5 Using Tag Signals and Interrogation and Acknowledgement Sequence for further protections based on PHYSEC concepts

Recall that, as establishing secret key or secret codes needs prior exchanges (see Deliverable D2.1), these exchanges should be authenticated and protected. If not, an active attacker can often counter them, by spoofing techniques or by protocol aware Intelligent Jamming. For example [10] [34] are relevant to standards 802.11n/ac and mention the following weaknesses:

- The channel state UL feedback message (being included in a Management frame and being not encrypted) is easy to intercept and then to compromise in order to facilitate further passive and active attacks.
- The Channel State Information is highly vulnerable to active attacks at the closed loop sounding procedure by a protocol aware jammer, either at the DL (sounding frame) or at the UL (feedback CSI frame).

Consequently, security pairing and authentication at the earliest stages of public RATs cannot be based only on (native) PHYSEC solutions.

In this section we will show how the implementation of such algorithms combined with the accurate synchronization and radio measurements allowed by tag signals can provide a practical solution to improve security pairing, authentication, integrity control and secrecy of legitimate link at access stages first, and later, for on-going communication. The major argument is that the radio advantage, provided by tag signals, strengthens secrecy capacity and provides added degrees of freedom for secret key generation [6].

5.1 TS and IAS for initiating and enhancing AN-BF schemes

Artificial noise consists in jamming any other direction than the legitimate link and can therefore be used to degrade the channel of a possible eavesdropper. The combination of artificial noise and beamforming provides a radio advantage to Bob (Eve being affected by an extra noise), which is fully controlled by Alice. Nevertheless, the critical step of this basic scheme is the first negotiation message and particularly the shared determination of the CIR which is the current flaw of Channel State Information (CSI) in many MIMO systems using explicit feedback sounding [10]. This feedback exposes to Eve the private knowledge of Alice-Bob CIR and must absolutely be protected. Indeed, active Eve can prevent CIR estimation procedure by intelligent jamming. MITM Eve can decoy it, and passive Eve can intercept and decode CIR message before the establishment of AN, which facilitates her rejection process. Finally, AN is efficient once set up, but its establishment protocol is weak. For these reasons, we propose to use TS to protect CIR negotiation in MIMO RATs.

5.2 TS and IAS for initiating SKG schemes

Given that propagation channel is reciprocal and inherently random, it may be considered as a shared pool of random secure key bits, between a pair of legitimate terminals [70]. Hence, after measuring the radio channel, Alice and Bob jointly employ a quantization algorithm able to generate a sequence of key bits from the common channel. Such sequences are required to be identical, long and sufficiently random in order to ensure reliability and confidentiality.

In the establishment of the secret key from channel observations, we specifically consider the channel quantization alternating (CQA) protocol proposed in [13], which has in particular the advantage of exploiting the full information contained in the channel coefficients (real and imaginary parts). To extract secure key bits from the shared source of randomness, Alice and Bob employ separately the CQA. A preliminary set of channel coefficients need be obtained in an initial learning phase in order define the quantization regions (QR) of a quantization map. The benefit of this approach is to define statistically equally probable quantization intervals, in order to make the guess of the quantized bits the least easy for Eve. Therefore Alice defines her map QR by quantifying the cumulative distribution function (CDF) of each of the aggregated real and imaginary parts of the channel coefficients into $\sqrt{M}$ statistically equal quantization intervals, which leads to M quantization regions. On the other hand, Bob defines two alternative maps from his own set of channel coefficients observations. As a consequence, it is likely that Alicee's and Bob's maps differ to some extent, which will certainly result in mismatched bits between Alice and Bob. The disagreement between the generated keys, which may also stem from noise or from estimation errors (e.g. from imperfectly

calibrated electronics), must be resolved for the key to be useable. In a practical system, a reconciliation procedure is necessary, e.g. through public exchanges between Alice and Bob [78].

Given that a significant key requires a number of key bits ≥ 128 in today's protocols, the SKG scheme must be able to provide such a number, which already allows to construct a significant statistical distribution. In other words, it is possible, although not optimal in terms of performance, to construct the quantization maps with the same set of channel coefficients as those used to generate the key. This makes possible a fast SKG scheme, e.g. for non stationary and highly time variant channels.

Secret Key Generation based on channel estimation is therefore a crucial help to traditional cryptography techniques as it provides unique and renewable secret keys avoiding therefore the use of pre-distributed keys whose vulnerabilities have been exposed several times in the press.

SKG schemes require that the legitimate link is authenticated. TS can then be employed to provide this secure pairing from the very early stage of the radio access protocol. In addition, the legitimate terminals can use either the dominant signal or the tag signal to estimate the channel. Section 4 showed that tag signal estimation provide CIR results which are not only more accurate but also more resilient to harsh propagation conditions and to multipath.

As an illustration, Figure 33 shows an example of SKG based on real field CIR extracted from WiFi signals (2.46 GHz) recorded over a few seconds at 6 synchronous antennas, published by the phylaws team during the last Winn Forum San Diego March 2015. Our purpose for next work on Transec and Netsec protection schemes with Tag signals is to provide the same kind of results with CIR extracted from Tag Signals.

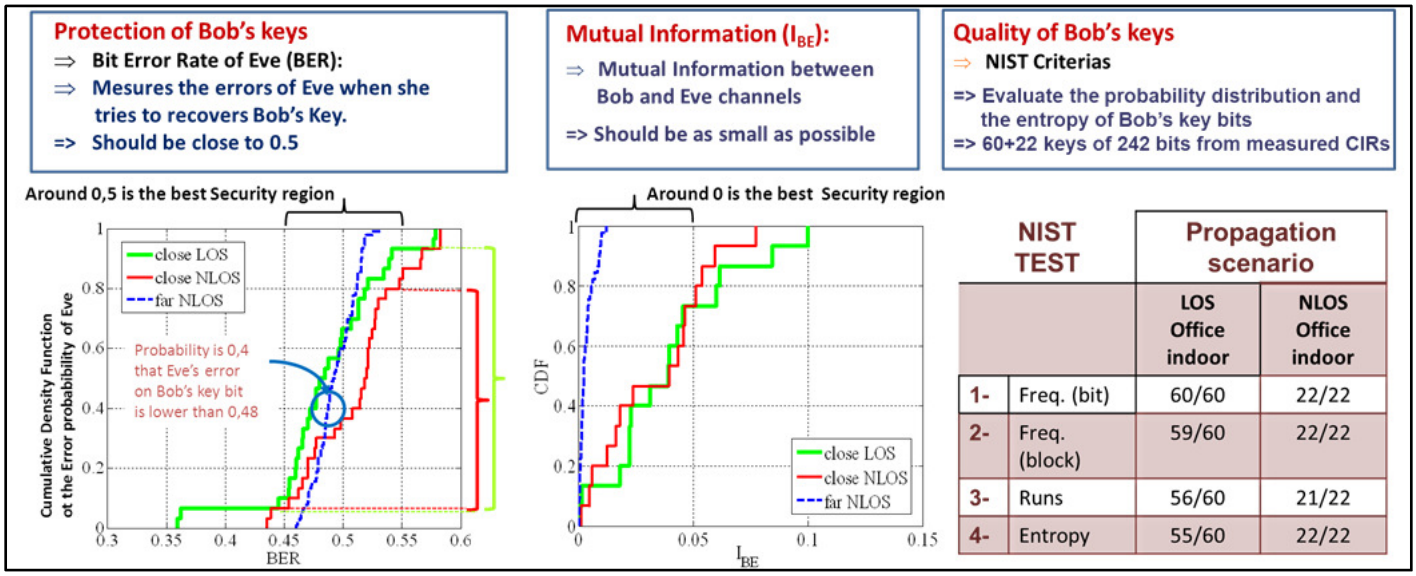

Figure 33: example of SKG generation from real Fied WiFi signals and analysis of their resilience an quality – signals are recorded and CIR are estimated with the test bed of Figure 17. SKG algorithm is derived from [13].

5.3 TS and IAS for initiating Secrecy codes

The goal of secrecy codes is to ensure reliable communication at the legitimate link and avoid any information leakage elsewhere. Secrecy codes conceal the information sent by Alice in the difference of SNR or of channel capacity between Bob and Eve. Therefore the legitimate receiver should have a better radio link than the eavesdropper. Without this permanent radio advantage, secrecy codes cannot provide a secure communication. Besides, secrecy coding supposes also an authenticated radio link. Tag signals are therefore a crucial help not only to authenticate the legitimate link but also to provide a radio advantage to legitimate users. Tag signals can also be combined with artificial noise to increase this radio advantage.

5.4 Toward a fully authenticated and secured radio protocol

Figure 34 explains how to combine TS, AN and PHYSEC techniques to secure the earliest stages of radio access protocols at both Forward sense (FWD, Alice to Bob) and Return sense (RTN, Bob to Alice). First, security pairing and CIR estimations are supported by IAS protected by TS. Then authenticated CIR initializes AN for the further on-going user communication. Finally, TS can be shut down while artificial noise still performs CIR estimations on user signal. Alternatively, to increase security, TS can continue to protect on-going CIR estimations from sounding exchanges during data transfer. Transec with tag signals is in practice very brief and corresponds to low data rates. Artificial Noise ensures Transec for further user data streams and for associated signalling.

To avoid an insecure explicit exchange of CIR over the air, two main ways have to be considered:

- designing a dedicated invertible correspondence for the TS DSS code determination (Alice recovering CIR_{FWD} from Bob's transmitted TS_{RTN} and Bob recovering CIR_{RTN} from Alice's transmitted TS_{FWD});
- or transmitting CIR_{FWD} and CIR_{RTN} estimates in dedicated PHYSEC protection messages [6] from the second IAS.

Finally SKG schemes or secrecy coding can be performed to achieve a fully authenticated and secure communication between legitimate terminals.

5.5 Further works

The design of a dedicated invertible correspondence for the TS DSS code determination will be studied in the final version of this report: deliverable D4.2 "TRANSEC upgrades of existing RATs – Simulation and Analyses complements".

The study of the enabling of SKG and SC supported by TS and IAS will be deepened in the final version of this report: deliverable D4.2 "TRANSEC upgrades of existing RATs – Simulation and Analyses complements" and in reports relevant to Netsec upgrades: deliverables D4.3 and D4.4.

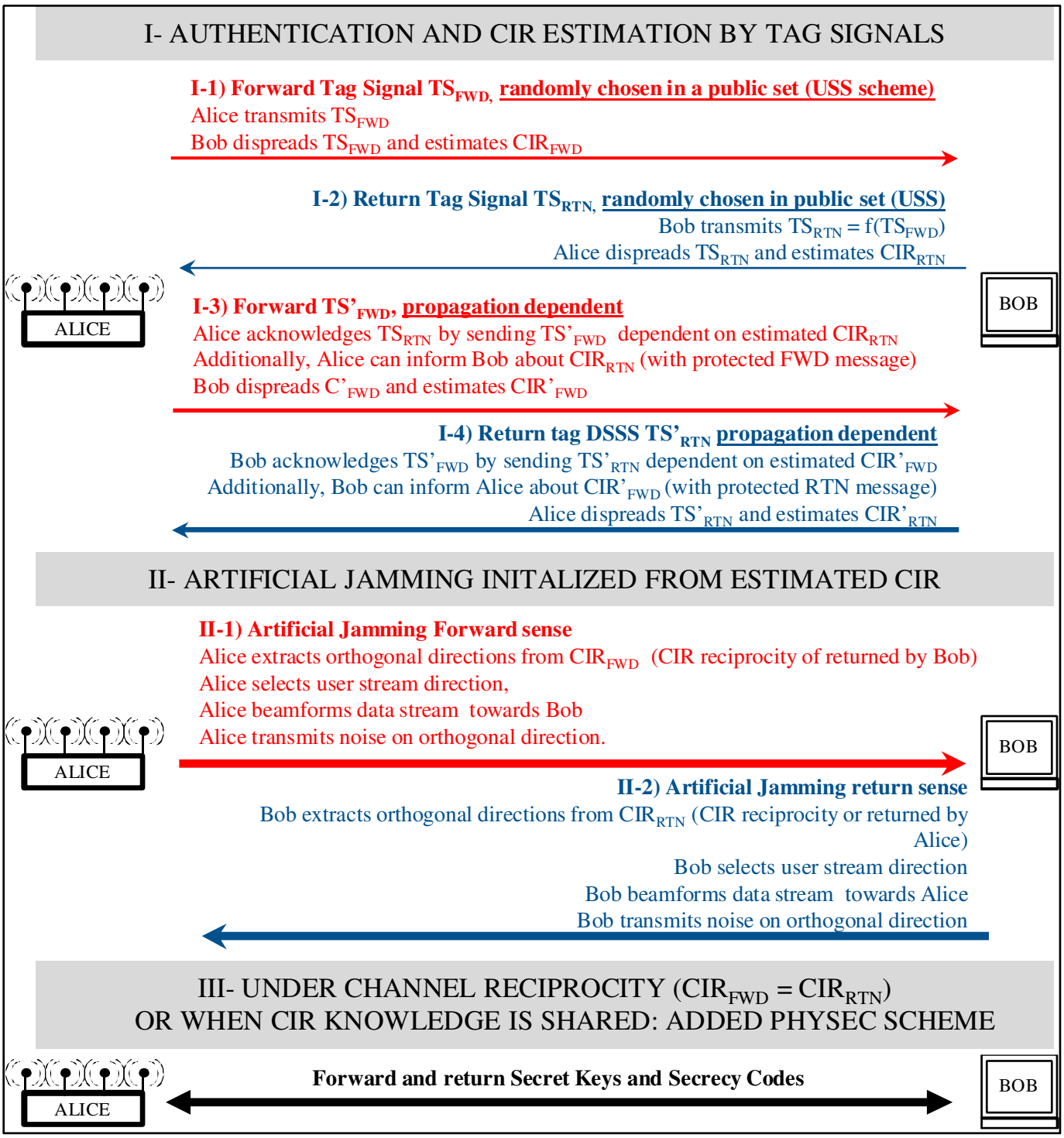

Figure 34: Protocol for secure pairing and communication combining tag signal and artificial jamming

6 Conclusion

This deliverable has surveyed Transec improvements dedicated to existing and future standards, by focusing on Time Division Duplex schemes which provides native reciprocity of the radio-channel.

Two main ways for transec were explored in this deliverable:

- Developing key-free prime security pairing between Alice and Bob, with Tag Signal and Interrogation and Acknowledgement Sequences in order to:
  - Provide a significant radio advantage to legitimate users; authenticated and protected CIR estimations for the first signalling and access exchanges.
  - Counter any kind of eavesdropper threat: passive, Intelligent Jamming (IJ), Man-In-The-Middle (MITM).
  - Implement further protection schemes based on PHYSEC concepts, such as artificial noise, Secret Key Generation and Secrecy Coding.

- Establishment of Artificial noises schemes:
  - AN enables a permanent and controlled radio advantage for the data flux transmission.
  - Such schemes also provide radio conditions for a full protection of data transmission with secret codes over the complete transmission.
  - In addition it should provide more degree of freedom for Secret Key generation.

Note that the basic advantage of such schemes relies on the fact that they are RAT-independent, and only Duplex-dependant.

Specific study of Artificial Noise Schemes

Resilience of enabled AN schemes is well known for on-going user data transmission and associated signalling. WiFi simulation and WiFi data flux evolving in AN schemes allowed us to quantify the relevant protection of bits which appears very good. In any WiFi modulation and coding Scheme, simulations show that established AN allows:

- dropping Eve's decoding capability to a few percent only (Packet Error Rate of Eve drecreases to less than 5%)
- keeping almost optimal decoding capability for Bob (Packet Error Rate of Bob keeps values greater than 95%).

Specific study of Tag Signals, Interrogationa nd Acknowledgement Sequences and CIR estimation

This deliverable also studied the best approaches to perform CIR estimations and established the design parameters of Tag Signals (TS) and Interrogation and Acknowledgement Sequences (IAS) for WiFi carriers.

First of all, analyses of the new concepts of TS and IAS revealed promising Transec resilience of the earliest exchanges between legitimate users when facing any kind of Eve: passive, Intelligent Jamming or Man-In-The-Middle. Our study confirms that Tag Signal is a good mean for enhancing security of first RAT exchanges and CIR estimation before establishing PHYSEC-based protection schemes such as Artificial Noise, Secret Key Generation or computation of Secret Codes.

Then, contribution of FuDu and requirements about Self-Interference Mitigation (SIM) at the receiving stages of IAS were also developed. This allowed us to quantify the radio processing parameters. As previously identified in work package WP2, the requirements found for SIM applied to TS perfectly meet the values found in the literature. This means that technology relevant to Fudu RAT should directly apply to TS, IAS and relevant PHYSEC protections.

Finally, comparison of numerous results from simulated and experimental WiFi radio configuration allow us to conclude about the relevance of tag signal for CIR estimation in any case. Moreover, simulations of CIR estimation through different techniques and different channel models (including real field measured CIR) have highlighted and quantified the benefit of tag signal for such purpose:

- From order 10 and length 1023 samples), tag signal starts to be much more accurate than any kind of estimation techniques based on WiFi signals, even at very negative TSR, and especially at low SNR

- This advantage becomes very important for order greater than 14 and length longer than 16383 samples.
- Moreover, tag signals designed with suitable DSS codes show very good resilience to harsh propagation conditions and to multipath thanks to optimized autocorrelation figure (low side lobes).
- Therefore, tag signal are not only highly recommendable for stealth and secure pairing but our study proofs that tag signals expose very good properties for CIR estimation and for extraction of propagation randomness, which is at the heart of PHYSEC.

Further complements of this deliverable.

This deliverable will be deepened and completed by Deliverable D4.2 (delivery T0+36).

- With additional experimental results relevant to CIR estimated under carriers of other 2G 3G and 4G standards.
- With study complement about Uncoordinated Spread Spectrum and Time Jitter schemes (used for a better resilience to IJ and MITM attackers): practical implementation, increase of complexity, increase of latencies
- With study completion of the design of "full arbitrary" Tag Signals (which would provide the best security properties).
- With proposal and studies for extension of TSs and IAS to Frequency Division Duplex schemes which are very common in 2G, 3G and 4G radiocellular RATs.

In addition:

- future deliverables D4.3 and D4.4 will focus on the use of Transec improvements provided by Tag Signals and Artificial Noise to ensure more secure exchanges of signaling and data thanks to SKG and SC schemes.
- Propagation studies and experiental measurements will be completed and deepened into Work Package WP3.

7 Annex 1: brief description of 802.11 OFDM Waveforms

7.1 Introduction

IEEE 802.11 is a set of MAC and PHY specifications for implementing WLAN (Wireless Local Area Network). It is commonly known as Wi-Fi. It is a serial of half duplex techniques that use the same basic protocol. The different versions of IEEE 802.11 use mainly two modulation techniques: DSSS and OFDM. In this document, only the OFDM waveforms are described and processed. The signal is sent in frames whose length is variable depending on the nature of the frame (management, control, data) and the amount of information to transmit.

Among all the IEEE 802.11 versions, the following ones use OFDM:

- 802.11a: Released in 1999, it allows transmission and reception of data at rates of 1.5 to 54 Mbit/s at 5.8 GHz. It has seen widespread worldwide implementation, particularly within the corporate workspace. While the original amendment is no longer valid, the term "802.11a" is still used by wireless access point (cards and routers) manufacturers to describe interoperability of their systems at 5.8 GHz, 54 Mbit/s. The physical layer of 802.11a is described in details in section 7.2.
- 802.11g: Released in 2003, this works in the 2.4 GHz band, but uses the same OFDM based transmission scheme as 802.11a. It operates at a maximum physical layer bit rate of 54 Mbit/s. The then-proposed 802.11g standard was rapidly adopted by consumers starting in January 2003, well before ratification, due to the desire for higher data rates as well as to reductions in manufacturing costs. By summer 2003, most dual-band 802.11a/b products became dual-band/tri-mode, supporting a and g in a single mobile adapter card or access point. The physical layer of 802.11g is described in details in section 7.2.
- 802.11n: Released in 2009, it is an amendment which improves upon the previous 802.11 standards mainly by adding MIMO (Multiple Input Multiple Output) and wider channels (40 MHz vs. 20 MHz). 802.11n operates on both the 2.4 GHz and the lesser used 5 GHz bands. It operates at a maximum net data rate from 54 Mbit/s to 600 Mbit/s. The physical layer of 802.11n is described in details in section 7.3.
- 802.11ac: Approved in 2014, it is an amendment that builds on 802.11n. Changes compared to 802.11n include wider channels (80 or 160 MHz vs. 40 MHz) in the 5 GHz band, more spatial streams (up to 8 vs. 4), higher order modulation (up to 256-QAM vs. 64-QAM), and the addition of multi-user MIMO. The physical layer of 802.11ac is not described this document.

7.2 Physical Layer of 802.11a and 802.11g

The main characteristics of the OFDM symbols used in 802.11a and 802.11g are summarized in Table 23.

Table 23: Main characteristics of an 802.11a and 802.11g OFDM symbol

Channel spacing	Occupied bandwidth	Sampling rate	Inter-carrier spacing	FFT size	Number of subcarriers (excluding DC)	Number of data carriers	Number of pilot carriers	CP size
20 MHz	16.25 MHz	20 Mcps	312.5 kHz	64	52	48	4	16 samples
10 MHz	8.125 MHz	10 Mcps	156.25 kHz	64	52	48	4	16 samples
5 MHz	4.0625 MHz	5 Mcps	78.125 kHz	64	52	48	4	16 samples

The structure of an 802.11a or 802.11g frame is described in Figure 35. It includes:

- A Physical Layer Convergence Procedure (PLCP) preamble, described in section 7.2.1.
- A signalization field, described in section 7.2.2.
- A data field, described in section 0.

In the following, all values are given for the 20 MHz channel spacing case.

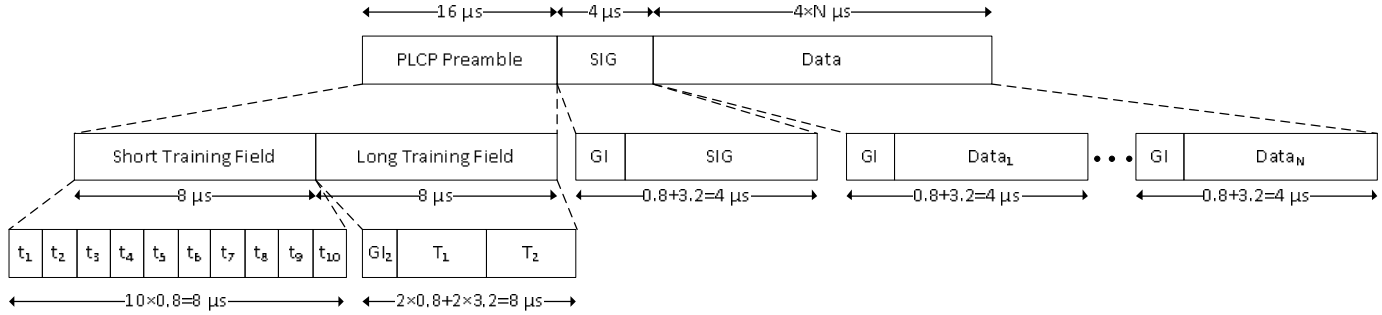

Figure 35: Structure of an 802.11a or 802.11g frame

More details about the OFDM physical layer of 802.11a and 802.11g can be found in chapter 18 of [71].

7.2.1 PLCP Preamble

The PLCP preambule is a fully known sequence of 16 µs (i.e. 320 samples). It comprises the Short Training Field (STF) and the Long Training Field (LTF). Each one lasts 8 µs.

The STF is made of 10 identical short OFDM training symbols. A short training symbol consists of 12 QPSK modulated subcarriers (1 every 4 subcarriers). The fact that only the subcarriers with indices that are multiple of 4 have non-zero amplitude results in a periodicity of $\frac{T_{FFT}}{4} = 0.8\ \mu s$. A short OFDM training symbol does not have a cyclic prefix.

The LTF is made of 2 identical long OFDM training symbols. A long training symbol consists of 52 BPSK modulated subcarriers. One single cyclic prefix for the 2 symbols is added but it is two times longer than the regular cyclic prefix (1.6 µs vs. 0.8 µs).

The PLCP preamble can be used for signal detection, synchronization, AGC (Automatic Gain Control), frequency offset estimation, time and frequency channel estimation, etc. It will be described in section 7.3.1, how it is used in our multi-antenna interceptor.

7.2.2 Signalization Field

As described in Figure 36, the signalization field contains information necessary to demodulate the data field i.e.:

- The data rate, coded on 4 bits, from which can be deduced the modulation (BPSK, QPSK, 16-QAM and 64-QAM) and the coding rate (1/2, 3/4 and 2/3) of the convolutional encoder.
- The length field indicating the number of bytes in the PSDU (PLCP Service Data Unit) that the MAC is currently requesting the PHY to transmit. It is coded on 12 bits.

It also contains:

- 1 reserved bit set to 0.
- 1 parity bit.
- 6 tail bits set to 0.

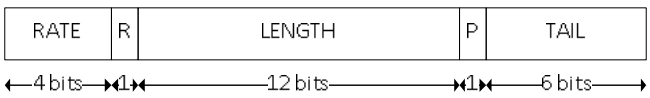

Figure 36: Signalization field bit assignment

It consists in a single BPSK modulated OFDM symbol whose bits are encoded with a convolutional code at a rate of 0.5 and interleaved.

7.2.3 Data Field

As described in Figure 37, the data field contains the service field, the PSDU, the tail bits and, if needed, the pad bits. All bits in the data field are scrambled.

The service field contains 16 bits. The 7 first bits are set to 0 and are used to synchronize the descrambler at the reception. The next 9 bits are reserved and set to 0.

The tail bits are 6 bits set to 0 to return the convolutional encoder to the zero state in order to improve the error probability of the convolutional decoder.

The pad bits are used so that the number of transmitted bits is a multiple of the number of bits per OFDM symbol.

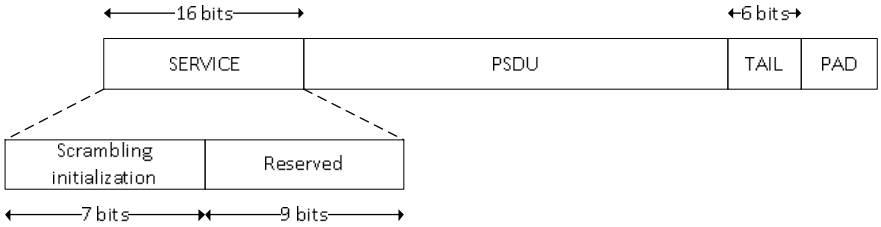

Figure 37: Data field structure

The data bits are scrambled, encoded with a convolutional encoder, interleaved, modulated then mapped to subcarriers.

7.3 Physical Layer of 802.11n

802.11n is often referred to as HT (High Throughput) 802.11.

The main characteristics of the HT OFDM symbols used in 802.11n are summarized in Table 24.

Table 24: Main characteristics of an 802.11n HT OFDM symbol

Channel spacing	Occupied bandwidth	Sampling Rate	Inter-carrier spacing	FFT size	Number of subcarriers (excluding DC)	Number of data carriers	Number of pilot carriers	CP size
20 MHz	16.25 MHz	20 Mcps	312.5 kHz	64	56	52	4	8 or 16 samples
40 MHz	35.625 MHz	40 Mcps	312.5 kHz	128	114	108	6	16 or 32 samples

In the following, all values are given for the 20 MHz channel spacing case.

The structure of an 802.11n frame is described in Figure 38. It includes:

- A Physical Layer PLCP preamble, described in section 7.3.1.
- A signalization field, described in section 7.3.1.
- An HT signalization field, described in section 7.3.2.
- An HT short training field, described in section 7.3.3.
- An HT long training field, described in section 7.3.4.
- A data field, described in section 7.3.5.

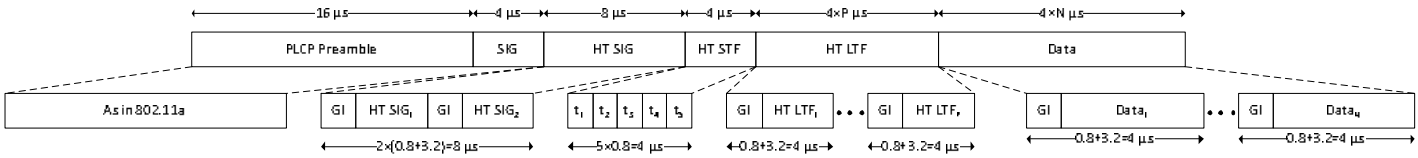

Figure 38: Structure of an 802.11n HT frame

More details about the OFDM physical layer of 802.11n can be found in chapter 20 of [71].

7.3.1 PLCP preamble and Signalization Field

The PLCP preamble and the signalization field are designed the same way as in 802.11a. Nevertheless, in the MIMO case a different cyclic shift is applied on the signal of each spatial stream. Cyclic shift is used to prevent unintentional beamforming when the same signal is transmitted through different spatial streams or transmit chains.

7.3.2 HT Signalization Field

The HT signalization field contains information necessary to demodulate and interpret the data field in the HT case i.e.:

- The Modulation and Coding Scheme (MCS), from which can be deduced the modulation (BPSK, QPSK, 16-QAM and 64-QAM), the coding rate (1/2, 3/4, 2/3 and 5/6), the number of spatial streams, the number of Binary Convolutional Code (BCC) encoders, if EQM (EQual Modulation) or UEQM (UnEQual Modulation) is used on each spatial stream.
- The type of FEC coding (BCC or LDPC).
- The bandwidth (20 or 40 MHz).
- The length of the CP.
- The number of bytes in the PSDU that the MAC is currently requesting the PHY to transmit.
- The number of space time stream when Space Time Bloc Coding (STBC) is used.
- The number of extension spatial stream, from which can be deduced the number of HT-LTF symbols.
- Is channel estimate smoothing recommended? If 95% of the sum of the energy from all impulse responses of the time domain channels between all space-time streams and all transmit chain inputs is contained within 800 ns, the smoothing bit should be set to 1. Otherwise, it shall be set to 0.
- Is the PPDU a sounding one? When the number of space-time streams is less than the number of transmit antennas, sending only HT-LTFs does not allow the receiver to recover a full characterization of the MIMO channel, even though the resulting MIMO channel measurement is sufficient for receiving the data field of the HT PPDU. However, there are several cases where it is desirable to obtain as full a characterization of the channel as possible, thus requiring the transmission of a sufficient number of HT-LTFs to sound the full dimensionality of the channel. These cases of MIMO channel measurement are referred to as MIMO channel sounding.

It also contains:

- A 8 bit CRC.
- 1 reserved bit set to 0.
- 6 tail bits set to 0.

It consists in two QBPSK ($\pi/2$ rotated BPSK) modulated OFDM symbols whose bits are encoded with a convolutional code at a rate of 0.5 and interleaved. The number of subcarriers corresponds to the ones in the non-HT case. This is done to accommodate the estimation of channel parameters needed to robustly demodulate and decode the information contained in the HT signalization field.

In the MIMO case a different cyclic shift is applied on the signal of each spatial stream. The cyclic shits are the same as for the PLCP preamble and the signalization field.

7.3.3 HT Short Training Field

The HT STF is made of 5 identical short OFDM training symbols. The short OFDM training symbol is the same as the 802.11 a one, described in section 7.2.1.

In the MIMO case a different cyclic shift is applied on the signal of each spatial stream. The cyclic shits are not the same as for the PLCP preamble, the signalization field and the HT signalization field.

7.3.4 HT Long Training Field

The HT LTF has two parts. The first part consists of one, two or four HT LTF symbols that are necessary for demodulation of the data portion of the PPDU. These HT LTFs are referred to as HT DLTF. The optional second part consists of zero, one, two or four HT LTF symbols that may be used to sound extra spatial dimensions of the MIMO channel that are not utilized by the data portion of the PPDU. These HT LTF are referred to as HT ELTF.

The HT LTF is made of identical (to a multiplicative coefficient equal to 1 or -1 depending on the spatial stream and on the index of the symbol) HT OFDM symbols. It consists in 56 BPSK modulated subcarriers.

In the MIMO case a different cyclic shift is applied on the signal of each spatial stream. The cyclic are the same as for the HT STF.

7.3.5 HT Data Field

If BCC encoding is used, the HT data field is as described in Figure 37, except that the number of tail bits can be equal to 6 or 12 depending if the number of encoders is equal to 1 or 2.

In the MIMO case a different cyclic shift is applied on the signal of each spatial stream. The cyclic are the same as for the HT STF and the HT LTF.

7.4 MAC level of 802.11

The MAC level of the different 802.11 standards is the same.

As described in Figure 39, each MAC frame consists of the following components:

- A MAC header which comprises frame control, duration, address, optional sequence control information, optional QoS control information (QoS Data frames only) and optional HT control fields (HTC frames only). The type and subtype of the frame are coded in the frame control. There are 3 types of frame (management, control and data) and 39 subtypes.
- A variable-length frame body, which contains information specific to the frame type and subtype. The minimum length of the frame body is 0 bytes. The maximum length of the frame body is defined by the maximum length MSDU plus the length of Mesh Control field, if present, plus any overhead for encryption, or by the maximum length A-MSDU plus any overhead for encryption. The overhead for encryption is described in section 11 of [71]. When the Mesh Control field is present in the frame body, the Mesh Control field is encrypted as a part of data.
- A 32 bits CRC.

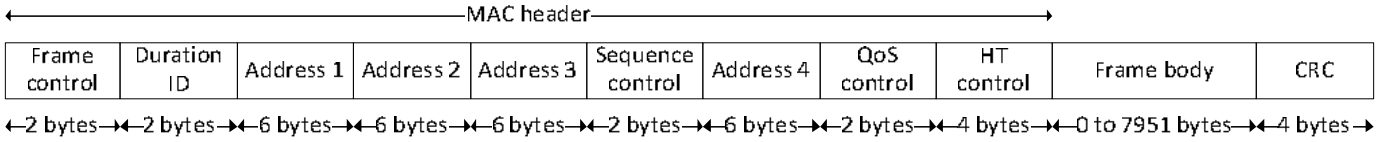

Figure 39: MAC frame format

More details about the MAC level can be found in section 8 of [71]

8 References

[1] University of Oulu, TTI, IMEC, University of Twente, University of Surrey, Thales, *EC Project: Full-Duplex radios for local access (DUPLO),* www.fp7-duplo.eu.

[2] CEA, “Méthode d'identification et de détection d'un signal radio pour système de communication opportuniste”. France Patent EP 2 640 027 A1.

[3] O. Cepheli and G. Kurt, “Efficient PHY layer security in MIMO-OFDM: Spatiotemporal selective artificial noise,” in *IEEE 14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Madrid, Spain, 2013.

[4] F. Delaveau, C. Germond, D. Robin and THALES, “Procede protocole oriente de traitement des signaux stationnaires, partiellement stationnaires”. France Patent FR2969450 A1, 2012.

[5] F. Delaveau, P. Viravau, P. Goguillon and THALES, “Procédé de taggage radio-électrique des signaux de brouilleurs et d’autres émetteurs”. France Patent FR 12.03071, 2007.

[6] M. Bloch and J. Barros, Physical-Layer Security, Cambridge University Press, 2011.

[7] D. H. F. Delaveau, «Method Of Controlling And Analysing Communications In A Telephone Network». FR - PCT Brevet FR 04.04043 - WO 2005/112497 A1, 2008.

[8] R. Gautier, G. Burel, J. Letessier and O. Berder, “Blind estimation of scrambler offset using encoder redundancy.,” in *36th Asilomar Conference on Signals, Systems and Computers*, Asilomar, USA, 2002.

[9] Y. Hong, P. Lan and C. Kuo, “Enhancing Physical-Layer Secrecy in Multiantenna Wireless Systems: An Overview of Signal Processing Approaches,” *IEEE Signal Processing Magazine,* vol. 30, no. 5, pp. 29-40, 2013.

[10] R. Miller and W. Trappe, "On the vulnerabilities in CSI in MIMO wireless communication systems," *IEEE Transactions on Mobile Computing,* vol. 11, no. 8, pp. 1386-1398, 2012.

[11] A. K. Khandani, “Two-Way (True Full-duplex) Wireless,” in *CWIT*, Kelowna, Canada, 2013.

[12] N. Romero-Zurita, M. Ghogho and D. McLernon, "Physical layer security of MIMO-OFDM systems by beamforming and artificial noise generation," *PHYCOM: Physical Communication,* vol. 4, no. 4, pp. 313-321, 2011.

[13] J. W. Wallace and R. K. Sharma, “Automatic secret keys from reciprocal MIMO Wireless channels: measurement and analysis,” *IEEE Transactions on information forensics and security,* vol. 5, no. 3, pp. 381-392, September 2010.

[14] S. Mathur, W. Trappe, N. Mandayam, C. Ye and A. Reznik, “Radio-telepathy: extracting a secret key from an unauthenticated wireless channel,” in *MobiCom '08 Proceedings of the 14th ACM international conference on Mobile computing and networking*, San Francisco, USA, 2008.

[15] A. Varshavsky, A. Scannell, A. LaMarca and E. De Lara, “Amigo: Proximity-based authentication of mobile devices,” in *Ubiquitous Computing (UbiComp '07)*, Innsbruck, Austria, 2007.

[16] C. Shannon, “Communication theory of secrecy systems,” *Bell System Technical Journal,* vol. 28, no. 4, pp. 656-715, 1949.

[17] L. Ozarow and A. Wyner, “A wire-tap channel II. Advances in cryptology,” in *Eurocrypt*, Berlin, Germany, 1984.

[18] F. Delaveau, A. Evestti, A. Kotelba, R. Savola and N. Shapira, “Active and passive eavesdropper threats within public and private cililian networks - Existing and potential future countermeasures - An overview,” in *Winncomm*, Munich, Germany, 2013.

[19] «http://www.metronews.fr/high-tech/une-enorme-faille-de-securite-permet-d-ecouter-vos-appels-et-de-lire-vos-sms/mnlv!YnqDbOgrtHFYk/,» [En ligne].

[20] «https://firstlook.org/theintercept/2015/02/19/great-sim-heist/,» [En ligne].

[21] F. Delaveau, C. Ling, E. Garrido, J.-C. Belfiore and A. Sibile, “Physec concepts for wireless public networks - Intoduction, state of the art, perspectives,” in *Winncomm*, Munich, Germany, 2013.

[22] A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin and J. Merolla, “Applications of LDPC codes to the wiretap channel - Information theory,” *IEEE Transactions,* vol. 53, no. 8, pp. 2933-2945, 2007.

[23] X. He and A. Yener, “Providing secrecy with lattice codes,” in *Forty-sith Annual Allerton Conference*, Urbana-Champaign, USA, 2008.

[24] H. Mahdavifar and A. Vardy, “Achieving the secrecy capacity of wiretap channels using polar codes,” *IEEE Transactions on Information Theory,* vol. 57, no. 10, pp. 6428-6443, 2011.

[25] B. Azimi-Sadjadi, A. Kiayias, A. Mercado and B. Yener, “Robust key generation from signal envelopes in wireless networks,” in *CCS 07 Proceedings of the 14th ACM conference on Computer and communications*

security, Alexandria, USA, 2007.

[26] S. Mathur, A. Varshavsky, W. Trappe, R. Miller and N. Mandayam, “ProxiMate: proximity-based secure pairing using ambient wireless signals,” in *MobiSys '11*, Washington, USA, 2011.

[27] S. Jana, S. Premnath, M. Clark, S. Kasera, N. Patwari and S. Krishnamurthy, “On the effectiveness of secret key extraction from wireless signal strength in real environments,” in *MobiCom '09*, Bejing, China, 2009.

[28] Q. Wang, H. Su, K. Ren and K. Kim, “Fast and scalable secrey key generation exploiting channel phase randomness in wireless networks,” in *IEEE INFOCOM*, Shangai, China, 2011.

[29] Z. Li, R. Yates and W. Trappe, “Secret communication with a fading eavesdropper channel,” in *ISIT '07*, Nice, France, 2007.

[30] Y. El Hajj Shehadeh, O. Alfandi and D. Hogrefe, “Towards robust key extraction from multipath wireless channels,” *IEEE Journal of communications and networks,* vol. 14, no. 4, pp. 385-395, August 2012.

[31] N. Anand, S. Lee and E. Knightly, “STROBE : Actively securing wireless communications using Zero-Forcing beamforming,” in *INFOCOM*, Las Vegas, USA, 2012.

[32] R. Negi and S. Goel, “Secret Communication using artificial noise,” in *IEEE Vehicular Technology Conference*, Dallas, USA, 2005.

[33] E. Tekin and A. Yener, “The general Gaussian multiple-access and two way wiretap channels : achievable rates and cooperative jamming,” *IEEE Transactions on Information Theory,* vol. 54, no. 6, pp. 2735-2751, 2008.

[34] J. Huang and A. Swindlehurst, “Cooperative jamming for secure communications in MIMO relay networks,” *IEEE Transactions on Signal Processing,* vol. 59, no. 10, pp. 4871-4884, 2001.

[35] ZEIT, "Wie Merkels Handy abgehört werden konnte," 18 12 2014. [Online]. Available: http://www.zeit.de/digital/datenschutz/2014-12/umts-verschluesselung-umgehen-angela-merkel-handy.

[36] S. Sodagari and T. C. Clancy, “Efficient jamming attacks on mimo channels,” in *IEEE ICC 2012 - Communication and Information Systems Security Symposium*, Ottawa, Canada, 2012.

[37] J. F. R. Bott, « Method for identifying a mobile phone user or for eavesdropping on outgoing calls.». Brevet Patent EP 1051053 B1, 2003.

[38] 3GPP, «3G Security: Security Architecture - release 8 ; System architecture evolution - release 8,» n° %13GPP TS 33.102 V8.0.0 ; 3GPP TS 33.401 V8.1.1, June 2008 ; October 2008.

[39] H. Mun, K. Han. and K. Kim., «3G-WLAN interworking: Security Analysis and new Authetication and Key Agreement based on EAP AKA,» *IEEE,* 1/09/2009.

[40] W. Diffie et M. Hellman, «New directions in cryptography,» *IEEE Transactions on Information Theory,* vol. 22, n° %16, pp. 644-654, 1976.

[41] P. Augustin, P. Elbaz-Vincent and J.-C. Bajard, “A Secure and Efficient Authenticated Diffie–Hellman Protocol,” in *6th European Workshop, EuroPKI*, Pisa, Italy, 2009.

[42] H. Krawczyk, “HMQV: A High-Performance Secure Diffie-Hellman Protocol,” IBM T.J.Watson Research Center, Yorktown Heights, USA, 2005.

[43] H. D. X. He, «Is link signature dependable for Wireless Security?,» *proceeding IEEE INFOCOM,* pp. 200-204, 2013.

[44] J. S. B. a. B. M. S. Paul L. Yu, «Physical-Layer Authentication,» *IEEE,* 2008.

[45] L. J. G. N. B. M. a. W. T. Liang Xiao, «Using the Physical Layer for Wireless Authentication in Time-Variant Channels,» *IEEE,* 2008.

[46] N. L. a. S. T. Paolo Baracca, «Physical Layer Authentication over MIMO Fading Wiretap Channels,» *IEEE,* 2012.

[47] Z. Y. C. L. a. X.-G. X. Xiaofu Wu, «A Physical-Layer Authentication Assisted Scheme for Enhancing 3GPP Authentication,» *IEEE,* 2015.

[48] R. Pickholtz, “Theory of spread spectrum communications - A tutorial,” *IEEE Transactions on Communications,* vol. 30, no. 5, pp. 855-884, 5 May 1982.

[49] C. Pöpper, S. Čapkun and M. Strasser, “Anti-jamming broadcast communication using uncoordinated spread specrum techniques,” *IEEE Journal on selected areas in communications,* vol. 28, no. 5, 5 June 2010.

[50] P. X. K. R. a. X. L. Q. Wang, «”Delay-Bounded Adaptive UFH-based Anti-jamming Wireless Communication",» *Infocom proceedings,* 2011.

[51] Thales, Celeno, Telecom ParisTech, Imperial College, VTT, "EC Project (Id 317562): PHYsical LAyer Wireless Security (PHYLAWS)," www.phylaws.org.

[52] M. Knox, “Single antenna full duplex communication using a common carrier,” in *IEEE 13th Annual Wireless and*

Microwave Technology Conference (WAMICON), Cocoa Beach, USA, 2012.

[53] Samsumg Research America ; Samsung Electronics, "Considerations for In-Band simultaneous transmit and receive (STR) feature in HEW," doc.: IEEE 11 -13/1122r1, 2013.

[54] D. Bharadia, E. McMilin and S. Katti, "Full Duplex Radios," in *SIGCOMM'13*, Hong Kong, China, 2013.

[55] J. I. Choiy, M. Jainy, K. Srinivasany, P. Levis and S. Katti, "Achieving Single Channel, Full Duplex Wireless Communication," in *MobiCom'10*, Chicago, USA, 2010.

[56] M. Jain, ,. J. I. Choiy, T. M. Kim, D. Bharadia and S. Seth, "Practical, Real-time, Full Duplex Wireless," in *MobiCom'11*, Las Vegas, USA, 2001.

[57] ITU-R, "Recommendation ITU-R SM.1600-1 - Technical identification of digital signals," ITU, 2012.

[58] T. Kaiser, A. Bourdoux, H. Boche, J. R. Fonollosa, J. B. Andersen and W. Utschick, Smart Antennas - State of the art, E. b. s. o. S. P. a. Communications, Ed., Hindawi Publishing Corp, 2005.

[59] F. Delaveau, D. Depierre and F. Sirven, "Oriented processing of Communication signals for Sensing and Disseminated Spectrum Monitoring," in *SDR Winncomm Forum*, Brussels, Belgium, 2001.

[60] QoSMOS Project, "Radio Context Acquisition algorithm - Final Version," FP7-ICT-2009-4/248454, 2012.

[61] P. Chevalier, F. Pipon and F. Delaveau, "Second-order optimal array receivers for synchronization of BPSK, MSK, GMSK signals corrupted by noncircular interferences," *EURASIP - Journal on Advances in Signal Processing,* vol. 2007, no. 3, p. 1, 2007.

[62] M. Dawei, F. Zhenming and L. Mingquan, "Anti-jamming with adaptive arrays utilizing power inversion algorithm," *Tsinghua Science and Technology,* vol. 13, no. 6, pp. 796-799, 2008.

[63] J. Mietzner, R. Schober, L. Lampe, W. H. Gerstacker and P. A. Hoeher, "Multiple-Antenna Techniques for Wireless Communications – A Comprehensive Literature Survey," *IEEE Communications surveys and tutorials,* vol. 11, no. 2, 2009.

[64] F. Delaveau and F. Pipon, "Passive Radar for Maritime Surveillance," in *MAST*, Cadix, Spain, 2008.

[65] J. Raout, "Rapport de thèse de doctorat - Traitements statio-temporels adaptés aux radars bistatiques à émetteurs non coopératifs," Université du Sud Toulon-Var, Toulon, France, 2010.

[66] E. Warner, B. Mulgrew and P. Grant, "Grant Triple correlation analysis of binary sequences for codeword detection," *Vision, Image and Signal Processing, IEEE Proceedings,* vol. 141, no. 5, pp. 297-302, 1994.

[67] L. Godara, "Application of anntenna arrays to mobile communications - Part II: Beam-forming and direction-of-arrival considerations," *Proceeding of the IEEE,* vol. 85, no. 8, pp. 1195-1245, 1997.

[68] E. Tuncer and B. Friedlander, Classical and Modern Direction of Arrival Estimation, Academic Press, 2009.

[69] P. V. Pursley and M. B. Sarwate, "Cross-correlations properties of pseudorandom and related sequences," *IEEE Proceedings,* vol. 68, no. 5, 1980.

[70] P. Sarwate, "Bounds on Cross Correlation and Autocorrelation of Sequences," *IEEE Transactions on Information Theory,* Vols. IT-25, no. 6, pp. 720-724, 1979.

[71] L. R. Welch, "Lowerbounds on the maximum cross correlation of signals," *IEEE Information Theory Society,* Vols. IT-20, no. 3, pp. 197-399, 1974.

[72] M. Pursley, "Performance Evaluation for Phase-Coded Spread Spectrum Multiple-Access Communication -- Part I: System Analysis," *IEEE Transactions on Communications,* Vols. COM-25, no. 8, pp. 795-799, 1977.

[73] P. Sarwate and M. Pursley, "Performance Evaluation for Phase-Coded Spread-Spectrum Multiple-Access Communication - Part II: Code Sequence Analysis," *IEEE Transactions on Communications,* Vols. COM-25, no. 8, pp. 800-803, 1977.

[74] P. Sarwate, M. Pursley and T. Basar, "Partial Correlation Effects in Direct-Sequence Spread-Spectrum Multiple-Access Communications Systems," *IEEE Transactions on Communications,* Vols. COM-32, no. 5, pp. 567-573, 1984.

[75] J. G. Proakis, Digital Communications Third edition, New York: McGraw Hill, 1995.

[76] EBITG, TUI, UOULU, CU/CRC, NOKIA, *IST-4-027756 WINNER II D1.1.2 V1.2 WINNER II Channel Models,* CEC, 2007.

[77] W. Jakes Jr, «Microwave Mobile Communications,» 1994Piscataway, NJ: Wiley-IEEE Press.

[78] U. Maurer, «Secret key agreement by public discussion from common information,» *IEEE Trans. Inf. Theory,* vol. 39, n° %13, pp. 733-742, May 1993.

[79] IEEE, "IEEE-802.11-2012: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE, 2012.

[80] F. Tong and A. Popescue, *User guide for 802.11ac waveform generator,* doc.: IEEE 802.11/0517r6, 2011.

[81] H. Li and Z. Han, "Catch me if you can: An abnormality detection approach for collaborative spectrum sensing in cognitive radio networks," *IEEE Transactions on Wireless Communications,* vol. 9, no. 11, pp. 3554-3565, 2010.

[82] P. Zimmermann, "Pgpfone: Pretty good privacy phone owner's manual, Version 1.0 beta 5, appendix c. 1996.," 1996.

[83] S. Viehböck, "Brute forcing Wi-Fi Protected Setup," 2011.

[84] ITU-R, "Combination of geo-localisation database and spectrum sensing techniques," ITU-R, 2004.

[85] J. Proakis and M. Salehi, Communications System Engineering, Prentice Hall Int, 2001.

[86] L. Chang, F. Wang and Z. Wang, "Detection of DSSS Signal in Non-Cooperative Communications," in *ICCT '06 International Conference on Communication Technology*, Guilin, China, 2006.

[87] S. Laur and K. Nyberg, "Efficient mutual data authentication using manually authenticated strings," in *Cryptology and Network Security*, Xiamen, China, 2005.

[88] L. Xiao, L. Greenstein, N. Mandayam and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," in *ICC '07 IEEE International Conference on Communications*, Glasgow, United Kingdom, 2007.

[89] IEEE 1900.6, "IEEE Standard for Spectrum Sensing Interfaces and Data Structures for Dynamic Spectrum Access and other Advanced Radio Communication Systems," IEEE, 2011.

[90] M. M. Sohul, R. Bettadapura, A. Singhal and J. H. Reed, "Information Assurance of LTE-Advanced Self-Organizing Networks". .," in *SDR Winncomm*, San Diego, USA, 2014.

[91] M. Cagalj, S. Capkun and J.-P. Hubaux, "Key agreement in peer-to-peer wireless networks," *Proceedings of the IEEE (Special Issue on Cryptography and Security),* vol. 94, no. 2, pp. 467-478, 2006.

[92] C. Gerhmann and C. B. K. Mitchell, "Manual authentication for wireless devices," *RSA Cryptobytes,* vol. 7, no. 1, pp. 29-37, 2007.

[93] D. Depierre and F. T. Pipon, "Method of optimising planning in a cdma-type communications system". France Patent WO2005088999 A1, 2005.

[94] B. Danev, D. Zanetti and S. Capkun, "On physical-layer identification of wireless devices," *ACM Computing Surveys (CSUR),* vol. 45, no. 1, p. 6, 2012.

[95] ViaSat, "Paired Carrier Multiple Access - PCMA Satellite Bandwidth Optimization," 2014. [Online]. Available: https://www.viasat.com/broadband-networks/paired-carrier-multiple-access-pcma.

[96] VT iDirect, Inc, "PCMA: Enhancing Bandwidth Efficiency in New and Old Networks," 2008. [Online]. Available: ftp://ftp.newcom-intl.com/docs/PCMA.pdf.

[97] P. Schor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer"," *SIAM Journal on Computing,* vol. 26, no. 5, pp. 1484-1509, 1997.

[98] ITU-R, "Radio Spectrum Policy Group « Opinion on Cognitive Technologies," ITU, 2011.

[99] S. Pasini and S. Vaudenay, "SAS-based authenticated key agreement," in *9th International Conference on Theory and Practice in Public-Key Cryptography*, New-York, USA, 2006.

[100] J. Xiong and K. Jamieson, "Secure array: improving Wi-Fi security with fine-grained physical-layer information," in *19th annual international conference on Mobile computing & networking*, Miami, USA, 2013.

[101] J. Massey, "Shift-register synthesis and BCH decoding," *IEEE Information Theory Society,* vol. 15, no. 1, pp. 122-127, 1969.

[102] ITU-R, "Spectrum Monitoring Handbook," ITU-R, 2010.

[103] A. Lakshminarayanan, "TAP-practical security protocols for wireless personal devices," in *15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Barcelona, Spain, 2004.

[104] End to End Reconfigurability II (E2RII), "The E2R II Flexible Spectrum Management (FSM) Framework and Cognitive Pilot Channel (CPC) Concept – Technical and Business Analysis and Recommendations," E2R II, 2007.

[105] W. Xu, W. Trappe, Y. Zhang and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *6th ACM international symposium on Mobile ad hoc networking and computing*, Urbana-Champaign, USA, 2005.

[106] T. Wu, "The SRP Authentication and Key Exchange System," IETF Standard, Standford, 2000.

[107] J. Ylitalo and M. Juntt, "Tutorial - MIMO Communications with Applications to (B)3G and 4G Systems," University of Oulu, Dept. Electrical and Inform. Eng., Centre for Wireless Communications (CWC), Oulu,

Finland, 2010.

[108] Satcom Ressources, “ViaSat PCMA - Paired Carrier Multiple Access,” 2014. [Online]. Available: http://www.satcomresources.com/ViaSat-PCMA-Paired-Carrier-Multiple-Access.

[109] T. Kasami, “Weight distribution formula for some class of cyclic codes,” Illinois Univ at Urbana Coordinated Science Lab, Champaign, USA, 1966.

[110] Wi-Fi Alliance, “Wi-Fi Protected Setup,” 2013. [Online]. Available: http://www.wi-fi.org/knowledge-center/articles/wi-fi-protected-setup%E2%84%A2.

[111] USB Implementers Forum, “Wireless Universal Serial Bus Specification 1.1,” 2010. [Online]. Available: http://www.usb.org/developers/wusb/docs/ ed.

[112] Q. Wang, P. Xu, K. Ren and X. Li, “Delay-Bounded Adaptive UFH-based Anti-jamming Wireless Communications,” in *Infocom*, Shangai, China, 2011.

[113] S. Bellowin and M. Merrit, “Encrypted key exchange: Password-based protocols secure against dictionary attacks,” in *Proceedings of the IEEE Symposium on research in security and privacy*, Oakland, New Zealand, 1992.

[114] J. Larsson, “Higher layer key exchange techniques for for bluetooth security,” in *Open Group Conference*, Amsterdam, The Nederlands, 2001.

[115] J.-C. Belfiore, C. Ling and L. Luzzi, “Lattice codes achieving strong secrecy over the mod-Λ Gaussian channel,” in *IEEE International Symposium on Information Theory Proceedings*, Cambridge, USA, 2012.

[116] G. Noubir, “On Connectivity in Ad Hoc Network under Jamming Using Directional Antennas and Mobility,” in *International Conference on Wired /Wireless Internet Communications (WWIC)*, Frankfurt, Germany, 2004.