SECURE DOWNLOAD SYSTEM BASED ON SOFTWARE DEFINED RADIO COMPOSED OF FPGAS

Hironori UCHIKAWA[1], Kenta UMEBAYASHI[2], Ryuji KOHNO[2]

[1] Graduate School of Engineering, Division of Physics, Electrical and Computer Engineering,
Yokohama National University, 240-8501 Yokohama, Japan,
gotz@kohnolab.dnj.ynu.ac.jp
[2] ume@kohnolab.dnj.ynu.ac.jp
[3] kohno@kohnolab.dnj.ynu.ac.jp

Abstract - In this paper, we focus attention on the development of security techniques using software defined radio (SDR) technologies. We propose a new secure download system which uses the characteristics of the field programmable gate arrays (FPGAs) composing the SDR. The proposed system has the novelty that realization of high security encipherment is possible. This is achieved using the characteristic of FPGAs which allows systems to be arranged in a variety of different layouts, as well as by using the configuration information as the key. This unifies the renewal of the key and the encipherment. In addition the proposed system has the merit that it has high security against illegal acquisition such as a wiretapping, and can also be used in conjunction with any other current cipher algorithm. As an evaluation of the security, we show that the proposed system has high immunity to illegal acquisition of software using replay attack, by verification of the protocol as well as by numerical computation. The proposed system can therefore realize high security software downloads based on SDR.

Keywords - Download, security, field programmable gate array (FPGA), software defined radio (SDR)

I. INTRODUCTION

Recently, various demands such as high data rate and high reliability for mobile communications exist. In order to satisfy these demands, many kinds of communication systems are used. For these systems, the importance of the software defined radio (SDR) which can comply with the various communication standards by changing its software becomes evident [1]. SDR reconfigures itself by software download. Various download methods have been considered such as wireless, cable, and storage [2]. However wireless or cabled download from software servers have proved to be more suitable from a versatility point of view and better for smaller and lighter terminals.

In such a case of download using wireless or cable (especially wireless) there is a possibility of wiretapping. If the software obtained by wiretapping circulates illegally, manufacturers lose out on a substantial amount of income from that software. There is also a fear that the security of a wireless system is threatened when software that has been wiretapped is illegally altered. Countermeasures against wiretapping must therefore be considered. Currently there are various secure communications technologies such as cryptography and secure protocol [3] to prevent such wiretapping. A more secure system is needed than those currently available in software download. Due to the fact that the computer capability will improve in the future, SDR which can receive multi-band will exist [5]. Two approaches for the realization of more secure communications systems for SDR are considered. Firstly the improvement of security using stronger cryptography than currently available. Secondly that security is developed using SDR technologies [5], [6]. In this paper, we focus our attention on the latter approach. We propose a new secure download system using the characteristics of field programmable gate arrays (FPGAs) composing SDR.

Recently the FPGA has been promoted as a device for the composition of SDR [4]. The reason being that FPGA realizes lower power consumption and faster signal processing when compared to common micro processors. Configuration data (CD) which is the composing data of FPGAs, has the characteristic that its size is decided by the FPGA device used and not by the logic nor circuit composition of the CD [7]. The size of the CD is the same when the FPGA composing the SDR is the same device. In addition FPGAs are made up of configuration logic blocks (CLBs). The "place-and-route" operation, which arranges the wiring of the CLBs on a FPGA, can be done freely due to the characteristic that each CLB is independent [7]. Currently SDR requires FPGAs composed of one million gates or more. Such FPGAs have more than six thousand CLBs. The number of possible place-and-route operation patterns can therefore run into astronomical numbers.

We propose a secure download system exploiting the above characteristics of FPGAs. The proposed system focuses its attention on the characteristic that the size of the CD is fixed. In the proposed system an SDR terminal downloads differential data, which is generated by an exclusive OR operation between the requested CD and the current terminal CD from the software server. After the download is completed, the SDR terminal performs an exclusive OR operation, like decryption, between the current CD and the differential data downloaded.

The SDR terminal then obtains its requested CD [8]. This system is similar to a private-key cryptosystem with the CD of the SDR being the key.

We also focus on the design freedom available in an FPGA which allows many arrangement layouts for any given system. Terminals without certification cannot decrypt the differential data downloaded due to the fact that each SDR terminal has a unique CD. In the proposed system, the degree of design freedom is the degree of security. The proposed system makes the realization of high security encipherment possible. This is achieved using the design freedom mentioned, as well as unifying the key renewal and encipherment by using the CD as the key.

We evaluate the proposed system by verifying resistance to replay attack, i.e. resistance to the software being obtained illegally. We also calculate the degree of design freedom or degree of security and compare the proposed system with download system using other cryptosystem. From evaluation results, the proposed download system is seen to have a resistance to replay attack and to wiretapping, as the probability that Attackers obtain the software illegally is almost zero. The proposed download system therefore realizes a high level of security.

This paper is organized as follows: In Sect.II, the system model for software download, the characteristics of the FPGA and the assumed attacker are described. In Sect.III, we present the proposed the secure download system. In Sect.IV, we evaluate this proposed system. Finally conclusions and future research subjects are given in Sect.V.

II. System Model

A. Download Model

Fig.1 shows the download model in SDR.

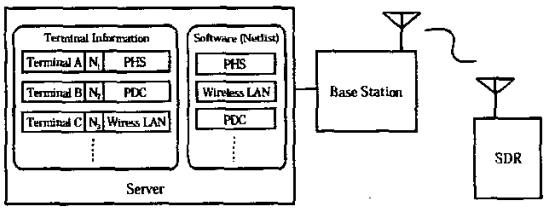

Fig. 1. Download model

An operator exists for SDR, and the model used in this paper assumes that this operator manages the software and the server. We can easily send messages to SDR by referring to this operator as the operator knows which network or which communications system each SDR belongs to. It is not possible for manufacturers to alter SDR's software illegally due to the fact that the operator manages the software which is after authorization.

The SDR terminal sends a download request to the base-station which then downloads the requested software from the server connected to the base-station. There is either a direct connection, a connection via the Internet, or other types of connection between the base-station and the server. The decision as to which type of connection is best, is decided by factors such as availability and security [2].

Some informations stored by the server are as follows,

- SDR terminal's information
  Each terminal's current configuration and a random number used in the place-and-route operation
- Software for the communications system
  Netlist of each communication service

The SDR is composed of FPGAs and the server stores softwares of which form is netlist. After the design is programmed using a hardware description language (HDL), the logic synthesizer which is similar to compiler transforms that design file to a netlist. The netlist is in effect the circuit layout and forms the stage before the configuration data. After the server receives a download request, it generates the requested CD from its netlist. The SDR terminal then downloads the CD. Additionally the server also manages other information such as what software is available for users, as a user can not download unavailable software.

B. Characteristics of FPGAs

FPGAs have the two following characteristics [7].

- The size of CD is decided by the FPGA device and not by logic nor circuit composition of the CD.
  The size of the downloading CD is always the same.
- The structure of an FPGA consists of independent CLBs which are lattice-shaped.
  We can design the arrangement layouts of the CLBs freely.

C. Attacker Assumptions

In this paper, we focus on illegal acquisition of the download. We propose a secure download system as a countermeasure against illegal acquisition.

Replay attack by impersonation and wiretapping is the illegal acquisition method assumed in the download. Attackers can impersonate any user, and can therefore tap the download stream of any user. Attackers however can not attack the server and can not extract information directly from a terminal of the SDR.

III. Proposed System

A. Protocol of the Proposed System

Fig.2 shows the protocol of the proposed system.

1) A user (SDR terminal) sends his terminal ID and download request to the server.
2) The server searches the current mode of the terminal using the terminal ID. The server then generates a random number for the place-and-route operation as well as the configuration data (CD) which the terminal requested. The server then produces the differential CD using an

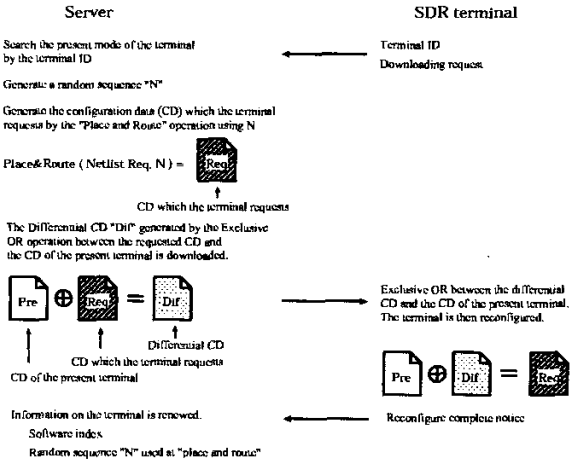

Fig. 2. Protocol of the proposed system

Exclusive OR operation between the requested CD and the current CD of the terminal. The user can now download the differential CD.

3) The user now performs an exclusive OR operation between the downloaded CD and its current terminal CD. The terminal of the user is now reconfigured.
4) The user sends a reconfigure complete notice to the server through the new downloaded communications system.

The random number is only used in the place-and-route operation. It is not necessary to share the random number between the server and the terminal. The characteristic of the proposed system is exploiting the fact that the size of the downloaded CD is always the same. SDR terminals download the differential data generated by the exclusive OR operation performed between the requested CD and the current CD of the SDR terminal. This system is therefore seen to be similar to a private-key cryptosystem in that the CD of SDR is used as the key. This key, or CD, is renewed every time the SDR is reconfigured.

Currently much time is spent on the place-and-route operation in FPGAs. It is therefore difficult for the server to perform this place-and-route operation in a timely manner depending on a request. As a countermeasure to this, some predesigned CDs are temporarily stored on the server in the proposed system.

In this paper, it is assumed that downloaded CDs do not have error bit. If transmission errors occur, the CD which a terminal has may be different from that stored on the server. The proposed system will then stops. Usually a parity check code is added to the CD, and a CD containing error bits is therefore never downloaded to the FPGA. Error correction such as channel coding is used as a countermeasure against transmission error, however is not discussed in this paper.

B. Place-and-route

Place-and-route is the operation that allocates all functions of a circuit to the CLBs and the wiring between these CLBs on an FPGA

The purpose of conventional place-and-route is to improve the FPGAs performance. The allocation of CLBs is therefore initially done randomly, then iterated so as to minimize the wiring length.

The purpose of place-and-route in this paper is not to minimize the wiring length however to generate a lot of allocation patterns and therefore realize diversity in the CD on the FPGA. The place-and-route in this paper simply allocates CLBs according to a random number. The place-and-route load is therefore no larger than the conventional case. Conventional place-and-route is run on tools made by Cadence or Synopsys using random numbers in about 100 ways. In this paper the place-and-route algorithm uses random numbers corresponding to the possible allocation of CLBs on an FPGA.

In the proposed system, security is achieved by the patterns that can be made of the CD. The independence of each CLB as a characteristics of FPGA is used to achieve the differing patterns. Fig.3 shows the layout pattern of an FPGA which has 4 CLBs and only uses 2 of them (module A and module B).

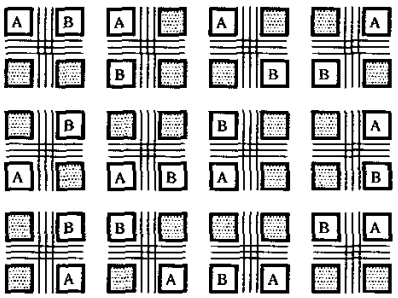

Fig. 3. Example layout

These patterns are calculated using eq.(1) where two optional CLBs are assigned to four possible CLB locations.

$$ {}_4P_2 = 4 \times 3 = 12 \tag{1} $$

In the general case the number of arrangement layout patterns for a certain logic that can be realized on an FPGA can be calculated as follows.

$$ {}_lP_m = l \times (l-1) \times \ldots \times (l-m+1) \tag{2} $$

where:

l = *The total number of CLBs on an FPGA*
m = *The number of CLBs used in the logic*

IV. Evaluation of the Proposed System

A. Resistance to Replay Attack

Replay attack describes when an attacker impersonates the user and transmits a wire-tapped download request message.

Fig.4 shows the protocol in the case of replay attack.

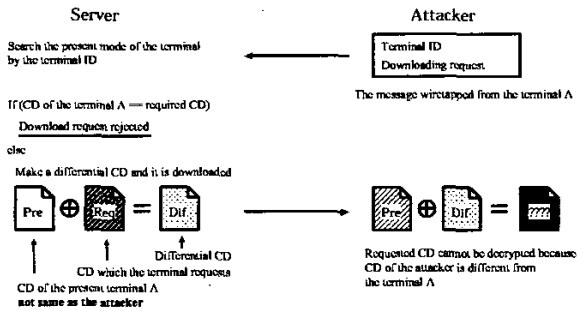

Fig. 4. Resistance to replay attack

An attack occurs when the attacker sends a download request wiretapped from the proper terminal to a server. The assumption in this paper is that the attacker impersonates another terminal easily, because authentication of the request is not strict. Attackers can therefore use replay attack easily.

The attacker sends a download request wiretapped from terminal A. The server searches for the current mode of the terminal from the terminal ID. If the CD of terminal A matches the requested CD, the request is rejected.

If on the other hand the CD of terminal A does not match the requested CD, the attacker can download the CD generated by the exclusive OR operation between the current CD of terminal A and the requested CD. The attacker however can not reconfigure his terminal as his current CD differs from that of terminal A. In this case the attacker obtains an unusable CD which can not be downloaded to an FPGA. Due to the fact that CDs usually use error correction codes, and CDs containing errors are not downloaded. The probability that the CD of an attacker matches that of terminal A is discussed in the following section. The proposed system can be seen to be resistant to replay attack.

B. Probability of Correspondence

1) Evaluation Method: In the proposed system the server produces a completely unique CD, even if the communication software is the same, through the use of a random number. Security is therefore achieved by the differing patterns that can be made of the CD. An attacker needs to tap a CD from the terminal using exactly the same configuration as a user in order to obtain the communication software illegally. In this section, we derive the probability that an SDR reconfigured with the same layout CD of another SDR exists.

The number of patterns of CD which realize a certain mode is given by n. The probability that CDs selected randomly are different from each other is derived as follows.

$$(1-\frac{1}{n})(1-\frac{2}{n})...(1-\frac{k-1}{n}) = \prod_{i=1}^{k-1}(1-\frac{i}{n}) \tag{3}$$

If n is a large real number, then $1-\frac{i}{n} \approx e^{-\frac{i}{n}}$. This estimate is derived by taking the first two terms of the following series expansion.

$$e^{-x} = 1 - x + \frac{x^2}{2!} - \frac{x^3}{3!}.... \tag{4}$$

The estimated probability of no correspondence is then

$$\begin{aligned} \prod_{i=1}^{k-1}(1-\frac{i}{n}) &\approx \prod_{i=1}^{k-1} e^{\frac{-i}{n}} \\ &= e^{\frac{-k(k-1)}{2n}} \end{aligned} \tag{5}$$

We, therefore, the probability of at least one corresponding CD to be

$$1 - e^{\frac{-k(k-1)}{2n}} \tag{6}$$

If we denote this probability as ϵ, we can solve for k as a function of n and ϵ:

$$e^{\frac{-k(k-1)}{2n}} \approx 1-\epsilon \tag{7}$$

$$\frac{-k(k-1)}{2n} \approx ln(1-\epsilon) \tag{8}$$

$$k^2 - k \approx 2n\, ln\frac{1}{1-\epsilon} \tag{9}$$

If the term $-k$ is ignored, then

$$k \approx \sqrt{2n\, ln\frac{1}{1-\epsilon}} \tag{10}$$

If we take $\epsilon = 1 \times 10^{-12}$, then

$$k \approx 10^{-6} \times \sqrt{n} \tag{11}$$

In sum, for the probability that SDRs with the same CDs exist to be over $10^{-10}\%$ is given by eq.(12).

$$k = 10^{-6} \times \sqrt{{}_{l}P_m} \tag{12}$$

2) Calculation Parameters: An FPGA which has at least a million gates is needed in SDR. The number of CLBs can range from several thousand to several ten thousand on such an FPGA. In this evaluation, we used an FPGA produced by XILINX, with the number ("I") of CLBs being 6144. Wireless LAN mounted on such an FPGA requires 2274 CLBs ("m_{w-lan}"), and personal handy phone (PHS) 1045 CLBs ("m_{phs}") [9].

Table 1
The number of CLBs used of FPGA

	CLBs
Wireless LAN	2274
PHS	1045

Table 2
Calculation result

	Layout pattern		Necessary (10^{-10}%)	
W-LAN	2.0×10^{8404}	2^{27918}	1.1×10^{4202}	2^{13959}
PHS	9.5×10^{3917}	2^{13015}	1.3×10^{1953}	2^{6488}

3) Calculation Result: Fig.5, 6, and table 2 show the calculation results for this FPGA from Eq.(11) and (12).

Results are indicated as both decimal and binary numbers. The necessary number shown in table 2 shows the number of randomly generated CDs required for the probability that 2 CDs with the same layout exist to be 10^{-10}%. In fig.5, 6, the probability that CDs with the same layout exists is shown to be 1% when the necessary number is about 10^{1958} in PHS and is about 10^{4202} in wireless LAN. If many SDR terminals are on the market, the probability that an SDR has exactly the same CD as another would be extremely low as seen by these results.

V. Conclusions and Future Studies

We proposed a secure download system exploiting the characteristics of FPGAs. We showed that the proposed system has very strong resistance to replay attack. Obtaining communication software from SDR illegally is therefore difficult in the proposed system.

However, more research is necessary to prove the security of the new cryptosystem.

Future areas of research are,

- Evaluation of security against other attacks
- Analysis of the structure of configuration data
- An attack specific to the proposed system

References

[1] Joe Mitola: "The Software Radio Architecture," IEEE Commun. Mag., vol. 33, no. 5, pp. 26-38, May 1995.

[2] "SDRF Technical Report 2.2 Chapter 6," SDR Forum, Nov. 1999

[3] Bruce Schneier: "Applied Cryptography ; 2nd Edition," John Wiley & Sons, Inc., 1996.

[4] Mark Cummings, Shinichiro Haruyama: "FPGA in the Software Radio," IEEE Communications Magazine, Feb. 1999.

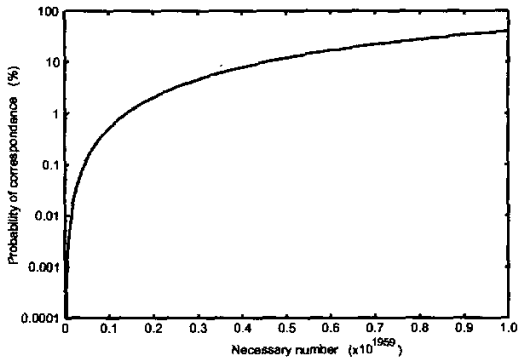

Fig. 5. Probability of correspondence (PHS)

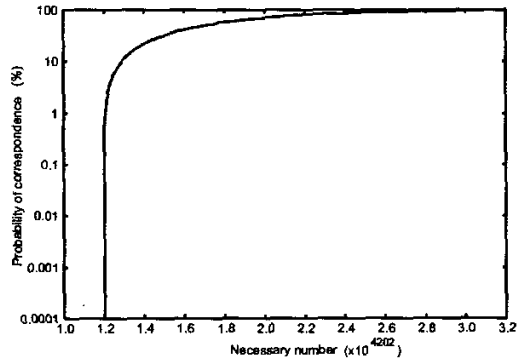

Fig. 6. Probability of correspondence (Wireless LAN)

[5] Makoto Sugita, Kazuhiro Uehara, and Shuji Kubota: "Flexible Security Systems and a New Structure for Electronic Commerce on Software Radio," Proc. of VTC2000, pp. 3033-3040, Sept. 2000.

[6] H. Uchikawa, K. Ikemoto, K. Mizutani, K. Umebayashi, and R. Kohno: "Adaptive Security Levels Control Method Based on Software Defined Radio," Proc. of WPMC'01, pp. 1503-1508, Aalborg, Sept. 2001.

[7] Xillinx Inc.: "Virtex 2.5V Gate Arrays," DS003 (v2.2), May 2000.

[8] H. Uchikawa, K. Umebayashi, and R. Kohno: "A Study on a Secure Download System for Software Defined Radio," IEICE Technical Report, SR01-24, Dec. 2001.

[9] T. Shono, H. Tanaka, H. Shiba, K. Uehara, S. Kubota, and M Umehira: "Software Defined Radio Prototype for PHS and Wireless LAN Systems (II) - Wireless LAN mode -," IEICE Technical Report, SR01-13, Oct. 2001.

[10] Douglas R. Stinson: "Cryptography," CRC Press, 1995.

[11] J. Daemen and V. Rijimen: "AES Proposal: Rijndael," http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf, 1998.