

ACU and RSM Based Radio Spectrum Management for Realization of Flexible Software Defined Radio World

Kei SAKAGUCHI^{†a)}, *Regular Member*, Chih FUNG LAM[†], Tien Dzung DOAN^{†*},
Munkhtur TOGOCH^{†**}, *Nonmembers*, Jun-ichi TAKADA[†],
and Kiyomichi ARAKI[†], *Regular Members*

SUMMARY A new spectrum management architecture for a flexible software defined radio (SDR) is proposed. In this architecture, the SDR hardware and software are certified separately so as not to destroy the SDR flexibility, but to ensure that any combinations of hardware and software are compliant to the radio regulations even at the system (vertical) handover, global (horizontal) handover, and upgrade (forward) or downgrade (backward) handover. This architecture is based on automatic calibration & certification unit (ACU), built-in GPS receiver, and radio security module (RSM). The ACU is a hardware embedded RF manager that dynamically controls the output power spectrum to be compliant to the local radio regulation parameters. This local radio regulation parameters are securely downloaded to the hardware as an electronic label of the SDR software and stored in the RSM which is a security manager of the hardware. The GPS position check is used, especially during roaming, to keep the compliancy of the terminal to each local radio regulations managed by the geographical region. The principle parties involved in this architecture are telecommunication certification body (TCB), SDR hardware maker (HW maker), SDR software maker (SW maker), and SDR user. The roles and relationships of these four parties in the proposed architecture are clarified in this paper.

key words: *software defined radio, spectrum management, automatic calibration and certification unit, radio security module, GPS*

1. Introduction

Traditionally radio spectrum is managed in frequency and space. But there is still one more dimension available, that is time. If the radio terminal can dynamically control its spectrum, a more efficient and flexible radio environment can be achieved. Such a policy is recently suggested in [1]. The key enabling technology is the software defined radio (SDR) [2]–[4].

The SDR can change its radio parameters, such as frequency, power, and modulation types, by downloading and installing a new SDR software in the field. This field upgradability enables system (vertical) handover, global (horizontal) handover, and upgrade (forward) or downgrade (backward) handover of the SDR terminal.

Together with this attractiveness, new security issues are also conceived. How to protect the radio spectrum from the misuse or abuse of SDR flexibility?

The US Federal Communication Commission (FCC) has recognized the importance of this security issue and reported an initial policy on the SDR [5]. According to this report, the radio spectrum is protected by proving the compliancy of the combination of SDR hardware and software to the local radio regulations in each telecommunication certification body (TCB) before this combination is brought to the market. And in the field the SDR hardware prevents unauthorized software to be installed by using the electronic label that contains the information about those approved combinations. This method is appropriate for the introductory period of the SDR, since it is a simple extension of the present approval test procedure. But in the mature period of SDR, it is not reasonable since exhaustive combinations of hardware and software must be tested. This problem is more serious if global roaming is considered. Moreover such a mechanism degrades the SDR flexibility since third party software maker cannot release their new software until they have negotiated with each hardware maker in the world. Therefore, a new spectrum management architecture, in which the hardware and software are certified separately as suggested in [6], is required. This is the principle motivation of this research.

First of all, it is better to clarify what are the threats, especially if the hardware and software are separately certified. There are two kinds of spectrum security threats. One is the threat during operation of the software, and the other is the threat at installation of the software.

During operation, there are three types of security threats.

- non ideal RF threat

Since the RF module in the hardware is not ideal, e.g. the nonlinearity in the power amplifier, the compliancy of the output spectrum is not guaranteed even with the combinations of the certified hardware and software.

- threat due to roaming

Since the radio spectrum is managed differently in dif-

Manuscript received April 9, 2003.

Manuscript revised August 14, 2003.

[†]The authors are with the Graduate School of Science and Engineering, Tokyo Institute of Technology, Tokyo, 152-8552 Japan.

*Presently, with the Sony Technology Center.

**Presently, with the IBM BCS.

a) E-mail: kei@mobile.ss.titech.ac.jp

ferent geographical regions, e.g. each country manages the radio regulations in different manner, there is a problem if the terminal roams from one country to the other with the same SDR software.

- bugs and Trojan horses in the software

As we can see in the PC environment, it is impossible to detect such problems even with a tremendous number of tests.

At the installation of the software, there are two security threats related to spectrum management.

- compatibility threat on hardware & software sets

Without checking the compatibility of the hardware and software during installations, problems may occur.

- illegal software and hardware

To prevent these, the hardware and software have to do mutual verification since these two are separately certified in the TCB.

To mitigate these threats, a new SDR hardware architecture and a new spectrum management architecture are proposed in this paper. The proposed hardware architecture has automatic calibration & certification unit (ACU) [7], built-in GPS receiver, and radio security module (RSM) [8]. The ACU is a hardware embedded module that dynamically controls the output spectrum to be compliant to the radio regulation parameters. Therefore this is the best measure against the non ideal RF threat and bugs and Trojan horses of softwares. The built-in GPS receiver is used for the terminal location check that mitigates the threat due to roaming. Finally the RSM manages the whole life-cycle of the software, that includes downloading, installation, operation, and termination. In the downloading, the RSM manages the mutual verification process to prevent illegal softwares and also illegal hardware. The compatibility check is performed in the installation process. In the operation process, the RSM manages the compliancy to the radio regulations by handling the ACU and GPS. In the case of an incident the RSM terminates the software, and instructs the SDR user to download another software. In the new spectrum management architecture, the radio regulation parameters and its geographical region are inserted to the electronic label of the SDR software. And these are securely downloaded to the SDR hardware with the digital signature signed by the TCB. After verification of the digital signature, these two parameters are used in the ACU and RSM respectively. Since the ACU has an ability to check the output spectrum, the principle task of the TCB is to check the functionality of the ACU as a hardware certification test and to insert the radio regulation parameters to the electronic label of the software as a certification. There is no need to test the combinations of the hardware and software as in [5]. Thus the separate certification procedure can be

realized. The involved parties in this architecture are not only the TCB but also the SDR hardware maker (HW maker), SDR SW maker (SW maker), and SDR user. The roles and relationships of these parties are clarified.

Some of the security issues and threats are discussed in the SDR Forum [9]–[12] and some other projects [13]–[18]. Among them an idea partly similar with the ACU was proposed in [17]. Our work can be considered as an extension of this work, since the overall spectrum management architecture is considered in this paper.

The organization of this paper is as follows. Section 2 proposes the new SDR hardware architecture including the ACU, GPS, and RSM. In Sect.3, the new spectrum management architecture is described, including the roles and relationships of the four involved parties and the separate certification procedures. Some discussions on security strength and implementation issues follow in Sect.4. Finally the concluding remarks are given in Sect.5.

List of acronyms and abbreviations

HW	: hardware
SW	: software
ACU	: automatic calibration & certification unit
RSM	: radio security module
TCB	: telecommunication certification body
SWP	: software package
PkTCB	: public-key of the TCB
PkHW	: public-key of the hardware
SkHW	: secret-key of the hardware
IdHW	: hardware ID
$DS_{TCB}[x]$	: digital signature x signed by TCB
$E_y[x]$	: encryption of x by the key y
$E_y^{-1}[x]$	: decryption of x by the key y
$V_y[x]$	: DS verification of x by the key y
SSL	: secure socket layer
WSP	: wireless service provider

2. Proposed SDR Hardware Architecture

The general architecture of the proposed SDR hardware is depicted in Fig.1. First of all, it is better to identify the reconfigurable and unconfigurable modules in the SDR architecture. The programmable upper layer and the programmable physical layer are in the reconfigurable part, where any SDR software can be installed. Since the upper layer, including application program, network protocol, etc., is not directly related to the output spectrum, we will emphasis on the physical layer. The analog RF module is partly reconfigurable by the control signal from the physical layer. The ACU is an unconfigurable module, and located between the programmable physical layer and RF modules. All the data signals and control signals going to

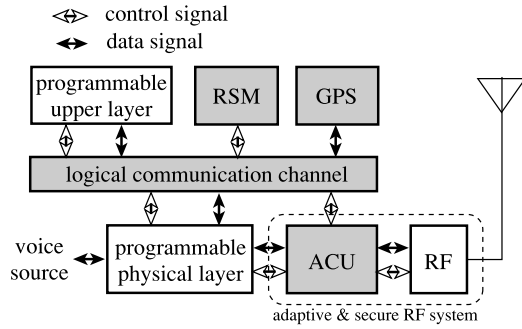


Fig. 1 Proposed SDR hardware architecture.

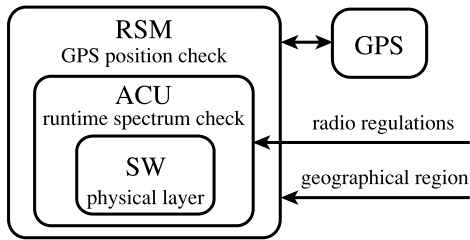


Fig. 2 The relationship between ACU, GPS, and RSM.

the RF module from the physical layer are under the management of the ACU. In this sense, the ACU can be called as RF manager. The proposed SDR hardware has a built-in GPS receiver, which is also in the unreconfigurable part, for the geographical management of the terminal. The RSM is also in the unreconfigurable part, and manages all the security components in the SDR.

The relationship of these three modules, ACU, GPS, and RSM, is illustrated in Fig. 2. The software of physical layer is under the management of the ACU. The principle function of the ACU is runtime spectrum check of the output signal, and judges whether it satisfies the local radio regulation parameters given by the TCB through the electronic label of the software. This ACU is under the control of the RSM. As one of the functions of the RSM, it manages the location of the terminal by using the GPS position check to judges whether it satisfies the geographical region of the local radio regulations also given by the TCB through the electronic label of the software. By using these functions, the proposed hardware architecture can ensure the spectrum security of the terminal.

2.1 Automatic Calibration & Certification Unit

The ACU is a core module for the proposed spectrum management architecture. The ACU has two important functions. The first one is called adaptive RF function and the other one is called secure RF function.

The block diagram for the adaptive RF function is shown in Fig. 3. The ACU adaptively controls the RF components or predistort the input signals in ac-

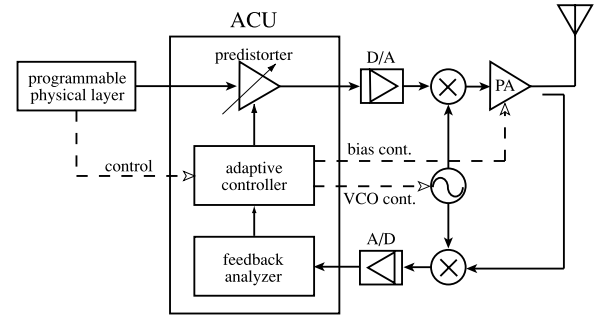


Fig. 3 Adaptive RF function of ACU in the SDR hardware.

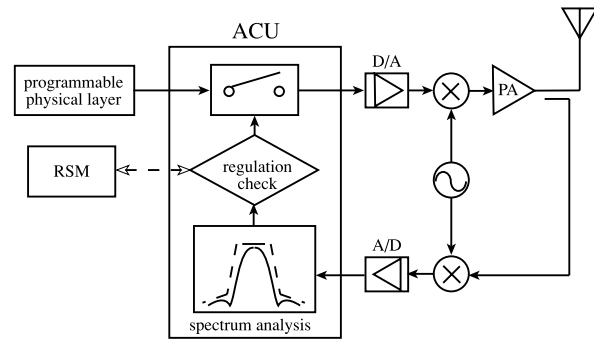


Fig. 4 Secure RF function of ACU in the SDR hardware.

cordance with the control signals from the SDR software. A part of the RF output signal is feed backed to analyze the condition of the RF module at the required frequency, power, and modulation type. In this sense it can be understood as automatic calibration of the hardware. The detailed architecture and algorithm of the adaptive RF function is discussed in the companion paper [19]. By using this mechanism, we can tune up the SDR hardware with respect to the specific SDR software, and resulting in the maximization of the power efficiency. Such a module is worth implementing even with an additional cost.

The second function of the ACU, namely the secure RF function, is directly related to the proposed spectrum management architecture. As shown in Fig. 4, the output power spectrum is monitored in the feedback analyzer, and checked the compliancy of the spectrum to the local regulations, which are stored in the RSM. In this sense, it can be understood as an automatic certification. The regulation parameters stored in the RSM are;

- center frequency
- signal bandwidth
- signal power
- adjacent channel power ratio

and test conditions. Since these parameters are dependent on the SDR software, it is reasonable to download them with the software itself. Such a mechanism is introduced in the proposed spectrum management ar-

chitecture. The adaptive RF function collaborates with this secure RF function to control the RF components or predistort the input signals until the output signal satisfies the regulations. If the output signal does not satisfy the requirements as the result of adaptation, the ACU terminates the SDR software and alarm it to the SDR user through the RSM security management function.

2.2 Radio Security Module

As shown in Fig.5, the RSM manages the security issues related to whole life-cycle of the software. It includes downloading, installation, storage, operation, and termination of the software. To perform these functions the RSM contains

- security components;
secrecy management, key & certification management, information integrity management, configuration management, and spectrum management
- public-keys of all TCBs (192 countries)
- hardware public-key (PkHW) and secret-key (SkHW).

These are given by the hardware maker. And also the RSM contains

- unique hardware identity (IdHW)
- hardware digital signature ($DS_{TCB}[IdHW, PkHW]$).

These two are inserted to the RSM by the TCB as the certificate of the test. Finally it also contains

- current software's radio regulation parameters
- current software's geographical region.

These two are supplied from the electronic label of the software. Among them, only PkHW, IdHW, and

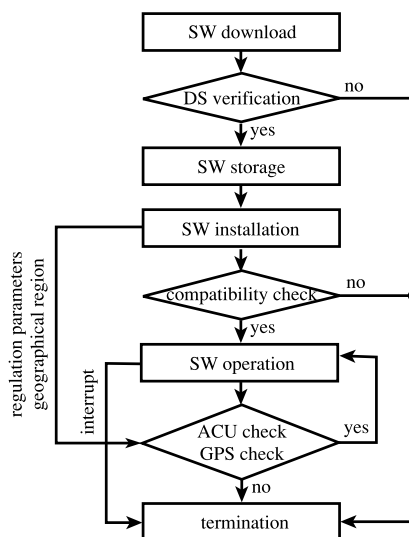


Fig. 5 Processes performed by the RSM.

$DS_{TCB}[IdHW, PkHW]$ can be accessed by the user to download a software. Security components and public-keys of TCBs can only be updated by the HW makers.

At the downloading of the software, the RSM instructs the secure download process and mutual verification of the hardware and software by using the hardware public-key, hardware digital signature and downloaded software digital signature. A more detailed description of this process is given in Sect.3.3. In the installation process, the RSM checks the compatibility of the software to the hardware by comparing the hardware capability parameters given by the TCB and hardware requirement parameters of the software. If the software is not compatible to the hardware, the RSM terminate the installation process. Such a function is called configuration management, and some discussions are provided in Sect.4.3. Detailed discussions are also given in [18]. After the successful installation, the software is stored in the internal memory of the RSM, and it can only be accessed by the RSM to make sure the information integrity. If the user instructs the execution, or the system is in the handover process, the stage moves to the operation. In the operation the RSM handles the ACU and GPS for runtime spectrum check and position check respectively to keep the compliancy of the terminal to the local radio regulations. If the ACU or GPS detects some problem, the RSM automatically terminates the software and informs the user to download another software. Thus the SDR terminal can be protected from the threats discussed in Sect. 1.

3. Spectrum Management Architecture

A new spectrum management architecture, in which the hardware and software are separately certified, is proposed in this section. Firstly, the roles and relationships of involved four parties, TCB, HW maker, SW maker, and SDR user are clarified. And then the roles of TCB and SW maker are discussed in detail. The role of HW maker is omitted here, since it is to integrate the ACU, GPS, and RSM in the hardware as described in the previous sections.

3.1 Roles and Relationships of Involved Four Parties

The roles and relationships of involved four parties are illustrated in Fig. 6. The SDR hardware and SDR software are certified separately in the TCB according to the request from each maker. Then HW maker sells the certified terminal to the SDR user. The SDR user requests download of a new SDR software from the SW maker. The SW maker verifies the source of the hardware based on the digital signature attached in the hardware, and provides the secure download where only the requested hardware can decrypt the software. This is a reasonable relationship between four parties since there is no direct path from the SDR user to the TCB

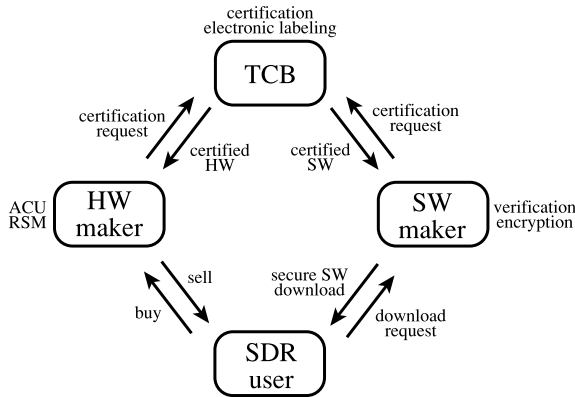


Fig. 6 The roles and relationships of involved four parties in the proposed spectrum management architecture.

and from the SW maker to the HW maker. It reduces the burden in the TCB and enhances the flexibility of the architecture.

The additional roles of HW maker is to construct a reliable ACU and RSM. And that of SW maker is to verify the source of hardware and provide the secure download process to protect the abuse of the certified software. The roles of TCB are to test the reliability of the ACU and RSM, attaching the radio regulation parameters to the electronic label of the software, and also attaching the digital signature both to the hardware and software. This mechanism ensures the compliancy of any combinations of hardware and software to the local radio regulations, since it can prevent the threats both at the installation and operation of the software.

The responsibilities of four parties are also clear. The responsibility of the HW maker is to protect the SDR hardware from illegal spectrum emission, e.g. due to the uncertified softwares or software bugs, by using ACU and RSM. And that of SW maker is to protect the SDR software from the illegal distribution or equivalently to be run on uncertified hardwares. The responsibility of the TCB is to protect the certification system from rogues. Since the responsibilities of the HW maker and SW maker are in good balance, this security architecture should work well.

3.2 SDR Certification Procedure

Since the proposed hardware architecture has an ability of runtime regulation check, the principle test in the TCB is to check the functionality of the ACU and RSM. On the other hand, the TCB inserts the radio regulations, which the software should obey, into the electronic label of the software and these parameters are used in the ACU and RSM during operation of the software. These mechanisms ensure the separate certification system. Finally the TCB attaches the digital signatures as the certificates to the hardware and soft-

ware individually.

3.2.1 Hardware Certification Procedure

Firstly the conventional test parameters that cannot be checked in the ACU should be tested. These are hardware specific parameters and are not related to the SDR software. These test parameters are

- frequency accuracy
- spurious emission
- collateral emission of receiver.

The following functionalities of ACU should be tested with the SDR software emulator and spectrum analyzer.

- ACU feedback chain accuracy
- ACU runtime regulation check test

These are most important test by the TCB in the proposed spectrum management architecture. The following functionalities of RSM should also be tested.

- RSM software download & installation test
- RSM operation test (with ACU and GPS)

If all above tests are passed, the following electronic labels are inserted into the RSM.

- hardware capability parameters (allowable frequency and power range where the ACU passed the test)
- unique hardware ID (IdHW)

The hardware capability parameters are used by the RSM to reject incompatible softwares. Finally the certification test procedure is completed by attaching the digital signature signed by the TCB as described below.

- $DS_{TCB}[IdHW, PkHW]$

This digital signature is used for the verification of hardware by the SW maker as described in Sect. 3.3.

3.2.2 Software Certification Procedure

Firstly, the applied SDR software is tested with the hardware emulator in the TCB. The test parameters are same with the ordinal certification test.

- SDR software operation test

Of course it is impossible to check all the viruses or bugs in the software by this test. Therefore we introduced the ACU for runtime regulation check. Thus the above mentioned software test is not so important, and is considered as the coarse filter to check for obvious viruses or bugs in the software.

The principle task of the software certification pro-

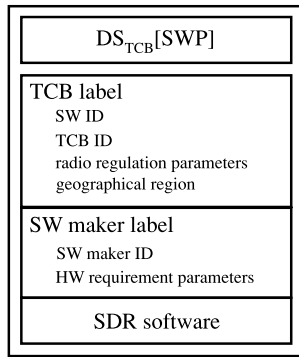


Fig. 7 SDR software package.

cedure is electronic labeling and attaching digital signature. There are two types of labels for each software, namely SW maker label and TCB label as in Fig. 7. The SW maker label contains

- SW maker ID and hardware requirement parameters.

TCB label contains

- software ID, TCB ID, radio regulation parameters, and geographical region of the regulation.

The radio regulation parameters and its geographical region are used for runtime regulation check in the ACU and RSM as described in Sect. 2. TCB ID, software ID, and SW maker ID are used to trace the responsibility in the case of serious security problems. Finally the hardware requirement parameters, which are radio operation parameters of the software, are for the compatibility check performed in the RSM.

The software and SW maker label are submitted by the SW maker to the TCB that manages the geographical region where this software is to be operated. If the software passes the TCB's test, the TCB creates the TCB label for the software. Combination of the TCB label, SW maker label and software is here after called as software package (SWP). A digital signature of the SWP is then created by the TCB as

- $DS_{TCB}[SWP]$.

It is used for the verification of the software in the hardware. With this, software certification process by the TCB is completed.

3.3 Mutual Verification & Secure Software Download

To prevent illegal hardware or softwares, the mutual verification of the hardware and software is performed between the SDR hardware and SW maker. There are three types of illegal softwares, that are certified but tampered software, uncertified virus software, and certified software but distributed by illegal syndicates. The first two can be refused by the verification of the digital signature given by the TCB. To prevent illegal

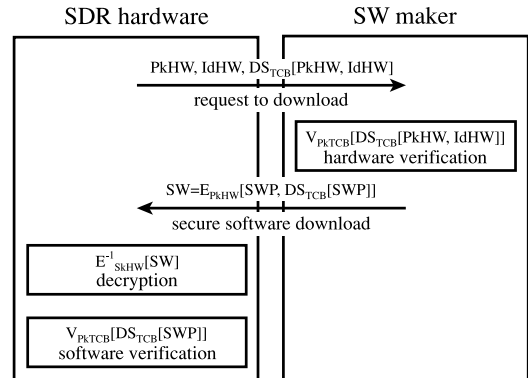


Fig. 8 Mutual verification of hardware and software.

distribution of the certified software, the secure download process is introduced.

The diagram of these sequences is illustrated in Fig. 8. The download process is triggered by the RSM in the SDR hardware by submitting the request of download with the PkHW, IdHW, and $DS_{TCB}[PkHW, IdHW]$ to the SW maker. The SW maker checks $DS_{TCB}[PkHW, IdHW]$ by using PkTCB to verify the source of hardware. The IdHW is used in the SW maker to trace the software in the market. After the successful verification, the SW maker prepares the secure download process by encrypting the SWP and $DS_{TCB}[SWP]$ by the submitted PkHW. To speed up the encryption process, an approach similar to SSL is used. Instead of encrypting the SWP by the public-key, a symmetric-key is used. This symmetric-key is then encrypted by the public-key (PkHW). Only the target hardware can decrypt it, since this is the terminal which has the corresponding secret-key (SkHW). Upon successful decryption, the RSM checks $DS_{TCB}[SWP]$ by using the stored PkTCB in the RSM to verify the source of software. With this, the mutual verification and secure download are completed.

4. Discussions

4.1 Case Studies

Typical cases related to the spectrum security issues were investigated as shown in Fig. 9.

- A certified hardware will run any certified softwares whilst the ACU and RSM keep the compliancy of the terminal to the local radio regulations by the runtime spectrum check and GPS position check. By this mechanism, the SDR terminal can be protected from all threats during the operation of the software.
- A certified hardware does not run any uncertified software because the RSM verifies the digital signature of the SWP.
- Uncertified hardware cannot download any SWP

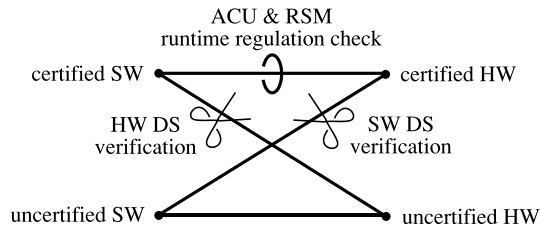


Fig. 9 Typical case studies.

because it does not have a valid hardware digital signature. Even if the hardware digital signature is copied, the uncertified hardware cannot decrypt the encrypted SWP because it does not have the corresponding hardware secret-key.

- Uncertified hardware will run uncertified softwares. In this case, it is left for the law enforcement team to eradicate these illegal terminals.

4.2 Visibility and Reliability of GPS Signal

The function of GPS position check in the RSM depends on the visibility and reliability of the GPS signal. For future work, some implementation issues need to be addressed in order to solve the problem of visibility and enhance the reliability of this function. For example, in the case where the GPS signal is unavailable, the last record can be used to predict the present location within a short time period.

4.3 Wireless Service Provider

Since the SDR hardware has hardware capability parameters and SDR software has hardware requirement parameters, a new type of service agency, it is called wireless service provider (WSP) in this paper, will be available in the future wireless market. The SDR user registers the type of hardware in the WSP database. And then the WSP searches the best fit SDR software according to the hardware capability parameters and the requirements from SDR user. Such a kind of business model will enhance the flexibility of the proposed spectrum management architecture.

4.4 Preliminary Implementation

The ACU and RSM were implemented on prototype hardware to emulate a SDR terminal. The ACU was implemented on a 1M gates FPGA board. It took about 300 k gates to implement adaptive RF and secure RF functions of the ACU. A normal PC was used as a platform to host the RSM. The RSM was implemented by using Java2 SE. The RSM was a Java program at administrator privilege. A system service was triggered by the user to perform software download and installation process by the RSM. All TCB public-keys and security

components were stored under administrator privilege. The RSM java class file size was about 300kbytes and executing memory size was less than 7 Mbytes.

As a result, we could confirm the capability of the proposed SDR architecture on the present off-the-shelf hardware devices.

5. Concluding Remarks

Traditional radio equipment certification procedure is not adequate for the SDR since the radio parameters can be changed dynamically by downloading the software in the field. With this consideration in mind, a new spectrum management architecture was proposed in this paper. In this architecture, the SDR hardware and software are certified separately so as not to destroy the SDR flexibility, but to ensure that any combinations of hardware and software are compliant to the radio regulations. This architecture is based on the ACU, built-in GPS receiver, and RSM. The ACU is a hardware embedded RF manager that dynamically controls the output power spectrum to be compliant to the local radio regulation parameters. This local radio regulation parameters are securely downloaded to the hardware as an electronic label of the SDR software and stored in the RSM which is a security manager of the hardware. The GPS position check is used, especially during roaming, to keep the compliancy of the terminal to each local radio regulations managed by the geographical region. The principle parties involved in this architecture are the TCB, SDR HW maker, SDR SW maker, and SDR user. The roles and relationships of these four parties in the proposed architecture, particularly the certification procedures in the TCB, were clarified.

Acknowledgement

This research is partly supported by the fund from the Telecommunications Advancement Organization (TAO) of Japan.

References

- [1] "Spectrum policy task force," Federal Communications Commission Report, ET Docket, no.02-135, Nov. 2002.
- [2] J. Mitola, III, Software radio architecture—Object-oriented approaches to wireless systems engineering, John Wiley & Sons, 2000.
- [3] W. Tuttlebee, Software defined radio—Origins, drivers and international perspectives, John Wiley & Sons, 2002.
- [4] J.H. Reed, Software radio—A modern approach to radio engineering, Prentice-Hall PTR, 2002.
- [5] "Authorization and use of software defined radio," Federal Communications Commission Report, ET Docket, no.00-47, Sept. 2001.
- [6] Y. Suzuki, "Interoperability and regulatory issues around software defined radio (SDR) implementation," IEICE Trans. Commun., vol.E85-B, no.12, pp.2564–2572, Dec. 2002.

- [7] M. Togooch, K. Sakaguchi, J. Takada, and K. Araki, "Automatic calibration unit (ACU) and ACU employed authorization procedure (AMAP) for SDR," SDR Forum Input Document, SDRF-02-I-0020, April 2002.
- [8] J.J. Fitton, "Security consideration for software defined radios," Proc. Software Defined Radio Technical Conference, vol.1, pp.137-143, Nov. 2002.
- [9] SDR Forum web site, <http://www.sdrforum.org/>
- [10] "Requirements for radio software download for RF reconfiguration," SDR Forum Approved Document, SDRF-02-A-0007, Nov. 2002.
- [11] "SDR system security," SDR Forum Approved Document, SDRF-02-A-0006, Nov. 2002.
- [12] R. Falk, J.F. Esfahani, and M. Dillinger, "Reconfigurable radio terminals—Threats and security objectives," SDR Forum Input Document, SDRF-02-I-0056, Nov. 2002.
- [13] TRUST web site, <http://www.ist-trust.org/>
- [14] SCOUT web site, <http://www4.in.tum.de/~scout/>
- [15] Mobile VCE web site, <http://www.mobilevce.com/>
- [16] SCA web site, <http://www.crc.ca/en/html/scari/home/home>
- [17] J.F. Esfahani, N. Greco, G. Vardoulas, and N. Drew, "Detection & control of the rogue SDR-terminals in the future network," SDR Forum Input Document, SDRF-01-I-0048, Aug. 2001.
- [18] K. Moessner, S. Hope, P. Cook, W. Tuttlebee, and R. Tafazolli, "The RMA—A framework for reconfiguration of SDR equipment," IEICE Trans. Commun., vol.E85-B, no.12, pp.2573-2580, Dec. 2002.
- [19] K. Sakaguchi and K. Araki, "Complex power series based dual loop digital predistortion linearizer dedicated for spectrum manager on the software defined radio," submitted to IEICE Trans.



Kei Sakaguchi was born in Osaka, Japan, on November 27, 1973. He received the B.E. degree in electrical and computer engineering from Nagoya Institute of Technology, Japan, in 1996, and the M.E. degree in information processing from Tokyo Institute of Technology, Japan, in 1998. From 2000 he is a Research Associate at Tokyo Institute of Technology. He received the Young Engineer Awards from IEICE Japan and IEEE

AP-S Japan chapter in 2001 and 2002, respectively. His current research interests are in mobile propagation measurement, MIMO communication systems, and software defined radio. He is a member of IEEE.



Chih Fung Lam was born in Johore, Malaysia, on July 2, 1977. He received B.E. degree in Computer Engineering from Multimedia University, Malaysia, in 2001, and the M.E. degree in electrical and electronic engineering from Tokyo Institute of Technology, Japan, in 2003. He is currently involved in D.E. program in Tokyo Institute of Technology, Japan. He received the president award from Multimedia University in 2001. His current research

interest is in software defined radio's security architecture. He is a member of IEEE.



Tien Dzung Doan was born in Hatay, Vietnam on October 28, 1976. He received the B.E. and M.E. degrees in electrical and electronic engineering from Tokyo Institute of Technology, in 2001 and 2003, respectively. He is currently working at Sony Technology Center in Japan. His research interest is in software defined radio.



Munkhtur Togooch was born in Ulaanbaatar, Mongolia on June 12, 1974. He received the B.E. and M.E. degrees in electrical and electronic engineering from Tokyo Institute of Technology, in 2000 and 2002 respectively. Currently he is a Management Consultant in IBM BCS in Japan.



Jun-ichi Takada was born in Tokyo in 1964. He received B.E., M.E. and D.E. degrees from Tokyo Institute of Technology, in 1987, 1989 and 1992, respectively. In 1992-1994, he was a Research Associate in Chiba University, Japan. From 1994 he is an Associate Professor at Tokyo Institute of Technology. He received the Excellent Paper Award and Young Engineer Award from IEICE Japan in 1993 and 1994, respectively. His current research

interests are array signal processing, mobile communication and numerical simulation of waves. He is a member of ITEJ, IEEE, SIAM, AGU and ACES.



Kiyomichi Araki was born in Nagasaki on January 7, 1949. He received the B.S. degree in electrical engineering from Saitama University, in 1971, and the M.S. and Ph.D. degrees in physical electronics both from Tokyo Institute of Technology, in 1973 and 1978, respectively. In 1973-1975, and 1978-1985, he was a Research Associate at Tokyo Institute of Technology, and in 1985-1995 he was an Associate Professor at Saitama University. In

1979-1980 and 1993-1994 he was a visiting research scholar at University of Texas, Austin and University of Illinois, Urbana, respectively. He is currently a Professor at Tokyo Institute of Technology. Dr. Araki is a member of IEEE and Information Society of Japan. His research interests are information security, coding theory, communication theory, circuit theory, electromagnetic theory, microwave circuits, etc.