Digital Signatures for Centralized DSA Networks

Chetan N. Mathur and K. P. Subbalakshmi
Department of Electrical and Computer Engineering,
Stevens Institute of Technology, Hoboken, NJ 07030.
Email:{cnanjund, ksubbala}@stevens.edu

***Abstract*— Over the past few years there has been a growing demand for radio resources and at the same time these resources are under utilized due to static spectrum allocation techniques. Dynamic spectrum access (DSA) has been thought of as a solution that would satisfy both the growing demand for radio resources and to efficiently utilize the spectrum. The radio devices that have the capability to dynamically sense the spectrum and access the under utilized bands are called cognitive radios (CR). There are two broad classes of users in CR, the primary user is a licensed user of a particular radio frequency band and the secondary users are unlicensed users who cognitively operate without causing harmful interference to the primary user.**

In this paper we consider a denial attack on centralized DSA networks where a malicious secondary user masquerades as a primary user and effectively shuts off access to all other secondary users. Note that this problem is unique to CR due to the distinction between primary and secondary users. We propose a public key cryptography based primary user identification mechanism that prevents malicious secondary users from masquerading as primary users. We show that the proposed identification mechanism and the associated key management are computationally light weight. We also discuss some advantages and limitations of the proposed identification mechanism.

***Index Terms*— Digital Signature, Cognitive Radio, Dynamic Spectrum Access, Denial of Service Attack .**

I. Introduction

The growth in demand for spectral resources and the static allocation model for spectrum bands has created a phenomenon called artificial spectral scarcity. This scarcity is considered artificial because spectrum bands are often under utilized [1],[2] by its primary users while at the same time there is an increased (often un-met) demand for the same spectrum resources by other users.

In an effort to increase the efficiency of spectrum utilization, the Federal Communications Commission (FCC) recently proposed a mandate [3] that allows unlicensed radios to operate in unused bands owned by primary licence holders as long as they do not cause harmful interference to the primary users. This dynamic allocation of unused spectrum temporarily to unlicensed secondary users is facilitated by the use of cognitive radios (CR) and is referred to as dynamic spectrum access (DSA).

The IEEE 802.22 [4] is the first wireless standard based on CRs and it is chartered with the development of a CR-based Wireless Regional Area Network (WRAN) Physical (PHY) and Medium Access Control (MAC) layers. This standard proposes a centralized architecture where the secondary users are managed by secondary base stations. The presence/absence of primary users is detected through a distributed sensing mechanism, where the sensing is performed synchronously by secondary users and the results are transmitted back to the associated base station.

In this paper, we consider the architecture proposed by IEEE 802.22 as a generic centralized DSA network architecture and show the existence of a simple yet lethal denial of service attack (DOS) on such networks. This attack is based on the inability of secondary users to distinguish the transmissions between primary users and malicious users. We then propose a simple yet efficient primary user identification scheme based on public key ciphers used as digital signatures.

Our proposal is generic in the sense that any public key cipher could be employed to implement the scheme. There are four players in the proposed scheme, the primary users, a certification authority, the secondary base stations and the secondary users. The primary user encrypts its identification with its private key and appends the encrypted value (signature) to its transmission. All secondary users, scan for the signature during the sensing period and the signatures from various secondary users are consolidated at the associated secondary base station. The secondary base station then verifies these signatures. Since only the primary knows its private key, a malicious secondary could not have produced a valid signature. If the signature is from a valid primary user, then the secondary base station is assured of the presence of a primary transmission and takes appropriate actions. We show that the proposed scheme is as secure as the underlying public key cipher. Some of the favorable features of the proposed scheme are; it is light weight, the key management is simple and it can detect accidental asynchrony in secondary users. We also discuss some of the limitations of the proposed scheme that make them unusable in certain situations.

The rest of the paper is organized as follows, in Section II we represent an architecture of centralized DSA based on IEEE 802.22. A simple yet lethal denial of service attack on centralized DSA is shown in Section III. In Section IV we propose a primary user identification scheme based on public key ciphers. The security of the proposed scheme is presented in Section V. Some of the advantages of the proposed scheme are discussed in Section VI and limitations are discussed in Section VII. We finally conclude the paper in Section VIII.

II. Centralized Dynamic Spectrum Access Network Architecture

We base the centralized dynamic spectrum access network architecture on the IEEE 802.22 standard. In a centralized

DSA network architecture, the network is divided into cells. The medium access in every cell is managed by a secondary base station as shown in Figure 1. The secondary users are associated with one or more secondary base stations. The base stations manage the association with the secondary users using frames. The frame structure in medium access control (MAC) layer of IEEE 802.22 is called the super frame [4]. The super frame consists of a preamble and a super frame control header (SCH) through which the secondary users initially synchronize with the base station. The base station has the responsibility to manage the upstream and downstream traffic, which may include ordinary data communication, measurement activities or coexistence procedures. In addition to associating with the secondary users, the base station is also responsible for detecting the presence of primary users through distributed sensing. This is achieved by distributing the load of sensing the spectrum to multiple secondary users, with each user sensing a portion of the spectral band. The base station sends synchronizing signals to the secondary users during the sensing (or quiet) periods. The quiet period mechanism in IEEE 802.22 is comprised of two stages. The first stage, called the fast sensing stage occurs frequently and periodically where the secondary users determine if the energy in the affected channel is always below the threshold. The measurements during the fast sensing stage are consolidated at the secondary base station, which decides if the second fine sensing stage is essential. In the fine sensing stage, a detailed analysis is performed in the affected channels to determine if the primary user transmissions are going on. The sensing operations are supported by the MAC super frame structure.

III. Denial of Service Attack on DSA

Consider a scenario in a centralized DSA network represented by Figure 2. Here there are five secondary users $S_1, .., S_5$ associated with a secondary base station B and are operating cognitively in the same band as that of the primary user P. All the secondary users synchronously and periodically sense the spectral band to detect a primary user transmission. Therefore, when primary user P begins transmission, secondary users S_1, S_2 and S_5 can sense it and report it to the secondary base station B. The secondary base station then orders all its associated secondary users to vacate the channel corresponding to the primary user and selects the next available channel.

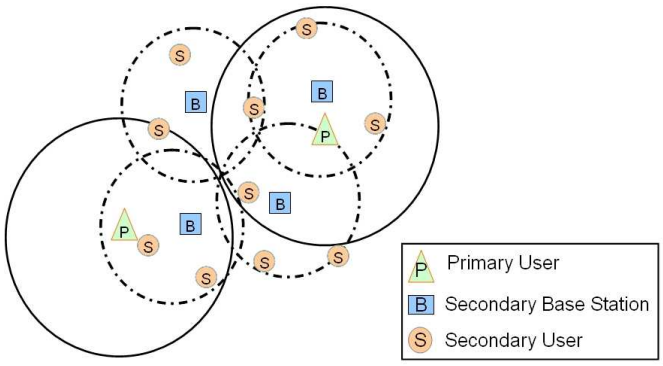

Fig. 1. Centralized DSA network architecture.

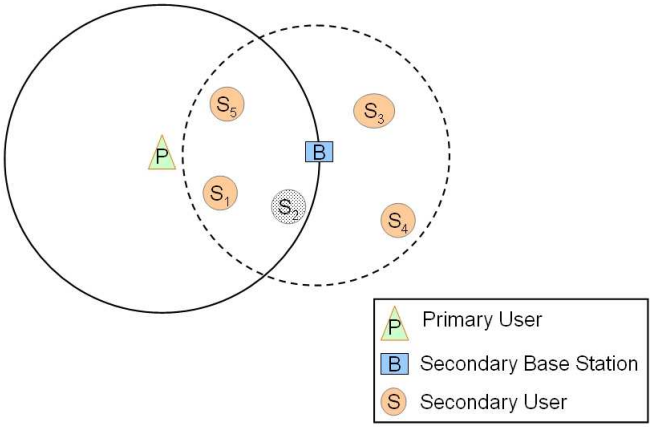

Fig. 2. A possible scenario for denial of service attack. The secondary user S_2 is assumed to be malicious.

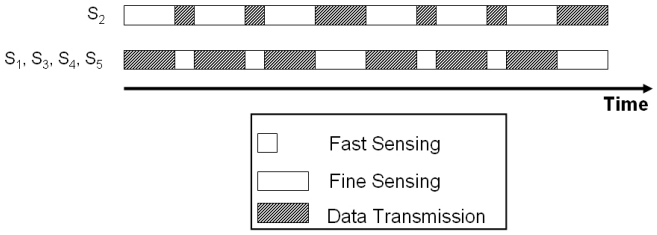

Fig. 3. Malicious user S_2 performing a DOS attack on the secondary user network.

Suppose that the secondary user S_2 was a malicious user. One of the objectives of S_2 could be to deny spectral access to other secondary users. To perform the denial attack, all that S_2 needs to do is to transmit during the sensing periods of other secondary users as shown in Figure 3. Since, the primary user detection scheme is energy based; the other secondary users cannot make an accurate distinction between the primary and the malicious secondary user's transmission. Furthermore, the malicious user S_2 can repeat this attack in all the channels selected by the base station B and effectively starve all the secondary users form access to the transmission medium. Since the malicious user needs to transmit only during the quiet periods, this attack can be performed by an adversary with limited resources. Hence, the denial of service attack against centralized DSA networks is very simple to implement and yet has lethal consequences. Note that this attack is unique to DSA networks due to the coexistence of two different classes of users, the licensed primary and the unlicensed secondary.

IV. Proposed Primary User Identification Scheme

We now propose a novel public key cryptography based identification mechanism with which the secondary users would be able to distinguish between malicious entities and the primary users' transmissions. Before we introduce our

proposal, we briefly discuss some aspects of public key ciphers.

A. Public key cryptography

Public key ciphers [6] rely on one key for encryption and a different but related key for decryption. The key that is revealed is called the public key (denoted by KU) and the key that is kept secret is called the private keys (denoted by KR). The encryption and decryption algorithms of public key ciphers satisfy the following properties,

$$X = D_{KU}[E_{KR}[X]] \tag{1}$$

$$X = D_{KR}[E_{KU}[X]] \tag{2}$$

Here, X is a message consisting of letters from a finite alphabet. E and D are encryption and decryption algorithms respectively. Therefore, the encryption operation with one key is inverted by the decryption operation with the other key. Some of the well known public key ciphers are RSA, ElGamal, Rabin and Elliptic curve cryptosystems. Public key ciphers can be used to provide confidentiality, as digital signature and to exchange secret keys. In this paper, we use public key ciphers as digital signatures. To use a public key cipher as a digital signature, the transmitter signs the message using its private key and the receiver verifies the signature using the transmitter's public key. Since only the transmitter possesses its private key, it is computationally infeasible for an imposter to sign the transmitter's message.

B. Certification authority

A certification authority (CA) is an entity that we assume to be connected to the primary users and the secondary base station through a wired backbone network. The purpose of the certification authority is to maintain public keys used by all primary users within a geographical area.

C. Actions performed by the primary users

The primary user generates a pair of public and private keys using a key generation algorithm [6]. The public keys are securely registered with the corresponding certification authority.

The data to be transmitted by the primary user at its link layer is called the message service data unit (MSDU). MSDUs are often broken down into many message protocol data units (MPDUs), where each MPDU consists of MAC (Medium Access Control) header and a data payload (see Figure 4. The MAC header consists of the primary user identity (PID) and the time stamp (TS). The primary user computes a digital signature, S, by encrypting its identity and the time stamp with its private key.

$$S = E_{KR}(PID||TS) \tag{3}$$

As shown in Figure 4, the signature is appended to the MPDU to obtain a signed MPDU. The signed MPDUs are then transmitted over the wireless medium.

$$MPDU_{\text{signed}} = MPDU||S \tag{4}$$

Every time the primary users change their public and private key pairs, the public key has to be registered with the CA.

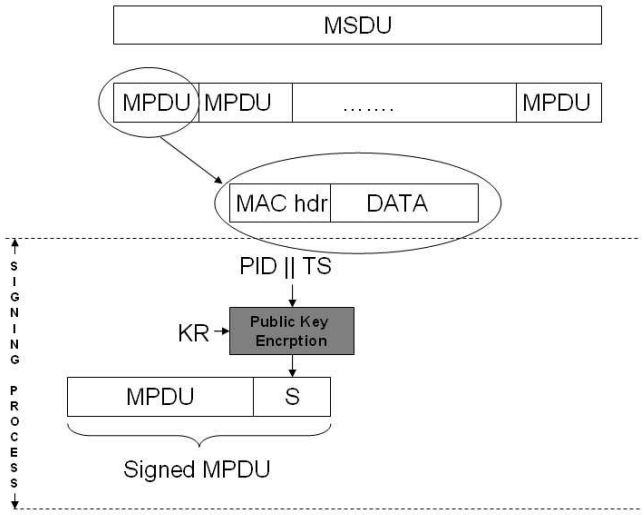

Fig. 4. Block Diagram Representing Primary User Signing Process.

D. Actions performed by the secondary users

The secondary users look for the presence of a primary user's transmission during their fine sensing operation [4]. If a transmission is detected, then the secondary users decode the signal to obtain the corresponding MPDU's. The MPDU's are then scanned for the presence of signatures. If the signatures are found, they are detached from the MPDUs and stored by the secondary users. These stored signatures are periodically transmitted to the secondary base station through an established control channel.

E. Actions performed by the secondary base station

The secondary base station securely obtains the public keys and the identities of the primary users within its vicinity from the CA. Whenever, the secondary users detect transmissions with signatures during their sensing periods, the corresponding signatures are transmitted to the secondary base station. The secondary base stations maintain only one copy of duplicate signatures. The set of unique signatures are then sequentially decrypted with the public key, KU_i, of each primary user, i, within its vicinity.

$$PID_i||TS = D_{KU_i}(S) \tag{5}$$

If the decrypted primary user's identity matches with one of the primary user identities in the list obtained from the CA, the base station checks for the validity of the time stamp. To do this, the base station selects a network delay parameter, δ, which defines the window of acceptable time stamps. If the absolute difference between the base station's current time and the decrypted time stamp is δ, the time stamp is accepted as a valid time stamp and the secondary base station is assured of the presence of a licensed primary user. The value of δ should be chosen such that the signature does not expire before it is decrypted by the secondary base station.

V. Security of the Proposed Scheme

The proposed scheme is secure as long as a malicious entity is unable to forge the signature of the primary user. We know that deriving the private key from a known public key is a hard problem. Since it is computationally infeasible for a malicious entity to forge the primary user's signature. The proposed scheme is as secure as the underlying public key cipher. We now briefly discuss some of the attacks on the proposed scheme and steps we take to mitigate the effects of such attacks.

A. Replay attack

A commonly used technique to circumvent signature schemes is to capture a valid signature and reuse it at a later time. This is called the *replay attack* [6]. However, the inclusion of time stamps while calculating the signature is to prevent this type of attack. However, a valid signature could be replayed within a δ time window. Therefore, selecting δ as small as possible will limit the impact of replay attack to a smaller window.

B. Base station draining attack

This is a novel attack that makes use of the proposed identification scheme to drain the base stations power and performance. Here, the malicious entity transmits a lot of random (junk) signatures during the sensing periods of other secondary users. These signatures would be forwarded by the secondary users to the secondary base stations. Now, the secondary base station would have to decrypt each of the signatures with all of the primary users public keys. This can significantly degrade the performance of the secondary base station, since the signatures are transmitted from multiple secondary users. One of the mechanisms to mitigate the effect of this attack is to discard the duplicate signatures.

C. Attack on CA

An attack on certification authority would severely compromise the security of the DSA network. Consider a scenario where an adversary attacks the CA and modifies the stored public keys. This would invalidate all the signatures created by the primary user and the secondary base station would never recognize the existence of a primary user in any band. This would result in harmful interference to the primary receivers and is against the objectives of DSA networks. Therefore, the CA, communications between primary users and CA and communications between secondary base stations and CA should be secured.

VI. Advantages of the Proposed Scheme

In this section we discuss some of the advantages of using the proposed identification scheme compared to traditional signature schemes and symmetric key ciphers.

A. Computationally light weight

Traditional public key signature schemes consume significant computational resources. However, unlike the traditional signature algorithms (for example the Digital Signature Algorithm [7], Elgamal Signature Algorithm [9]), the proposed scheme does not use Hash functions and it does not sign the entire MPDU. This significantly reduces the computational complexity of the proposed identification scheme. On a 2 GHZ Pentium processor the signature/verification process runs in the order of milliseconds [10].

B. Simplified key management

The key management process in the proposed scheme is simple. Since the base station gets the public keys directly from the CA, there is no need for key pre-distribution/ distribution [8] operations. For example, in a symmetric key setting, a key refresh operation would take as many updates as the size of the network. However, in the proposed scheme, whenever a primary refreshes its key, only one update operation per associated base station needs to be performed by the CA. Therefore, the key management in the proposed scheme has constant time complexity irrespective of the network size.

C. Detect accidental asynchrony in secondary users

Some of the frequency bands (e.g. TV bands) cover a large geographical area and it is harder to maintain synchronization between secondary users in these bands. Consider the following scenario where one or more secondary users are temporarily not synchronized with the rest of the secondary user network. These secondary users may transmit during the sensing periods of other secondary users. Such transmissions are detected and discarded by the other secondary users due to the lack of signatures in the transmitted signal. Had the proposed identification mechanism not been employed, accidental asynchrony in secondary users would result in missed opportunities [12].

VII. Limitations of the proposed scheme

The proposed identification scheme can be easily implemented in a centralized DSA setting like the IEEE 802.22 [4]. However, there are some instances where the proposed scheme would be hard to implement. Some of these issues are discussed in this section.

A. Analog primary users

The proposed scheme assumes that primary users operate in a digital domain. This is not true in all cases. For example, if the primary users transmit analog TV signals, our proposed scheme cannot be employed. In fact, when primary signals cannot be digitized, most of the cryptographic primitives cannot be employed. Since, cryptography is implemented in a digital domain.

In [5] the authors propose a technique wherein, transmission from distinct users are identified based on the electromagnetic characteristics of the transmission device. Such an approach cannot guarantee that a malicious user would not mimic the primary user's signal characteristics. Securely identifying primary users in analog domain is still an open issue.

B. Existence of CA

In the proposed scheme, reliability of public keys depends on the existence of a secure certificate authority. However, it may not be possible to have such an infrastructure where the CA is connected to the primary users and secondary base stations via a wired backbone network. This is because some frequency bands span over a huge geographical area which makes such an infrastructure expensive.

C. Decentralized DSA architectures

In a decentralized DSA architecture, there are no secondary base stations to coordinate between the secondary users. Therefore, the secondary users would have to verify the signature by themselves. This implies that the primary user's public keys have to be securely transmitted to all the secondary users within that vicinity. To do this, one of the secondary users should assume the responsibility of the certification authority and should be reachable from all other secondary users. As discussed in Section V-C a compromise in CA would collapse the security of the entire network. Threshold cryptography schemes that are employed to distribute the role of CA to multiple nodes in ad-hoc networks [11] could be employed in distributed DSA networks as well. However, such an arrangement would require significant message exchanges. Unfortunately, lack of a common control channel and dynamically changing transmission bands make it a harder problem for decentralized DSA networks.

VIII. Conclusions

A denial of service attack on a generic centralized DSA network architecture based on the IEEE 802.22 standard is proposed. It is shown that an adversary with limited resources could easily bring down service of the entire secondary network within a geographical location.

A secondary users inability to distinguish between the transmitted signals of primary and an adversary is identified as the primary cause of the DOS vulnerability. A light weight and efficient signature scheme based on public key cryptography is proposed to identify valid primary users. It is shown that the proposed scheme has constant time key management complexity and that it is robust against reply attack. Some advantages and limitations of the proposed scheme are discussed.

References

[1] McHenry, M. "Spectrum white space measurements," *New America Foundation Brodband Forum*, June 2003.

[2] FCC Spectrum Policy Task Force, "Report of the spectrum efficiency group," Nov., 2002.

[3] Federal Communications Commision (FCC), "Notice of Proposed Rule Making," *ET Docket no.04-113*, May 25, 2004.

[4] Carlos Cordeiro, Kiran Challapali, Dagnachew Birru, and Sai Shankar N., "IEEE 802.22: The First Worldwide Wireless Standard based on Cognitive Radios," *IEEE DySPAN*, pp. 328–337, November 2005.

[5] K.A. Remley, C.A. Grosvenor, R.T. Johnk, D.R. Novotny, P.D. Hale, M.D. McKinley, A. Karygiannis, E. Antonakakis, "Electromagnetic Signatures of WLAN Cards and Network Security," *The 5th IEEE International Symposium on Signal Processing and Information Technology (IEEE ISSPIT 2005)*, Athens, Greece, December 18-21, 2005.

[6] B. Schneier, *Applied cryptography: protocols, algorithms, and source code in C*, 2nd ed. New York: Wiley, 1996.

[7] FIPS-186-2, "The second revision to the official Digital Signature Algorithm (DSA) specification".

[8] D. R. Stinson, *Cryptography: Theory and Practices*, ser. Discrete Mathematics and its Applications, K. H. Rosen, Ed. 2000 Corporate Blvd., N.W., Boca Raton, Florida 33431: CRC Press Inc., 1995.

[9] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Transactions on Information Theory*, Volume 31, pp. 469-472, 1985.

[10] http://www.eskimo.com/ weidai/benchmarks.html

[11] Zhou, L., Hass, Z.J., "Securing Ad Hoc Networks," *IEEE Network Magazine*, pp. 24-30, 1999.

[12] Visotsky, E., Kuffner and S. Peterson, "On collaborative detection of TV transmissions in support of dynamic spectrum sharing.", *IEEE DySPAN.*, pp. 338-345, November 2005.