Chapter XX
Key Generation System Using Smart Antenna

Toru Hashimoto
ATR Wave Engineer Laboratories, Japan

Tomoyuki Aono
Mitsubishi Electric Corporation, Japan

ABSTRACT

The technology of generating and sharing the key as the representative application of smart antennas is introduced. This scheme is based on the reciprocity theorem of radio wave propagation between the two communication parties. The random and intentional change of antenna directivity that is electrically changed by using such an ESPAR antenna as variable directional antenna is more effective for this scheme, because the propagation environment can be undulated intentionally and the reproducibility of the propagation environment can be decreased. In this chapter, experimental results carried out at many environments are described. From these results, this system has a potential to achieve the "unconditional security."

INTRODUCTION

The wireless communication has become more popular and convenient by progressing of the key technologies. PDC (Personal Digital Cellular) and WLAN (Wireless LAN) have become an indispensable for many persons. On the other hands, wireless communications have danger that it is hard to notice to tapping by eavesdroppers unlike the wired communication. The common key encryption scheme is the best way to protect the wireless communication data from the eavesdroppers.

The common encryption scheme consists of two parts: encrypt and decrypt part and key management part. The encrypt and decrypt part adopts the cryptographic algorithm like AES (Advanced Encryption Standard) standardized by NIST (National Institute of Standards and Technology) in recent systems. The key management part is more important part for the communication system, especially wireless communication system. Although it has many kinds of key management scheme, many schemes only have "computational security." If the eavesdroppers have much computational power like quantum computer, they can obtain the key in practical time.

Thus the information-theoretic (unconditional) security technology attracts attention recently in various communications. One of the technologies for key generation that achieve "information-theoretic (unconditional) security" is using fluctuation of the communication channel with such smart antenna as variable directional antenna. The "information-

theoretic (unconditional) security" means that although the eavesdroppers have much computational power, it can not be unguessable from the information the eavesdroppers obtain.

The generated key is used to the common key encryption that is suitable for wireless communication data encryption between legitimate terminals. In general, the reciprocity theorem of radio wave propagation is established between legitimate terminals in wireless communications. The propagation environment of the third party listening in another place is different from that of legitimate terminals, so the eavesdropper is difficult to generate an identical key that generated between legitimate terminals. In addition, the random and intentional change of antenna directivity that is electrically changed by using such smart antenna as variable directional antenna is more effective for this system, because the propagation environment can be undulated intentionally and the reproducibility of the propagation environment can be decreased.

The technology of generating and sharing the key for common key encryption as the application of smart antenna is described in this chapter including the principle, component of this system, procedure of key generation and the experimental results at various environments performed by Aono et al(Aono, Higuchi, Ohira, Komiyama & Sasaoka, 2005) (Aono, Higuchi, Ohira, Komiyama & Sasaoka, 2006) (Aono, Higuchi, Taromaru, Ohira & Sasaoka, 2005).

KEY GENERATION SYSTEM USING THE FLUCTUATION OF RADIO WAVES

In this section, to achieve "information-theoretic (unconditional) security" in encrypted wireless communication, adopting the key generation method that the fluctuation of the radio wave channel response is used is the most suitable.

Smart antenna like an ESPAR antenna (Ohira & Cheng, 2004) is effective to an intentional fluctuation of the radio waves. This fluctuation of radio waves and the reciprocity theorem of radio wave propagation are the key technology to achieve security.

The Principle of the Key Generating and Sharing System

This system is based on the reciprocity theorem of radio wave propagation between the two terminals such as Access Point (AP) and User Terminal (UT). In addition, a smart antenna like an ESPAR antenna is used for intentional fluctuation. The key is made by this fluctuation of radio waves.

The principle of key generation and sharing is described. The beam-forming technique of the ESPAR antenna; that is, adjusting the DC voltage given to the varactors with reverse bias is used effectively. Furthermore thanks to the reciprocity theorem of radio wave propagation, the Received Signal Strength Indicator (RSSI) obtained by alternately transmitting short packets between the two terminals has the proportional relation. From this relation, RSSI profile obtained by AP and UT independently has also the proportional relation and the same encoded value is provided by making these profiles multilevel coding, for example, binary coding. As a result, these encoded values can treat as generated and shared keys.

The propagation characteristics between AP and eavesdropper (EV) is different from it between AP and UT so that an EV listening at another place has difficulty to obtain the same encoded value. Thus "unconditional (information-theoretic) Security" is achieved practically by using the fluctuation of radio waves.

The Procedure of the Key Generating and Sharing System

Configuration

The configuration of this key generating and sharing system describes below. This system consists of two terminals, AP and UT.

AP's outline drawing is shown in Fig.1, and its function block diagram is shown in Fig. 2. It consists of four parts: "Communication device," "Microcontroller," "D/A converter," and "7-elements ESPAR antenna."

- The "Communication device" sends and receives such data as syndrome, initial value, etc. which are set by a microcontroller and communicate with packets through an ESPAR antenna. The received level of packets is measured and converted into an RSSI value in this device.
- "Microcontroller" carries out the "making RSSI profile" and "generating the key" steps in the "key generator" function. These steps are based on the RSSI value from the "Communication device." The "7-element ESPAR