A survey of Security Issues in Software Defined Radio and Cognitive Radio

Ali Shamsizadeh
Isfahan University of
Technology

ABSTRACT

The introduction of software-defined radio will trigger new security problems that are unlike those faced by legacy wireless communication systems. A software-defined radio can change its functions by changing its software. Therefore, many security problems that have never been seen in the conventional fixed wireless terminals will arise. We assess the security issues of the SDR system by taking the distribution model of SDR terminal software into account. The cognitive radio paradigm introduces entirely new types of security threats to wireless networks and makes the development of effective security models and mechanisms very challenging. However, wireless security in cognitive radio networks is a technical area that has received relatively little attention to date, even though security will likely play a key role in the long-term commercial viability of the technology. This paper has delineated some of the key challenges in providing security in cognitive networks this paper summarize the security necessary for software defined radio (SDR) systems, secure software download in SDR, cognitive radio (CR) and cognitive radio networks (CRN).

1. INTRODUCTION

A Software Defined Radio (SDR) terminal may be regarded as a programmable radio transceiver whereby the user equipment is able to reconfigure itself, in terms of its capability, functionality and behavior in order to dynamically accommodate the needs of the user. It is expected that SDR as a technology will help bring together the different forms of communications. The incorporation of mobile communications. Broadcast receivers, location services, internet, multimedia, dedicated point-to-point communications, personal computing, and digital aids (PDAs) would all be possible with the help of a mature and reliable SDR technology.

The introduction of software-defined radio will trigger new security problems that are unlike those faced by legacy wireless communication systems. A software-defined radio can change its functions by changing its software. On top of the problems posed by hardware modifications, we will see new problems created by illegal software. As the examples of hacking and viruses on the Internet show, illegal software can be significantly easier to implement than hardware modifications. Therefore, new security measures are needed to realize software-defined radio services.

Cognitive radio offers the promise of intelligent radios that can learn from and adapt to their environment. Much research is currently underway developing various reasoning and learning algorithms that allow cognitive radios to operate optimally in a large variety of different situations. However, as with many new technologies, initial research has not focused on security aspects of cognitive radio.

Since cognitive radios can adapt to their environment and Change how they communicate, it's crucial that they select Optimal, secure means of communications. Data integrity and confidentiality can be handled by higher-layer cryptographic security, so here we focus on attacks fundamental to the cognitive radio itself, and independent of its higher-layer communications techniques.

By putting artificial intelligence (AI) engines in charge of our wireless devices, we need to be aware that these engines can be provided false sensory input by adversaries, and this false input affects its beliefs and behavior. We need to look at threats we would ordinarily see in social networks, rather than computer networks. We define three classes of attacks: sensory manipulation attacks against policy radios, belief manipulation attacks against learning radios, and self-propagating behavior leading to cognitive radio viruses. All types of attacks manipulate the behavior of a cognitive radio system such that it acts either sub optimally or even maliciously.

Protecting against attacks like these cannot be done through

Cryptographic means. It involves imparting some amount of Intuition and common sense into a cognitive radio that allows it to debunk beliefs that don't make sense. In this paper we explore these ideas.

In section-2 we are giving a background on the security in mobile system and common threat models currently used in security analysis, specifically the Internet threat model, and extensions assumed in wireless networks. Section 3 discusses threats to software defined radios, section 4 describes Characteristics of cognitive radios and its security issues are described in section 5. After introduce the cognitive radio network's Characteristics in section 6, section 7 extend security analysis to networks of cognitive radios. Finally Section 8 concludes.

2. Security Concerns in Mobile Systems

The role of security mechanisms is to ensure the privacy and integrity of data, and the authenticity of parties involved in a transaction. In addition, it is also desirable to provide functionality such as non-repudiation, copy protection, preventing denial-of-service attacks, filtering of viruses and malicious code, and in some cases, anonymous communication [1]. Some of the major security concerns from the perspective of a mobile appliance are:

- User identification attempts to ensure that only authorized entities can use the appliance.
- Secure storage addresses the security of sensitive information such as passwords, PINS, keys, certificates, etc. that may reside in secondary storage (e. g., flash memory) of the mobile appliance.
- A secure software execution environment is necessary to ensure that attacks from malicious software such as viruses or Trojan horses are prevented.
- A tamper-resistant system implementation is required to ensure security of the hardware implementation from various physical and electrical attacks.
- Secure network access ensures that only authorized devices can connect to a network or service.
- Secure data communications considers the privacy and integrity of data communicated to from the mobile appliance.
- Current security refers to the problem of ensuring that any content that is downloaded or stored in the appliance is used in accordance with the terms set forth by the content provider.

Wireless data communications can be secured by employing security protocols that are added to various layers of the network protocol stack, or within the application itself. Security protocols utilize cryptographic algorithms (asymmetric or public-key ciphers, symmetric or private-key ciphers, hashing functions, etc.) as building blocks in a suitable manner to achieve the desired objectives (peer authentication, privacy, data integrity, etc.).
Many of these protocols address only network access domain security, i.e., securing the link between a wireless client and the access point, base station, or gateway.

The wireless standards need to be complemented through the use of security mechanisms at higher protocol layers. The security measures must be distributed between the different players involved in the system (handset, base station, vendor, etc.) and it is imperative to lake a hierarchical approach where each layer of security provides a foundation for the one above it. Practically speaking no one believes that there is any solution to SDR security which doesn't involve the application of software as pan of the threat mitigation strategy. So software is necessary but is it sufficient? We asset that SDR Security with any degree of confidence will require some elements to be enforced by hardware measure.
Combining hardware and software crypto components plays a significant role in providing a strong crypto foundation that meets the basic security requirements mentioned above (i.e. authentication, confidentiality, integrity, and non-repudiation). To make the assertion more directly, not only can security Mechanisms be implemented in a hardware module, they must be to prevent tampering. The envisioned hardware mechanisms include a processing core, protected internal memory, and additional features necessary to implement whatever security measures are standardized.[1],[2]

3. SDR SECURITY

The SDR Security Working Group is focusing on a broad set of security issues that arise from the introduction of SDR technology. In particular, it seeks to manage the following SDR-related risks:

- Propagation of malicious radio software.
  Radio interference.
- Adverse health and safety impacts to SDR users
  (i.e., those caused by inappropriate electromagnetic
  Radiation).
- The unauthorized release of trade secrets incorporated in radio software.
- The circumvention of billing systems related to SDR.

The high-level security requirements listed in this paper address these risks, not all possible risks that might be associated with SDR communications. In particular, they do not attempt to restate general information, communications, transmissions, or network security requirements, all of which have been well-studied in other forums. The high-level SDR security requirements apply to any use Of SDR; they are not targeted at a particular market segment (e.g., commercial wireless telephony). They apply to both Infrastructure and terminal devices. They also apply to broadcast, peer-to-peer and adhoc networking applications of SDR. [3]
The statement of high-level security requirements is the Beginning of a process that will culminate in the specification of SDR security mechanisms. First, the high level requirements will be used to develop detailed security requirements, each of which will be traceable to one or more of the high-level requirements. The detailed requirements, in turn, will be used as the basis for SDR security architecture. Finally, the architecture will lead to an integrated set of SDR security solutions.
The SDR Security Working Group seeks to maximize the potential future growth and social value from SDR

technology. It does not seek to create a maximum security solution or one tailored for the highest assurance environments. It is Cognizant that there are tradeoffs between costs of security Controls and the risks they mitigate. It also understands that there can often be a tension between security and functionality. At the same time, robust and flexible security solutions must be built-in to SDR technology from the early stages on if SDR technology is to achieve wide regulatory and consumer acceptance.[4]

3.1. Definitions

Download: Transfer of data from outside the device into the device. Download may occur through a variety of means, including over-the-air, using wired media, or using device peripherals such as jump drives or memory cards

Installation: The process of storing and configuring software so that it can be subsequently instantiated

Instantiation: The process of setting up for execution

Operating state: The current configuration of the SDR device's resources including access control rules and radio Parameters such as frequency, power and modulation

Radio communications service provider: Network operators (e.g., commercial cellular wireless, public safety agencies), radio broadcasters (including FM/AM, television and satellite), peers in peer-to-peer or mobile ad-hoc networks, and other entities that provide radio communication to a device. An SDR device that is serving in an infrastructure capacity (e.g., a base station or access point) may not have a radio communication service provider if its distribution system is a wired network.

Resource: Hardware, software (to include firmware), configuration data and policy

Run-time: The period of time during which a program is being executed, as opposed to compile-time or load time.

SDR device: A computing platform or integrated collection of computing platforms that provide radio functionality using SDR technology.

SDR-related: Something on which the operation or security of radio communications is dependent. SDR-related items include radio and computing resources such as boot read-only memory, the operating system, hardware drivers, SDR middleware, cryptographic modules, software enforcing the SDR security policy, as well as the radio software itself (i.e., software implementing the "waveform").

SDR security policy: A set of permitted operating states. The SDR security policy may also contain rules regarding authentication mechanisms, events to be audited, and actions to be taken in response to an event.

Stakeholders: Hardware component manufacturers, regulators, radio communications service providers, device owners and entities authorized by a device owner.

Trusted: Established using cryptographic mechanisms such that invalidation is computationally infeasible if cryptographic secrets are maintained. [1],[7]

3.2. Requirements

Policy-driven behavior

An SDR device SHALL enforce a device-specific SDR security policy that governs the behavior of the device at all times.

Policy freshness

The SDR device SHALL ensure that its device-specific SDR security policy incorporates the SDR security policies of its stakeholders within the scope of their authority.

Device attestation

An SDR device SHALL provide trusted configuration information to its communications service providers on request.

Protected download

An SDR device SHALL provide confidentiality and integrity services for download of SDR-related software and configuration data.

Policy-compliant installation and instantiation

An SDR device SHALL only install and instantiate SDR related software and policy that have been appropriately certified to be compliant with the device's SDR security policy.

Run-time control

An SDR device SHALL at run-time prevent transmissions that violate its SDR security policy.

Resource integrity

An SDR device SHALL detect the unauthorized modification of its SDR-related resources and use that information to prevent additional unauthorized behavior.

Access control

SDR devices SHALL control access to each SDR-related resource on the device.

Audit

An SDR device SHALL detect, log and notify specified Processes of security related events.

Process separation

An SDR device SHALL have mechanisms to prevent SDR Applications from compromising the security of non-SDR related applications and data.

Implementation assurance

Information assurance mechanisms SHALL be based on industry standards and validated technology.

Supportive operations

Operational practices supporting information assurance mechanisms SHALL be consistent with and supportive of the SDR security policy.[7]

3.3. Secure software downloads in SDR

One of the most pressing issues for the commercial introduction of software defined radio (SDR) system s is the authentication and verification of integrity of the software that is downloaded. For a SDR terminal, since reprogrammable hardware is used, if the software is illegally modified from when it was submitted to the authorities, then the use of such software may cause interference to other users or physical harm to the user.[5]

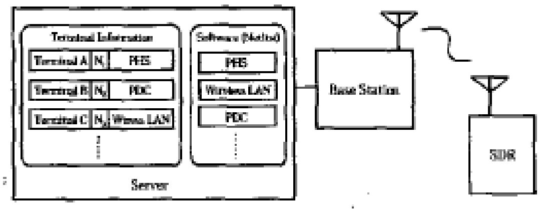

Figure 1: download model in SDR

Therefore, there must be a method of ensuring that the software downloaded is intact and has not been modified (verification of integrity) and that it has obtained government approval (authentication). Furthermore, in the event that some illegally modified software is created, there should be some mechanism to prevent the spread of that illegal software. As a further necessity for the introduction of software downloadable SDR system, the software should protected against theft by people or companies who would like to know the details of the software employed by a rival company.[1],[6]

4. Characteristics of cognitive radio

The terms software-defined radio and cognitive radio were promoted by Mitola in 1991 and 1998, respectively. Software-defined radio(SDR), sometimes shortened to software radio, is generally a multiband radio that supports multiple air interfaces and protocols, and is reconfigurable through software run on DSP or general-purpose microprocessors. CR, built on a software radio platform, is a context-aware intelligent radio potentially capable of autonomous reconfiguration by learning from and adapting to the communication environment. And cognitive radio represents a much broader paradigm where many aspects of communication systems can be improved

Via cognition [8]. Compared with traditional radio, CR has its special characteristics, such as artificial intelligence functionality and dynamic spectrum access application, which will be described as follows. Figure 2 show the characteristics of CR:

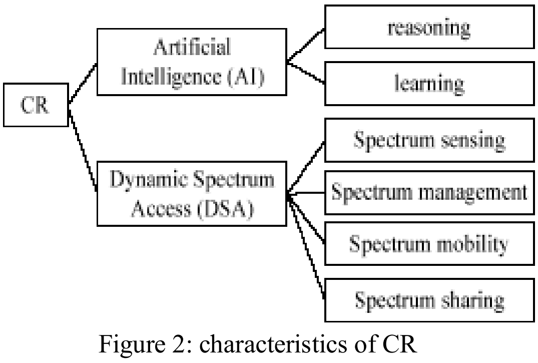

Figure 2: characteristics of CR

4.1. Artificial intelligence cognitive radio

Cognitive radio offers the capabilities of learning from and adapting to their environment through its artificial intelligence (AI) characteristics including reasoning and learning. In paper [10], Dietterich describes a standard agent model consisting of four primary components:

Observations, actions, an inference engine, and a knowledge base. In this agent model, reasoning and Learning is a result of the combined operation of the inference engine and the knowledge base. Many researches are directing into learning and reasoning algorithms currently, assisting CRs to performance optimally in various situations.

A CR requires policies for reasoning to deal with different environments or react to different conditions. In another word, policies are the basis of reasoning. A reasoning engine is a set of logical inference rules [8].

It provides policies including a set of actions, under what conditions the actions should be execute, and how those actions affect the state of knowledge base. However, the shortage of reasoning engine is that it cannot adapt to new situations, and it needs preprogrammed policies, while the learning engine can make up this shortage.

A CR with learning functionalities can learn the experience from past statistics and present situation in order to predict future environment and select optimal operations. Learning is the process that the inference engine evaluates relationships, such as between past actions and current observations or between different concurrent observations, and converts this to knowledge to be stored in the knowledge base [8].

Learning engine can adapt to new situations and it start

With no preprogrammed policies. These AI features provide the advanced and flexible functionalities to CR, however, with the flexibility and the advanced performance, the security threats has also been exposed to the attackers.

4.2. Dynamic spectrum access characteristics.

Current regulation to spectrum is a kind of fixed (or static) spectrum assignment policy. The spectrum is regulated by governmental agencies and is assigned to license users on a long term basis for large geographical regions [8]. The spectrum is a constrained resource. With dramatic increase of wireless devices and communication demands, radio spectrum is running out of usable. However, according to Federal Communications Commission (FCC), temporal and geographical variations in the utilization of the assigned spectrum range from 15% to 85%. Thus, increasing the efficiency of spectrum utilization is a way to deal with the problem. The FFC is considering on using DSA to opening up the licensed bands to unlicensed users on the basis of non-interference. DSA is an important application of CR, which provides the capability to use or share the spectrum in an opportunistic manner. Specifically, in order to realize DSA, CR provides functions as follows [8]:

- Spectrum sensing: detecting spectrum holes and sharing the spectrum without interfering with other users.
- Spectrum management: selecting the best Available channels.
- Spectrum mobility: maintaining seamless Communication during the transition to better spectrum.
- Spectrum sharing: coexisting with other users in one channel.

5. Security threats in CR

5.1 Artificial intelligence behavior threats

5.1.1. Policy threats: In order to communicate more effectively in an intelligence way, a CR needs policies for reasoning in different environment or from different conditions. Policy threats come from two aspects: lack of policy and failure when using policy. If there is a lack of policy, a CR cannot make appropriate operations according policy in some certain conditions which are regulated by the lacked policy. Even, if a CR cannot receive any policy, it will not communicate. Policies are introduced at time of device manufacture, and the policies can be updated and extended during using. A CR can remote policy database for policies, and transfer policies from other CR. A CR also can receive announced local policies from radio beacon. In addition, policies can be distributed in the form of certifications with a period of validity. [8] The ways for a CR to receive policies are so variety. Thus, it is difficult for a CR to prevent from receiving any policies. However, reduce the chance of receiving policies, or decline required policies could affect the communication quality. For example, an attacker can decline the effective of communication by blocking accesses of policies. Or, an attacker can jam the radio beacon which announced policies. Failure when using policy can also cause security problems. There are three types of threats when using policies: modification to policies, using false policies, and false input caused threat. First, policies may be modified by attackers. An attacker can get control of a CR, or get the administration of policy database to modify the policies inside. Second, using false policies also leads to security threats. An attacker can try to Inject false policies into the CR policy database. If a CR operates according to the false policy, it may cause interference. Attackers can inject or modify policies when the CR is updating through radio beacons, from CRs transferring policies, and policy database. It is vulnerable these times. In addition, if an attacker spoof or mask sensor information, which is the input of policies, it will cause sub-optimal or false selection for communication. As mentioned in [8], by understanding how a radio's statistics are calculated, an attacker can manipulate them. Since these statistics operate on raw RF energy, there is no cryptographic means of securing them, as is frequently done to prevent typical communications threats. Through manipulating to the statistics, an attacker can provide a false sensor information, and leads to sub-optimal performance or false of communication. Therefore, robust the policy management mechanism is an important task to CR's security.

5.1.2 Learning threats: Some CRs are designed with the capability of learning. These CRs can learn from the past experiences or current situations to predict future environment and select optimal operations, and they are vulnerable because of the learning capability. Attackers can modify past statistics or spoof current conditions to impact the CR predicting accurately. Based on the inaccurate prediction, the CR will operate sub-optimal or lead to a failure in communication. These attacks can have long-term effects on CRs, and are difficult to find out.[9]

5.1.3. Parameters threats: In this section, we discuss on the threats of altering parameters. A CR control a large number of radio parameters. Both in policies and learning process, CR use parameters to control operations and estimate its performance. The functionalities of these parameters are variety. For example, some of these parameters are used to weigh and estimate the performance of CR; some of them are the conditions or the switching bases of policies. Altering these parameters can cause sub-optimal or wrong operations for a CR.

In addition, an attacker can also manipulate a CR to behave malicious, and teach the CR to alter the parameters to impact the CR to operate sub-optimal.[9]

5.2. Dynamic spectrum access threats

5.2.1. Spectrum sensing threats: In DSA environment, primary users have the license to use the certain frequency band whenever they want. When the primary uses don't use their spectrum, the spectrum is idle, and secondary users could use the available spectrum opportunistically. Such secondary users need sensing algorithms to detect spectrum holes for communication, and CRs have the capability of detecting the spectrum holes. In addition, a CR has to vacate the channel when the primary user uses it. One of the threats comes from attackers who want to spoof or mask primary user. The attackers provide a feint of the channel will be used by a primary user, so the secondary within range will believe a primary user is active, and vacate the channel. This kind of attack is called Primary User Emulation (PUE. As a result, this attack provides the attacker accessing to the spectrum.[10]

However, this attack effects transient, because when the attackers vacate the channel, or stop to spoof a primary

user, the secondary user could detect the idle channel and use it. There is also another kind of threat, which prevents CR from receiving sensor information or provides the CR false information. The CR cannot receive information about spectrum holes or active primary user, or it receive the false information, so it cannot do right communication decisions. In some CR, sensor information was transmitted through a common control channel. It is easy for the attackers to jam or control the unique channel. Thus, designers of CR who want a common control channel should take consideration of this problem. Also, paper [8] showed us the leveraged jamming example: in some CR, the sensor and the radio share the same front end. Even when they are separate, the sensor sensitivity can be impaired by a nearby transmitter. So sensing and transmission cannot occur at the same time. The radio can only operate for some fraction of the time, f, with the remaining time being used for sensing. In this case, any jamming becomes leveraged by a factor 1/f , For instance, because of sensing, the radio can only operate for
f=70% of the time. Then jamming 35% of the time will reduce the time for communication by 35%/f=50%. Jamming the sensing time can impact the communication time seriously. The key to avoid leveraged jamming is to make the fraction of time devoted to transmission, f, as close to one as possible. Thus, we need good sensing strategies.[9]

5.2.2. Spectrum management threats: Through spectrum sensing, CR detected the idle spectrum bands for communication. These spectrum bands show different characteristics according to time-varying radio environment, operating frequency, bandwidth, and so on. Spectrum management should have the capacity of selecting the most appropriate bands from these bands for users. It should decide on the best spectrum band to meet the QoS requirement over all available spectrum bands [8]. In [8], the functions of spectrum management are classified as spectrum analysis and spectrum decision. Spectrum analysis enables the characterization of different spectrum bands; while spectrum decision select the appropriate spectrum band for the current transmission considering the QoS requirements and the spectrum characteristics. The threats here come from the possibility of false or fake spectrum characteristic parameters. The false or fake parameters impact the results of spectrum analysis, and then impact the results of spectrum decision. So a CR may select the wrong band or the sub-optimal band, and the performance of communication may be impaired. For example, in spectrum analysis, spectrum characterization is focused on the capacity estimation recently.

5.2.3. Spectrum mobility threats: The function of spectrum mobility is to make sure seamless connection when a CR vacates a channel and moves to a better channel. In a CR, the available spectrum bands depend on the factors such as time and place. One should vacate the current band if the band is not available for the reasons like: a primary user is active, or the one moves from one place to another .etc. In order to maintain the communication smoothly as soon as possible, the CR needs to select a new appropriate Spectrum band, and moves to the band immediately. The process from a CR vacating the current spectrum band to the CR moving to a new available spectrum band is called spectrum handoff [8],[10].
During spectrum handoff, the security threats are seriously. Because a failed handoff may need a long time to resume the communication. An attacker can induce a failed spectrum handoff through ways of: Compelling the CR vacating the current band by masking primary user; jamming to slower the process of selecting for a new available band or to cause a communication failure .
For example, some CRs use common control channel. Attacker can gain control of the common control channel, to change the characteristic parameters of available band, or to interfere with primary users. And then prevent smoothly transmission functionality of spectrum mobility. Thus, robust and simple algorithms for seamless connection of spectrum mobility are needed.[9]

6. Characteristics of cognitive radio network

A cognitive radio network (CRN) is a network composed of CR nodes that, through learning and reasoning, dynamically adapt to varying network conditions in order to optimize end-to-end performance. Mitola first makes brief mention of how his CRs could interact within the system-level scope of a cognitive network . Spectrum sharing is right for solve the problems when the CR nodes interact with each other and share the constraint resources such as spectrum. There are three types of classification (as shown in Figure 3) about existing solutions for the CRN or spectrum sharing as follows [9].

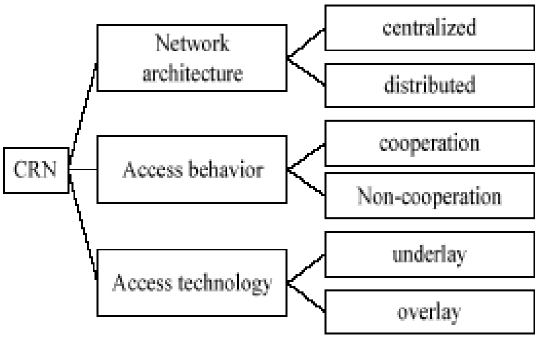

Figure 3: types of classification in CRN

The first classification is based on the network architecture, which can be described as centralized network architecture and distributed network architecture. In the centralized network architecture, a centralized entity controls the spectrum allocation and access procedures, and each sub-centralized entity is proposed to forward its' measurement and information to the centralized entity. While in the distributed network architecture, each node is responsible for the spectrum allocation and access is based on local policies. Second, based on the access behavior, there are cooperation and non-cooperation way. Cooperation solutions consider the effect of the node's communication on other nodes [11]. All the centralized solutions can be regarded as cooperative, and there are also distributed cooperative solutions. In the contrary, non-cooperative solutions consider only the node at hand [10].

Finally, considering the access technology, spectrum sharing can be classified into spectrum overlay and spectrum underlay [8]. A CR node using spectrum overlay approach accesses the spectrum which has not been used by licensed users. So, interference to primary users is minimized. Spectrum underlay exploits the spread spectrum techniques developed for cellular networks . A CR using spectrum underlay approach operate below the noise floor of primary users, in another word, its transmit power at a certain portion of the spectrum is regard as noise by the primary user.

7. Threats in cognitive radio network

In this section, we discuss about the security threats specially aiming at CRN. We have detailed described the characteristics of CRN through three types of classifications in previous section, and here we will point out the security threats accordingly. Comparing the centralized and distributed architectures and the cooperation and non-cooperation connecting approaches, obviously, the centralized architecture and cooperation approach are more vulnerable to attacks. The most severe attack to these two solutions is Denial of service (DoS) attack. In centralized architecture network, if an attacker can manipulate the central entity or prevent the central entity from communication, the whole network is under control of the attacker. In cooperation CRN, if an attacker controls one of the nodes, he can transmit fake information to other nodes, or terminate transmitting information to others. This kind of attack is valid the most in ad hoc network. Especially, common control channel is a target for DoS attacks since successful jamming of this one channel may prevent or hinder all communication [6][16]. In distributed architecture or non-cooperation network, an attack against one CR will not affect others, because other devices operate Independently. In addition, in spectrum overlay environment, a node accesses the network using a portion of the spectrum that has not been used by licensed users [8]. Thus, an attacker can use the method mentioned in section 5.2.1, spoofing or masking primary users to prevent the normal node from using the spectrum, and the worst-case is that the normal node cannot sense any available spectrum, and it would consider there is no spectrum to be used. Spectrum underlay environment requires sophisticated spread spectrum techniques and increased bandwidth [8]. Thus, it is comparatively easy for an attacker manipulating a CR node, and jamming to interference primary users.

8. Conclusion

In this paper, we give a background on the security in mobile system and common threat models currently used in security analysis, specifically the Internet threat model, and extensions assumed in wireless networks. And the new security threats that will arise with the use of software-defined radio were summarized.

When protocols, architectures and mechanisms are designed to efficiently distribute resources in the cognitive radio paradigm, misbehaving weaknesses and security vulnerabilities are not of primary concern. CR techniques are still in the early age of its development. It is significant to consider security factors into the design and application techniques for CR. In this paper, the special characteristics of CR and CRN are described as the AI characteristic, DSA characteristic, and three aspects of classifications for CRN. Furthermore, the security threats due to these special characteristics are mentioned in detail, besides some countermeasures and keys need to attention are mentioned. In order to follow the flexible and cognition characteristics of CR, new and robust architectures and techniques are required. In addition, corresponding countermeasures against these security threats are also required.

9. References

[1] D.S.Dawoud"A Proposal for Secure Software Download in SDR" IEEE AFRICON 2004

[2] John A. Davidson. San Diego, CA. "ON THE ARCHITECTURE OF SECURE SOFTWARE DEFINED RADIOS" in 978-1-4244-2677-5/08/$25.00 ©2008 IEEE

[3] Hiroyuki Shiba,. Kazuhiro Uehara. Katsuhiko Araki."Proposal and Evaluation of Security Schemes for So ftware-De fined Radio"in The 1 4fh IEEE 2003 lnternational Symposium on Persona1,lndoor and Mobile Radio Communication Proceedings

[4] Hironori UCHIKAWA,KentsUMEBAYASHI,RYUJI KOHNO,"SECURE DOWNLOAD SYSTEM BASED ON SOFTWARE DEFINED RADIO COMPOSED OF FPGAS,in IEEE 2002.

[5] Lachlan B.Michael. "A PROPOSAL OFARCHITECTURAL ELEMENTS FOR IMPLEMENTING SECURE SOFTWARE DOWNLOAD SERVICE IN SOFTWARE DEFIEND RADIO"IEEE.2002

[6] Scott Chuprun, Chad Bergstrom, and Dr. Bruce Fette." SDR STRATEGIES FOR INFORMATION WARFARE

AND ASSURANCE" in 0-7803-6521 6/$10.00 (C) 2000 IEEE

[7]"High-Level SDR Security Requirements" Approved Document SDRF-06-S-0002-V1.0.0 (formerly SDRF-06 A-0002-V0.00) 12 January 2006

[8] Yuan Zhang, Gaochao Xu*, Xiaozhong Geng." Security Threats in Cognitive Radio Networks" The 10th IEEE International Conference on High Performance Computing and Communications.IEEE.2008

[9] Jack L. Burbank. Laurel, MD. "Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security"IEEE.2006

[10] T. Charles Clancy. Nathan Goergen. "Security in Cognitive Radio Networks: Threats and Mitigation" *IEEE Wireless Communications*,August 2008

[11] S. Arkoulis. L. Kazatzopoulos *C. Delakouridis* G.F. Marias. "Cognitive Spectrum and its Security Issues" The Second International Conference on Next Generation Mobile Applications, Services, and Technologies. IEEE.2008