Signal Fingerprinting in Cognitive Wireless Networks

Simone Soderi[†], Giulio Dainelli[†], Matti Hämäläinen[‡], Jari Iinatti[‡]
[†]GE Transportation Systems, Florence, Italy. email:firstname.lastname@ge.com
[‡]Centre for Wireless Communications, University of Oulu, Oulu, Finland email:firstname.lastname@ee.oulu.fi

***Abstract*—Future wireless communications are made up of different wireless technologies. In such a scenario, cognitive and cooperative principles create a promising framework for the interaction of these systems. The opportunistic behavior of cognitive radio (CR) provides an efficient use of radio spectrum and makes wireless network setup easier. However more and more frequently, CR features are exploited by malicious attacks, e.g., denial-of-service (DoS). This paper introduces active radio frequency fingerprinting (RFF) with double application scenario. CRs could encapsulate common-control-channel (CCC) information in an existing channel using active RFF and avoiding any additional or dedicated link. On the other hand, a node inside a network could use the same technique to exchange a public key during the setup of secure communication. Results indicate how the active RFF aims to a valuable technique for cognitive radio manager (CRM) framework facilitating data exchange between CRs without any dedicated channel or additional radio resource.**

***Index Terms*—Fingerprinting; Cognitive; Security; Wireless.**

I. Introduction

Nowadays, mobile devices are equipped with several air interfaces. A definite upward trend in the number of air interfaces for each terminal has defined two possible approaches. The first, *multi-modality* uses different chip solutions to implement air interfaces diversity. On the other hand, *flexible* air interfaces implemented via software defined radio (SDR) enabled the opportunistic use of spectrum [1]. In the late 1990s, SDRs progressed up to cognitive radio (CR). Starting from radio frequency (RF) processing functions, typically provided by SDRs, CRs *sense* and *understand* the wireless scenario. After the understanding process is concluded the device has all the information needed to *decide* which configuration and parameter shall be changed. Finally, the cognitive cycle ends with the *adaption* phase where the terminal makes changes so as to realize the new wireless link [1].

Radio regulations don't efficiently use the radio spectrum because most of the time certain licensed frequency bands remain unused. CRs improve spectral efficiency by filling holes discovered in the wireless channel during the sensing of the scene [1]. However, an attacker could use CR features to implement a denial-of-services (DoS) attack. For example, he could unduly burden network resources. This threat raises the need to find countermeasures in terms of CR network security. RF fingerprinting (RFF) has been proposed in [2] to make a distinction between emitters in CR networks exploiting physical properties of the emitter. The idea proposed in this paper uses RFF, not only to mark an existing wireless communication, but also to exchange a secret shared key.

This paper is organized as follows: Section II reports background and motivations. Section III introduces security aspects and continues with digital I/Q demodulation architecture. Section IV further formulates the proposed method. In Section V, the results from simulations are shown. Finally, the paper is concluded in Section VI.

II. Background and Motivation

The archaic pre-allocation scheme of radio spectrum is evolving toward a dynamic allocation scheme, and CR is a promising approach to obtain spectrum flexibility. In modern wireless communications, CRs are able to sense and to adapt their behavior to the radio environment to provide intelligent solution during wireless network setup. A typical cognitive scene is composed by the primary user on a licensed band, and with secondary unlicensed users. In the case where the secondary user is a CR it could opportunistically access the channel when it is not used by primary licensed user. The aforementioned mechanism is particularly important during wireless network setup. Users of this network could be organized into clusters based on their location but in order to build this infrastructure they assume the availability of a common-control-channel (CCC). Due to radio regulations only a few global channels are available for this task, and typically, CRs utilize spectrum holes for the communication [1].

This paper proposes a different approach to solve the CCC issue using existing main communication. However, the proposed method implements at the physical (PHY) layer, the key exchange needed in security protocols.

III. Security Introduction

For a long while computer security and electronic warfare have been known as two different fields, even if they used the same technologies (e.g., cryptography). Many theories developed during electronic warfare are applied nowadays by security engineers. Security services included in wireless communications are: authentication, confidentiality, integrity and availability [3]. On the other hand, electronic warfare is

Project co-funded by the Tuscany Region and European Community under the 2007-2013 POR CREO FESR program.

CROWNCOM 2014, June 02-04, Oulu, Finland

DOI 10.4108/icst.crowncom.2014.255374

concerned with control of the electromagnetic (EM) spectrum through with the following actions:

- electronic attack (e.g., jamming);
- electronic protection (e.g., EM attacks rejection);
- signal/communications intelligence to support attacks and protections.

Passive RFF is one signal intelligence technique used in electronic warfare during site surveys. Many years ago it was used in computer security to identify cloned cellular telephony [4].

Now, there is a need to differentiate between different types of RFFs. *Passive RFF* exploits the unique EM signature (EMS) of the transmitter in the mobile devices. *Active RFF*, proposed in this paper, intentionally introduces an EMS encoding a watermark at the PHY layer.

Host identity protocol (HIP) combined with a tunnel technology was the architecture proposed in [5] to secure wireless communications against DoS and man-in-the-middle (MitM) attacks. HIP allows the separation between the identification and localization information that normally comes with the IP address (Figure 1). HIP introduces the host identity layer in the TCP/IP stack between networking and transport layers, as specified in RFC5201 [6] by the Internet Engineering Task Force (IETF). HIP establishes a security association (SA) between hosts via a four way handshake protocol named base exchange (BEX). When SA succeeds hosts uses IP security (IPSec) encapsulating security payload (ESP) to exchange data through a secure tunnel.

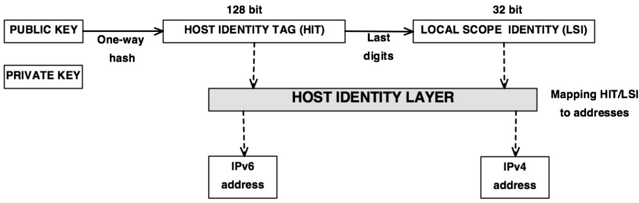

Fig. 1. Host Identity Layer.

This paper discusses (Section IV) an innovative method to exchange CCC information such as host identity tag (HIT) or local scope identity (LSI) tags (Figure 1) at the PHY layer instead of via BEX protocol.

IV. Proposed Method

The reference scenario studied is a cognitive mesh (CogMesh) network as shown in Figure 2. CogMesh is a typical example of a multi-channel and multi-access network [1] where global channels are usually utilized to discover neighbors or for access control.

The CogMesh presented in Figure 2 is composed of CRs organized in a cluster. Inside *Cluster-A* there is a main communication between *Cluster-Head* and *Node-1* through *Channel-1*. Without any dedicated CCC (hypothesis), CRs sense the environment detecting a secondary communication between nodes. With the flexibility given by cognitive devices, the proposed method describes how CRs could encapsulate CCC information in *Channel-2* using active RFF. Otherwise, the same RFF technique could be used to exchange identity tags (i.e., HIT or LSI) and then secure wireless communication with HIP protocol inside the same cluster or between different clusters using gateways.

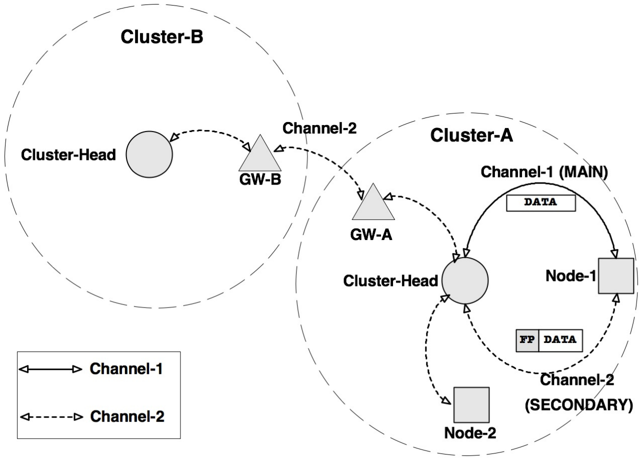

Fig. 2. RF fingerprint CCC information.

Transmitter

Figure 3 shows the block diagram of the transmitter. The signal fingerprinting is done combining the original modulated signal at intermediate frequency (IF), f_{IF}, with an in-band modulated information at f_{FP}. Which is the fingerprinting signal carrier frequency. The CR adapts parameters of fingerprinting signal sensing the main communication. Finally, the signal is mixed at radio frequency (RF) and radiated by the antenna.

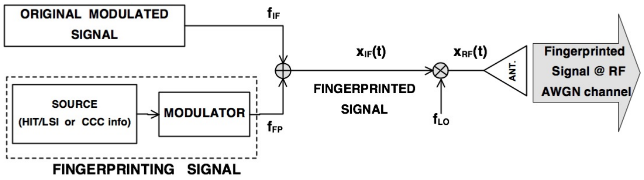

Fig. 3. Transmitter structure for digital fingerprinting.

Receiver: I/Q demodulation

An in-phase (I) and quadrature (Q) demodulator was selected for the digital radio receiver. Conventional I/Q demodulator splits the received signal mixing each part of the signal with a local oscillator and its 90° shifted replica. This architecture presents some limitations due to the I and Q arms being unbalanced [7]. The technological advance of the analog-to-digital-converter (ADC) allows the implementation of IF sampling strategies. High-speed ADCs enable direct down-conversion performing I/Q demodulation digitally that overcomes the aforementioned issues in a conventional receiver. Nowadays, more and more frequently SDR, and as consequence CR, uses this technique for receivers implementation [7].

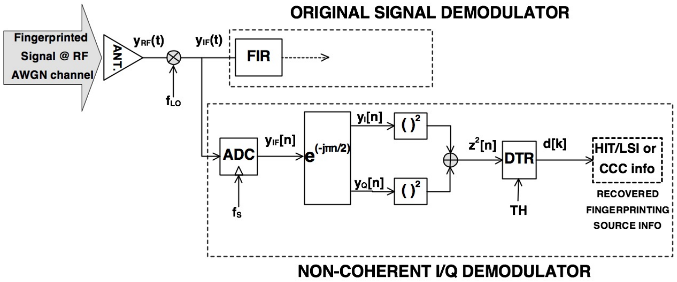

Fig. 4. Receiver with fingerprinting information recovery.

As could be observed from Figure 4, the received signal after the antenna is mixed to the IF and then processed by the original signal demodulator to recover data exchanged through *Channel-1*. In parallel the incoming signal at IF is led to an additional demodulator used to recover the active RFF.

V. Simulations and Results

The first part of this section presents the simulation scenario studied while the second part shows the results achieved.

A. Scenario

The main objective of these simulations was to demonstrate the feasibility of the proposed method. The goal was to fingerprint an existing wireless communication between CR devices with a modulated signal. The scenario is shown in Figure 2 (i.e., CogMesh network) where nodes in the cluster exchange data (i.e., through *Channel-1*). CRs sensing the scene could detect another wireless communication, i.e., *Channel-2* and transmit CCC information or security public key using active RFF through that channel. The simulated scenario, implemented using the signal processing toolbox in MATLAB [8], represented the original signal on *Channel-2* with a direct sequence spread spectrum (DSSS) signal and implemented the active RFF with amplitude shift key (ASK) signal. The transmitter used refers to Figure 3 and it marks the DSSS signal adding an ASK with $f_{FP} = f_{IF}$. Thus, the received IF signal perturbed by noise is given by

$$y_{IF}(t) = x_{DSSS}(t) + x_{FP}(t) + \nu(t), \tag{1}$$

where $x_{DSSS}(t)$ is the DSSS signal, $x_{FP}(t)$ is the additive fingerprinting signal and $\nu(t)$ the additive-white-gaussian noise (AWGN). When the quadrature phase shift key (QPSK) is used, the $x_{DSSS}(t)$ can be expressed as [9]

$$\begin{aligned} x_{DSSS}(t) = A_d\sqrt{\frac{1}{T_{sd}}} \cdot d_1(t) \cdot c_1(t) \cdot cos(2\pi f_{IF}t) + \quad (2) \\ -A_d\sqrt{\frac{1}{T_{sd}}} \cdot d_2(t) \cdot c_2(t) \cdot sin(2\pi f_{IF}t), \end{aligned}$$

where A_d is the amplitude, T_{sd} is the symbol period, $d_1(t)$ and $d_2(t)$ are data derived by splitting the bit-stream in I and Q channels. Finally, $c_1(t)$ and $c_2(t)$ are the spreading codes for I and Q channels. The $x_{FP}(t)$ when the ASK is used can be expressed as

$$x_{FP}(t) = \begin{cases} A_a\sqrt{\dfrac{2}{T_{sa}}} \cdot cos(2\pi f_{FP}t), & \text{for } 0 \le t \le T_{sa}, \\ 0, & \text{elsewhere} \end{cases} \tag{3}$$

where A_a is the amplitude, T_{sa} is the symbol time. The incoming IF signal (i.e., $y_{IF}(t)$), after the RF chain, feeds the original signal demodulator and a second arm needed to recover the fingerprinted information. The receiver principle is sketched in Figure 4. The non-coherent I/Q demodulator, used for decoding the RFF, is based on IF sampling [7]

$$\begin{cases} f_{FP} = f_{IF} = kf_s \pm \dfrac{f_s}{4}, & \forall k \in \mathbb{Z} \mid k \ge 1, \\ f_s \ge 4B, \end{cases} \tag{4}$$

where $f_s = \frac{1}{T_s}$ is the ADC sampling rate and B the received fingerprinting signal bandwidth (i.e., ASK). The ADC output provides the received sampled version of IF signal given by:

$$\begin{aligned} y_{IF}[n] &= V[n] \cdot cos(2\pi f_{IF} \cdot nT_s + \theta[n]) + g[n], \quad (5) \\ V[n] &= A_a\sqrt{\frac{2}{T_{sa}}}, \quad \theta[n] = pT_s, \\ g[n] &= x_{DSSS}[n] + \nu[n], \end{aligned}$$

where $V[n]$ and $\theta[n]$ are the envelope and the phase of fingerprinting signal respectively. $g[n]$ represents the spread-spectrum signal and the additive noise. In accordance with (4), $f_{IF} = \frac{3f_s}{4}$ could be selected. The I and Q components of the baseband signal can be expressed as

$$\begin{aligned} y_I[n] &= \frac{V[n]}{2} \cdot cos(p) \cdot (1 + (-1)^n) + \tilde{g}_I[n], \quad (6) \\ y_Q[n] &= \frac{V[n]}{2} \cdot sin(p) \cdot (1 - (-1)^n) + \tilde{g}_Q[n], \end{aligned}$$

where $\tilde{g}_I[n]$ and $\tilde{g}_Q[n]$ are I/Q components of resulting signal when multiplied by $e^{-j\frac{\pi}{2}n}$. The sum of these two components squared feeds a detector (DTR) that judges the received signal as

$$d[k] = \begin{cases} 1, & \text{if } z^2[kT_s] \ge \dfrac{E_s}{2}, \\ 0, & \text{otherwhise} \end{cases} \tag{7}$$

where the threshold (TH) for detection is fixed to $\frac{E_s}{2}$ and E_s is the signal energy per symbol.

Next, as shows in Figure 4, the bit-stream, $d[k]$, is led to another block where the fingerprinting information (e.g., 32 bits LSI) is recovered. E.g, this block could support upper layer protocols developed for this specific application. Actually more and more frequently CRs implement a cognitive resource manager (CRM) in order to facilitate auto-configuration and network optimization using machine learning algorithms [1]. CRM provides cross-layers communication linking $d[k]$ with a tool to recover the active RFF information.

B. Results

The main goal of this study was to verify the feasibility of the active RFF method to encapsulate information in a host wireless communication (i.e., DSSS in *Channel-2*).

Table I presents the radio signal parameters used during simulations. The DSSS signal was generated using Hadamard pseudo-noise (PN) sequences on QPSK modulation at $f_{IF} = 19.2$ MHz. The chip-rate was 12.8 MHz, the processing gain 128 and transmitted signal had rectangular shape. On the other hand, the narrow band signal used to implement the active RFF was an ASK with $f_{IF} = 19.2MHz$ and bit-rate $R_{b-ASK} = 320$ kHz. IF sampling technique requires at least 4 samples per symbol and $f_s = 25.2$ MHz verifies (4).

TABLE I
RADIO SIGNAL PARAMETERS

Description	Parameter	Value
ADC	Sampling rate (f_s)[1]	25.6 MHz
DSSS	Carrier Frequency (f_{IF})[2]	19.2 MHz
	Energy of signal waveform	0 dB
	Bit-rate (R_b)	100 kbps
	Processing Gain (M)[3]	128
	Chip-rate (R_c)	12.8 MHz
	Number of bits (N)	32
	Modulation	QPSK
ASK	Carrier Frequency (f_{FP})[4]	19.2 MHz
	Energy of signal waveform	$[15 \div 20]$ dB
	Number of bits	32
	Bit-rate (R_{b-ASK})	320 kbps
Other	SNR[5]	$[0 \div 12]$ dB
	Channel	AWGN
	FP information	32 bits

[1] $f_s \geq 4B$;
[2] $f_{IF} = 3/4 \cdot f_s$;
[3] Using Hadamard PN code;
[4] $f_{FP} = f_{IF}$;
[5] Signal-to-noise ratio.

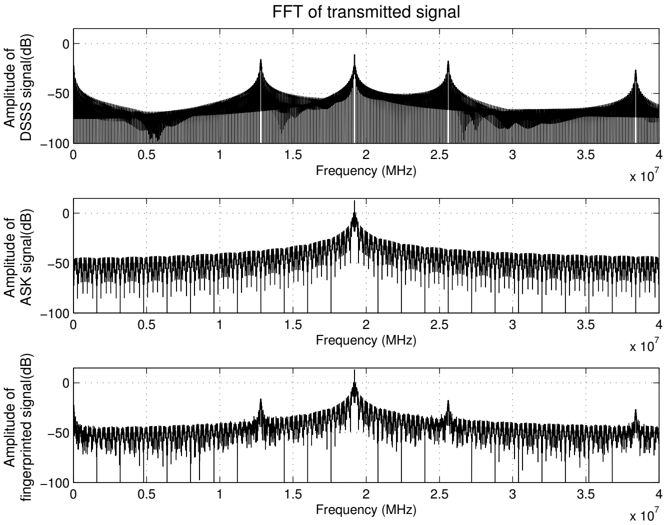

Fig. 5. Spectrum of transmitted signal.

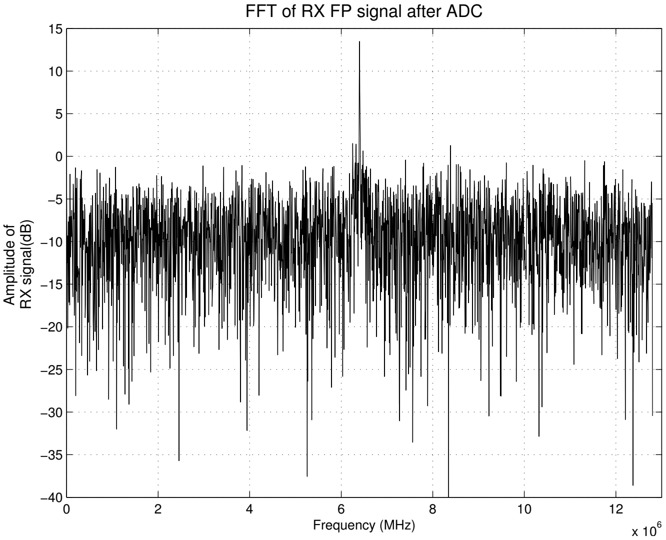

Fig. 6. Spectrum of fingerprinted received signal $(Y_{IF}^{ADC}(f))$.

Figure 5 the spectrum generated by the transmitter when the DSSS signal is fingerprinted with an ASK with the same carrier frequency. The combination of these two signals is reasonable because it exploits the built-in rejection of spread-spectrum against narrow-band signals. The number of information bits per symbol and their oversampling during simulations, were considered to calculate the relative power of noise (N_0) in AWGN channel model used. The relationship between $\frac{E_s}{N_0}$ and signal to noise ratio (SNR) both expressed in dB is given by [8]

$$\frac{E_s}{N_0} = 10log_{10}(k) + 3 + SNR, \tag{8}$$

where k is the number of samples for each symbol.

Figure 6 shows the spectral density of the received fingerprinted signal, i.e. $Y_{IF}^{ADC}(f)$ after the frequency shift introduced by the ADC. Then the signal signal replica is downconverted in baseband multiplying $Y_{IF}^{ADC}(f)$ by $e^{-j\frac{\pi}{2}n}$.

Bit error rate (BER) results versus SNR are shown for both ASK fingerprinting signal and host channel, i.e., DSSS. The error probability for fingerprinting signal was similar to theoretical curve (Figure 7). On the other hand, Figure 8 shows a minimal perturbation for lower SNR, $(SNR \leq 4)$.

VI. CONCLUSIONS

The active RFF was proposed as an innovative method to encapsulate inside a host wireless communication. Furthermore it could be used, at PHY layer, to exchange public key during setup of security protocol. The performance are similar to any conventional narrow band communication but this method refers to stenography transmitting securely information that is hidden in spread-spectrum communication. The proposed

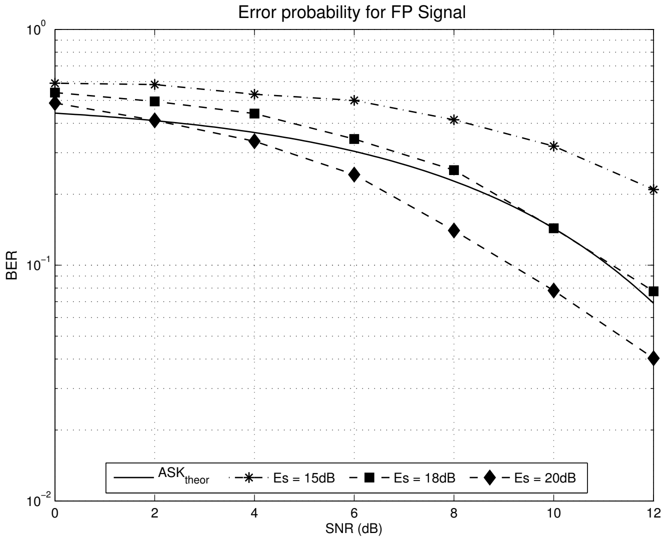

Fig. 7. Error probability for fingerprinting ASK signal.

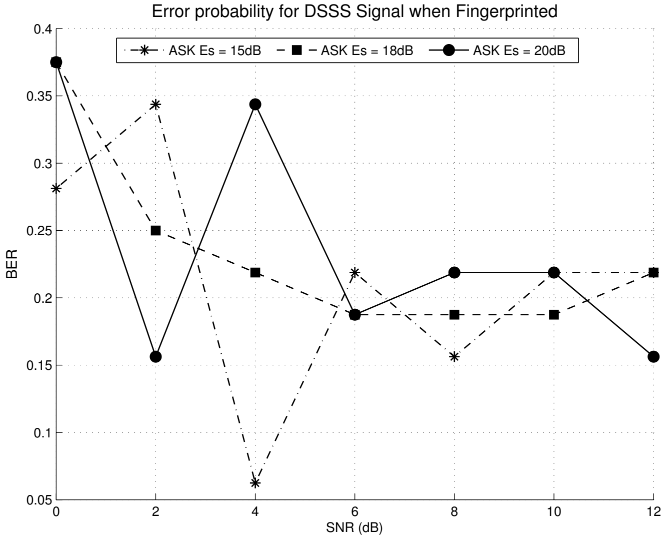

Fig. 8. Error probability for DSSS fingerprinted signal.

technique was successfully applied to recover fingerprinting information (i.e., 32 bits) added on DSSS/QPSK with an acceptable degradation (Figure 8) of the host link. Actually, the proposed solution improves the spectrum efficiency usage at cluster level avoiding the utilization of dedicated control channels. However, the combination of signal fingerprinting and IF sampling provide an attractive solution for CRs in terms of a simpler demodulator with a lower the number of inputs for digital signal processing. Finally, active RFF aims to a valuable technique for CRM facilitating data exchange between CRs without any dedicated channel or additional radio resource.

References

[1] F. Fitzek and M. Katz, Eds., *Cognitive Wireless Networks: Concepts, Methodologies and Visions Inspiring the Age of Enlightenment of Wireless Communications*, ser. ISBN 978-1-4020-5978-0. Springer, Jul. 2007.

[2] O. Afolabi, K. Kim, and A. Ahmad, “On secure spectrum sensing in cognitive radio networks using emitters electromagnetic signature,” in *Computer Communications and Networks, 2009. ICCCN 2009. Proceedings of 18th Internatonal Conference on*, 2009, pp. 1–5.

[3] S. Soderi, H. Viittala, J. Saloranta, A. Mancini, M. Hamalainen, and J. Iinatti, “Emulation of secure wi-fi communication: A performance gap analysis against a virtual test-bed,” in *ITS Telecommunications (ITST), 2013 13th International Conference on*, 2013, pp. 226–231.

[4] R. J. Anderson, *Security engineering - a guide to building dependable distributed systems (2. ed.)*. Wiley, 2008.

[5] D. Kuptsov, A. Khurri, and A. Gurtov, “Distributed user authentication in wireless lans,” in *World of Wireless, Mobile and Multimedia Networks Workshops, 2009. WoWMoM 2009. IEEE International Symposium on a*, 2009, pp. 1–9.

[6] R. Moskowitz, P. Nikander, T. Henderson, “Host Identity Protocol,” IETF RFC 5201, April 2008.

[7] D. Bernal, P. Closas, J. A. Fernandez-Rubio, “Digital I/Q Demodulation in array processing: theory and implementation,” in *16th European Signal Processing Conference (EUSIPCO 2008)*, Lausanne, Switzerland,, 2008.

[8] MathWorks. [Online]. Available: http://www.mathworks.com

[9] R. L. Peterson, R. E. Ziemer, and D. E. Borth, *Introduction to Spread Spectrum Communications*. Englewood Cliffs, NJ: Prentice-Hall, 1995.