A Review on Implementation and Working of Software Defined Radio in Critical Communication Set Up for Ad Hoc Networks

Tanu Preet Singh, Vishal Sharma, Harpuneet Kaur
Department of Computer Science & Engineering, Amritsar College of Engineering & Technology, Punjab Technical University, Jalandhar,India

R.K. Singh
Professor & HOD, Department of Electronics & Communication Engineering, Uttarakhand Technical University, Dehradun, India.

ABSTRACT
Telecommunication systems, with the support of digital technology had proven their efficiency in the world market. Digital processors had given rise to a new invention called Software Defined Radio which allows dynamic programming of the radio equipment i.e. A flexible architecture whose behavior is dependent on the software behind it and not only on its hardware. It reflects the convergence of two dynamic technologies: Digital radio and Real-time downloadable software. Runtime download also give rise to some security issues such as unauthorized modification of the software, customizing the software and misusing it, resulting in radio malfunction. In this paper the origin of the SDR technology along with its basic principle of operation, download mechanisms and the supporting technologies has been discussed.
The comparison between the traditional architecture and new secure architecture has been illustrated. The new architecture has proven to be more secure and robust in the vulnerable conditions. SDR can therefore be implemented in many general purposes and embedded applications.

General terms
Telecommunication networks, software defined radio, SDR, digital processors, radio equipment, A2D converter, base station, tamper proof radio, primary and secondary user, Virtual machine,

Keywords
RF front end, OTA download, GNU Radio, Radio Operation Environment (ROE),Radio Application(RA), Quality of Service (QoS), Service provider application(SPA), User application(UA), User application environment(UAE), Virtual hardware V-HW, Secure radio middleware(SRM),

1. INTRODUCTION
In the past few decades the telecommunication system had undergone a continuous evolution in its standards.
The digital technologies had given rise to the new inventions. In the present scenario the digital processors provide the capability of dynamically programming the transmission and receiving signals over the available bandwidth. The behavior of the radio equipment can be changed simply by re-programming the software working behind it. Reconfiguration of the software under operation at the runtime had given rise to the new radio model called *Software Defined Radio (SDR).* In this model, only the RF-front end is confined to the hardware control and the actual behavior of the radio is decided by the software behind it. Thus the radio behavior is now not restricted to the hardware circuits but had become dynamic element, having the capability to change its operating characteristics. The operating characteristics of software radio include Bandwidth, Modulation, Frequency, Coding rate etc. With the introduction of Software defined radio these operating characteristics can even be modified during the data transmission. Therefore SDR leads to the development of *Software Reconfigurable Digital Radio*.

1.1 What is software radio?

The architecture for purist radio is shown in fig 1.The software radio is a step towards achieving a common global standard for the radio communication. It is a reconfigurable radio interface in which the software working behind the radio is reconfigured using OVER-THE-AIR (OTA) download. It assumes that an A2D converter is present at the antenna that converts a wireless analog signal into the digital information signal.

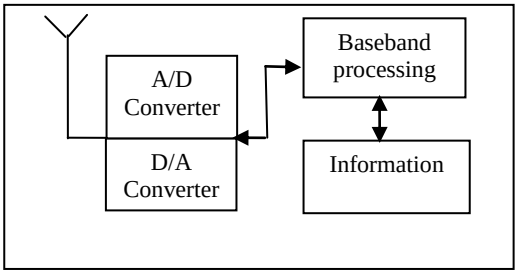

Fig 1: Architecture of purist software radio implementation [12]

Although it will take some time to implement the SDR technology but beginning towards the software radio reconfiguration approach is done. Example: Dynamic download on java phones is successful now.

1.2 Commercial and technical scope of SDR

The SDR technology is setting a direction towards the commercial development and providing a better service level to the customers using various applications like mobile applications. Thus the SDR attracts the customers for using the secure and high quality services provided by it and have the potential to influence the world of wireless communication.

*New user applications***:** It can be used to get easy and quick information about the new services, interactive subscriber services and operator customization of the handset interface.[12]

*1.2.1 Flexible services to the subscriber***:** It provides the interactive services to the user i.e. it considers the choice of the user and behaves according to the response issued by the user. Example: Bandwidth on demand. Also it has been implemented in some of the 2G technologies.

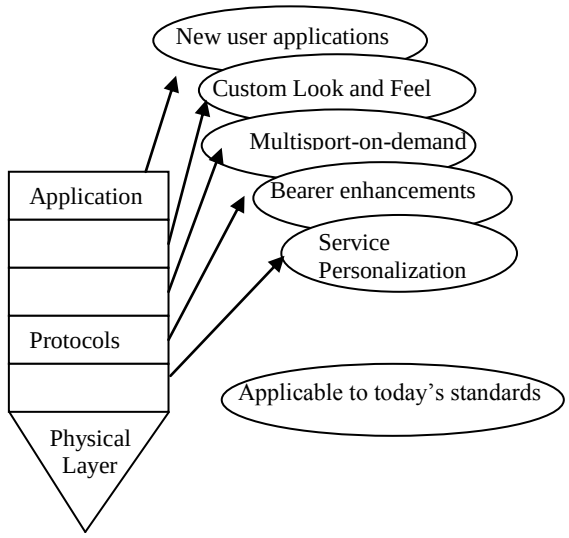

Fig 2: Benefits offered by reconfiguration

1.2.2 Customization by operator: In SDR the operator can customize the handset interface according to the quality of service he could provide.

1.2.3 Potential source of revenue: The SDR has proved to be a greater source of revenue for the network operators as it attracts the customers due to the dynamic services and benefits provided by it. These benefits are discussed in the section below.

1.3 Benefits of SDR

SDR provides a huge benefits in monetary or non-monetary terms to its users. Different categories that draw the benefits of SDR are:

1.3.1 To subscribers: The radio users or customers will have more flexible services, easy international roaming and increased liberty and right to choose accordingly.

1.3.2 Mobile Network Operators: The SDR allows the capability of providing personalization and customization services to the customers. The operators can also provide the tools for value added services.

1.3.3 Hardware manufacturers: The SDR has helped the handset and base station manufacturers to add the new features with a great ease thereby leading to the rapid evolution of the product resulting in increased productivity.

2. TECHNOLOGY SUPPORTING THE SOFTWARE RADIO

Software radio is being supported by the various technologies as shown in the fig 3 below:

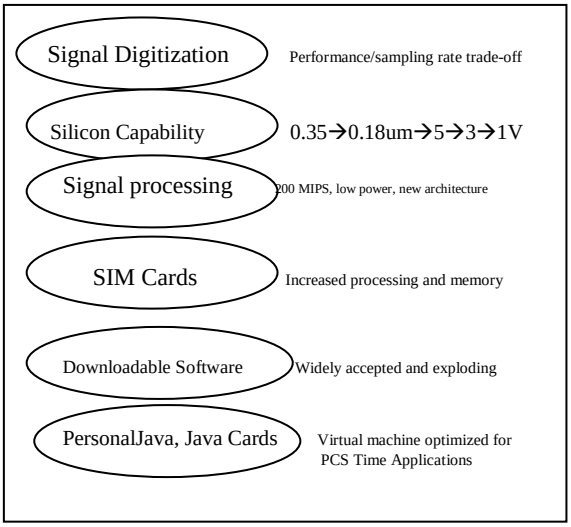

Fig 3: Technology trends enabling software radio handset terminal implementation [12]

*2.1 Signal Digitization***:** The continuous development in the A2D technology has influenced the growth of wireless applications. Wireless communication is digitized by A2D conversion of the signals in the air. It has resulted in the improvement of accuracy, linearity and sampling rates and quality of the wireless communication. However the trade-off between the A2D performance and sampling rate is the limitation of this method. Also this technology cannot be used as the base station hardware due to greater power consumption [12].

2.2 Semiconductor Silicon: The memory and complexity in the structure of the silicon chip increases contrary to the decrease in size of the semiconductor chip every time. It solves the problem of power consumption as the Silicon digital signal processor (DSP) consumes only a fraction of the power consumed by 3v portable devices because it only uses 1v for operating.

2.3 DSP power: Digital signal processor is modified by introducing new architectural designs and customization features for hardware. Nowadays, digital signal processors with very low power consumption are being invented (non-Von-Neumann architecture). These DSP's offer 200MIPS at power consumption rate of 0.5w. Thus it can be helpful in

designing of the base station hardware for software designed radio (SDR).

*2.4 Personal java and java card***:** Java Virtual Machine provides the 'WRITE ONCE RUN ANYWHERE CONCEPT'. It gives rise to the designing of platform independent applications. As the java programs can run on any platform, it allows importing and using the software components dynamically while the java program is under execution. This feature of java platform is of great significance for implementing the Software Reconfigurable Radio.

*2.5 Smart Card Technology***:** Smart card is an IC whose processing and memory capability increases with the decrease in size. Developments in this field may lead to rapid evolution in the capability of technology and flexibility in the performance. Smart card application is growing in faster in *E-cash* and *Pay-per-view* access to broadband.

2.6 Software Download: Development of Internet had brought a revolution in the pricing, sales and distribution of software. Internet provides instant impulse buys, easy access, try-before-buy features. Downloading is still slow over PSTN networks but despite this limitation software download demand is widely increasing over the wired media and is also going to be implemented on wireless media

3. ADAPTIVE SPECTURUM MANAGEMENT

In many countries, only a small portion of the electromagnetic spectrum is used by the user in reality and most of the part is just wasted. But with the increasing economic significance of the Radio Spectrum, it is not worthy to waste the radio spectrum so this wastage cannot be continued in the future. Therefore adaptive spectrum management provides the methods to utilize the wasted spectrum by introducing the concept of Software Reconfigurable Radio. Adaptive radio spectrum is already being used in some wireless technologies like Digital Enhanced Cordless Telecommunication. In this both, the terminal and the base station, monitors the real usage of their total Radio spectrum. It then identifies the spectrum wastage carried out by the user and reserves this spectrum. It uses the unused spectrum from the available spectrum in a dynamic way. This method is referred to as Dynamic Channel Assignment. ASM has the potential to dynamically allocate the components of the spectrum i.e. frequency, time and space. It can also use the radio interface optimally according to the service requirements, operational range(area), environment of RF usage etc. Soft antennas or smart antennas cannot be implemented using the present 2G strategies because it uses the analog radio frequency signals. Thus the new technology needs special platform for implementation. Soft antennas require the architecture that supports digital receivers. Soft Base stations are the handset equipment that requires the soft antennas for implementation. The present base station suffers from the limitations of large size and high power consumption**.**

4. NEED FOR SECURE ARCHITECTURE OF SOFTWARE DEFINED RADIO

Software Defined Radio facilitates the user to use SDR according to their preferences, thus making it a very flexible mechanism to implement the radio functionality. But along with providing flexibility and reconfiguration it also leads to serious security issues. The user can easily adapt the SDR technology according to his own requirement but if in case any unauthorized user grasps access to it, he can modify and misuse it. The ability to reconfigure can also cause the SDR to suffer from the security threats like: Unauthorized modification in software, Radio malfunctioning, interfacing problems.

To protect the SDR from such malicious access and security threats, a robust architecture is introduced with the concept of *Virtualization*. The technique of virtualization is based on the principle of separating the Radio Operation Environment (ROE) from the User Application Environment (UAE)**.** The operations being performed at the user level are not allowed any type of access to the actual area of radio operation and are confined only to the user interface. Every attempt to reconfigure the radio software is traced and checked against the security mechanism to ensure the secure radio configuration.

4.1 Steps towards reliable reconfiguration

Some of the Operating systems are vulnerable to security related threats, so deploying any of the security mechanism layered within or above the OS will be as insecure as the OS itself is. To curb up the problem of software vulnerability we need to follow these steps:

4.1.1 Identify the threats and security requirement: A detailed analysis of the suspected threats on the network must be carried out to develop a log of the possible attacks. One must take initiative to prevent such malicious attempts.

4.2.2 Secure downloading of new radio functionality: It proposes a way to develop the security module for safe downloading and installation of the RF configuration parameters. This can be done by using- Software solutions or Tamper-proof hardware.

Software Solutions are the not widely used because the software modules are prone to malicious updations. Even the checking mechanisms themselves may be corrupt or blocked in the malicious environment. The tamper proof hardware banned the right of tampering the internal functional components. It do not allow the user to enter and hamper the internal operations of the radio equipment. But it also have intrinsic drawback of not being modified or altered. Moreover they are not easy to reconfigure.

4.2 Security Modules

The secure SDR is developed by implementing the policies for the safer download mechanisms. They can be implemented in the form of hardware and software.

4.2.1 SOFTWARE: The software implementation is a flexible approach but it is very easy to maliciously modify the software modules. The malicious user may tamper the OS and the tampered OS can lead to the corruption of the software security module and can pass illegal reconfiguration parameters.

4.2.2 HARDWARE: This refers to the hardwired approach for ensuring the safe and secure download of the SDR. It uses very strict monitoring to keep check on the reconfiguration parameters and the unauthorized users. This is very inflexible approach so it violates the basic principle of SDR. And also some of the attributes like cryptography level, encryption algorithm etc. are difficult to determine.

4.3 Spectrum Sharing

The radio spectrum is available in limitation so instead of allocating individual channel to each user, the spectrum must be shared among all the users requesting for reconfiguration.

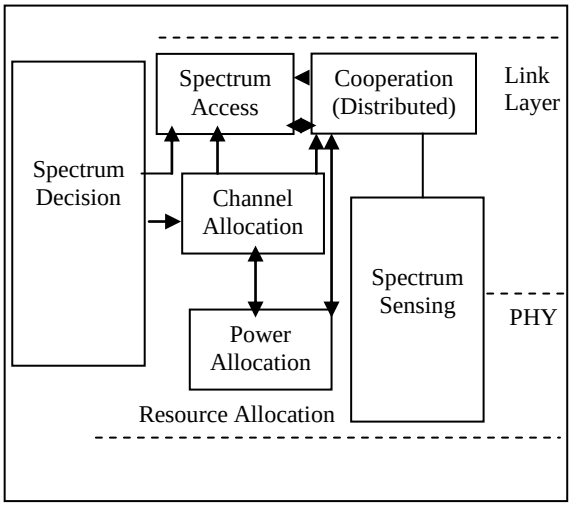

Fig 6: Spectrum Sharing at SDR networks [25]

Commonly the users sharing the radio spectrum are classified broadly into two main categories- Primary users and Secondary users. The primary users are the licensed users who had actually for the spectrum they use. The secondary users are those which share the unused spectrum of the primary users for optimal utilization of network resources. The primary users do not use the whole spectrum they pay for. So this unused spectrum is then allowed to be used by the secondary users but without interfering the operation of the primary user. The primary allows the sharing of the bandwidth only up to a limit of tolerable interference and promised level of Quality of Service (QoS).

The secondary user can tamper the shared spectrum in the following ways:

Disproportionate spectrum*:* The greedy secondary can produce the interference with the normal execution of primary user's operations. It can maliciously modify the SDR software causing disproportionate division of the spectrum.

Jamming entire traffic: The malicious user may try to jam the entire channel by blocking the normal communication signals of the primary channels.

5. SECURE SOFTWARE DEFINED RADIO ARCHITECTURE

As it is discussed in the above sections that SDR dynamic reconfiguration is prone to the certain security issues so the architecture designed for such applications must be very secure, robust and fool-proof to handle different attacks.

5.1 Basic Principle of SDR

The principle method behind the operation of the secure architecture is illustrated below:

5.1.1 Separation of ROE and UAE: The working of secure SDR is based on separating the most vulnerable User Application Environment from the most crucial Radio Operation Environment. It is separated so that the changes due to security threats in one part could not be reflected in the other part. The ROE is more sensitive portion of the SDR. The damages caused in the Radio operation environment are more severe and can cause the malfunctioning of the underlying Operating system. Even the malicious OS cannot effect the ROE in this newly proposed architecture.

5.1.2 Verification against security policy: Secure SDR architecture introduces the new module namely Security Policy Monitor (SPM) which cross check the target reconfiguration against the security mechanism applied before it is allowed to operate in the radio environment.

5.2 SDR software components

The components of the SDR software listed below are defined as per the guidelines provided by the SDR Forum.

5.2.1 Radio Operation Environment (ROE): The radio operation environment forms the core part of the SDR software that includes the required device drivers, Operating system and the Middleware layer.

5.2.2 User Application Environment (UAE): User Application Environment is the environment where only the user application is executed. It is exclusively meant for user related operations. The reconfiguration request is generated in this section according to the user choices and preferences.

5.2.3 Radio application (RA): This module acts as the air interface of the SDR radio. This component is responsible for actually controlling the access of users to the radio reconfiguration. Radio application defines the modulation techniques, interface standards and communication protocols for carrying out communication between the user and the radio network. It is the most delicate component of the SDR software that may be illegally modified by the unauthorized user access.

5.2.4 User Application (UA): User application refers to all the applications running on the user terminal. Some examples are Browser, games, word processing. UA is the most distrusted component that can tamper the OS with maliciously downloaded software and can have unauthorized access to reconfiguration process that can bypass hamper the security mechanism.

5.2.5 Service provider application (SPA): The Service provider ensures the integrated platform for different services Voice, Video, Data to his customers conforming to the QoS parameters.

5.3 The Proposed Secure SDR Architecture

The new architectural design for SDR is more secure in terms of tolerance and robustness. In this architecture the Radio Operation Environment and the User Application Environment from each other as UAE is very easy to modify and tamper with. This makes the basic radio operation much secure and less vulnerable to malicious modification by restricting the signals from outside to make any attempt to interfere with the actual radio signals.

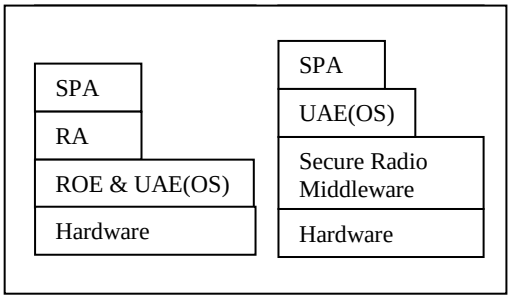

Fig 7: Traditional and Proposed architecture of SDR [2]

In this architecture whenever a secondary user is allocated with a limited access to spectrum , a corresponding security mechanism is designed for that channel. For every SDR reconfiguration attempt, the reconfiguration request parameters are checked across the security policy designed. If it operates within the legal constraints then the changes demanded by that requesting user are allowed to reflect and blocked if it does not comply the security policy. To prevent the OS (kernel) from being tampered the secure SDR architecture introduces a new secure sub-layer called SECURE RADIO MIDDLEWARE (SRM). The architecture of this SRM sub-layer is shown in the fig 8 below.

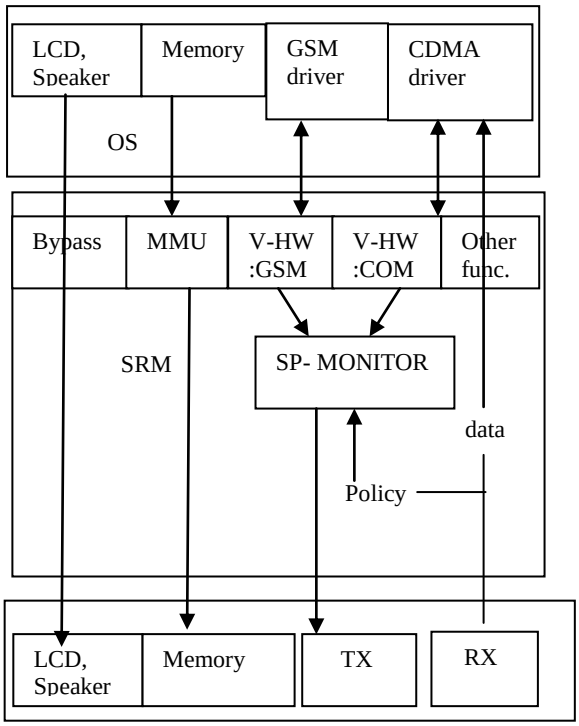

Fig 8: Architecture of SRM [2]

The secure radio middleware encapsulates the security-critical software components (Radio application and Radio operation environment) . The SRM sub-layer provides the immunity to SDR against the unauthorized access attempts by the User application (UA) and User application environment (UAE). It defines the proper checking and validation methods verifying the reconfiguration requirements and ensures that they comply with the pre-defined security measures.

5.4 Components of Secure Radio Middleware

The SRM layer consists of the following parts:

5.4.1 *Bypass:* "Bypass" is the part of SRM where non-critical operations from the OS to hardware go through directly, *e.g.*, LCD, speaker device drivers.

5.4.2 Memory management unit (MMU): The MMU is important in SRM because it controls the behavior of the OS in memory read and write. In the new architecture based on the SRM, the MMU performs access control and breaks the whole memory space into three parts:

• Memory where OS has no permission to read or write**.** It is used for storage of private keys and secrets that UA should never know.

• Memory where OS has permission to read-only**.** It is used for some modules like the V-HW and security policy monitor discussed below. These modules need to
be protected from alteration by the OS.

• Memory where OS has full permission. The OS can use this area for its normal use.

5.4.3 Virtualized hardware (V-H): V-HW is a critical part of the SRM. All the RA are implemented as V-HW.
Why is V-HW called hardware? In the proposed SDR Architecture, the integrity of RA modules can be protected like hardware because they are execute-only to the OS. Even the kernel in the OS does not have the right to write into this segment of memory. Thus, the OS cannot write into V-HW, but only has a control interface to it – just like an ASIC in cell phones nowadays. And why is V-HW called virtualized? Because it is essentially still software in the SRM. It still has all the nice characteristics of software in the SDR: it can be downloaded through networks, installed under supervision, and altered in different environments. The key point here is that only the SRM, which is more securing than the UAE (OS), can perform these functions.

5.4.4 Security policy monitor: We can ensure the integrity of V-HW through the above mechanism. However, UA and SPA will pass to V-HW the parameters they would like to implement, such as frequency, power level, modulation method, cryptographic algorithms, key size, *etc.* Hence, a security policy monitor becomes necessary, which tries to decide a normal value or range for the radio parameters and compare them to the ones the OS passes to V-HW. If a violation is found, suitable recovery mechanisms are triggered.

6. IMPLEMENTATION

This section describes our implementation of the proposed architecture, evaluates the performance penalties it incurs, and performs a security analysis of the architecture under various attacks.

6.1 Underlying Infrastructure

Here the implementation of the proposed architecture is done by using the VMware framework and GNU Radio[2].

6.1.1 VMware Server: VMware is a free virtualization product for Windows and Linux servers. It creates a virtualization layer above the host OS in which it is installed. This thin virtualization layer separates the computation resources in the host machine into several partitions, each of which is called a virtual machine, and each virtual machine is isolated from its host and other virtual machines.

6.2.2 GNU Radio: GNU radio is a free software development toolkit that provides runtime and processing blocks for signal processing to implement software radios using readily-available, low-cost External RF hardware and commodity processors.

6.2 Implementation using VMware

In our implementation, shown in Fig. 3, we realize the SRM in the host OS and the VMware Server layer, and the UAE is realized using a virtual machine. The V-HW and security policy monitor are implemented in the host OS just on top of the hardware, and the Bypass and MMU parts are already present in VMware.

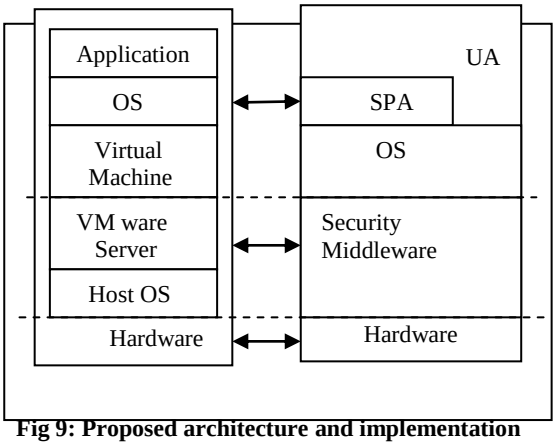

Fig 9: Proposed architecture and implementation using VMware [2]

This is implemented exactly as stated in the conceptual proposal. The Radio Application (RA) and User Application (UA) are totally separated. The actual complete host was having a large overhead where as VMware now divides the Host Layer into thinner SRM layers. which definitely incurs a smaller and tolerable overhead. VMware sever provides an ETHERNET AIR INTERFACE to transfer the signals. These signals carry the information having following components:

Process id: Process id is the identification of which process the data packet is from[2].

V-HW id: V-HW id represents the RA module that must be used [2].

Parameters*:* The parameters are the reconfiguration information passed to V-HW and are specific to the V-HW[2].

Data: Data are also passed to V-HW for transmission. Either the data or the memory addresses that store the data can be passed here. In our implementation, the data themselves are transmitted from the virtual machine to the host OS, which may result in more overhead, but also leads to greater safety [2].

6.3 Security Policy

The V-HW lies between the Operating System and the machine (hardware). The Security Policy Monitor (SPM) will check each reconfiguration parameter issued by the user application (UA) to the virtual hardware. These parameters include the frequency at which signals will travel power consumption rate of the equipment etc. The SPM verifies whether or not the issued parameters follow the security standards for a process. If yes, then it allows the reconfiguration of SDR or process is abandoned otherwise.

For the purpose of illustration, we take FRS (Family Radio Service) and GMRS (General Mobile Radio Service). as examples. In our implementation architecture, V-HW is an FRS/GMRS module. FRS is a license-free walkie-talkie system FM (frequency modulation) UHF (ultra high frequency) radio service, while GMRS is a licensed land-mobile FM UHF radio service. Recent hybrid FRS/GMRS consumer radios have 22 channels in all. Suppose process 1 has a license for GMRS, but process 2 does not and only has the right to operate on FRS. The security policy monitor would check the UAE parameters sent to VHW

and see whether the frequency and power are within the Regulations for each process: process 1 can transmit data from Channels 1 to 7 and 15-22 with power less than 5W; process 2 can transmit data from Channels 1 to 14 with power less than 0.5W.

7. RESULTS

7.1 Overhead

Overhead refers to the efforts done by the SPM to validate the authorized user and block the unauthorized one to ensure the secure software download. Here we will demonstrate that the overhead incurred in the secure SDR is less and tolerable than the conventional architecture.

7.2 Types of overheads

The overhead occurred are broadly classified into two categories:

7.2.1 Communication overhead: It is the overhead that incurred while transferring the data and control information from virtual machine to the Host operating system. Secure SDR uses virtual Ethernet interface provided by Virtual Hardware(V-Hware) for communicating across UA and RA.

7.2.2 Security Policy Check overhead: This is totally unavoidable in the secure SDR architecture. The security check is needed only once when the reconfiguration occurs thus the overhead depends only on reconfiguration parameters list, which is expected to incur a smaller overhead.

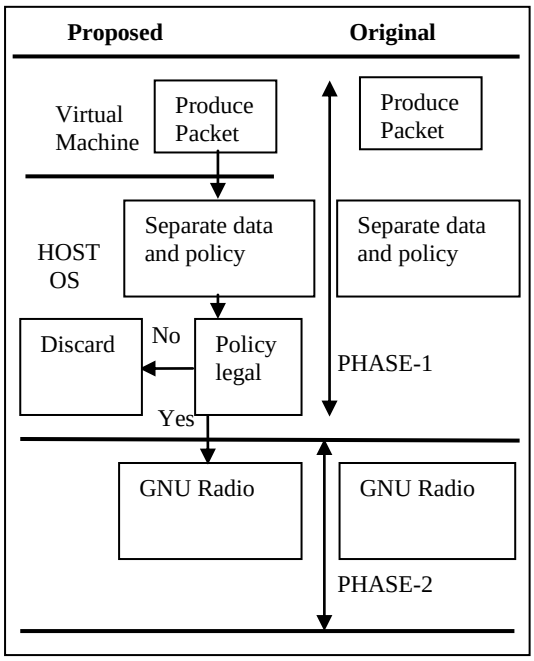

Fig 10: Performance measurement setup [2]

The table below shows the difference between the traditional and new architecture.

Table1. Difference between traditional and secure SDR architecture

Conventional architecture	Proposed secure architecture
1)Packets are generated and processed or manipulated at single OS layer.	Virtual machine issues the packets having data and control parameters to
2) No security policy monitor is applied in this architecture.	Os Middleware. The packet is checked against the security policy by SPM and transmitted to GNU for signal processing if it is valid.
3) Ultimate overhead due to malfunctioning of OS is much more. Even the process may fail.	Overall overhead is very less and tolerable as the reconfiguration is very smooth and under inspection.

7.3 Performance Measurement

Reconfiguration only once per packet , therefore the packet size determines the overhead. The more is the packet length, bigger is the configuration parameter list. Now for a small packet the processing time is less and for a lengthy packet GNU Radio takes more processing time. Thus if the packets arrived would be longer then each of them will take more time, reconfiguration occurs less frequently and thereby reducing the overhead incurred for each reconfiguration request. We measure the processing time for 10000 packets to be produced, passed through different parts, and then processed by GNU Radio. The data in each packet are produced randomly. Reconfiguration occurs once per packet. Thus, the packet size determines the reconfiguration overhead. The larger the packet size is, the longer this set of SDR configuration parameters lasts.

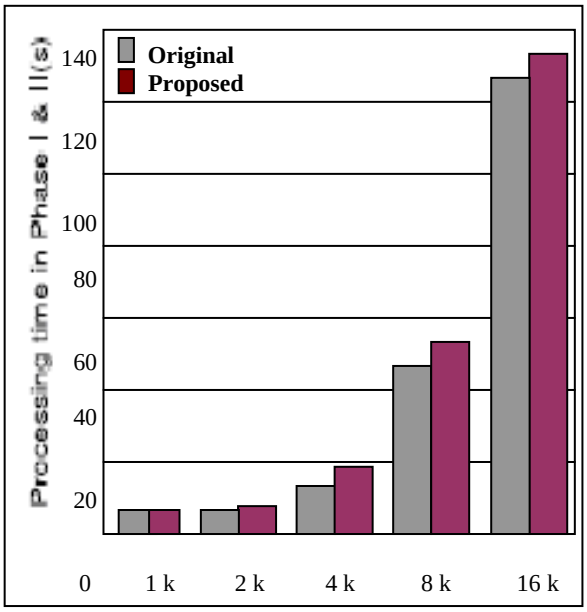

Fig 11: Processing time for 10000 packets [2]

In Fig. 11 and 12, the processing time and overhead for processing 10000 packets are measured for both the proposed and original architectures. We can see that for a packet size of 1kB through 16kB, the overhead is reduced from 4.0% to 3.2%. As the packet size increases, reconfiguration occurs less often and the overhead becomes smaller. It is worth pointing out that the GNU Radio processing part is a very simple FM module.

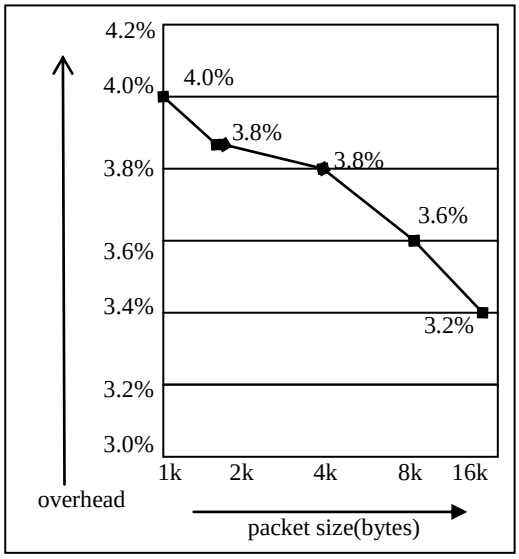

Fig 12: Overhead for processing 10000 packets [2]

If a more complex protocol is used, such as GSM or CDMA, every packet needs more time in Phase II (which requires the same processing time in both the proposed and original architectures). Thus, the overhead would be smaller.

8. LIMITATIONS OF PROPOSED ARCHITECTURE

The above proposed architecture is very simple, efficient and easy to implement. It gives the concept of the separation of the UAE and ROE. It plans the security policy to check the reconfiguration parameters. In spite of being so capable and efficient still this architecture have some flaws . These can be the fields for the future development of this technology. Some of the detriments are discussed below:

8.1 Based on PC Test bench: This implementation is based on the simple PC test bench and carried out with the available resources whereas SDR is designed to operate in a resource-constrained environment like Mobile Phones.

8.2 Based on FM technology: This implementation uses Fm Radio applications which have a lower data rate and less cryptic security code which can be easily decrypted. But the future need for SDR may be- More elaborated security mechanism in more complex communication scenario.

8.3 Need for higher security level: This model mainly focus on protecting the reconfiguration parameters from the unauthorized access by unofficial users (UAE) while operating. But many security measures are still to be taken for improving efficiency of this model. they include: (1) Encryption and decryption functions (2) Information Integrity (3) Access control (4) Secure software radio downloading.

8.4 Optimization of methods: Algorithms used for implementing security policy can be optimized to reduce the SDR overhead further.

9. SECURITY ANALYSIS

The newly proposed SDR architecture ensures that even if the UAE is tampered with, even then the SDR radio device is within the regulations and compliance to security policy and the ROE is retained.

To break the SDR compliance a malicious user can :

9.1 Attack the hardware: malicious operating system can modify the device drivers operating between virtual and actual hardware.

Remedy: There is no direct interface between UAE and actual hardware. SRM prevents the malicious operating system from tempering the actual hardware.

9.2 Modify virtual hardware, SPM and MMU: the tempered operating system can even change the code of the Virtual hardware, MMU and SPM and then modify it to break compliance.

Remedy: Virtual hardware, MMU and SPM are located in memory and UAE has read only access to the memory.

9.3 Changes in data structure: (a) Changed parameters can be verified across the security policy (b)Change in data i.e. confidential information like Keys can be leaked by the defected OS. This is prevented by managing all the keys and confidential information in the secure SRM, where the UAE is not granted any access.(c) Non repudiation i.e. falsifying the process id. Unauthorized process can attempt to draw the access rights of the valid processes by changing their process id.

Remedy: Introspection can be carried out that keeps on accounting the information of the current process under execution.

10. CONCLUSION

The development in the field of Software radio is in progress. Scientists all over the world are trying to understand the impacts of the software radio and boom that it will provide to the technology. it had also provided answers to some of the questions of the network operations regularly the issues of customer services and loyalty. After some time, when it will be possible to implement the concept of software reconfigurable radio, the benefits and implications of this technology will have profound impacts on the telecommunication and other industries. In this paper, a new architecture to protect SDR devices from malicious reconfiguration is proposed. In this architecture, an SRM layer is used to separate the most vulnerable environment (UAE) from the most security-critical environment (ROE). The SRM contains a security policy monitor that checks all the RA reconfigurations against the specified security policies. This achieves the goal that even if the OS is compromised in the UAE, secure reconfiguration can still be ensured in the ROE. The architecture is implemented using VMware and GNU Radio. The overhead incurred by the new architecture is shown to be small.

11. REFERRENCES

[1] SDR Forum, "Report on issues and activity in the area of security for software defined radio, SDRF-02-A-0003," Tech. Rep., 2002.

[2] Chunxiao Li, Anand Raghunathan, Niraj K Jha, "An Architecture for Secure Software Defined Radio", EDAA no.5, pp.978-3,November 2009.

[3] "SDR system security, SDRF-02-A-0006," Tech. Rep., 2002.

[4] "A structure for software defined radio security, SDRF-03-I-0010," Tech. Rep., 2003.

[5] "SDR wireless security, SDRF-04-I-0023," Tech. Rep., 2004.

[6] R. Falk, J. F. Esfahani, and M. Dillinger, "Reconfigurable radio terminals- threats and security objectives, SDRF-02-I-0056," Tech. Rep., 2002.

[7] A. F. B. Selva, A. L. G. Reis, K. G. Lenzi, L. G. P. Meloni,, S. E. Barbin, "Introduction to the Software-defined Radio Approach", IEEE latin america transaction , vol 10,no.1, Jan 2012.

[8] SDR Forum, "SDR security requirements, SDRF-04-W-0006," Tech. Rep., 2005.

[9] R. Hill, S. Myagmar, and R. Campbell, "Threat analysis of GNU software radio," in Proc. World Wireless Congress, May 2005.

[10] L. Michael, M. Mihaljevic, S. Haruyama, and R. Kohno, "A framework for secure download for software-defined radio," IEEE Communications Magazine, vol. 40, no. 7, pp. 88–96, July 2002.

[11] "A proposal of architectural elements for implementing secure software download service in software defined radio," in Proc. IEEE Int. Symp. Personal, Indoor and Mobile Radio Communications, vol. 1, Sept. 2002, pp. 442–446.

[12] Walter H. W. tuttlebee**, "***Software Defined Radio:*

Facets of a Developing Technology", IEEE Personal Communications,pp.1070-9916,no.99, April 1999.

[13] A. Brawerman, D. Blough, and B. Bing, "Securing the download of radio configuration files for software defined radio devices," in Proc. Int. Wkshp. Mobility Management & Wireless Access Protocols, Sept. 2004, pp. 98–105.

[14] A. Brawerman and J. Copeland, "An anti-cloning framework for software defined radio mobile devices," in Proc. IEEE Int. Conf. Communications, vol. 5, May 2005.

[15] H. Uchikawa, K. Umebayashi, and R. Kohn, "Secure download system based on software defined radio composed of FPGAs," in Proc. IEEE Int. Symp. Personal, Indoor and Mobile Radio Communications, vol. 1, Sept. 2002, pp. 437–441.

[I6] W. H. W Tuttlebee, "Software Radio Technology: A European Perspec- [2] IEEE Commun. Mag., Special Issue on Software Radio, May 1995.

[17] W. H. W. Tuttlebee, "Software Radio - Impacts and Imlications," Proc. IEEE 5th lnt'l. Symp. Spread Spectrum Techniques and Apps., South Africa, Sept. 1998.

[18] Proc. Ist lnt'l. Software Radio Wksp**.,** Rhodes, reece, June 1998, jointly organized by the EC DG Xlll and the SDR Forum.

[19] H. Huomo, "Software Radio, A Manufacturer's Perspective," Proc. Ist lnt'l. Software Radio Wksp., Rhodes, Greece, June 1998.

[20] Y. Shinagawa, "Software Radio Technologies: From the Viewpoint of the Terminal Manufacturer," Proc. I s t lnt'l. Software Radio Wksp, Rhodes, Greece, June 1998.

[21] G. Fettweis et al., "Integrated Broadband Mobile System (IBMS) featuring Wireless ATM," 2nd ACTS Mobile Commun. Summit, Aalborg, Denmark, Oct. 1997.

[22] V. Brankovic et al., "Integrated Broadband Mobile System (IBMS) Demonstrator, "Proc. 3rd ACTS Mobile Commun. Summit, Rhodes, Greece, June 1998.

[23] G. Fleming et al., "A Flexible Network Architecture for UMTS," IEEE Pers. Commun., Apr. 1998. pp. 8-1 5.

[24] G. Fleming et al., "A Radio Independent Network - The Enabler for Software Radio," Proc. 3rd ACTS Mobile *Commun.* Summit, Rhodes,Greece, June 1998.

[25] Ian F. Akyildiz , Won-Yeol Lee, Kaushik R. Chowdhury, "CRAHNs: Cognitive radio ad hoc networks", vol 332, pp.810–836, January 2009.