COMBINING ARTIFICIAL NOISE BEAM FORMING AND CONCATENATED CODING SCHEMES TO EFFECTIVELY SECURE WIRELESS COMMUNICATIONS

Christiane L. Kameni Ngassa (Thales Communications and Security (TCS), Gennevilliers, France; Christiane.Kameni@thalesgroup.com); Jean-Claude Belfiore (Telecom ParisTech (TPT), Paris, France; jean-claude.belfiore@telecom-paristech.fr); Renaud Molière (TCS; Renaud.Moliere@thalesgroup.com); François Delaveau (TCS; Francois.Delaveau@thalesgroup.com); Nir Shapira (Celeno Communications, Ra'anana, Israel; Nir.Shapira@celeno.com)

ABSTRACT

In this paper we present a new scheme combining Artificial Noise Beam Forming and Secrecy Coding to strengthen the security of existing wireless communication systems. Artificial Noise and Beam Forming guarantee a Radio Advantage to legitimate users, enabling the use of our Secrecy Coding scheme to provide reliability and secrecy. This overall security protocol is compliant with existing widespread Radio Access Technologies and it can be considered as a key-free add-on to improve security of the physical layer of wireless networks.

1. INTRODUCTION

Most of existing security mechanisms for wireless communication rely on pre-shared cryptographic keys to encrypt exchanged data. However, recent news about public Radio Acces Technologies (RATs) revealed that attackers can have access to these encryption keys by exploiting weakness of SS7 protocol and international roaming [1, 2]. Furthermore, the recent hacking of SIM card manufacturers to get encryption keys proves that the cryptographic key distribution approach can no longer be considered as completely secure [3]. Physical layer security (Physec) appears therefore as a crucial help to strengthen wireless communication security as it leverages inherent properties of the wireless channel to provide secrecy without the need of a pre-distributed secret key.

Secrecy (or wiretap) Coding is one of the main Physec techniques. Its goal is to provide both reliability and secrecy without using any secret key. The reliability is defined as the ability to transmit information over a noisy channel without errors. The secrecy is defined as the ability to transmit information over a wiretap channel with confidentiality.

Secrecy Coding (SC) has three major adavantages:

- SC needs only a guaranteed Radio Advantage (RA) for the legitimate nodes and terminals [4]. No accurate propagation measurement and no channel reciprocity are required. Thus, any established and resilient radio protocol that achieves a controlled Radio Advantage to legitimate users enables the use of SC. This radio advantage can be provided by several means such as Directive Antennas, Artificial Noise (AN) combined with Beam Forming (BF), Full Duplex Communications technologies [5].
- SC requires no secured radio link nor authentication
- SC is independent of eavesdropper's computational capability, thus it remains secure from attacks with unlimited computational power.

Nevertheless, the design of a practical wiretap code is very challenging: despite numerous theoretical results, secrecy coding schemes proposed in the literature were applied only to ideal wiretap radiochannels and cannot be readily implemented in existing wireless communication networks.

In this paper we propose a practical implementation of secrecy coding schemes combined with Artificial Noise and Beam Forming. This implementation, which is slighly suboptimal when compared to theoretical schemes [4] is derived form the work performed in the Phylaws project [5].

In section 2, we describe how the Artificial Noise scheme provides a controlled Radio Advantage to legitimate users, while the Beam Forming allows reliable link to the legitimate terminal.

Section 3 presents the construction of proposed secrecy coding schemes. An "outer" code (polar code or a Reed Muller (RM) code) is concatenated with an "inner" code (a standard Forward Error-Correction (FEC) code). The outer code provides the secrecy to the legitimate radio link while the inner code provides the reliability.

Section 4 describes the tuning of radio parameters of the Artificial Noise and Beam Forming in order to provide the desired Radio Advantage .

Section 5 provides results obtained from simulated WiFi signals transmitted over an AWGN channel. We use the LDPC code defined in the 802.11 standard as inner code. We provide simulation results for a total of 7 designed Secrecy Codes and for 2 polar decoding algorithms.

In section 6 we implement proposed AN-BF + SC schemes within real WiFi chipsets and provide experimental results. The promising results show that our secrecy coding schemes can easily be implemented in existing RATs with limited impact on the chipset.

Finally, section 7 concludes the paper and highlights the practical performance of designed secrecy codes and implementations perspectives in the next future.

2. ARTIFICIAL NOISE AND BEAM FORMING

2.1. Achieving Radio Advantage

In MIMO RATs, the Radio Advantage is achieved by combining Beam Forming of data towards the legitimate receiver with the emission of interfering signals (Artificial Noise) elsewhere (Figure 1).

The Artificial Noise power is controlled and the user signal is steered to optimize the decoding capability at legitimate links while decreasing it at eavesdroppers.

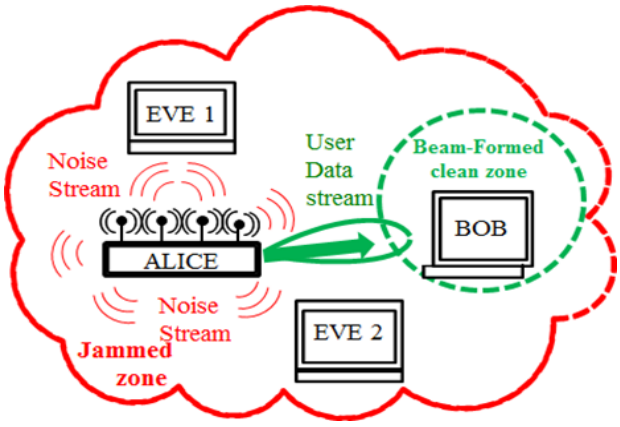


Figure 1: Scheme of transmission with AN-BF protections by Artificial Noise and Beam-Forming

2.2. Artificial Noise processing

Most promising Artificial Noise (AN) schemes studied in the literature proceed as follows [6][7]:

- Estimation of the legitimate Channel Frequency Response (CFR) or Channel Impulse Response (CIR), from Alice to Bob, and extraction of orthogonal directions of the legitimate CFR or CIR.
- Transmission of noise streams on orthogonal directions. As Eve cannot estimate the legitimate channel matrix, she is thus forced into low Signal to Interference Noise Ratio (SINR) regime and is unable to decode.
- Beam Forming (BF) of the Alice-Bob data stream for Bob to maximize the legitimate link budget. Bob extracts Alice's channel and suppresses orthogonal noisy channel directions thanks to BF. In ideal cases, the Interference at Bob's side completely vanishes and the Signal to Interference Noise Ratio at Bob's side reduces to a Signal to Noise Ratio ($SINR_{Bob}=SNR_{Bob}$).

When AN and BF techniques are established, a better SINR is provided to Bob than to Eve in any case and the SINR at Eve's side is controlled by Alice. The relevant Radio Advantage ($RA=SINR_{Bob}-SINR_{Eve}$) is thus guaranteed and it can be further exploited by the legitimate link to compute secrecy codes.

2.3 AN and BF for initiating Secrecy Coding schemes

The goal of Secrecy Codes is to ensure reliable communication at the legitimate link and to avoid any information leakage elsewhere.

Secrecy Codes conceal the information sent by Alice up to a secrecy capacity. In the general case, the secrecy capacity equals the difference of channel capacities at Bob and Eve's side; in simplest models such as AWGN channel, it is directly driven by the Radio Advantage. Without a positive Radio Advantage, secrecy capacity is null.

Moreover, in real scenarios (time and space varying channel, shadowing, fading), the Radio Advantage should be controlled to guarantee a minimum secrecy capacity, so that Alice and Bob can properly choose and control the secrecy coding parameters.

3. SECRECY CODING SCHEME

The design of Secrecy Codes for continuous channels is challenging [4]. However since polar codes provide strong security for discrete channels [8], the idea is to concatenate them to a capacity approaching code. Hence, the channel between the polar encoder and the polar decoder can be viewed as a Binary Symmetric Channel. Thus, we propose a scheme which is initially composed of a LDPC code as inner code and of a polar code as outer code.

The inner code could be any FEC codes employed currently for practical wireless communications such as LDPC codes or Turbo Codes. The design of the inner code is therefore straightforward as we only follow the requirements defined in those standards.

In this work we consider particularly LDPC codes defined in 802.11 standard (WiFi).

Figure 2: Secrecy coding scheme

3.1 Construction of the outer code using polar codes

We first consider two nested polar codes of length $N = 2^n$ as the outer code.

The rate of the first polar code is the target rate for Eve denoted R_E and the rate of the second polar code is the target rate for Bob, denoted R_B .

We suppose that legitimate users have a Radio Advantage over Eve, $R_E < R_B$. Therefore Eve can perfectly decode $N.R_E$ bits and Bob $N.R_B$.

In order to confuse Eve and to ensure 0.5 error probability at her side, we send random bits over $N.R_E$ perfect bit-channels. In other words, over the bit-channels for which Battacharyya parameters are zeros.

The design strategy of the outer code is then the following.

- Battacharyya parameters are computed for Bob target's error probability at the output of the inner decoder
- Bit-channels are sorted in ascending order of their Battacharyya parameters
- Random bits are sent over the first $N.R_E$ bit-channels.
- Information bits are sent over the following $N(R_B - R_E)$ bit-channels
- Frozen bits (i.e. zeros) are sent over the remaining bit-channels.

3.2 Construction of the outer code using Reed-Muller codes

We propose to use Reed-Muller codes as an alternative to polar codes in the design of the outer code [9].

The constructions of Reed-Muller codes and polar codes are similar. The main difference is the selection of bit-channels over which information bits are sent. Indeed, for polar codes the selection criteria is the Battacharrya parameter while the selection criteria for bit-channels for the Reed-Muller codes is the Hamming weight of rows of the generator matrix. Consequently, for a given code length, the Reed-Muller code usually has a larger minimum distance and better performance than the corresponding polar code for small and moderate code length.

The design strategy for the outer RM code is then modified as follows.

- Hamming weights of generator matrix's rows are computed
- Bit-channels are sorted in ascending order of their Hamming weight
- Random bits are sent over the $N.R_E$ first bit-channels.
- Information bits are sent over the $N(R_B - R_E)$ following bit-channels
- Frozen bits (i.e. zeros) are sent over the remaining bit-channels.

3.3. practical Construction of secrecy codes

We use the LDPC code of length 1296 and rate 5/6 defined in the 802.11 standard as the inner code. The outer code is either a polar code of length 2^{10} = 1024 or a Reed-Muller code of the same length.

For simulation purpose, five outer codes are designed using polar and Reed-Muller codes of different rates.

The parameters of these five secrecy codes are presented in Table 1. Note that R, I and F denote respectively the number of random bits, information bits and frozen bits.

Table 1: Resulting secrecy codes

	Secrecy code 1	Secrecy code 2	Secrecy code 3	Secrecy code 4	Secrecy code 5
Inner code	LDPC code of length 1296 and rate 5/6 defined in the 802.11 standard				
Outer code	Polar code	Polar code	Polar code	Reed-Muller code	Reed-Muller code
Eve's target rate	0.1	0.1	0.1	0.05	0.05
Bob's target rate	0.6	0.5	0.4	0.5	0.4
(R,I,F)	(102, 512, 410)	(102, 409, 513)	(102, 307, 615)	(56, 430, 538)	(56, 330, 638)
Secrecy code rate	0.4	0.33	0.24	0.33	0.25

4. TUNING THE RADIO ADVANTAGE

The Bit Error Rate at the output of the secrecy decoder should be 0.5 up to a given "*attacker threshold*" of the Signal to Interference + Noise Ratio ($SINR_{RxEve}$), depending on the modulation and concatenated coding scheme, that ensures no information leakage.

We denote $SINR_{RxBob}$ the Signal to Interference + Noise Ratio at Bob's side. When $SINR_{RxBob}$ increases, the bit error rate at the output of the polar decoder should vanish. When $SINR_{RxBob}$ is high enough (greater than a "*user threshold*" $SINR_{user}$) the bit error rate at the output of the polar decoder should tend to zero.

Note that in linear scale the SINR is denoted $\rho_{SINR}=S_{Rx}/(J_{Rx}+N_{Rx})$, where S_{Rx} is the received user signal, N_{Rx} the receiving noise, and J_{Rx} the received interference. When no Interference occur, SINR reduces to a Signal to Noise Ratio (SNR), meaning $\rho_{SINR}=\rho_{SNR}=S_{Rx}/N_{Rx}$. When receiving noise is negligible SINR reduces to a Signal to Interference Ratio (SIR), meaning $\rho_{SINR}=\rho_{SIR}=S_{Rx}/J_{Rx}$.

Taking into account existing AN-BF schemes and other means for providing the Radio Advantage (such as Directive Antennas for transmission, Full Duplex communications technologies), the typical value of SINR=-1 dB (0.8 in linear scale) should be considered as the maximum SIR_{RxEve} tolerated (By Alice and Bob) at Eve's receiver.

Therefore the corresponding $\rho_{min,Eve}$ should be equal to 0.8 to be used at Alice's transmitters to tune the Artificial Noise power from the value of the user data stream power with a ratio $J_{Tx} \geq S_{Tx}$ greater than $1/\rho_{min}$.

Then the power of the user (signaling or data) stream and of the Beam Forming performance is tuned in order to achieve reliable communication at legitimate receive Bob. When considering the mean channel propagation losses (noted l_{AB} in linear values L_{AB} in dB), the beam forming rejection (denoted below bf_{rej} in linear value, BF_{rej} in dB), the receiving noise at Bob's side (denoted N_{Rx} in linear values), and the SNR threshold of Bob's receiver (denoted $\rho_{Thres,Rx}$ in linear value),

- the global signal to noise + interference ratio at Bob is given by $\rho_{SINR,Rxbob}=[S_{Tx}/l_{AB}]/[(J_{Tx}/l_{AB}/bf)+N_{Rx}]$,
- and the global signal to noise ratio by $\rho_{SNR,Rxbob}=[S_{Tx}/l_{AB}]/[N_{Rx}]$.

In practice, one has to:

- define two margin values $\eta 1$ and $\eta 2$ such that $1<\eta 2<\eta 1$ to tune of the radio engineering;
- tune the user (signaling or data) stream S_{Tx} to achieve enough receiving power such that $\rho_{SNR,Rxbob} \geq \rho_{Thres,Rx}.\eta 1$.
- tune the BF rejection bf_{rej} such that $\rho_{SINR,Rxbob} \geq \rho_{Thres,Rx}.\eta 2$

As a summary, two main radio parameters are necessary to implement the secrecy coding schemes:

- A **"minimum $SINR_{user,min}$"** for the legitimated link, which is relevant to the performance of the modulation and coding schemes at Bob's receiver. Achieving SINR values greater than $SINR_{user,min}$ for ongoing legitimate radio-communications involves some network engineering activities: management of the network topology (real field path losses, transmit power, energy budget link, and control of the Beam Forming performance BF_{rej} in the established AN scheme (Alice and Bob processing input by Channel State Information). Note that all these parameters are involved in the equalization processing and in the Quality of Service Management.
- A **"SINR Security gap"** $SINR_{SG}$ that represents the lower bound of the Radio Advantage to be provided at the legitimate link by increasing the interference J_{Tx} at Alice transmitter (and consequently at Eve side). BF_{rej} being controlled by Alice and Bob, $SINR_{SG}$ drives the tuning of the Artificial Noise power by the Node to ensure the Radio Advantage at any Eve's location.

In the general case, Alice and Bob have thus to manage parameters S_{Tx} J_{Tx} and bf so that $SINR_{user,min}=10.\log_{10}(\rho_{Thres,Rx})$ $+10.\log_{10}(\eta 2)$. Nevertheless, the exact radio advantage remains dependent on Eve's Receiver capabilities.

In simplified optimal case where jamming signal transmission is co-located with user signal transmission (Eve has no spatial rejection capabilities whatever is her receiver performance), and receiving noise at Bob is negligible (thus $SINR_{RxBob} \approx SIR_{RxBob}=SIR_{TxAlice}+BF_{rej}$ while we have in any case $SINR_{Eve} \leq SIR_{Eve}$), Alice and Bob get facilitated radio management of the link with parameters $SIR_{Tx,Alice}$ and BF_{rej} such that $SIR_{Tx,Alice} + BF_{rej} \geq SINR_{user,min}$ and $SIR_{RxEve} \approx SIR_{TxAlice} \leq SNR_{user,min} - SINR_{SG}$. Hence, the Radio Advantage verifies $RA \geq BF_{rej}$ (non-equality occurs when Eve's receiver noise is significant – increasing the advantage of Bob), and a simplified requirement for BF_{rej} is achieved by considering $BF_{rej} \geq \text{Max}\{SINR_{SG}, SINR_{user,min} - SIR_{TxAlice}\}$.

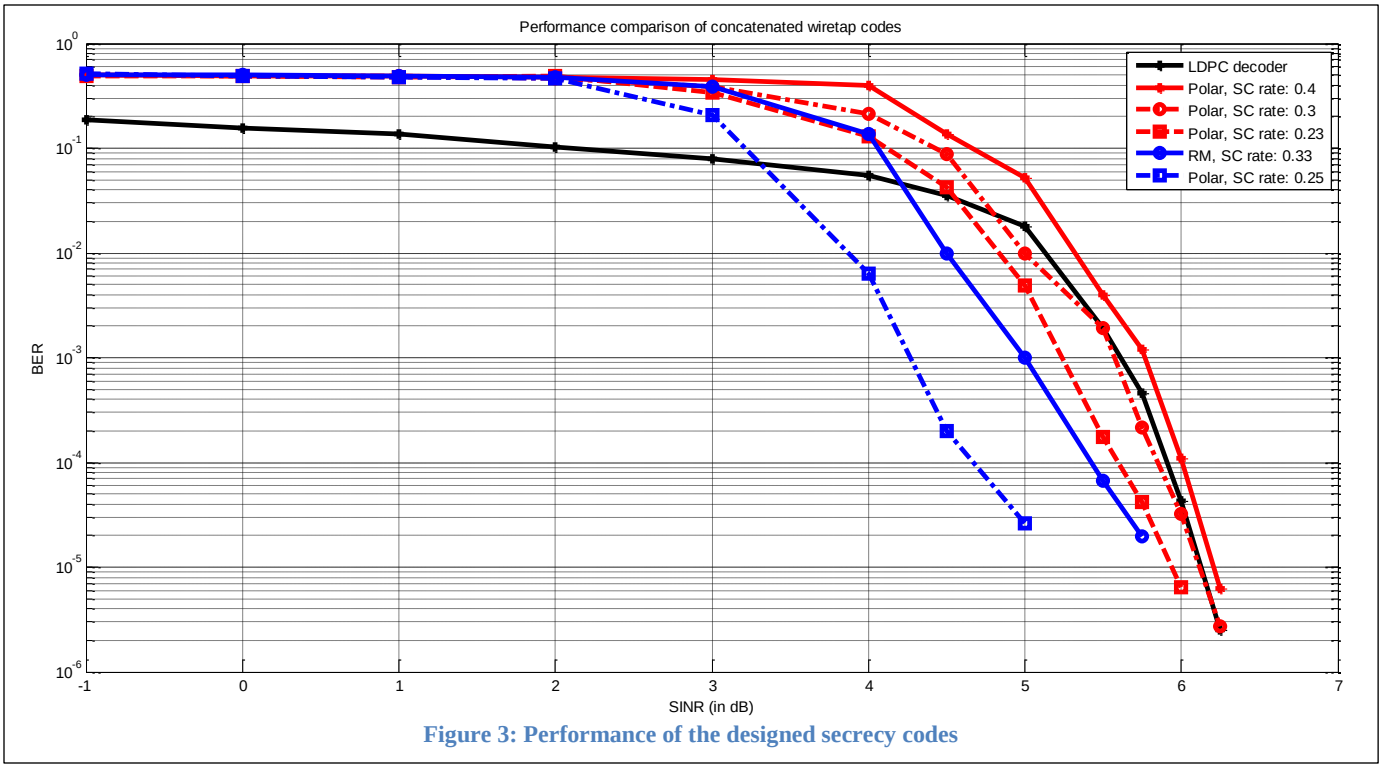


Figure 3: Performance of the designed secrecy codes

5. SIMULATION RESULTS

Simulations were carried out using MATLAB and messages were sent over an AWGN channel using a QPSK modulation. A WiFi transmission is simulated. The Belief Propagation (BP) algorithm is used for decoding LDPC, Polar and Reed-Muller codes.

5.1 Performance analysis from simulated signals

Figure 3 shows the performance of the designed secrecy codes.

- The black curve represents the Bit Error Rate (BER) at the output of the LDPC decoder
- Red curves represent the BER at the output of secrecy polar decoders
- Blue curves represent the BER at the output of secrecy Reed-Muller decoders

The results show that:

- When SINR $\leq$ 2 dB, the BER at the output of the five secrecy codes is equal to 0.5. Meaning that, all secrecy codes guarantee no information leakage if Eve's SINR is less than 2 dB. Only the polar based secrecy code with rate 0.4 (Secrecy code 1) guarantees no information leakage until 3 dB.
- All Reed-Muller based secrecy codes have better reliability performance than polar based secrecy codes.
- For a target error probability of 5.10^{-5} for Bob, the require Radio Advantage is only 3 dB to 4 dB.

These simulation results show that Eve cannot retrieve any transmitted information when a slight Radio Advantage ($<$ 4 dB) is provided to legitimate users. The secrecy is achieved with a limited increase in coding and decoding complexity.

5.2 Performance illustration for simulated signals

Still taking into account characteristics of Wifi encoders and BP decoders, we illustrate the performance of our secrecy coding scheme by simulating the transmission of the cameraman image (Figure 4) over an AWGN channel, for different values of the SINR.

Figure 5 shows the received image for SINR $\leq$ 2 dB. No clue on the transmitted image can be deduced from the received image. The BER at the output of the secrecy code is equal to 0.5.

Figure 6 represents the received image when the SINR increases. The BER at the output of the secrecy code for the three images is respectively, 0.46, 0.30 and 0.04. At BER=0.46, the information leakage is negligible and Eve cannot guess the transmitted image.

However, when BER=0.3, Eve can guess the transmitted message. Even though 0.3 is a high value for a BER, the amount of information leaked is enough to reconstruct the cameraman image. Consequently, Eve's BER should be as close as possible of 0.5 (>0.45) to guarantee no information leakage.

Figure 7 shows the received image at higher SINR values. The BER at the output of the secrecy code for the two images is respectively, 10^{-3} and 10^{-5}. A few errors remain in the first image and no error is detected for the second image. Meaning that Bob can perfectly receive the transmitted information when his SINR is high enough (>5dB to 6 dB depending on the designed secrecy code).

Figure 4: Original image to be transmitted over the channel

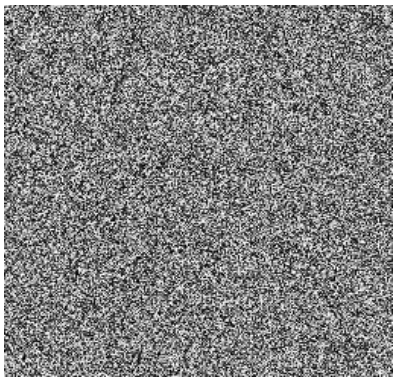


Figure 5: Received image around SINR targeted for Eve

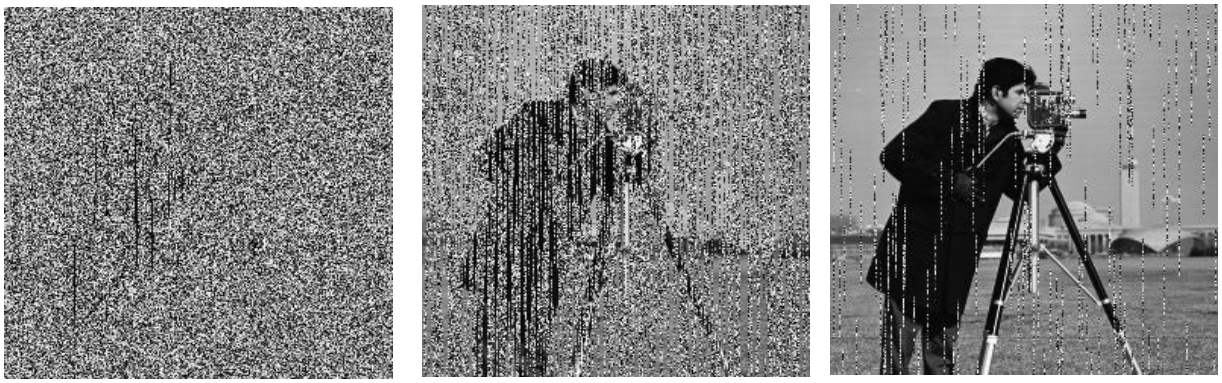


Figure 6: Received image in the transition region

Figure 7: Received image around SINR targeted for Bob

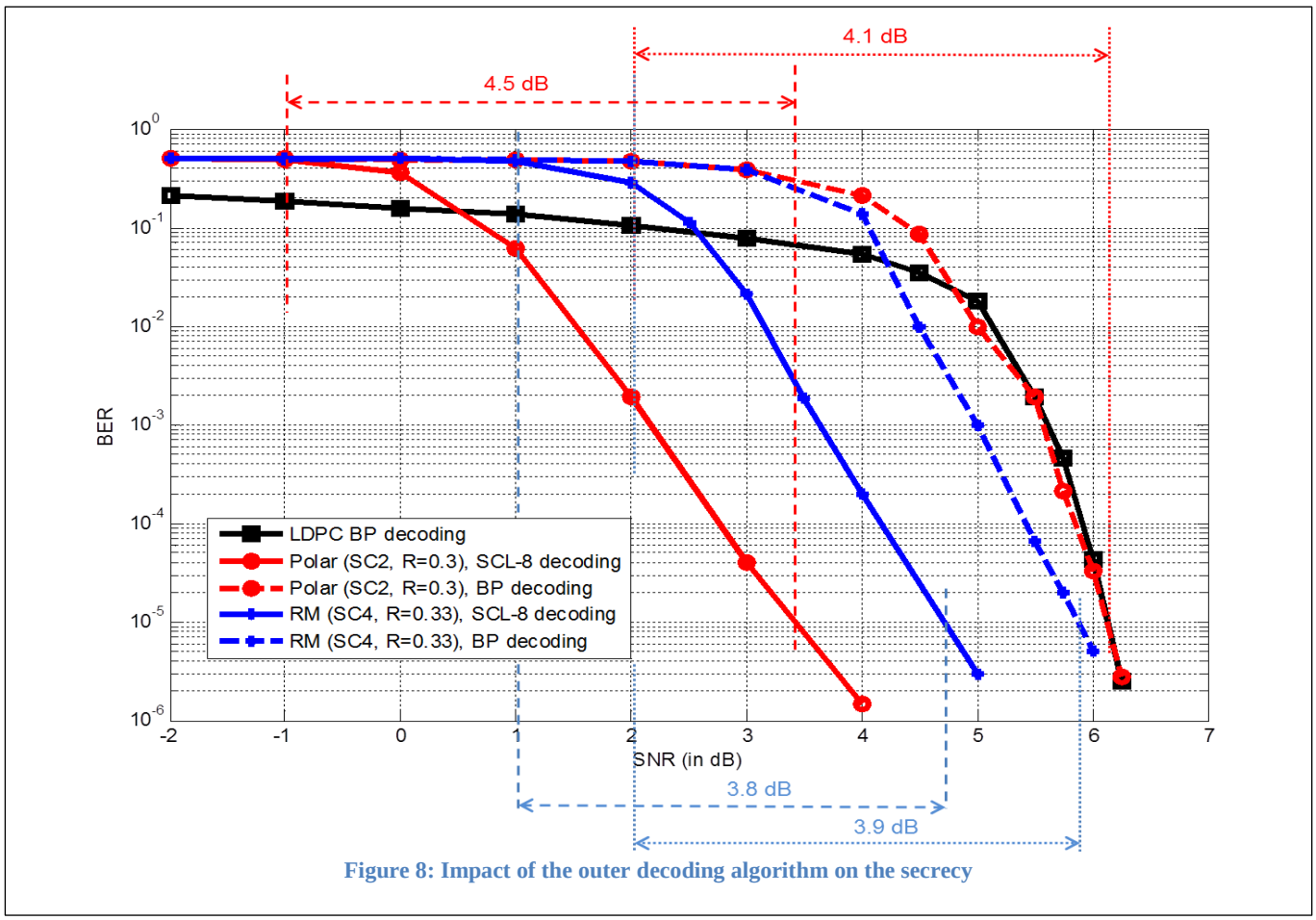


Figure 8: Impact of the outer decoding algorithm on the secrecy

5.3 Impact of the polar decoding algorithm

When Arikan introduced polar codes, he also proposed a low-complexity decoding algorithm named the successive cancellation (SC) decoding algorithm [10]. However, the SC decoder has limited performance at moderate block length.

In [11], Tal and Vardy proposed an improved version of the SC decoder referred to as successive cancellation list (SCL) decoder. We use in this paper the LLR-based SCL decoding algorithm presented in [12] for comparison purpose (list size of 8). We have also chosen secrecy codes of comparable secrecy rate, SC2 and SC4 described above.

Figure 10 shows that SCL decoding algorithm significantly improves the performance of the polar decoder and allows a gain of about 3 dB. The SCL decoder also improves the performance of the Reed-Muller decoder but leads only to 1.5 dB. This is because the SCL decoder was designed to optimize the polar decoding performance.

For both polar and Reed-Muller codes, the SCL decoder has a limited impact on the required Radio Advantage. Indeed for the polar-based secrecy code, the required Radio Advantage increases from 4.1 dB to 4.5 dB. For the RM-based secrecy code, the required Radio Advantage decreases from 3.9 dB to 3.8 dB.

5.4 Design and performance of new secrecy codes

Table 2 provides the parameters of the new polar-based secrecy codes (SC6 and SC7) designed with a target of SINR = -1 dB for Eve and taking into account the performance of the SCL decoding algorithm.

Figure 9 shows the performance of SC4, SC5, SC6 and SC7 when the Belief Propagation algorithm is used for LDPC decoders and the LLR-based successive cancellation list decoding algorithm is used for polar and Reed-Muller decoders.

Table 2: New secrecy codes

	SC4	SC5	SC6	SC7
Inner code	LDPC code of length 1296 and rate 5/6 defined in the 802.11 standard			
Outer code	Reed-Muller code	Reed-Muller code	Polar code	Polar code
Eve's target rate	0.05	0.05	0.05	0.13
Bob's target rate	0.5	0.4	0.55	0.52
(R,I,F)	(56, 430, 538)	(56, 330, 638)	(51, 512, 461)	(133, 399, 492)
Secrecy code rate	0.33	0.25	0.4	0.3

- The black curve represents the Bit Error Rate (BER) at the output of the LDPC decoder.
- Red curves represent the BER at the output of secrecy polar decoders.
- Blue curves represent the BER at the output of secrecy Reed-Muller decoders.

The results show that:

- Polar-based secrecy codes have better reliability performance than RM-based secrecy codes of similar rates.
- When SINR $\leq$ 1 dB, the BER at the output of the four secrecy codes is equal to 0.5. Meaning that, all secrecy codes guarantee no information leakage if Eve's SINR is less than -1 dB.
- When SINR $\leq$ 0 dB, the BER at the output of secrecy codes SC4 and SC5 is equal to 0.5 while the BER at the output of secrecy codes SC6 and SC7 is above 0.45. Meaning that if Eve's SINR is less than 0 dB, SC4 and SC5 guarantee no information leakage while only a limited amount of information (less than 5%) is leaked for SC6 and SC7.
- For a target error probability of 10^{-5} for Bob, the required Radio Advantage to ensure no information leakage is limited to 4.4 dB to 4.7 dB.

These simulation results demonstrate that Eve cannot retrieve any transmitted information when a slight Radio Advantage (< 5 dB) is provided to legitimate users. The secrecy is achieved with a limited increase in coding and decoding complexity.

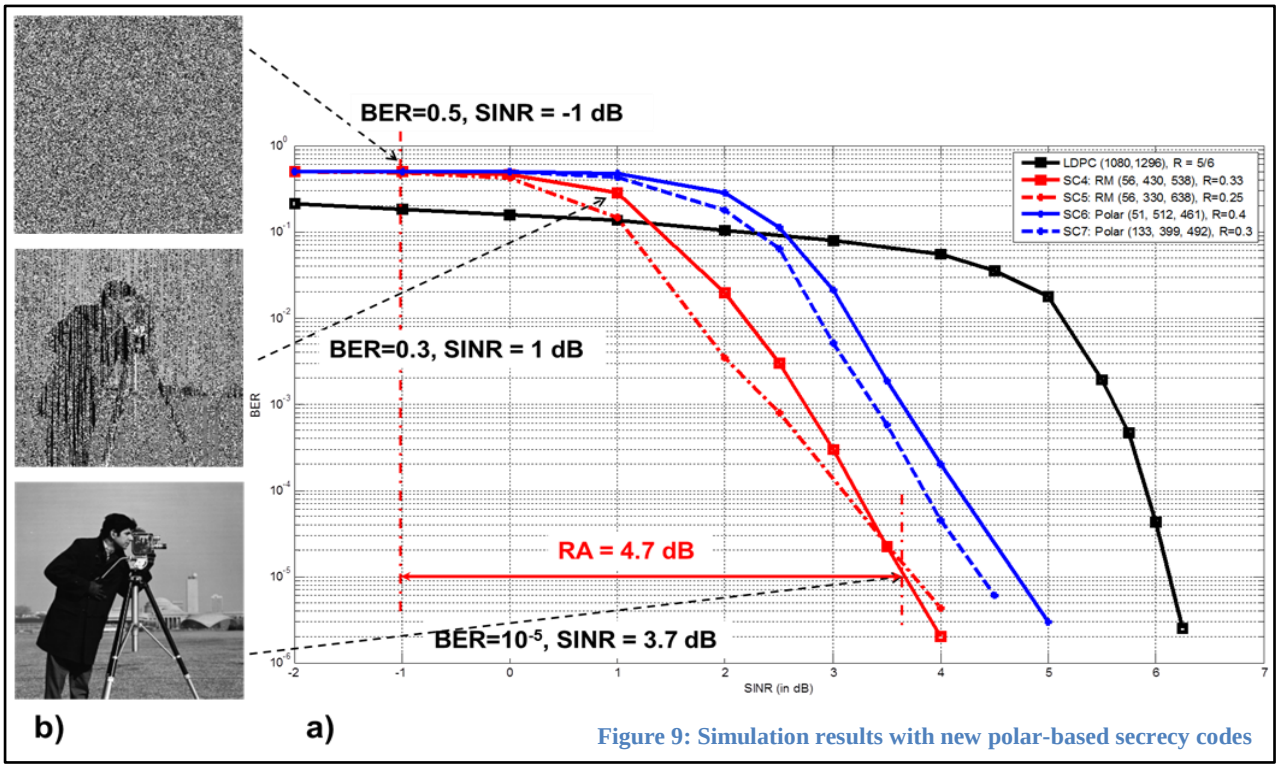
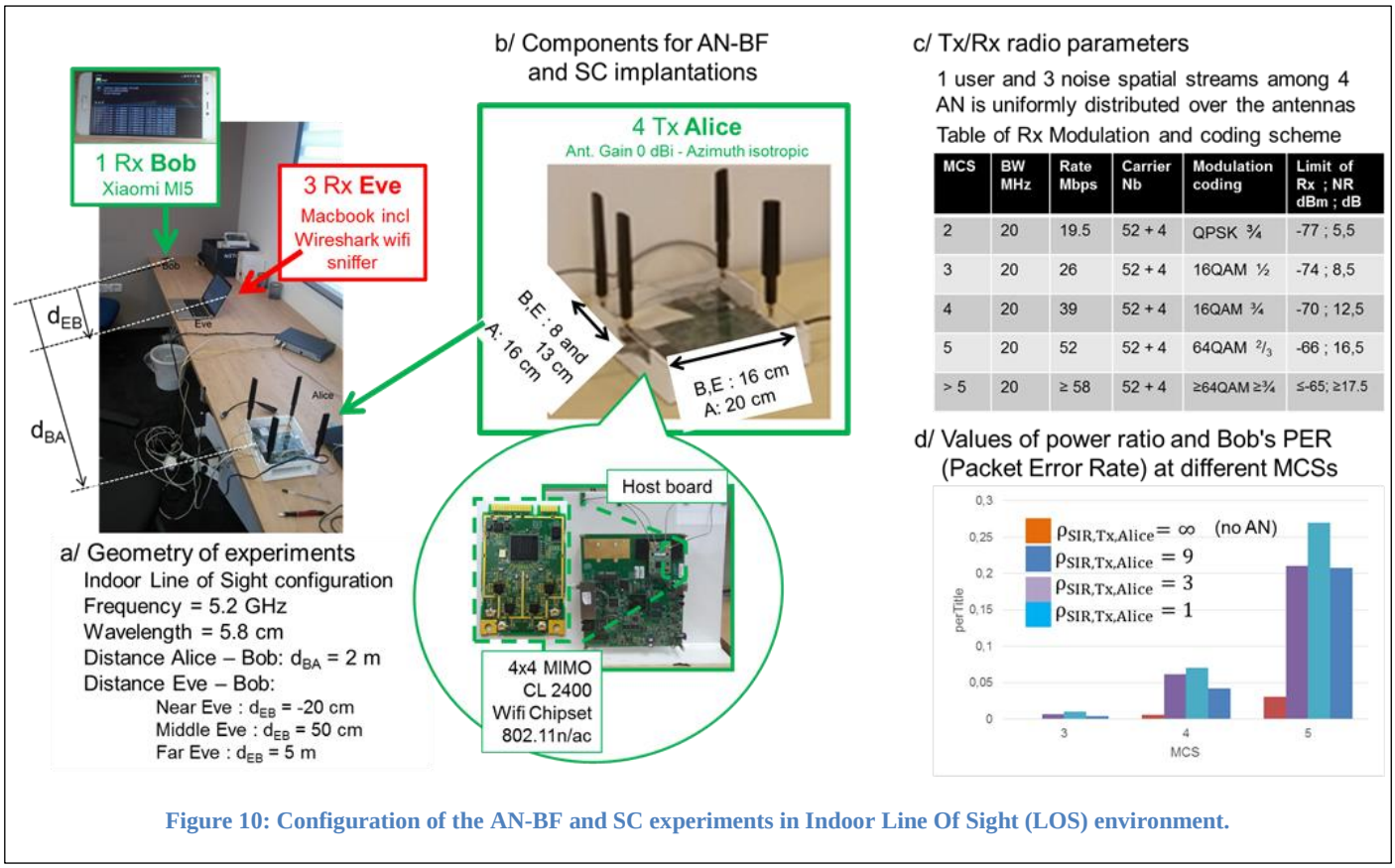


Figure 9: Simulation results with new polar-based secrecy codes



MCS	BW MHz	Rate Mbps	Carrier Nb	Modulation coding	Limit of Rx ; NR dBm ; dB
2	20	19.5	52 + 4	QPSK ¾	-77 ; 5,5
3	20	26	52 + 4	16QAM ½	-74 ; 8,5
4	20	39	52 + 4	16QAM ¾	-70 ; 12,5
5	20	52	52 + 4	64QAM 2/3	-66 ; 16,5
> 5	20	≥ 58	52 + 4	≥64QAM ≥¾	≤-65; ≥17.5

Figure 10: Configuration of the AN-BF and SC experiments in Indoor Line Of Sight (LOS) environment.

6. EXPERIMENTAL RESULTS USING REAL WIFI SIGNALS

6.1 Configuration parameters of experiments

We performs experiments using 802.11ac WiFi links at frequency 5.2 GHz, with standard modulation coding schemes at transmitter Alice and at receivers Bob and Eve. The geometry is indoor and Line of Sight (LOS).

The access point Alice is implemented on a 4-antenna dedicated chipset (CL 2400), developed by Celeno Communications. Through the IPERF test application (commonly used to generate TCP and USP traffic), Alice transmits a pre-defined bit pattern as User Signal (US) to facilitated Bit Error Rate (BER) Evaluations. In addition, Alice adds Artificial Noise (AN) to the data part of the US bit pattern and Beam Forms it towards Bob.

Bob is implemented by using a single-antenna Smartphone device (XIAOMI's MI5).

Eve is implemented by using a 3-antennas MacBook Pro, working in sniffer mode with the Wireshark application. The Wireshark application outputs Packet Error Rates and stores Rx signals frames. The BER at Eve side is then computed offline (using a Matlab script) by comparing the stored received packets to the known transmitted pattern.

The overall geometry and locations of Alice Bob and Eve are represented into Figure 10a.

The overall hardware and software components hosting the AN-BF application are represented Figure 10b (CL 2400 wifi chipsets and host board). The AN-BF processing is based on a Spatial Multiplexing (SM) transmit matrix which is computed from a Single Value Decomposition (SVD) of the Channel Matrix (CM) issued from channel sounding exchanges. Note that when antennas are calibrated at Alice and Bob's side, AN-BF can be based on channel reciprocity assumption, without any added information exchanged over the air.

During computations, Alice has to restrict Rx or Tx operations and match numerous technological constraints. Thus, several compressions, acceleration and parameterization capabilities are added to support AN-BF:

- QR decomposition and size reduction of the matrix involved in the computations,
- adjustment of the number of noise spatial streams (NAN=3 among 4) and user spatial stream (NSS=1 among 4),
- adjustment of the power ratios $\rho_{SIR,Tx,Alice}$ between the data and the noise streams,
- uniform distribution of independent noise samples over all transmitting antennas,
- gain scaling of the entire signal to ensure that the total Tx power matches the required digital back-off level and avoids saturation of the Digital to Analog Converter.

The Wifi transmitting and receiving radio parameters are recalled Figure 10c.

Figure 10d provides the values of the power ratios $\rho_{SIR,Tx,Alice}$ and the relevant values of Packet Error Rates (PER at Bob's Side) that lead to the experimental results shown in the following paragraphs.

6.2 Transmitting and processing of the secret encoded Wifi signals

To experiment the decoding of secret codes by Eve and Bob, a fixed frame is still sent by Alice over repeated transmissions (by using the same IPERF application as above). This frame is then off-line pre-computed from the initial bit pattern and one of the designed secrecy encoder. The parameters of the secrecy code used in the experiments results below is the polar-based secrecy code SC2 with (R,I,F) = (102, 409, 513).

Note that the code-word length of 1024 bits perfectly matches the Wifi Frame length. The decoding at Bob's and Eve's side is done offline from signal frames records by using a Matlab script.

The whole procedure enables the estimation of the performance of Secrecy Coding through BER estimates at Eve's side. Moreover, comparison of Eve's BER when using the native the WiFi FEC scheme (e.g., LDPC or BCC) concatenated to nested polar codes or Reed-Muller codes, allow the analyze of the basic protection of the Radio Advantage provided by AN-BF alone and the security enhancement due to the secrecy coding scheme itself.

Recall that Eve has 3 receiving antennas and is supposed to have the complete information about the secret code. Moreover, she can test any Modulation and Coding Scheme in her attempts to recover parts of the legitimate user information, MCS2 being the best for Eve regarding the resilience of her decoding when facing Artificial Noise.

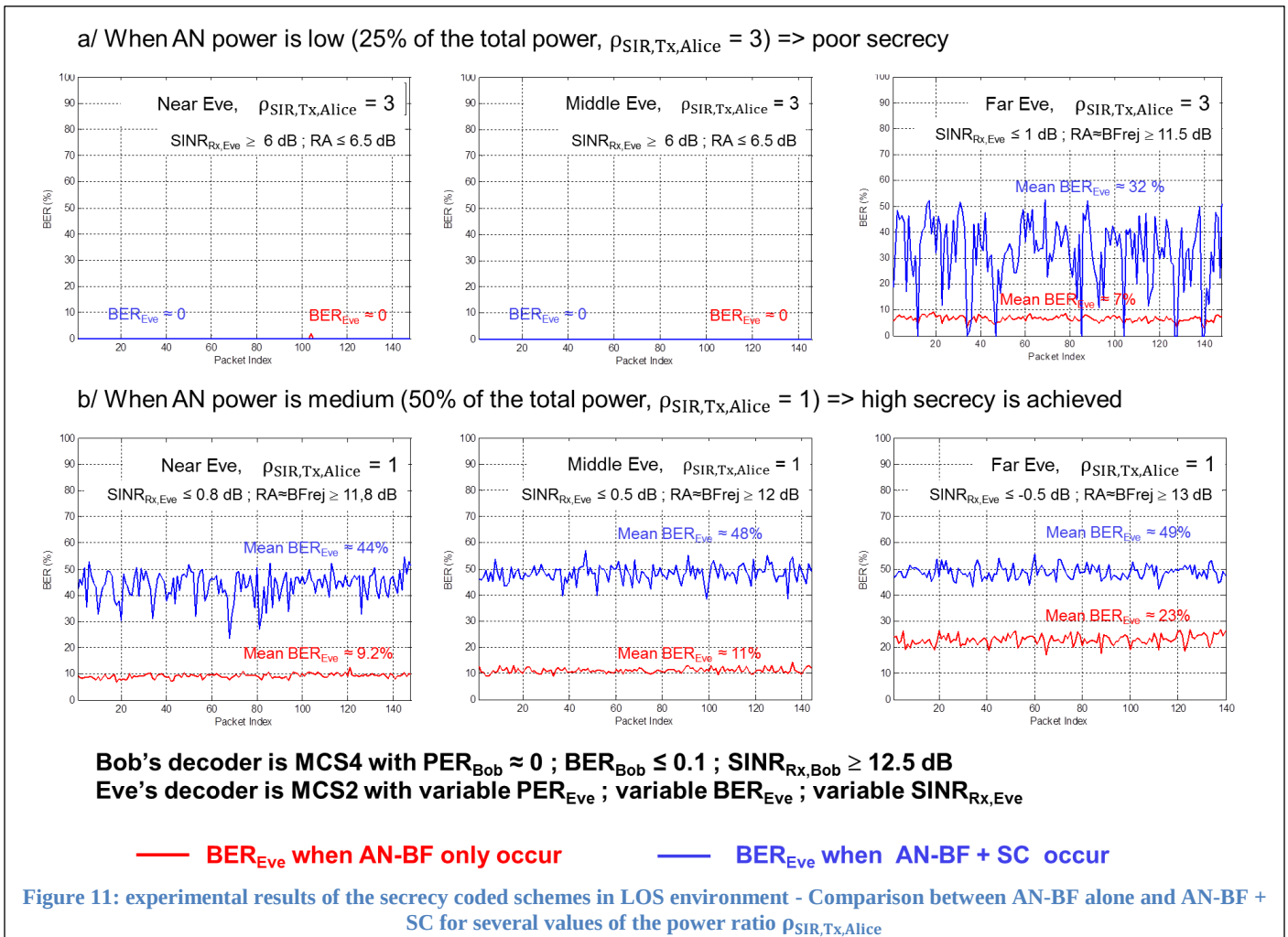


Figure 11: experimental results of the secrecy coded schemes in LOS environment - Comparison between AN-BF alone and AN-BF + SC for several values of the power ratio $\rho_{SIR,Tx,Alice}$

6.3 Transmitting and processing of the secret encoded Wifi signals

Figure 11 shows the results of the AN-BF scheme and of the combined AN-BF + SC scheme on recorded Wifi frames.
Two (low and middle) values of the power ratio $\rho_{SIR,Tx,Alice}$ are taken into account:

- $\rho_{SIR,Tx,Alice} = 3$ in figure 5a while the AN power is 25 percent of the total power,
- $\rho_{SIR,Tx,Alice} = 1$ in figure 5b while the AN power is 50 percent of the total power.

In any cases, Bob uses the MCS4 decoder with $PER_{Bob} \approx 0$, $BER_{Bob} \leq 0.1$, $SINR_{Rx,Bob} \geq 12.5$ dB while Eve attempts to decode the signal frames by using the MCS2 decoder, providing her an advantage by decreasing the radio Advantage of Bob over Eve gets about 4 dB more compared to the MCS4.

The Radio Advantage indications in the figure are given with respect of one received antenna at Eve's side.
Considering the particular propagation properties of Indoor LOS configurations and considering the low and medium values of power ratio $\rho_{SIR,Tx,Alice}$, we can note the following trends:

- At far Eve's locations, even in LOS geometry when the power ratio $\rho_{SIR,Tx,Alice}$ remains low, the radio advantage is very significant. This very favorable situation for security occurs mainly thanks to the Beam Forming (BF) that achieves significant BF rejection performance.
- We can be confident that similar trends would occur in any NLOS environments, whatever is Eve's location, because the BF rejection should be enhanced thanks to the positive effects of propagation reflectors in the neighborhood of Alice and Bob.
- When coming back to LOS configuration and considering now Eve locations closer to Bob. One has to interpret the decreasing performances of the AN-BF + SC scheme in the following sense. First, a main lobe is most often the result of LOS propagation impact to BF processing. Second, this main lobe can be intercepted by Eve. In addition, the 3 Rx of Eve in our experimental configuration can provide some array discrimination and processing gain on the data user signal. Finally the effect of BF at Alice side can be partially mitigated by Eve close to Bob. To counter this, the power ratio $\rho_{SIR,Tx,Alice}$ should be decreased down to value $\rho_{SIR,Tx,Alice} = 1/4$ (that correspond to an AN power that is 6 dB over the US power), and the antenna aperture at Alice's side should be enlarged to decrease the main lobe size and improve the rejection performances of BF.

Finally, the experimental results above are evidence that the designed secrecy schemes can be successfully implemented into real world WLAN chipsets and propagation with limited AN power in most of practical NLOS and LOS configurations.

Even, when very adverse conditions occur (LOS configurations, Eve very close to Bob or very close to Alice), secrecy efficiency can easily be achieved through a suitable tuning of the radio parameters (increasing of the AN noise, enlarging of the Alice antenna array).

7. CONCLUSION

As a summary, the proposed secrecy coding scheme ensure no information leakage when the SINR is lower than -1 dB for all designed secrecy codes. This value of the SINR can thus be considered as maximum SINR tolerated for Eve.

In addition, only a few dB of Radio Advantage (typically 3 dB to 5 dB) is required to provide reliability and secrecy to legitimate users.

These reasonable values ensure the compatibility of SC schemes with exiting AN-BF schemes and other means for providing the Radio Advantage (such as Directive Antennas at Tx, Full Duplex Communications technologies).

To the best of our knowledge, this is the first work that proposes a complete and practical secrecy coding scheme composed of outer and inner codes and combined with Artificial Noise and Beam Forming. This paper also provides several simulation results.

Our promising results, not only from theoretical channel models but also from real WiFi chipsets, are evidence that the proposed secrecy coding scheme is efficient as long as a small Radio Advantage is achieved (3 dB to 5 dB).

- The provided secrecy rate is significant (as shown table 1) even though it remains sub-optimal when compared to theoretical results in ideal case (that have no constraints on code lengths and operated in non-realistic radio channels).
- Moreover, proposed secrecy coding scheme can easily be implemented in existing wireless MIMO or MISO communication systems that propose AN-BF services (such as in many emerging WLAN, 4G and 5G standards). Once the AN-BF scheme is activated, only minor modifications of the software architecture of the nodes and terminals are required for the implementation of the secrecy coding scheme. All modifications are located at the coding stage only and remain transparent for upper protocol layers. The same simplification arguments apply for most of other "Radio Advantage technologies".

8. REFERENCES

[1] 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.

[2] Metronews, "Une énorme faille de sécurité permet d'écouter vos appels et de lire vos SMS," 22 12 2014. [Online]. Available: http://www.metronews.fr/high-tech/une-enorme-faille-de-securite-permet-d-ecouter-vos-appels-et-de-lire-vos-sms/mnlv!YnqDbOgrtHFYk/.

[3] T. Intercept, «The Great SIM Heist. How Spies Stole the Keys to the Encryption Castle,» 2015. [En ligne]. Available: https://theintercept.com/2015/02/19/great-sim-heist/.

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

[5] PHYLAWS, «www.Phylaws-ict.org,» [En ligne].

[6] 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.

[7] N. O. Tippenhauer, L. Malisa, A. Ranganathan et S. Capkun, «On Limitations of Friendly Jamming for Confidentiality,» chez 2013 IEEE Symposium on Security and Privacy (SP), Berkeley, CA, 2013.

[8] 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.

[9] E. Arikan, «A performance comparison of polar codes and Reed-Muller codes,» Communications Letters, IEEE, vol. 12, n° %16, pp. 447-449, 2008.

[10] E. Arikan, «Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels,» Information Theory, IEEE Transactions on , vol. 55, n° %17, pp. 3051-3073, 2009.

[11] I. Tal et A. Vardy, «List Decoding of Polar Codes,» Information Theory, IEEE Transactions on, vol. 61, n° %15, pp. 2213-2226, 2015.

[12] A. Balatsoukas-Stimming, M. B. Pariz et A. Burg, «LLR-Based Successive Cancellation List Decoding of Polar Codes,» IEEE Transactions on Signal Processing, vol. 63, n° %119, pp. 5165-5179, 2015.

9. BIODATAS

Christiane L. Kameni Ngassa received the "Diplôme d'ingénieur" (M.S. degree in electrical engineering) from Ecole Supérieure d'Electricité (Supelec), France, in 2011, the M.S. degree in electrical and computer engineering from Georgia Institute of Technology, USA, in 2011. From 2011 to 2014, she was a Ph.D. student at CEA - LETI, France, and received, in 2014, the Ph.D. degree in Information and Communication Sciences and Technologies from Cergy-Pontoise University, France. Since 2014, she has been a Research Engineer at Thales Communications and Security, France. Her research interests include error-correction coding, physical-layer security, and cryptography.
Dr. Kameni Ngassa has served as a Thales delegate for 3GPP and ITU standardization bodies. She has also been a European Commission expert for ICT topics since 2016.

Jean-Claude Belfiore received the "Diplôme d'ingénieur" (Eng. degree) from Ecole Supérieure d'Electricité (Supelec) in 1985, the "Doctorat" (PhD) from ENST in 1989 and the "Habilitation à diriger des Recherches" (HdR) from Université Pierre et Marie Curie (UPMC) in 2001. From 1989, he was with the "Ecole Nationale Supérieure des Télécommunications, ENST, also called "Télécom ParisTech" as a full Professor in the Communications & Electronics department. In 2015, he joined the Mathematical and Algorithmic Sciences Lab of Huawei as head of the Communication Science Department. Jean-Claude Belfiore has made pioneering contributions on modulation and coding for wireless systems (especially space-time coding) by using tools of number theory. He is also one of the co-inventors of the celebrated Golden Code of the Wi-Max standard. Jean-Claude Belfiore is author or co-author of more than 200 technical papers and communications and has served as advisor for more than 30 Ph.D. students.
Prof. Belfiore was Associate Editor of the IEEE Transactions on Information Theory for Coding Theory and has been the recipient of the 2007 Blondel Medal.

Renaud Molière is graduated from Supelec (Ecole Supérieure d'Electricité, France) in 2014 and received an MSc in Space Science and Engineering from UCL (University College London, United Kingdom) in 2013. For his studies, he was rewarded by the prizes of best overall achievement and best individual project. He joined Thales in 2014 and works on signal processing for radio communication systems both for military and civilian applications. He was involved in the Phylaws FP7 project and published several patents and publications about physical layer security.
In parallel, he is the Thales delegate for the working group SA3 in 3GPP.

François Delaveau received the M.Sc degrees from Ecole Nationale Supérieure de Techniques Avancées (ENSTA), Paris, France, in 1987, and from Mathematics University (maîtrise Paris VII - 1988; agrégation - 1990). His various activities (development, marketing support, project manager and head of laboratory...) covered several domains: radio communications, RADARS, SONARS, infra-red and Acoustic sensors and systems. Since 1997 within Thales Communications, he led researches and developments of new instruments for spectrum monitoring; of smart antennas for anti-jammed modems, direction finders and COMINT sensors (terrestrial, maritime, airborne and satellite); and of passive radars (Thales award 2007). More recently, he focused on advanced security schemes for Radio Access Technologies of wireless networks (coordinator of the EC-FP7 PHYLAWS project).
As a Thales' expert for radio communications, signal processing and electronic warfare, François Delaveau is author or co-author of numerous papers, tutorials and patents, and of several ITU-R recommendations.

Nir Shapira received a B.Sc. in Electrical Engineering and Physics (summa cum laude) from the Technion, Israel's Institute of Technology, and an MBA from the Tel-Aviv University. He is the CTO of Celeno Communications and has brought to Celeno over two decades of experience in the fields of communication theory, signal processing and wireless communications. He joined Celeno from the day of its inception and was responsible for forming the technological infrastructure and intellectual property of the company. He also represents Celeno in IEEE 802.11 standardization activities. Prior to joining Celeno, He held various managerial roles in Conexant, developing state-of-the-art wireless, DSL and voice band communication technologies. He served in an elite R&D unit of the IDF.