Wireless Secret Key Generation Exploiting Reactance-Domain Scalar Response of Multipath Fading Channels

Tomoyuki Aono, *Member, IEEE*, Keisuke Higuchi, Takashi Ohira, *Fellow, IEEE*, Bokuji Komiyama, *Member, IEEE*, and Hideichi Sasaoka, *Member, IEEE*

***Abstract*—We describe a secure communication scheme that uses the random fluctuation of the natural environment of communication channels. Only the transmitter and the receiver share the communication channel characteristics. From reciprocity between a transmitter and a receiver, it is possible for them to share one-time information of their fluctuating channel. This can provide a secret key agreement scheme without key management and key distribution processes. In this paper, we propose a new secret key generation and agreement scheme that uses the fluctuation of channel characteristics with an electronically steerable parasitic array radiator (ESPAR) antenna. This antenna, which has been proposed and prototyped, is a smart antenna designed for consumers. Using the beam-forming technique of the ESPAR antenna, we can increase the fluctuation of the channel characteristics. From experimental results, we conclude that the proposed scheme has the ability to generate secret keys from the received signal strength indicator (RSSI) profile with sufficient independence.**

***Index Terms*—Beam-forming, channel characteristics, electronically steerable parasitic array radiator (ESPAR), key distribution, key management, received signal strength indicator (RSSI), secret key agreement.**

I. Introduction

THESE days, with the explosive growth of wireless communication systems such as LANs, security has become a critical issue. Generally, there are two types of cryptographic methods: public key cryptography [1] and secret key cryptography [2]. They each have their own characteristics, as shown in Table I.

TABLE I
CHARACTERISTICS OF CRYPTOGRAPHIES

	Secret key	Public key
Encryption speed	rapid	slow
Key distribution	secret	public
Key interception	vulnerable	strong
Key management	difficult	easy

In wireless LAN systems, secret key cryptography is used because its processing speed is higher and it can deal with bulk data. This method, however, has two problems: key distribution and key management. The problem of key distribution involves the danger of the secret key being intercepted as it is transmitted to the other communication party for secret key agreement. The problem of key management involves the necessity of administrating many keys because a different key is used for each communication party. Moreover, as wireless LAN systems have spread and general-purpose computers have come into wide use as wireless terminals, the problem of leaked and invalidated keys due to lost or stolen terminals has grown significantly. Key distribution generally uses a method of encrypting secret keys by public keys as they are transmitted, and this involves all of the aforementioned problems. Another method has been studied in which receivers use User ID's to generate secret keys themselves, eliminating the need to transmit secret keys [3]. This method requires ID administration instead of key management, and it provides no effective countermeasure to the invalidation of secret keys. Recently, studies of quantum cryptography, of which BB84 is representative [4], have shown promise. However, they have not reached a practical level due to many technical problems, such as the need to speed up the data rate as well as various constraint conditions [5].

The noise and fluctuation of radio wave channels are uncontrollable random phenomena; therefore, secret key methods have been used [6]. One of these methods is to make agreement with secret keys by using the fluctuation of channel characteristics without distributing keys [7], [8]. Since this can provide a one-time key when it is needed, it is an excellent method to solve the problems of key distribution and key management. This method still has another problem: it is easy to break the secret keys under an environment with small fluctuation of channel characteristics.

There is a solution to this problem. Using smart antennas, the fluctuation of channel characteristics can be further undulated by electronic means. Digital beam-forming (DBF) array antennas, however, need very complex circuits and require a measurable amount of power. Consequently, they are not suitable for wireless consumer system such as wireless LAN at this time. Therefore, we need another approach.

In this paper, we describe a new secret key generation and agreement scheme based on the fluctuation of channel characteristics by using the electronically steerable parasitic array radiator (ESPAR) antenna [9]–[17], which is a variable-directional antenna. This scheme is based on "reactance-domain" beam-forming with the ESPAR antenna [18], [19], in which

Manuscript received December 20, 2004; revised May 31, 2005. This work was supported by the National Institute of Information and Communications Technology (NICT).

T. Aono, K. Higuchi, T. Ohira, and B. Komiyama are with the Advanced Telecommunications Research Institute International (ATR), Kyoto 619-0288, Japan (e-mail:aono@atr.jp; ohira@atr.jp).

H. Sasaoka is with Doshisha University, Kyoto, 610-0394, Japan

Digital Object Identifier 10.1109/TAP.2005.858853

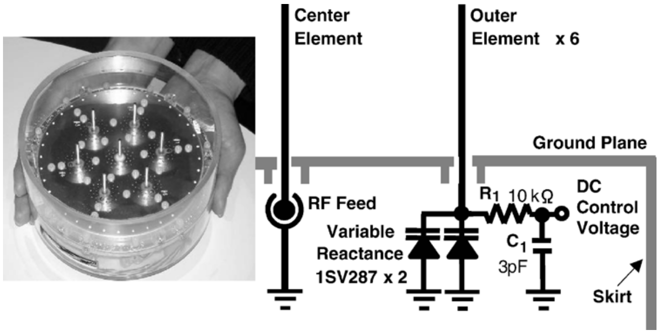

Fig. 1. 7-element ESPAR anntena.

TABLE II
REACTANCE VALUES FOR BEAM-FORMING

N	pattern	x_1	x_2	x_3	x_4	x_5	x_6
0	Omni	high	high	high	high	high	high
1	0 degree	low	high	high	high	high	high
2	60 degree	high	low	high	high	high	high
3	120 degree	high	high	low	high	high	high
4	180 degree	high	high	high	low	high	high
5	240 degree	high	high	high	high	low	high
6	300 degree	high	high	high	high	high	low

we can fluctuate the channel characteristics artificially by controlling the reactance values of the ESPAR antenna. We give an overview of the ESPAR antenna in Section II, the proposed system in Section III, the principle of secret key agreement with the ESPAR antenna in Section IV, the detailed design of the proposed system in Section V, feasibility experiments on generating secret keys in Section VI, and finally our conclusions in Section VII.

II. ESPAR ANTENNA

A. Configuration

The ESPAR antenna proposed and prototyped is a variable-directional array antenna with a single central active radiator surrounded by parasitic elements loaded with variable reactors. As an example, an overview of a 7-element ESPAR antenna is shown in Fig. 1. The single central active element is surrounded by six parasitic elements at equal intervals. The parasitic elements are each loaded with varactor diodes, which are variable-capacitance diodes, in parallel. By adjusting the dc voltage given to the varactors with reverse bias, the antenna's beam can be formed. Because it has only a single RF radiator, it is expected to have lower power consumption than DBF array antennas.

B. Reactance-Domain Beam-Forming

By adjusting the dc voltage to each varactor, reactance values are changed and variable beam patterns are formed. For example, in the case of Table II, beam patterns are shown as Fig. 2. In Table II, "high" and "low" mean the highest and the lowest reactance values of the varactors, respectively. In the case of "$\mathrm{N}\ =\ 0$," the beam pattern is formed omnidirectionally. In other cases, single-lobe directional beams are shaped. The reactance-domain beam-forming technique of the ESPAR antenna can also form a multilobe beam pattern [20].

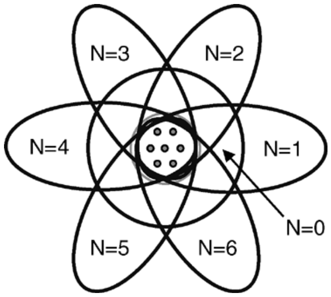

Fig. 2. Reactance-domain beam-forming.

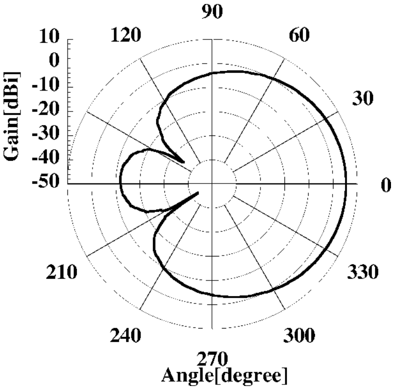

Fig. 3. Example measured radiation pattern of an ESPAR antenna.

C. Variation Performance

The gain of the ESPAR antenna is about 6 dBi. Fig. 3 shows an example of the measured radiation pattern of an ESPAR antenna. According to the 1SV287 variable reactance specification, the allowable range of the bias voltage is from 20 to $-0.5\ \mathrm{V}$ [21]. If the bias voltage is given by an 8-bit resolution digital value, the number of radiation patterns that an m-element ESPAR antenna can form is $(2^8)^{m-1} = 2^{48}$. Although most of these patterns would be indistinguishable in terms of their RSSI profile, a selection of hundreds of patterns is used.

III. PROPOSED SYSTEM

We can control beam-forming by adjusting the dc voltage given to the varactors with reverse bias. Using the beam-forming technique of the ESPAR antenna, we can intentionally undulate the fluctuation of the channel characteristics to create strong secret keys. Moreover, we can acquire an undulated received signal strength indicator (RSSI) profile in a short time and generate a secret key more easily than in the case of using delay profiles. Furthermore, by repeating this process at short intervals, we can update a secret key and realize strong security. In generating secret keys, the precondition is set as follows. The system configuration is shown in Fig. 4. By measuring the RSSI of the radio waves communicated to "access point A" and to "user terminal B" to make RSSI profiles, we can generate secret keys independently for each communication party and share them in common. It is thus difficult for "eavesdropper C" to generate the same key by using the measured RSSI because its channel characteristics are different.

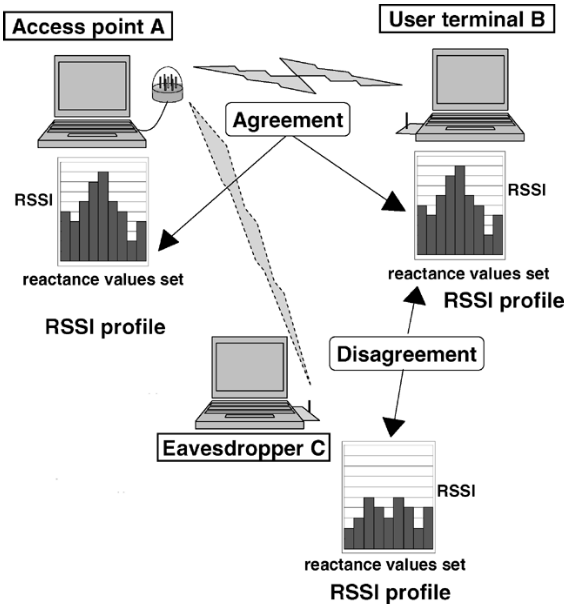

Fig. 4. System configuration.

IV. Secret-Key Generation and Agreement Principle

Here, we describe in detail the process for generating secret keys. The preconditions are set as follows. Working together, "access point A" with the ESPAR antenna and "user terminal B" with a conventional omnidirectional antenna generate agreed secret keys. "Eavesdropper C" is the same as B. A and B can communicate at the same frequency by using a method such as time division duplex (TDD). The reactance values set at each parasitic element of an m-element ESPAR antenna are expressed as the reactance vector. A set of N-units of reactance vectors is expressed as the reactance vector series. The key-generation process is shown in Fig. 5.

The procedure of generating secret keys is described as follows.

1) A series of packets is transmitted from A, each with a different beam pattern generated by a reactance vector. The packets are received by B, which builds up a sequence of RSSI data in B. For a key length K, a sequence of length $K + \alpha$ should be captured, where $\alpha > K$ to allow for disagreement data as described here.

2) Not all beam patterns are transmitted by turning their main lobes to the direction of B. If a packet is not received by B, A will change the beam pattern and retry transmission.

3) After each packet transmission, A switches to receive mode while keeping the same beam pattern, and B transmits a packet. This builds up a sequence of RSSI data in A.

4) Thanks to the reciprocity theorem of radio wave propagation between uplink and downlink, the sequences in A and B should be identical, as shown in **Fig. 6**, except for the random noise and the differences in transmission powers, receivers' noise figures, and antenna performance (sensitivity or directivity). The former can be reduced by using the averaged response method. The latter effects can be normalized out, so it is not necessary to calibrate both transmission powers.

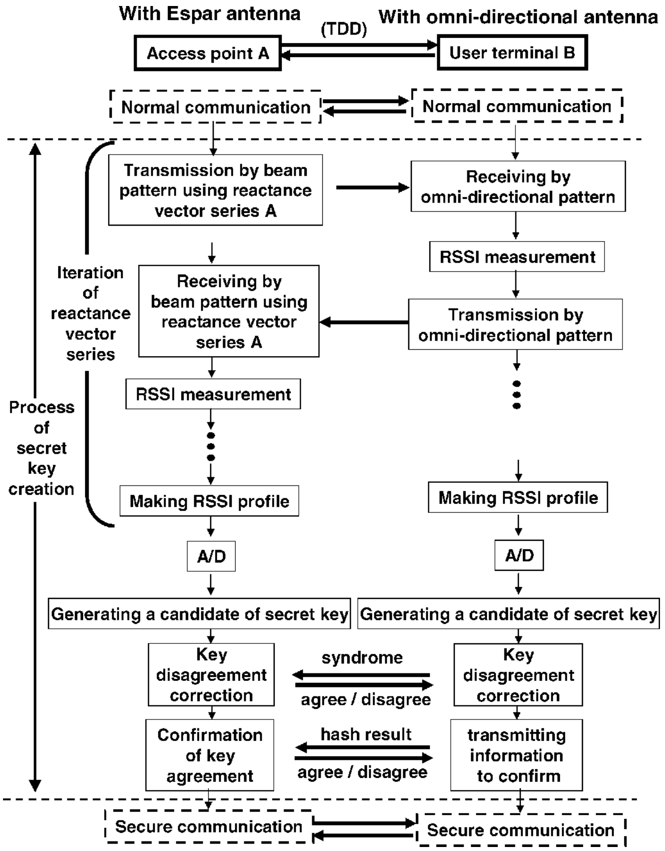
With Espar antenna
(TDD)
With omni-directional antenna
Access point A
User terminal B
Normal communication
Normal communication
Transmission by beam pattern using reactance vector series A
Receiving by omni-directional pattern
RSSI measurement
Iteration of reactance vector series
Receiving by beam pattern using reactance vector series A
Transmission by omni-directional pattern
RSSI measurement
Process of secret key creation
Making RSSI profile
Making RSSI profile
A/D
A/D
Generating a candidate of secret key
Generating a candidate of secret key
Key disagreement correction
syndrome
agree / disagree
Key disagreement correction
Confirmation of key agreement
hash result
agree / disagree
transmitting information to confirm
Secure communication
Secure communication

Fig. 5. Key-generation process.

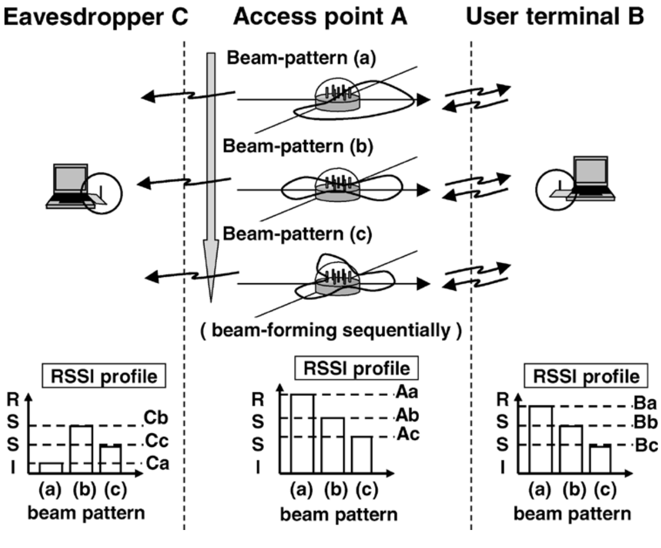

Fig. 6. Reactance-domain scalar response (RSSI Profile).

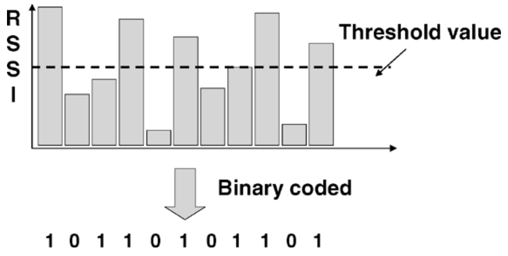

Fig. 7. Binary quantization of RSSI profile.

5) At A a subset of the sequence is chosen to be least susceptible to noise, by picking the largest $K/2 + \beta$ and smallest $K/2 + \beta$ RSSI values, with $\beta < \alpha/2$. Those RSSI values not chosen are deleted.
6) The positions of deleted values are sent to B and deleted from the sequence in B.
7) At B, the process is repeated, this time choosing the largest $K/2$ and smallest $K/2$ RSSI values from those remaining. Unchosen values are deleted and their positions are sent to A, where they are also deleted from the sequence in A.
8) Both A and B now have candidate sequences for a secret key of length K.
9) The RSSI profiles are sampled and binary coded after the threshold level has been defined as shown in Fig. 7. By considering the variance of binary bits, the threshold level is defined as the median value of the RSSI profiles.
10) A further disagreement-correction process is carried out by applying an error-correction technique. We describe it near the end of this section.
11) If no agreement is obtained after disagreement-correction, the generated key is rejected and the entire process is repeated.
12) Agreement on the key is obtained using a one-way transformation (e.g., hashing). B transmits a transformed version of the candidate key to A, where it is compared with a similarly transformed version of A's candidate key.
13) If agreement is obtained, then confirmation is transmitted to B and the process is complete. If agreement is not obtained, the generated key is rejected and the entire process is repeated.

If C were located at the point of symmetry toward B from A, it could not estimate the RSSI profile of B simply by exchanging the maximum RSSI value for the minimum shown in Fig. 6. This is because the ESPAR antenna can form multilobe beam patterns. Consequently, it is difficult for a knowledgeable and active eavesdropper to influence the RSSI profile. Since most wireless communication systems are based on carrier sense multiple access/collision avoidance (CSMA/CA), an eavesdropper would have to synchronize with the timing of packet transmissions of the access point and the user terminal in order to influence the propagation channels.

The generated secret keys become more complicated due to the influence of the multipath waves, which provides a good condition for the proposed scheme under multipath-wave environments. On the other hand, the influence of the multipath waves may cause disagreement between common keys. To avoid such disagreement, both the above-described averaged response method and a disagreement-correcting process as follows are carried out. In the proposed scheme, the bit patterns of the secret key candidates are coded by some kind of block code, such as BCH code. We calculate each syndrome, $S_a = x_a\, \mathbf{H^T}$, and $S_b = x_b\, \mathbf{H^T}$, where x_a and x_b are bit patterns in the secret key candidates of the access point and the user terminal, respectively, $\mathbf{H}$ denotes a check matrix, and the superscript $\mathbf{T}$ is the transpose of the matrix. In the next step, we define the difference in the syndrome as $S = S_a - S_B$ and that in the bit pattern as $e = x_a - x_b$. The relationship between these is expressed as $S = e\mathbf{H^T}$. If $S = 0$ is true, $e = 0$ will be true and both bit patterns will agree. If $S = 0$ is false, we will be able to estimate (correct) e to minimize the number of disagreeing bits by the method of error correction. If these syndrome bits are eavesdropped, the secret keys cannot be estimated. The number of effective bits is decreased only by the number of the syndrome bits.

If information on the reactance vectors and the reactance vector series used for generating the secret keys were opened to the public, the possibility of estimating the correct RSSI profile would remain because the positions of the transmitter, receiver and reflectors would be open knowledge. Therefore, this information should be kept confidential. It is not necessary, however, for user terminals to have this information, because only the access point can control the beam pattern of the ESPAR antenna. Therefore, this scheme can provide a very high level of security. If the number of beam patterns is small, an eavesdropper located near the access point may be able to deduce information by near-field probing of the ESPAR antenna. The number of beam patterns, however, is 2^{48} as described in Section II, and the presence time of a beam pattern is a few milliseconds. Therefore, it is much too difficult for an eavesdropper to deduce this information.

V. System Design

For the proposed system, function blocks of "access point A" and "user terminal B" are shown in Figs. 8 and 9, respectively.

"A" consists of four parts: an "ESPAR antenna," a "D/A converter," a "ZigBee chip [22], " and a "microcontroller." The "microcontroller" carries out the "making the RSSI profile" step and generates the secret keys in the "Secret-key generator" function. This is based on measured RSSI values from the "ZigBee chip." In the "ZigBee chip," the RF module conforms to IEEE802.15.4

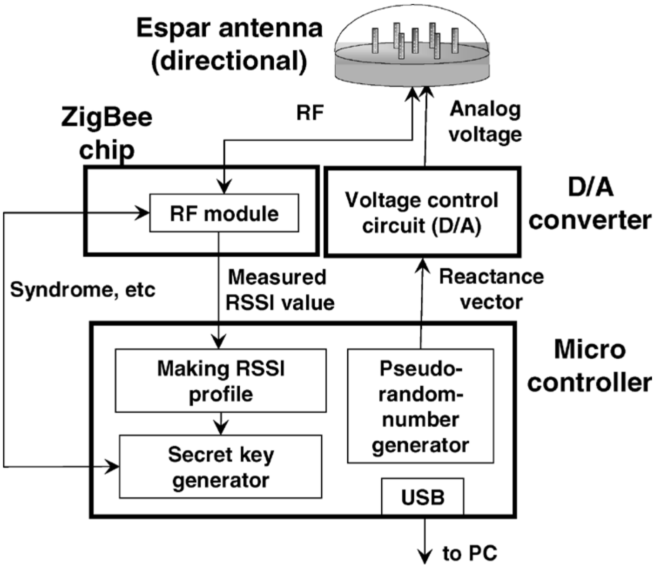

Fig. 8. Block diagram of access point A.

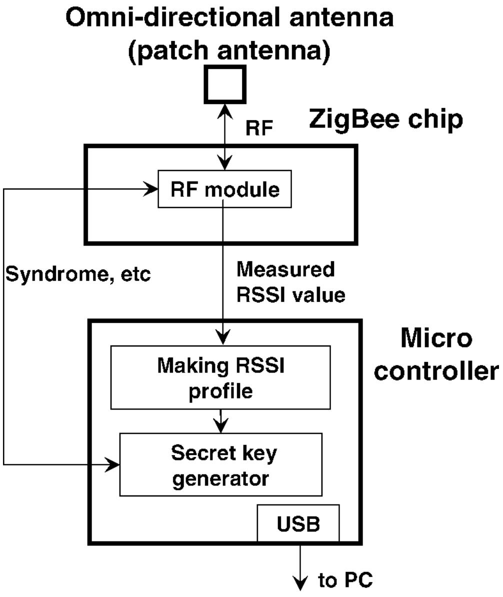

Fig. 9. Block diagram of user terminal B.

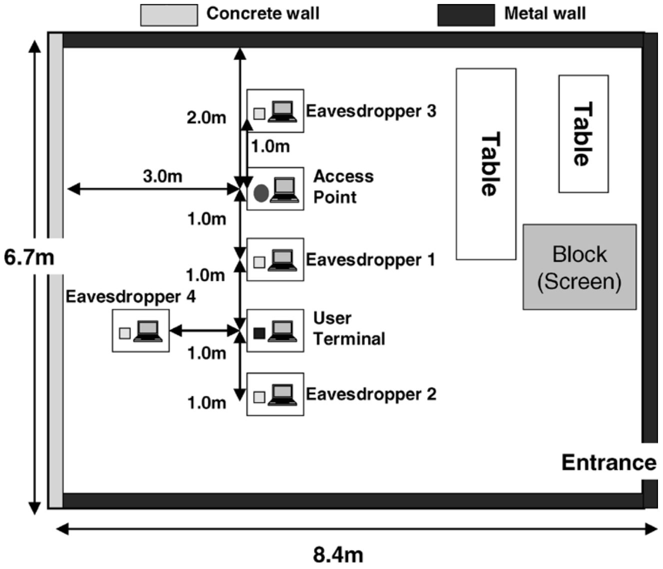

Fig. 10. Sketch of experimental room.

and controls, as a network coordinator, the I/O of the data transmission and receiving and that of the RF signal to the "ESPAR antenna" part. The "microcontroller" can send the generated secret keys to a PC through a USB cable to apply them to the security functions for wireless LAN or IPSec-VPN systems. Furthermore, "A" has the function of beam-forming with the ESPAR antenna. In the "microcontroller" part, a pseudorandom-number generator randomizes reactance vector values as needed, and each dc voltage given to the varactor is calculated. In the next process, each dc voltage is generated by the "voltage control circuit" of the "D/A converter" and applied to the "ESPAR antenna."

"B" consists of three parts: an "Omnidirectional antenna," a "ZigBee chip," and a "microcontroller." The functions of each block are the same as those of "A."

TABLE III
SPECIFICATIONS OF ZIGBEE CHIP CC2420

Frequency	2.4 GHz (ISM band)
Transmission power	1mW
Data modulation	offset-QPSK
Data rate	250 kbps
Spread spectrum modulation	DSSS
Chip rate	2Mcps

VI. FEASIBILITY EXPERIMENT

A. Preparations

We conducted an indoor experiment on generating secret keys with the ESPAR antenna. A sketch of the experimental room is shown in Fig. 10.

The experimental room has three metal walls and a fourth concrete wall. We set up an "access point" with the ESPAR antenna, a "user terminal" with a conventional omnidirectional antenna, and an "eavesdropper" with the same antenna as the user terminal. These were located as shown in Fig. 10. At the beginning of the experiment, the eavesdropper was located at the position of "eavesdropper 1." After the end of the first measurement cycle, the eavesdropper moved to the positions of "eavesdropper 2," "eavesdropper 3," and "eavesdropper 4" successively in each cycle. We generated a 128-bit secret key from 384 measured RSSI values, that is, α in Section IV equals 256, and this took about one second. As described in Section II, the number of beam patterns that a 7-element ESPAR antenna can form is 2^{48}, which is sufficient to select 384 values at random. One measurement cycle included 170 generations of the 128-bit secret key. We used the ZigBee chips Chipcom-CC2420 [23], and their specifications are shown in Table III. CC2420 measures the RSSI value for each packet in its internal autogain control process. Prototypes of the access point and the user terminal are shown in Figs. 11 and 12, respectively. This system design is suitable for mobile users, since the prototype of the user terminal is smaller than a person's palm and has low power consumption. Moreover, we have developed a prototype shaped like

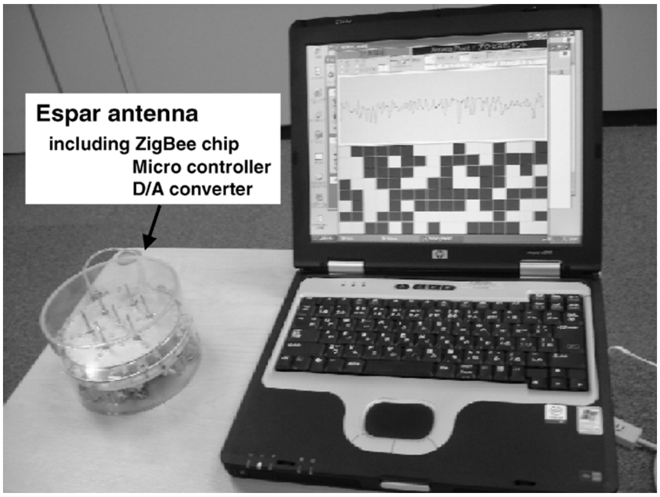

Fig. 11. Prototype of access point.

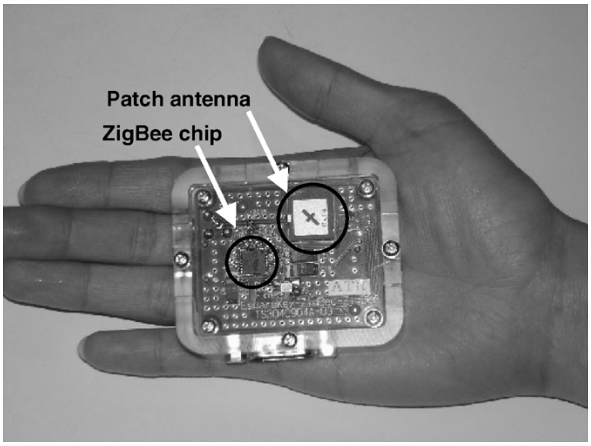

Fig. 12. Prototype of user terminal.

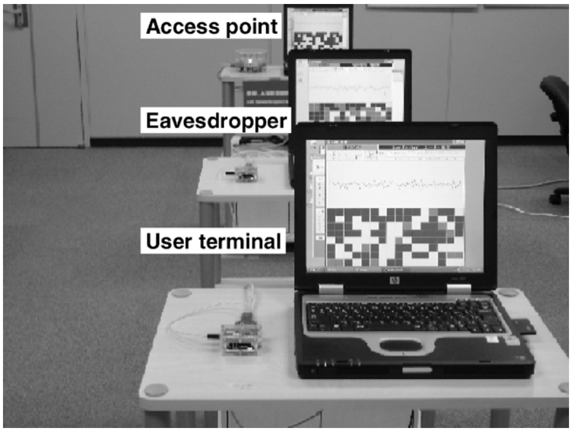

Fig. 13. Snapshot of experiment.

a USB memory stick. A snapshot of the experiment is shown in Fig. 13.

B. Distribution of Disagreement Bits in Generated Secret Keys

The distribution of disagreement bits for the generated secret keys is shown in Figs. 14 and 15. In this case, the eavesdropper was located at the position of "eavesdropper 4." In the case of Fig. 14, secret keys were generated without a disagreement reduction process, that is, $\alpha = 0$ in Section IV. The upper graph

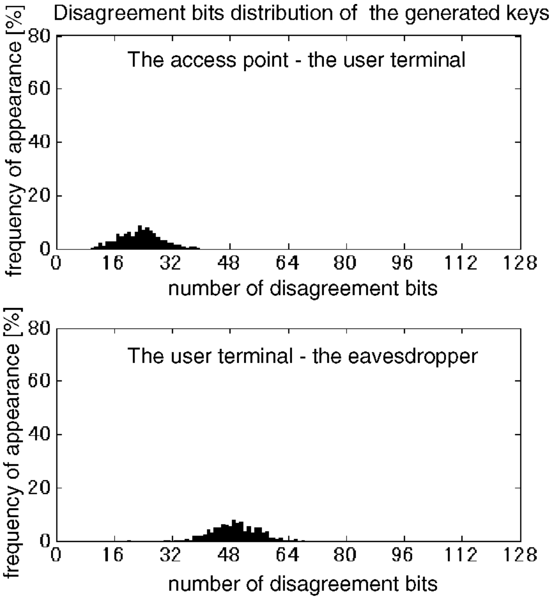

Fig. 14. Disagreement bits distribution (without disagreement reduction: $\alpha = 0$).

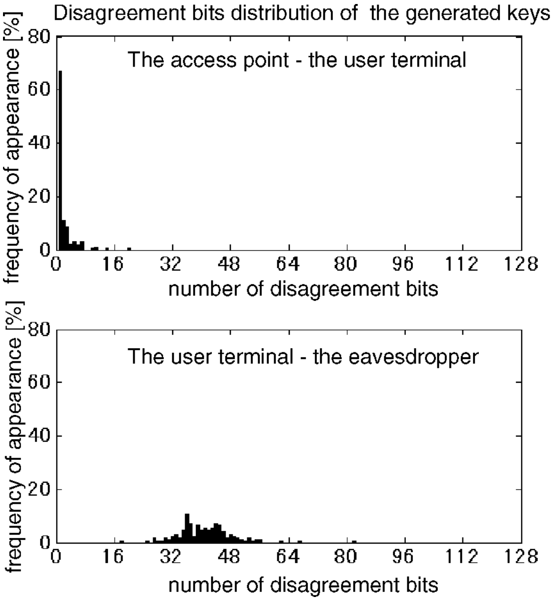

Fig. 15. Disagreement bits distribution (with disagreement reduction: $\alpha = 256$).

shows the disagreement bits distribution of the generated secret keys between the access point and the user terminal, and the lower graph shows that between the user terminal and the eavesdropper. Both graphs show that many disagreements occur. Although the upper case involves regular communication parties, there are too many disagreement bits to correct the disagreement. On the other hand, in Fig. 15, the upper graph shows that the disagreement bits are not so serious, and thus the disagreement correcting process is effective. An 8-bit disagreement correction may be sufficient to handle almost any secret key.

C. Generated Key Agreement Ratio

Fig. 16 shows the generated key agreement ratio between the access point and the user terminal. The agreement ratio means

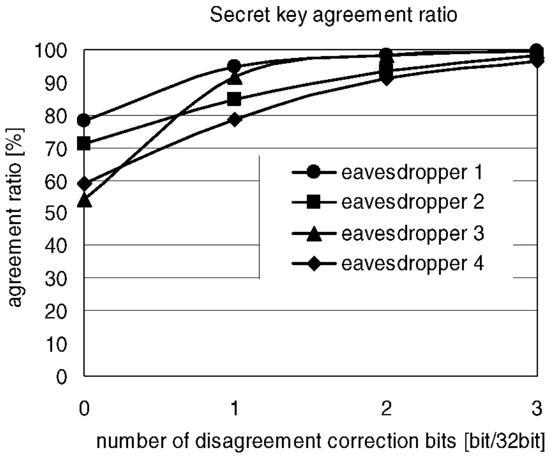

Fig. 16. Secret key agreement ratio.

the percent of generated keys for which complete agreement is obtained. This graph shows the number of bits needed for disagreement correction in a 32-bit process, and, as described in the previous subsection, by using 8-bit disagreement correction (2-bit correction for a 32-bit situation), the agreement ratio improved to more than 90% regardless of where the eavesdropper was located as a barrier.

D. Independence of Generated Secret Key

Here, we define the correlation coefficient of two secret keys: one is generated by the user terminal and the other is generated by the eavesdropper. The former is expressed as $X = [x_1, \ldots, x_i, \ldots, x_N]$, and the latter is expressed as $Y = [y_1, \ldots, y_i, \ldots, y_N]$. N is the key length in bits. The correlation coefficient is defined as follows:

$$\rho = \frac{S_{xy}}{\sigma_x \sigma_y} \tag{1}$$

where S_{xy} is the covariance between X and Y given by

$$S_{xy} = \frac{1}{N}\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y}) \tag{2}$$

and σ_x and σ_y are the standard deviations of X and Y, respectively.

Fig. 17 shows the correlations of measured RSSI. The right-side lines are the correlations of the access point and the user terminal, and the left-side lines are those of the user terminal and the eavesdropper. The vertical scale of this graph is the complementary cumulative distribution function (CDF). Although the lines of the graph are differently influenced by the eavesdropper's position, the correlation of the user terminal and the eavesdropper is nearly as low as 0.5. As a result, we conclude that the proposed scheme has the ability to generate secret keys with sufficient independence.

E. Experiment Under a Dynamic Environment

We set up the access point, the user terminal and the eavesdropper in the experimental room. They were located as shown in Fig. 18. The access point was located in the center of the room. The user terminal kept moving at random around the room at the speed of a person walking. The eavesdropper was located next to the access point. We also generated a 128-bit secret key from 384 RSSI values. One measurement cycle included 200 generations of the secret key.

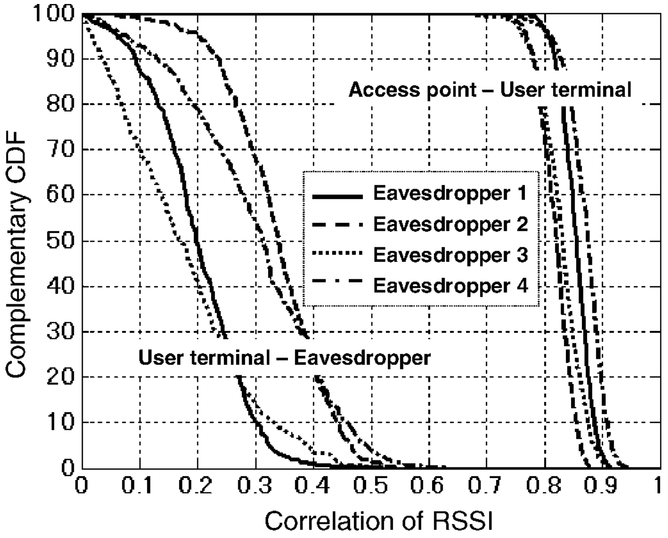

Fig. 17. Correlations of RSSI values.

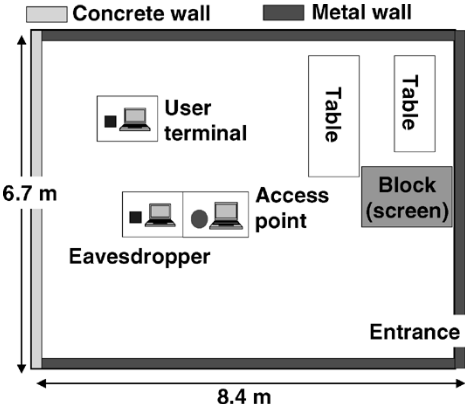

Fig. 18. Location of each communication party in the experiment under a dynamic environment.

Fig. 19 shows the experimental results for the disagreement bits distribution. The upper graph shows that the disagreement bits are very few in many cases, in the same way as depicted in Fig. 15. If an 8-bit disagreement correction is used, key agreement can succeed in almost any case. As a result, we confirmed that there was no problem in generating secret keys by the proposed scheme under a dynamic environment.

F. Experiment at Different Height

We set up the access point, the user terminal, and the eavesdropper in the experimental room. They were located as shown in Fig. 20. In this case, the access point was located at a high position near the ceiling of the room. We also generated a 128-bit secret key from 384 RSSI values. One measurement cycle included 200 generations of the secret key.

Fig. 21 also shows the experimental results for the disagreement bits distribution. The upper graph shows the same results

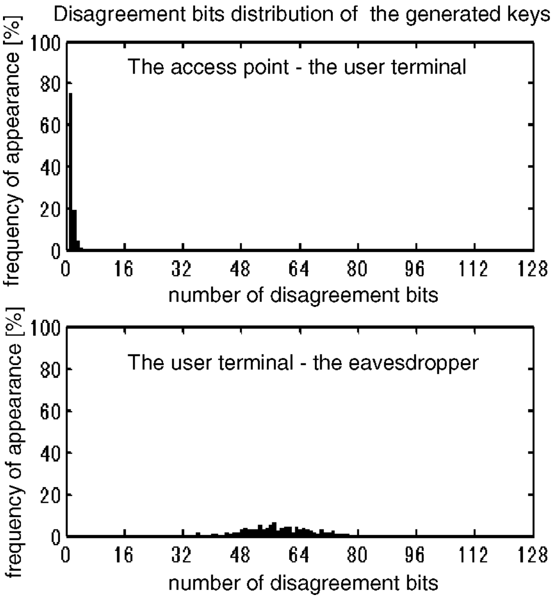

Fig. 19. Disagreement bits distribution under a dynamic environment.

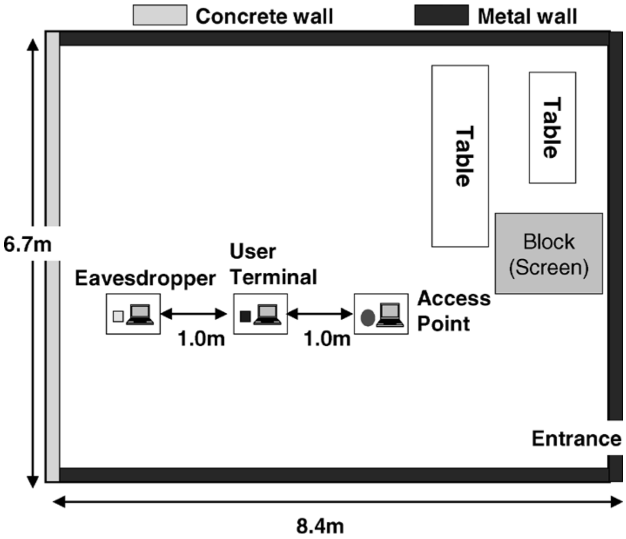

Fig. 20. Location of each communication party in the experiment at different height.

as in the previous case. Therefore, we confirmed that there was no problem in generating secret keys at a different height from the access point and the other parties.

VII. Conclusion

We proposed a new secret key agreement scheme that exploits the fluctuation of channel characteristics by using the ESPAR antenna. We also designed systems for this scheme and conducted feasibility experiments. In the communication between "access point A" with the ESPAR antenna and "user terminal B" with a conventional omnidirectional antenna, if "access point A" transmits and receives by changing its beam-form using the same reactance vector series, the RSSI profile of "access point A" and that of "user terminal B" will show the same fluctuation characteristics. This phenomenon provides a secret key agreement scheme that does not require key distribution for "access point A" or "user terminal B" but instead generates secret keys from each of their RSSI profiles. Since they can be used as one-time keys, a high-security wireless communication system can be realized without the need for key management, including key invalidation. In our feasibility experiment, the channel characteristics were fluctuated intentionally by using the beamforming techniques of the ESPAR antenna. We conclude that the proposed scheme has the ability to generate secret keys from the RSSI profile with sufficient independence.

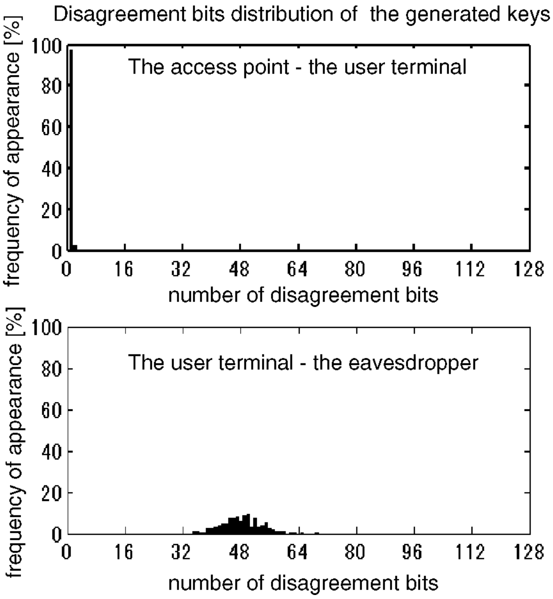

Fig. 21. Disagreement bits distribution at a different height from the access point and other parties.

References

[1] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, pp. 120–126, Feb. 1978.

[2] *U.S. National Bureau of Standards(NBS) "Data Encryption Standard"*, Federal Information Processing Standards Publication 46 (FIPS-46), 1977.

[3] T. Matsumoto and H. Imai, "On the key predistribution system: A practical solution to the key distribution problem," in *CRYPTO'87*. New York: Springer-Verlag, 1987, pp. 185–193.

[4] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Com. Syst. Signal Processing*, Bangalore, India, Dec. 1984.

[5] D. Mayers, "Unconditionally secure quantum bit commitment is impossible," *Phys. Rev. Lett.*, vol. 78, no. 17, pp. 3414–3417, 1997.

[6] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, pp. 733–742, May 1993.

[7] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Trans. Commun.*, vol. 43, pp. 3–6, Jan. 1995.

[8] M. Horiike and H. Sasaoka, "A scheme of secret key agreement based on the random fluctuation of channel characteristics in land mobile radio," IEICE, Tech. Rep. RCS2002–173, 2002.

[9] R. F. Harrington, "Reactively controlled directive arrays," *IEEE Trans. Antennas Propag.*, vol. AP-26, no. 3, pp. 390–397, May 1978.

[10] R. J. Dinger, "Reactively steered adaptive array using microstrip patch elements at 4 GHz," *IEEE Trans. Antennas Propag.*, vol. AP–32, no. 8, pp. 848–856, Aug. 1984.

[11] R. Schlub and D. V. Thiel, "Switched parasitic antenna on a finite ground plane with conductive sleeve," *IEEE Trans. Antennas Propag.*, vol. 52, no. 5, pp. 1343–1347, May 2004.

[12] N. L. Scott, M. O. Leonard-Taylor, and R. G. Vaughan, "Diversity gain from a single-port adaptive antenna using switched parasitic elements illustrated with a wire and monopole prototype," *IEEE Trans. Antennas Propag.*, vol. 47, no. 6, pp. 1066–1070, Jun. 1999.

[13] R. Vaughan, "Switched parasitic elements for antenna diversity," *IEEE Trans. Antennas Propag.*, vol. 47, no. 2, pp. 399–405, Feb. 1999.

[14] D. V. Thiel and S. Smith, *Switched Parasitic Antennas for Cellular Communications*. Norwood, MA: Artech House, 2001.

[15] J. Cheng, M. Hashiguchi, K. Iigusa, and T. Ohira, "Electronically steerable parasitic array radiator antenna for omni- and sector-pattern forming applications to wireless ad hoc networks," in *Proc. Inst. Elect. Eng. Microwaves Antennas Propagation*, vol. 150, Aug. 2003, pp. 203–208.

[16] T. Ohira and J. Cheng, "Analog smart antennas," in *Adaptive Antenna Arrays*. Berlin, Germany: Springer Verlag, 2004, pp. 184–204.

[17] C. Sun, A. Hirata, T. Ohira, and N. Karmakar, "Fast beamforming of electronically steerable parasitic array radiator antennas: Theory and experiment," *IEEE Trans. Antennas Propag.*, vol. 52, no. 7, pp. 1819–1832, Jul. 2004.

[18] A. Hirata, T. Aono, H. Yamada, and T. Ohira, "Reactance-domain SSP MUSIC for the ESPAR antenna to estimate the DOA's of coherent waves," in *Proc. Int. Symp. Wireless Personal Multimedia Communications, WPMC2003*, vol. WA4–3, Yokosuka, Japan, Oct. 2003.

[19] C. Plapous, J. Cheng, E. Taillefer, A. Hirata, and T. Ohira, "Reactance domain MUSIC algorithm for electronically steerable parasitic array radiator," *IEEE Trans. Antennas Propag.*, vol. 52, no. 12, pp. 3257–3264, Dec. 2004.

[20] H. Mori, H. Sasaoka, and T. Ohira, "Performance estimation of secret key agreement system exploiting an ESPAR antenna and a received signal strength indicator," presented at the Proc. ISSSE, vol. IS-0518, Aug. 2004.

[21] E. Taillefer, A. Hirata, and T. Ohira, "Direction-of-arrival estimation using radiation power pattern with an ESPAR antenna," *IEEE Trans. Antennas Propag.*, vol. 53, no. 2, pp. 678–684, Feb. 2005.

[22] [Online]. Available: http://www.zigbee.org/en/resources/

[23] [Online]. Available: http://www.chipcon.com

Tomoyuki Aono (M'05) received the B.E. degree from Kansai University, Osaka, Japan, in 1991.

In 1991, he joined Mitsubishi Electric Corp., Hyogo, Japan, where he was engaged in design and development of wireless communication systems and the direction finding systems to government and municipal offices. He has been engaged in research and development on wireless communication systems and adaptive array antennas at ATR Wave Engineering Laboratories in Kyoto, Japan.

Mr. Aono is a Member of IEICE of Japan.

Keisuke Higuchi received the B.E and M.E. degrees from Doshisha University, Kyoto, Japan, in 2002 and 2004, respectively.

In 2004, he joined ATR Wave Engineering Laboratories, Kyoto, where he was engaged in design and development of wireless communication systems and adaptive array antennas. Since 2005, he has been with Sanyo Electric Company, Ltd., Gifu, Japan. His research interests are land-mobile communication systems.

Mr. Higuchi is a Member of IEICE of Japan.

Takashi Ohira (S'79–M'83–SM'99–F'04) received the B.E. and D.E. degrees in communication engineering from Osaka University, Osaka, Japan, in 1978 and 1983.

In 1983, he joined NTT Electrical Communication Laboratories, Yokosuka, Japan, where he was engaged in research on monolithic integration of microwave semiconductor devices and circuits. He developed GaAs MMIC transponder modules and microwave beamforming networks aboard Japan national multibeam communication satellites, Engineering Test Satellite VI (ETS-VI) and ETSVIII, at NTT Wireless Systems Laboratories, Yokosuka. From 1999, he was engaged in research on wireless *ad hoc* networks and microwave analog adaptive antennas for consumer electronic devices at ATR Adaptive Communications Research Laboratories, Kyoto, Japan. Concurrently, he was a Consulting Engineer for the National Space Development Agency (NASDA) ETS-VIII Project in 1999, and an Invited Lecturer for Osaka University from 2000 to 2001. Currently, he is Director for ATR Wave Engineering Laboratories, Kyoto. He coauthored *Monolithic Microwave Integrated Circuits* (Tokyo, Japan: IEICE, 1997).

Dr. Ohira serves as Chair for URSI Commission C Japan Branch. He was awarded 1986 IEICE Shinohara Prize, 1998 APMC Japan Microwave Prize, and 2004 IEICE Electronics Society Prize.

Bokuji Komiyama (M'91) received the B.E. and M.E. degrees in electronics engineering in 1968 and 1970, respectively, and the D.E. degree in 1987, all from Tohoku University, Sendai, Japan.

From 1970 to 1995, he was with the CRL (currently reorganized to NICT), where he worked on low noise frequency synthesis, superconducting cavity stabilized oscillators, and low-loss material measurements at mm-wave region. In 1995, he joined ATR, Kyoto, Japan, as a project manager, where he was involved with projects of mobile wireless networks. Since 2005, he has been with Nippon Information Communications Association where he is currently in charge of approval of timestamp services. His research interests include adaptive antennas, microwave photonics, and wireless mobile communications.

Dr. Komiyama is a Member of the IEICE, the IEE of Japan, and the Japan Society of Applied Physics.

Hideichi Sasaoka (M'82) received the B.E. degree in electrical engineering from Kyoto Institute of Technology, Kyoto, Japan, in 1971 and the M.E. and Dr.Eng. degrees from Kyoto University, Kyoto, Japan, in 1973 and 1996, respectively.

In 1973, he joined the Radio Research Laboratories [presently the National Institute of Information and Communications Technology (NICT)], Japan. From 1973 to 1983, he was engaged in research on satellite communications. Since 1983, he has conducted research on mobile radio communications. He was the Director of the Communication Science Division from 1994 to 1997 and of the Intelligent Communications Division from 1997 to 1998. From 1998 to 2000, he was a Professor at Osaka Electro-Communications University, Osaka, Japan. He is currently a Professor at Doshisha University, Kyoto. His research interests are fourth-generation land-mobile communication systems, modulation and coding, and information security in mobile-radio communications.

Prof. Sasaoka is a Member of IEICE of Japan.