H_i)$$

4) Result of Trail Complexity

The trail complexity, noted as TC, is defined as follows:

$TC = (N(K') \cdot E(H))^n \qquad$ where n is the length of the trail

5) Evaluation of Protecting Trail

The $N(K')$ depends on the value of ρ and V, a variance of the speed of the movement of an MT. We assumed that the speed is distributed according to the gamma-distribution to simplify the calculation. **Table 1** shows the $N(K')$ according to the ρ and the variance V.

Figure 8 shows the relation between the trail length and the trail complexity of the case shown in Table 1, where the $E(H)$ would be 1, which indicates a simple wireless network system. Even in case 1 or 2, which are slow user models,

Table 1 Ratio, variance and choice of hexagons.

	ρ	V	$N(K')$
Case 1	1	$10/\lambda_m^2$	7
Case 2	1	$1/\lambda_m^2$	7
Case 3	5	$10/\lambda_m^2$	19

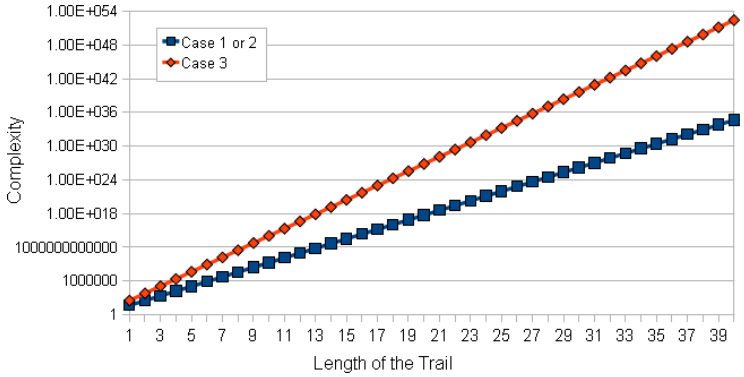

Fig. 8 Trail complexity.

the key management can take high confidentiality even if the trail is short.

5.2 Carousel Complexity

1) Model and Result of Carousel Complexity

This section describes the difficulty of reproducing a carousel. Assume that an adversary succeeds in identifying the trail of the target MT by using any of the attacks described above. Due to the uncertainty of the initial random bits, the adversary cannot construct the same carousel unless every cell of the carousel is overwritten by location information. Therefore we have to consider a case in which the adversary is trying to build the carousel after $m(>= n)$ rounds of movement (where n is the carousel length).

We define carousel complexity, CC_n^m, as the number of assignments of location information entered into the carousel such that all n cells in the carousel would be overwritten by location information after m rounds of movement. Carousel complexity is the complement of the set, PS, which describes cases where at least one cell of the carousel would keep its initial random bits. Lastly, we define US to be the set of every potential case of assigned information. The US contains n^m assignments. We may consider PS to also be the union of the sets, PS_i, where PS_i is the set of assignments such that only i cells maintain the initial bits. Obviously, $i < n$. Therefore, we can define the following:

$$CC_n^m = n^m - \sum_{i=1}^{n-1} \binom{n}{i} CC_{n-i}^m$$

$\binom{n}{i}$ means the combination of i cells that retain the initial random bits. Clearly:

$$CC_2^m = 2^m - 2$$

The probability, PR_n^m, that all n cells in the carousel will be overwritten by location information within m rounds of movement is defined as:

$$PR_n^m = \frac{CC_n^m}{n^m}$$

2) Evaluation of Protecting Carousel

Figure 9 shows the carousel complexity according to the length n of the carousel and the number of rounds m of rotation. And **Fig. 10** plots the probability that all cells of a carousel are filled with location information after m rounds of user movements.

Figure 10 shows that it is probable that the carousel contains unpredictable random bits if it is long enough. It means that an adversary cannot reproduce the carousel even if it has long rounds of trail of the target MT.

Additionally, Fig. 9 shows that if the carousel of the MT is long enough, the carousel is well-protected even though the adversary has a very long trail by tracing and monitoring the target MT.

5.2.1 Estimating Sufficient Length of Carousel

In this section, we estimate the length of carousel that would be sufficient to protect against a carousel-reproducing attack.

Our target confidentiality level is 2^{128} because 128 is currently recognized as the length of a sufficiently strong key for the current generation of symmetric

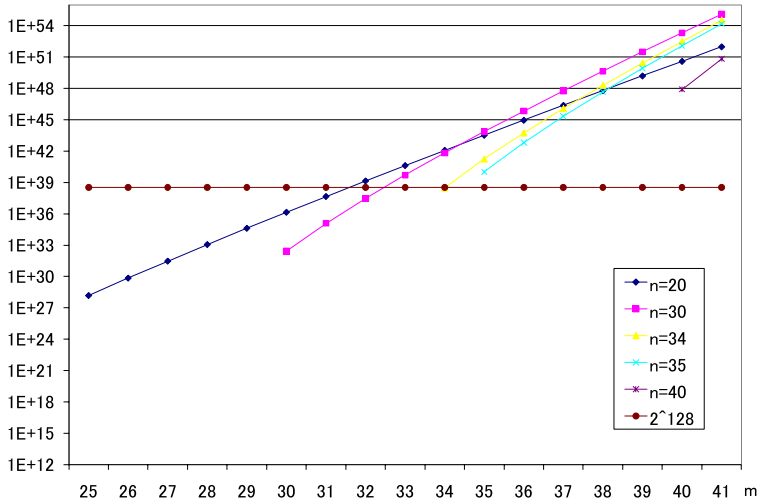

Fig. 9 Carousel complexity.

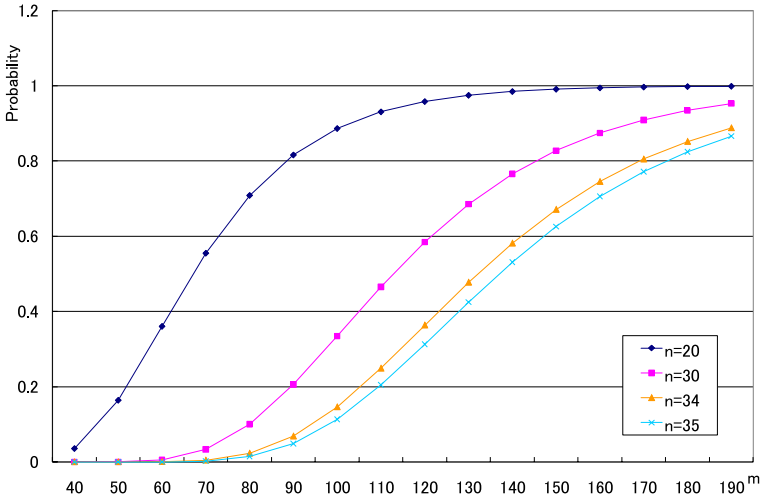

Fig. 10 Probability of case that carousel is filled with location.

ciphers. Using our derivations outlined earlier, we have assessed that a carousel containing at least 35 cells is sufficient for providing our target level of security, as shown in Fig. 9.

Figure 10 shows the probability in the case of n = 35. This means that an adversary needs to move along with a mobile user more than 190 ($\gg n$) rounds to have the same location information in the carousel. We can conclude that it is difficult for an adversary to duplicate a carousel both when m is small ($m < 35$) and also when m is large ($m >= 35$).

The length $n = 35$ affects the performance evaluation of the EAP-CRP.

5.3 Integrity of EAP-CRP

Integrity is the property with which a message is not modified or corrupted in transit between an MT and a network system. The integrity of the EAP-CRP depends on the difficulty of cracking messages between the MT and a BS. If the MT and BS cannot connect directly with each other, the malicious device deployed by an adversary can intrude between them and crack messages passed to each other, which is called a man-in-the-middle attack.

We assume that the malicious device cannot know the carousel of the legal device. Though the malicious device may try to modify the messages of the EAP-CRP, the MT and the BS can detect modified messages because the messages are encrypted with a message authentication code (MAC). Therefore, the MT and the BS can drop these modified messages to protect the EAP-CRP.

Additionally, though the malicious device may illegally drop the EAP-CRP messages, the legal device and legal BS can keep synchronization such as:

1. Even if the malicious device drops AuthREQ(), RotateREQ() or RotateREP() message, both the MT and the BS can stop the authentication process. The carousel synchronization will be protected because the old carousel will be kept.
2. Even if the malicious device drops AuthREP() message, both the MT and the BS have finished synchronization of the carousel. Both may confirm the synchronization by passing messages.

5.4 Availability of EAP-CRP

Availability is the property of being accessible and usable upon demand by an authorized entity. A denial of network availability of the EAP-CRP arises from

corrupting carousel synchronization. An adversary may deploy a fake device of a target MT starting the illegal authentication request. It may also deploy a fake BS that sends illegal reply messages to the target MT that tries to authenticate. These kinds of malicious device attacks will fail unless the device has a correct carousel of the target MT. An adversary may deploy a malicious device that tries a man-in-the-middle attack, and a device deployed between the MT and BS may illegally stop relaying the EAP-CRP messages. Section 5.2 describes the protection against corrupting carousel synchronization by the attack.

A replay attack is a method by which an adversary tries to be in disguise as the MT by re-sending a correct sequence of messages. By the man-in-the-middle attack described above, the malicious device can sniff correct messages and stop relaying messages. The malicious device can send the sniffed messages to the target MT. However, when it sends the RotateREP() message, the BS will drop the message because it does not contain a random value R1 created by the target MT at each authentication process and passed to the BS via RotateREQ() message. Therefore the replay attacks from the malicious devices always fail.

6. Evaluation of Performance of EAP-CRP

Performance evaluation of the EAP-CRP was conducted by focusing on the relative difference between the results of experiments performed by using prototype implementation or network simulation software.

6.1 Prototype Environment

Evaluation was made on platforms as follows:

- Mobile Terminal
  CPU: Intel Centrino, 1.7 GHz
  OS: Ubuntu 9.01
- BS (Authenticator)
  CPU: Intel Core 2 Duo
  OS: Ubuntu 9.01

We built a prototype implementation of the EAP-CRP. Cipher algorithms adopted on the implementation are as follows:

- Encrypt/Decrypt of packet
  AES-CBC128
- Message digest function for key generation
  SHA-1

The EAP-CRP implementation links with the commonly used OpenSSL crypto library.

For the experiment, the length of carousel n is set to 35, as described in Section 5.1.3.

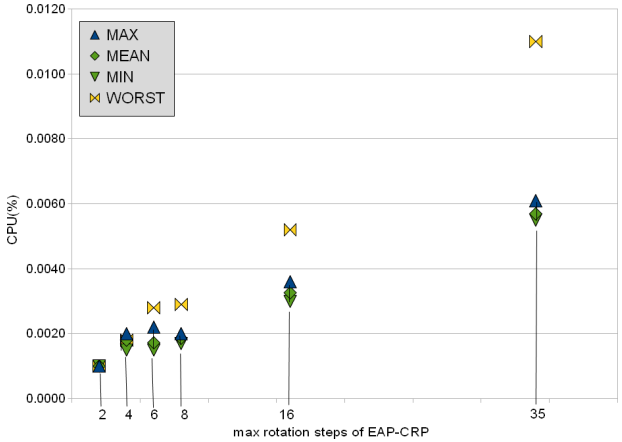

Fig. 11 CPU usage of MT for EAP-CRP.

6.2 CPU Usage on Mobile Terminal

This section shows the results of an examination of CPU usage on an MT when the EAP-CRP is executed between the MT and a BS. The CPU usage of the MT depends on the times of carousel rotation at 6), in Section 4.3.

Figure 11 shows the relation between CPU usage and the times of rotation of the carousel of an MT. Each vertical line and corresponding symbol plots the CPU usage on the MT when the respective times of rotation are up to 2, 4, 8, 16 and 35. The symbols MEAN, MIN and MAX respectively specify the mean, maximum and minimum of the result of 10 examinations. WORST shows the CPU usage for which the times of rotation are always the same as the upper bound; i.e., 2, 4, 6, 8, 16 and 35. **Figure 12** appends the CPU usage of EAP-

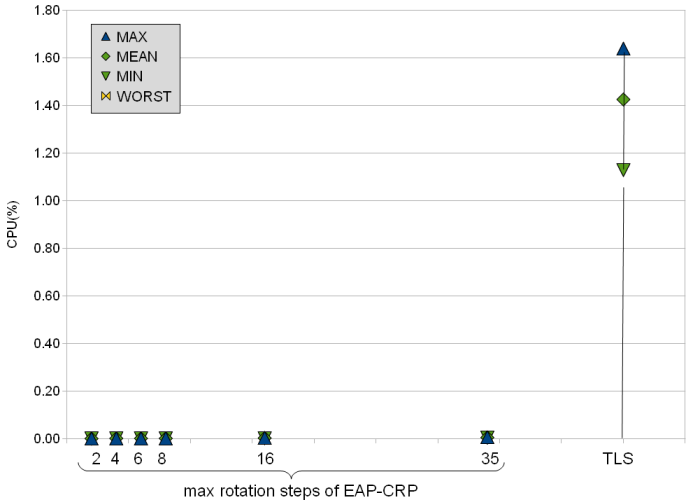

Fig. 12 CPU usage of MT for EAP-CRP and TLS.

TLS to that of EAP-CRP in Fig. 11. The value of the CPU usage of EAP-TLS differs widely from that of EAP-CRP. If the MT adopts a low-performance CPU, the CPU usage of EAP-TLS will be scaled up and the TLS process will place pressure on total the performance of the MT. In contrast, EAP-CRP will not affect the performance of the MT even if it mounts a low-power CPU. And the EAP-CRP requires such a small amount of CPU usage that it helps to save the electric power of the MT.

6.3 Response Time of Authentication

This section shows the results of an evaluation of the response time of EAP-CRP. **Figure 13** shows the set of the elapsed times caused by 20 trials of the program. The elapsed times of the TLS examined by a TLS evaluating program are also shown in **Fig. 14** for comparison. The TLS evaluating program performs mutual authentication that requires both the server certificate and client certificate.

There are three types of values in Figs. 13 and 14, "Real" shows the response time for accomplishing authentication by each protocol. "User" shows the time elapsed on an authentication program running in a user mode. "Sys" shows the

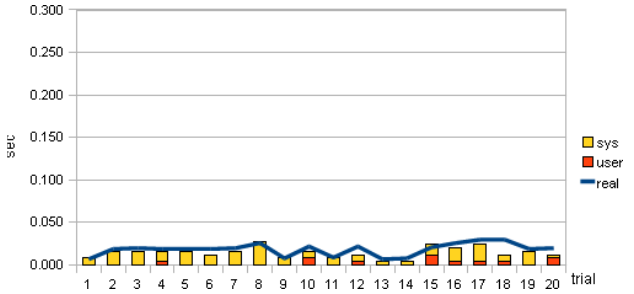

Fig. 13 Response time of EAP-CRP.

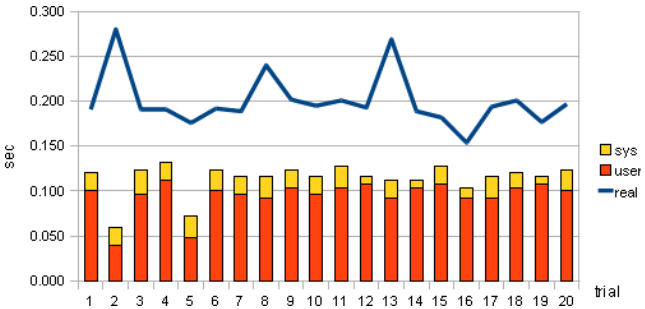

Fig. 14 Response time of TLS.

time elapsed in a kernel mode such as system call operations. The time, the difference between Real and the sum of User and Sys, is the time during whch the evaluation program had stopped being caused by blocking I/O, preemption and so on, called a "blocked" time hereinafter.

Table 2 shows the means of each value. The sys times of EAP-CRP and TLS are almost the same. This means there is no difference regarding the kernel mode operation between EAP-CRP and TLS.

The EAP-CRP "user" time is fairly negligible and that of the TLS is relatively large. This is because the TLS requires a server authentication process on an MT using the server certificate sent from a BS. The process is a PKI-based execution composed by complex formulas. On the contrary, EAP-CRP is shared-key-based mutual authentication process which uses only a lightweight cipher algorithm

Table 2 Means of times (sec).

	Real	Sys	User	blocked
CRP	0.018	0.012	0.002	0.004
TLS	0.190	0.018	0.090	0.083

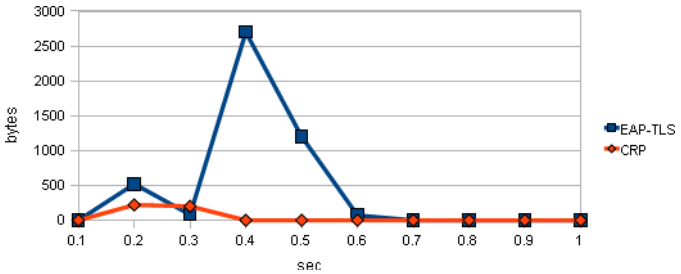

Fig. 15 Data transfer between MT and BS.

and message-digest algorithm.

The "blocked" time of the TLS also is larger than that of EAP-CRP. One of the reasons for the blocking is that the MT waits for receiving packets via a wireless network from the BS during authentication. The TLS requires heavy message passing during the authentication phase. On the contrary, EAP-CRP requires less traffic on wireless networks when the authentication took place between the MT and the BS. **Figure 15** shows that the bytes of packets transferred during the authentication phase of EAP-CRP and TLS.

In total, the "real" time of EAP-CRP is much smaller than that of the TLS because of the lower amount of messages passed and the non-requirement of the PKI algorithms. Therefore EAP-CRP makes a quick response for mutual authentication.

6.4 Response Time of Re-authentication

In earlier work, we reported that the EAP-CRP re-authentication protocol works well during the handover of an MT between two BSs [25].

This section describes the evaluation of the EAP-CRP re-authentication protocol compared to EAP-ER [22].

Suppose that an MT has been communicating on the CR network using BS1.

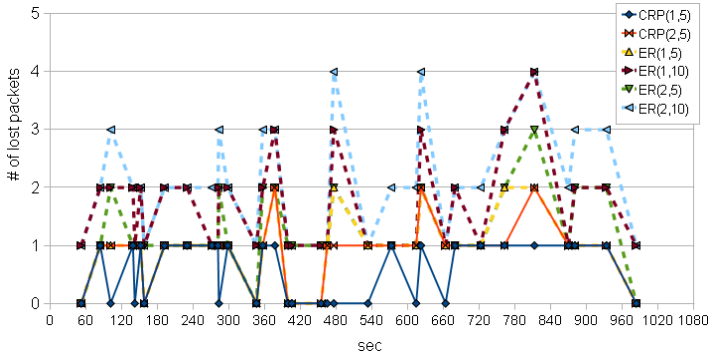

Fig. 16 Packet loss during re-authentication.

When the MT decides to switch over BS2 from BS1 due to reasons such as a lost of signal of the BS1 due to moving of the MT, the MT must re-configure itself as quickly as possible to maintain the QoS of the communication channel between the MT and the CR network. Slow-responding re-authentication is one of the obstacles of the re-configuration process.

We evaluate the decline of QoS of a VoIP application program on the wireless network during the re-authentication process. The VoIP application program transfers packets that contain the modulated audio by using an audio codec such as G.711 [26] or G.729 [27]. The packets are transferred every 25 milliseconds on RTP to maintain the quality of the audio communication.

Figure 16 shows the number of missing packets of the VoIP application disturbed by the re-authentication process. The solid line indicates the lost packets caused by the EAP-CRP re-authentication. The dashed line means the lost packets caused by the EAP-ER re-authentication [22]. Symbols such as the triangle and diamond indicate when the re-authentication occurred. The name of each line, such as CRP (x, y) and ER (x, y), represents the type of protocol. The x means the assumption of response time, in milliseconds, of short-range transmission, such as between BS1 and BS2, and the y indicates a query to an AAA server that is necessary on the EAP-ER.

As shown in Fig. 16, the EAP-CRP re-authentication drops a smaller amount of application packets than the EAP-ER. This is because the EAP-CRP re-

authentication processes a re-authentication query in a short period of time rather than re-authentication methods that require AAA servers such as EAP-ER. Our assumption based on the evaluation is that the response time of the AAA server will not be less than 5 milliseconds because the AAA server, which is a trust anchor of the wireless network system security, will be centered on the network system.

As a result, the EAP-CRP maintains the QoS of communication better than the EAP-ER. This is true unless the AAA server responds as quickly as the short-range transmission.

7. Conclusion

In this paper, we proposed EAP-CRP as a radio-free mutual authentication method. EAP-CRP and EAP-CRP re-authentication achieve a mutual authentication protocol for the CR network system for the following reasons:

1. EAP-CRP is independent architecture for any radio system. There is no need to implement several authentication methods on an MT to support the heterogeneous CR system.
2. EAP-CRP is lightweight because it requires little CPU usage on the MT and a lower number of packet transmissions.
3. EAP-CRP and EAP-CRP re-authentication perform the authentication process quickly so that it does not degrade the QoS of the CR system.

We explained that the EAP-CRP is fully confidential because it is difficult for an adversary to reproduces an MT carousel if the carousel is long enough. We estimated that the carousel length should be greater than 35. EAP-CRP also obtains the integrity and availability of the wireless network security.

The first step of the CR system anticipates already-deployed wireless networks such as 3G and WiFi and focuses on the handover between them. The re-authentication procedure of the CR system is designed to follow legacy wireless system methods. The next-generation CR system, which is designed not only for the handover but also changing the spectrum/radio system in a short period of time, will not be allowed to adopt a long authentication process. EAP-CRP enables a short authentication process and will fit the authentication method of the next-generation CR. Therefore we are planning to make EAP-CRP a standard authentication method for the CR system, such as by proposing it to the Internet Engineering Task Force (IETF).

References

1) IEEE 802.22, (online), available from ⟨http://www.ieee802.org/22/⟩.
2) Cordeiro, C., Challapali, K., Birru, D. and Shankar, S.N.: IEEE 802.22: The first worldwide wireless standard based on cognitive radios, *Proc. IEEE International Symposium, New Frontiers Dynamic Spectrum Access Networks* (2005).
3) IEEE1900.4, (online), available from ⟨http://grouper.ieee.org/groups/scc41/4/index.htm⟩.
4) Kuroda, M., Ishizu, K. and Harada, H.: A study of Radio Information Service for Networks of Cognitive Radios, *Proc. IEEE Workshop on Networking Technologies for Software Defined Radio* (*SDR*) Networks (2007).
5) IEEE: Amendment to IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems – Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation Licensed Bands, IEEE Standard 802.16e (2005).
6) IEEE 802.16, (online), available from ⟨http://www.ieee802.org/16/⟩.
7) IEEE 802.11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE (1999).
8) Nomura, R., Kuroda, M. and Inoue, D.: Location-based Key Management for Ubiquitous Wireless Network, *WPMC'05*, Vol.1, pp.51–55 (Sep. 2005).
9) Kuroda, M. and Nomura, R.: Radio-independent Mobile Authentication Protocol for Ubiquitous Network, *WPMC'05*, Vol.3, pp.1703–1707 (Sep. 2005).
10) Kuroda, M., Nomura, R. and Trappe, W.: A Radio-independent Authentication Protocol (EAP-CRP) for Networks of Cognitive Radios, *Proc. IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, Vol.1, pp.70–79 (2007).
11) Xu, W., Kamat, P. and Trappe, W.: TRIESTE: A Trusted Radio Infrastructure for Enforcing Spectrum Etiquettes, *1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks* (2006).
12) Bian, K. and Park, J.-M.: Security Vulnerabilities in IEEE 802.22, ICST WICON (2008).
13) Pawelczak, P.: Protocol Requirements for Cognitive Radio Networks (online), available from ⟨https://doc.freeband.nl/dscgi/ds.py/Get/File-60831⟩ (2005).
14) Chen, R., Park, J.-M. and Reed J.H.: Defense against Primary User Emulation Attacks in Cognitive Radio Networks, *IEEE Journal on Selected Araas in Communications Special Issue on Cognitive Radio Theory and Applications* (2008).
15) Trusted Computing Group: (online), available from ⟨http://www.trustedcomputinggroup.org/⟩.
16) 3G Security, Security Architecture (Releases 5), 3GPP TS33.102 V5.5 (2004).

17) RFC-4186: Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM), IETF (2006).
18) RFC-4187: Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA), IETF (2006).
19) IEEE 802.11i Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE (2004).
20) IEEE 802.1X Port-Based Network Access Control, IEEE (2001).
21) Johnston, D. and Walker, J.: Overview of IEEE802.16 Security, IEEE Security and Privacy, *IEEE Security and Privacy* (May/June 2004).
22) Narayanan, V. and Dondeti, L.: EAP Extention for Efficient Re-authenticaton (online), available from ⟨http://tools.ietf.org/html/draft-vidya-eap-er-02⟩.
23) Wireless Network Security 802.11, Bluetooth and Handheld Devices, NIST Special Publication 800-48 (2002).
24) Lin, Y.-B.: Reducing Location Update Cost in a PCS Network, *IEEE/ACM Trans. Networking*, Vol.5 (1997).
25) Nomura, R., Kuroda, M. and Mizuno, T.: Evaluation of EAP based Reauthentication Protocol for High-speed Vehicular Handover in Cognitive Radio Networks, *CrownCom* (2007).
26) ITU: Pulse Code Modulation (PCM) of Voice Frequencies, ITU-T Recommendation G.711 (1988).
27) ITU: Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP), ITU-T Recommendation G.729 (2007).

(Received May 21, 2010)
(Accepted November 5, 2010)
(Original version of this article can be found in the Journal of Information Processing Vol.19, pp.88–102.)

Ritsu Nomura received his M.E. degree in Systems Science from Tokyo Denki University, Japan, in 1989. He joined Mitsubishi Electric Corporation, Japan in 1989. Since then, he was engaged in OS/network developments and information security system developments. In 2004, he joined the next generation wireless network R&D project in NICT and worked on the wireless security.

Masahiro Kuroda received his M.E. degree in Systems Science from Tokyo Institute of Technology, Japan, in 1980, M.S. degree in Computer Science from University of California, Santa Barbara, CA, in 1989, and received Ph.D. degree in Computer Science from Shizuoka University, Japan, in 2000. He joined Mitsubishi Electric Corporation, Kamakura, Japan in 1980. Since then, he was engaged in OS/network developments, mobile network computing R&D, and cellular Java standardizations. In 2002 he joined National Institute of Information and Communications Technology (NICT) (Former name was Communications Research Laboratory, CRL) under the ministry of Internal affairs and Communications and was working on wireless network, wireless security, mobile systems, and next generation wireless systems architecture. He is currently working on secure body-area netwoking technologies targeted for ubiquitous healthcare/medical systems and international standardizations including the networking technologies at the headquarters of NICT, Japan. He is a member of the IEEE Computer Society.

Tadanori Mizuno received his B.E. degree in Industrial Engineering from Nagoya Institute of Technology in 1968 and received his Ph.D. degree in Computer Science from Kyushu University, Japan, in 1987. In 1968, he joined Mitsubishi Electric Corp. Since 1993, he is a Professor of Shizuoka University, Japan. Now, he is a Professor of Graduate School of Science and Technology of Shizuoka University. His research interests include mobile computing, distributed computing, computer networks, broadcast communication and computing, and protocol engineering. He is a member of IPSJ, IEICE, IEEE Computer Society, ACM and Informatics Society.