Wireless Pers Commun (2010) 53:329–347
DOI 10.1007/s11277-010-9950-6

A Novel Approach for Physical Layer Cryptography in Wireless Networks

L. Mucchi · L. S. Ronga · E. Del Re

Published online: 12 March 2010

Abstract Due to the enormous spreading of applied wireless networks, security is actually one of the most important issues for telecommunications. One of the main issue in the field of securing wireless information exchanging is the initial common knowledge between source and destination. A shared secret is normally mandatory in order to decide the encryption (algorithm or code or key) of the information stream. It is usual to exchange this common a priori knowledge by using a "secure" channel. Nowadays a secure wireless channel is not possible. In fact normally the common a priori knowledge is already established (but this is not secure) or by using a non-radio channel (that implies a waste of time and resource). The information is encrypted by means of a private key that must be known by both the transmitter and the receiver. One of the main weak point about security is the private key exchanging interval. The key cannot be public and cannot be known a priori. The problem is how to exchange this private key through a totally secure wireless channel. This contribution deals with the review of the main physical layer techniques for encrypting the information and the proposal of a new physical layer technique ensuring secure communication in a full wireless environment. The information is modulated, at physical layer, by the thermal noise experienced by the link between two terminals. A loop scheme is designed for unique recovering of mutual information. The probability of error/detection is analytically derived for the legal users and for the third unwanted listener (passive or active attacker). Both the case of passive and active attacks have also been implemented and simulated by using Matlab-Simulink software. The analytical results have been compared to the simulated ones. All the results show that the performance of the proposed scheme yields the advantage of intrinsic

L. Mucchi (✉) · E. Del Re
Department of Electronics and Telecommunications, University of Florence,
Via Santa Marta 3, 50139 Florence, Italy
e-mail: lorenzo.mucchi@unifi.it

E. Del Re
e-mail: enrico.delre@unifi.it

L. S. Ronga
CNIT, University of Florence Unit, Via Santa Marta 3, 50139 Florence, Italy
e-mail: luca.ronga@cnit.it

security, i.e., the mutual information cannot be physically demodulated (passive attack) or denied (active attack) by a third terminal.

Keywords Physical layer security · Modulation · Key exchange · Cryptography · Noise loop · Wireless communications

1 Introduction

Along with the rapid development of wireless communication networks, wireless security has become a critical concern. Unfortunately, security risks are inherent in any wireless technology. Some of these risks are similar to those of wired networks, some are exacerbated by wireless connectivity and some other are completely new. First, the most significant source of risks in wireless networks is that the technology's underlying communications medium, the airwave, is open to intruders. Second, mobile and handheld wireless devices are resource constrained (e.g.: battery life); hence such devices have limited transmission power and may use weaker cryptographic mechanisms for saving power, thereby making them easy targets for powerful adversaries. Third, the lack of trusted third party (TTP) or certification authority (CA) in ad hoc wireless networks pose serious challenges to identity and trust management. Fourth, multi-hop wireless network inherently assumes cooperation between nodes for packet routing and forwarding, whereas a compromised node may refuse to cooperate (by being greedy or malicious). Fifth, handheld mobile devices cannot afford the same level of physical security as an enterprise server and thus, may be easily stolen. A direct consequence of these risks is the loss of data confidentiality and integrity and the threat of denial of service (DoS) attacks to wireless communications. Unauthorized users may gain access to agency's system and information, corrupt the agency's data, consume network bandwidth, degrade network performance, launch attacks that prevent authorized users from accessing the network, or use agency's resources to launch attacks on other networks. These problems are even exacerbated in future unstructured sensors and ad-hoc networks with dynamically and rapidly varying topology.

1.1 Wireless is Different from Wired

While many security techniques developed in wired networks can be applied, the special characteristics of wireless networks call for innovative wireless security design. Since physical-layer security techniques can address directly such special wireless characteristics, they are helpful to provide boundary control, to enhance efficiency, as well as to assist upper-layer security techniques for innovative cross-layer security designs.

1.2 Wireless Secret Channel

One of the fundamental issues for physical-layer built-in security is the capacity of the transmission channel when built-in security is guaranteed without relying on upper layer data encryption. Such capacity is named secret channel capacity (SCC). The secrecy is defined as information-theoretic secrecy, i.e., the adversary's received signal gives no more information for eavesdropping than purely guessing. Information-theoretic secrecy is in fact equivalent to perfect secrecy [1]. Practically, it means null or negligibly low interception probability (LPI). Many existing physical-layer secure transmissions either can not withstand

a strict LPI analysis, or rely on encryption keys so that the security is not in the physical layer.

1.3 Public and Private Keys

In symmetric key cryptography, both parties must possess a secret key which they must exchange prior to using any encryption. Distribution of secret keys is problematic, because it involved face-to-face meeting, use of a trusted courier, or sending the key through an existing encryption channel. The first two are often impractical and always unsafe, while the third depends on the security of a previous key exchange.

The distinguishing technique used in public key cryptography is the use of asymmetric key algorithms, where the key used to encrypt a message is not the same as the key used to decrypt it. Each user has a pair of cryptographic keys, i.e., a public key and a private key. The private key is kept secret, while the public key may be widely distributed. Messages are encrypted with the recipient's public key and can only be decrypted with the corresponding private key. In public key cryptography, the key distribution of public keys is done through public key servers. When a user creates a key-pair, it keeps one key private and the other, public-key, is uploaded to a server where it can be accessed by anyone to send the user a private, encrypted, message. Unfortunately, all public-key schemes are susceptible to brute force key search attack, and cannot be said completely safe.

1.4 PHY Security

Securing a wireless communication means providing a set of privacy services to a confined set of users. The services include Authentication, Authorization, Accounting (AAA) as well as Cyphering and Integrity. Security services are mainly located at application level (es. Internet) but some solutions exist for link layer (as in WiMAX [2], Wi-Fi [3,4] and Bluetooth [5]), at network layer (as in IPSEC [6]) and at physical layer. Security at physical layer is nowadays mainly intended as the use of a spread spectrum techniques (frequency hopping, direct sequence coding, etc.) in order to avoid the eavesdropping. Eavesdropping at the physical layer refers to hiding the very existence of a node or the fact that communication was even taking place from an adversary. This means that the communication of the legal user is already on, i.e., that the authentication of the legal user has been already performed. Moreover, scrambling the information data with a code does not assure a totally secure channel, but just a long-time activity before getting the code by an unwanted listener, i.e., the security is moved on the quantity of resources (hardware, time, etc.) that the unwanted listener must have in order to get the information.

It is well known that classical encryption techniques have only unproven complexity-based secrecy [1]. We also know that strong information-theoretic secrecy or perfect secrecy is achievable by quantum cryptography based on some special quantum effects such as intrusion detection and impossibility of signal clone [7]. Unfortunately, the dependence on such effects results in extremely low transmission efficiency because weak signals have to be used. One of the recent attempts on specifying secret channel capacity is [8], where the MIMO secret channel capacity is analyzed under the assumption that the adversary does not know even his own channel. Unfortunately, such an assumption does not seem practical if considering deconvolution or blind deconvolution techniques. Moreover, such techniques are not low-complex, due to the fact that they need a high number of antennas on both sides of the radio link to correctly work. As a matter of fact, almost all existing results on secret

channel capacity are based on some kinds of assumptions that appear impractical [9–11]. It has been a challenge in information theory for decades to find practical ways to realize information-theoretic secrecy.

Moreover, one of the most weak point of wireless networks is the initial data exchange for authentication and access procedures. Initially some data must be exchanged in a non-secure radio channel or anyway by sharing a common known cryptographic key. At the moment, no physical layer techniques are present in the literature which can efficiently create a secure wireless channel for initial data exchanging between two network nodes/terminals without a priori common knowledge.

The main need is to exchange cryptographic keys between two users along an intrinsically secure radio channel. As stated before, classical encryption techniques have only unproven complexity-based secrecy. Information-theoretic secrecy or perfect secrecy is achievable by quantum cryptography, but unfortunately this technique is suitable (when applicable) only to optical networks. Derived by the Ultra WideBand (UWB) communications, the radio channel identifier (RCI) is another promising technique. But, again, the information exchanging process is not absolutely secure.

1.5 A New PHY Technique for Encrypting Information

A novel idea for low-complex intrinsic secure radio link without any a priori knowledge is here presented. One of the main advantages of this new technique is the possibility to have a physically secure radio channel for wireless systems without any a priori common knowledge between legal source and destination. This feature is particularly useful for future wireless pervasive network scenarios.

The thermal noise, received from a radio channel, has the unique property to be perfectly adapted to the transmission environment. In a traditional communication system, the information is carried by an artificial signal that is usually designed to fully exploit the available radio channel. The technique described in this paper employs a scaled and delayed version of the received noise to carry mutual information between two terminals.

1.6 Potential Applications

Potential applications of the proposed techniques are found in wireless communications systems where an initial shared secret is not available. In 4G systems as an example, roaming users accessing local services are usually able to provide a strong identity credential (via the manufacturer's embedded certificate) but may not have any authorization agreement with the hosting system. In that case a secure channel cannot be established with ordinary techniques, while is possible with the proposed one. Moreover, since the initial coupling between terminals is obtained through delays, in a context where the desired user has a known geographical position (i.e. a tactical scenario), a secured channel can be established without any additional information. Once the secure channel is established, an unwanted listener is unable to decode the flowing information even if it reveals the user's position.

1.7 Noise Loop: How it Works

Due to the intrinsic unique nature of the thermal noise along each radio link between the specific transmitter and the specific receiver, this novel technique is particularly suitable for secure communications and privacy. Moreover, it acts at the physical layer level, reducing the

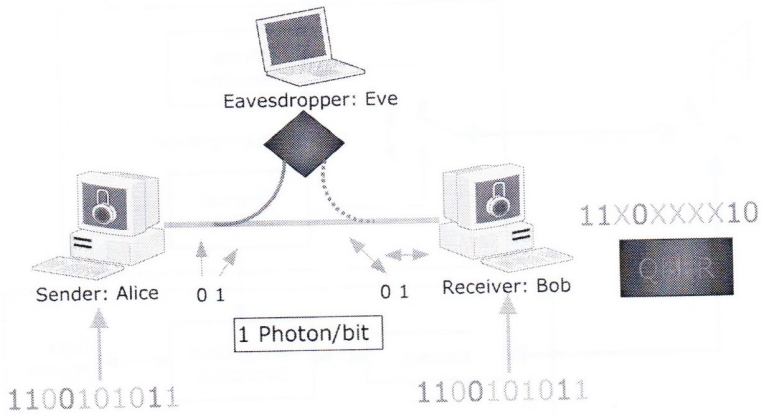

Fig. 1 Quantum cryptography

costs compared to the (sometimes) complex security algorithms that level 2 and 3 must apply to the information. Finally, it is important to highlight that the proposed technique does not assure any mechanism of identification of the user. The identification process must be controlled by the higher level, but nothing else than this because the information is made secure by the physical layer itself, i.e., the transmission cannot be demodulated by an unwanted user.

The information is modulated, at physical layer, by the thermal noise experienced by the link between two terminals. A loop scheme is designed for unique recovering of mutual information. All results show that the mutual information exchanged by the two legal terminals cannot be demodulated or denied by a third terminal. At the same time the two legal users do not suffer from the presence or not of a third unwanted user from the performance point of view.

A review of the main physical layer techniques for secret key distribution is reported in the following sections. Then the novel technique is described and detailed.

2 Quantum Cryptography

The quantum cryptography [12], or quantum key distribution (QKD), method uses quantum mechanics to guarantee secure communication (Fig. 1). It enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages. The process of measuring a quantum system in general disturbs the system and thus render the information unreadable. A third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies. Nowadays, quantum cryptography is only used to produce and distribute a key, not to transmit any message data. This method is suitable only for optical networks. If the optical network is wireless, a high-SNR line of sight is mandatory, which makes the method not properly flexible for real applications.

3 Channel Identifier

This technique [13] is based on transmitting a short pulse and measuring the channel impulse response (Fig. 2). The impulse response of the channel between the two users can be the encryption key of the transmission. The procedure can be summarized as follows:

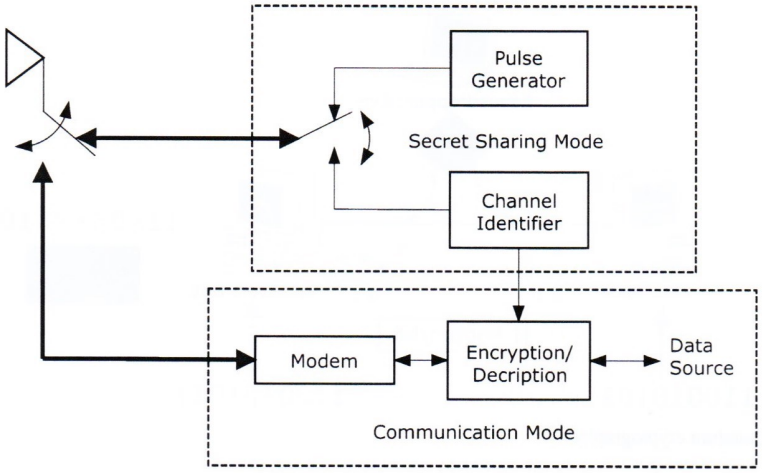

Fig. 2 Channel identifier method

- Each radio terminal (the two legal users, for example) transmits an identical signal.
- Each user observes the channel impulse response of the channel.
- The users exchange some information about what they observed, e.g., part of the sampled channel impulse response that have been observed previously.
- The users use a public channel to determine the channel identifier (the encryption key, i.e., the shared secret).
- The users begin communicating data, encrypting it using the channel identifier as a key.

Mainly, this method is based on the assumption that a third radio in a different location will observe a different channel impulse response, and that the channel is reciprocal. If two users transmit the same pulse and possess identical receivers, then the observed channel impulse response can act as a source of common randomness for secret key generation. The main drawbacks of this method is that the two users still have to share some information through a non-secure channel, and again the users have to share a common knowledge in other to build a secure shared secret.

4 MIMO

One of the recent attempts on specifying secret channel capacity by using MIMO (Multiple Input Multiple Output) technique [14]. The mobile terminals are equipped with multiple antennas, N transmitting and M receiving (Fig. 3). The symbol is encrypted by using the matrix $N \times M$ of channel impulse responses provided by the multiple channels [15], [16]. A valid way to guarantee a high error rate for the eavesdropper is to prevent it from channel estimation. In terms of channel estimation, the legal receiver has no advantage over the eavesdropper. Therefore, our objective is to design a transmission scheme so that the legal receiver can detect signals without channel knowledge, which can be realized by shifting the channel estimation task from the receiver to the transmitter. Once the transmitter has the channel knowledge, it can adjust the MIMO transmission so that the receiver does not need to estimate channel in order for symbol estimation. Reciprocity of the forward and backward channels is normally used. The receiver first transmits a pilot signal to the transmitter using

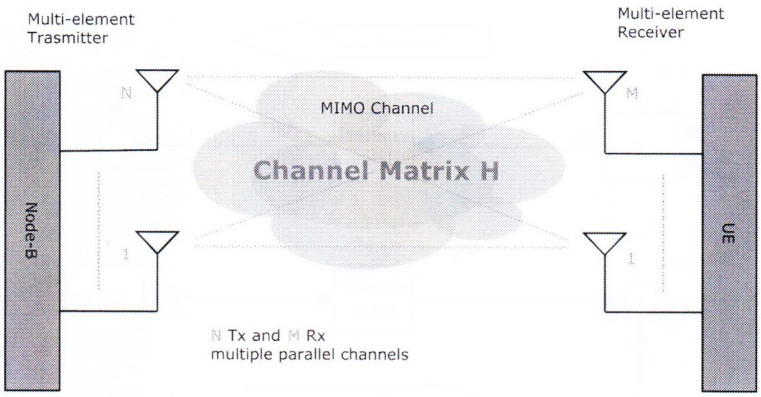

Fig. 3 MIMO method

the same carrier frequency as the secret channel, during which the transmitter can estimate the backward channel, and use it for array transmission. Such techniques are not low-complex, due to the fact that they need a high number of antennas on both sides of the radio link to correctly and securely work. Moreover, the two legal hosts are forced to exchange information (the initial pilot channel, in a non-secure channel) which can be exploited by the eavesdropper.

5 The Noise-Loop Transmission Chain

In order to illustrate the proposed technique, let us suppose two terminals exchanging information: terminal 1 and terminal 2. Two different channels are considered: one for the link from terminal 1 to terminal 2 and one for the reverse link. The two channels are considered on different frequency bands and the thermal noise on one link is considered uncorrelated with the other.[1] Each link is modeled as a conventional AWGN channel.

5.1 Symbols in the Paper

The following symbols have been adopted in the paper:

- b_i binary antipodal ($b_i \in \{-1; +1\}$) information signal originating form terminal i,
- $n_i(t)$ Gaussian, white, continuous time random processes modeling the received noise at the receiver on terminal i, characterized by zero mean and variance σ_n^2,
- α_i global link gain ($0 < \alpha < 1$) for the signal generated from terminal i. It includes transmission gain, path loss and channel response. It is also supposed to be known by the receivers,
- τ_p propagation delay for the channel. It is assumed without loss of generality that both forward (1 to 2) and reverse (2 to 1) links have the same delay,
- $y_i(t)$ baseband received signal available at the terminal i

[1] This is a very mild assumption in radio communications.

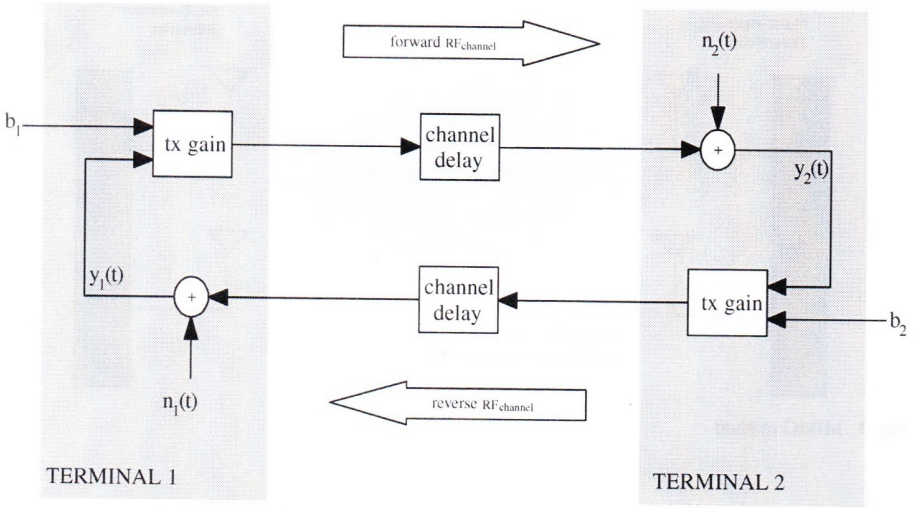

Fig. 4 Noise-loop chain scheme. Two terminals communicates by using the noise loop. The parameters in the scheme are explained at the beginning of the Sect. 5.1

5.2 Transmission Chain

In this simple transmission system the terminal operations are described in the Fig. 4. The signal from the inbound channel is modulated by the information and re-transmitted on the outbound channel. The reception is obtained by extracting the sign of the $2\tau_p$-delayed auto-correlation term of the incoming signal, multiplied by the own informative bit. The whole process is detailed in the following sections.

Let us focalize without loss of generality on the user terminal 1.

The reception, i.e., the extraction of the information bit b_2, is obtained by extracting the sign of the $2\tau_p$-delayed autocorrelation term of the incoming signal, multiplied by the own informative bit b_1. Hence, the instantaneous $2\tau_p$-delayed auto-correlation term is given by :

$$
\begin{aligned}
& y_1(t)y_1(t-2\tau_p) \\
&= \left[\sum_{j=0}^{\infty}(b_1b_2\alpha_1\alpha_2)^j n_1(t-2j\tau_p) + \sum_{j=0}^{\infty}(b_1b_2\alpha_1\alpha_2)^j b_2\alpha_2 n_2(t-(2j+1)\tau_p)\right] \\
&\times \left[\sum_{j=0}^{\infty}(b_1b_2\alpha_1\alpha_2)^j n_1(t-2(j+1)\tau_p) + \sum_{j=0}^{\infty}(b_1b_2\alpha_1\alpha_2)^j b_2\alpha_2 n_2(t-(2j+3)\tau_p)\right] \quad (1)
\end{aligned}
$$

5.3 Stationary Signal Analysis in Unlimited Bandwidth

In this section a stationary condition on the system inputs is analysed.[2] Due to the additive nature of the model, the received signals $y_1(t)$ available at terminal 1, after infinite loop iterations, is defined by the following series:

[2] By stationary we intend a constant behavior over time of the information bits b_i, of the link gains and of the statistic parameters of the random processes involved.

$$y_1(t) = \sum_{j=0}^{\infty}(b_1 b_2 \alpha_1 \alpha_2)^j n_1(t - 2j\tau_p) + \sum_{j=0}^{\infty}(b_1 b_2 \alpha_1 \alpha_2)^j b_2 \alpha_2 n_2(t - (2j+1)\tau_p) \quad (2)$$

An analogue expression can be obtained for $y_2(t)$ simply exchanging the subscript 1 and 2 in (2).

The first term of (2) represents the recursive contribution of the received noise $n_1(t)$ through the transmission loop. The second series on the other hand, is due to the injection of the noise process $n_2(t)$ by the other terminal. It is important to note that each term appears with a different delay on the received signal.

If the noise processes $n_i(t)$ are white on a unlimited bandwidth, then:

$$\mathrm{E}[n_i(t)n_j(t-\tau)] = \begin{cases} \delta(\tau)\sigma_n^2 & i = j \\ 0 & i \neq j \end{cases} \quad (3)$$

The structure of the signal in (2) draw our attention in the shifted correlation term

$$y_1(t - 2\tau_p)y_1(t) \quad (4)$$

By resorting the terms obtained by the expansion of the above expression, the expectation of the autocorrelation in (4) can be written as following

$$\mathrm{E}[y_1(t - 2\tau_p)y_1(t)] = b_1 b_2 \sigma_n^2 (1 + \alpha_2^2) \sum_{j=0}^{\infty}(\alpha_1 \alpha_2)^{2j+1} + \mathrm{E}[\text{residual cross correlation terms}] \quad (5)$$

The last term in (5) is null for an ideal AWGN channel, so the described autocorrelation term is dominated by the information bearing $b_1 b_2$ term, weighted by a term which is constant in the stationary case. The term contains the information of both terminals. Since terminal 1 is depicted to detect information bits of terminal 2, it is sufficient to perform a post-multiplication by b_1 in order to estimate the sign of b_2.

The receiver at terminal 1 is illustrated in Fig. 5.

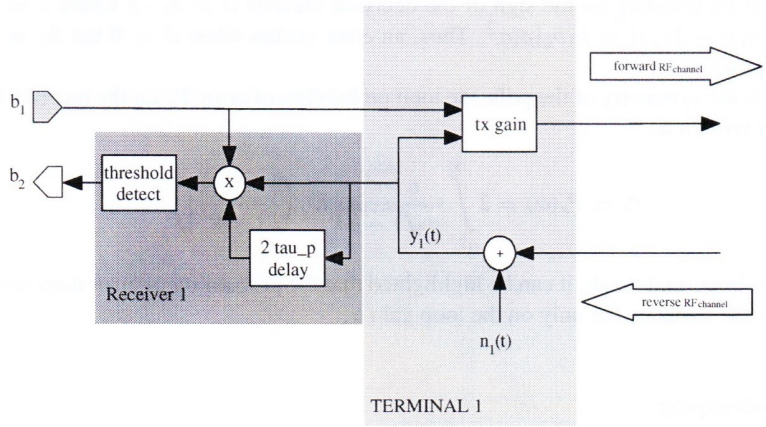

Fig. 5 Receiver scheme for terminal n.1. The first terminal demodulates the signal coming from terminal 2 (with who it is active the noise loop modulation) by using this receiver scheme colored in orange in the figure. The box named "2 tau p delay" simply acts as a delayer of $2\tau_p$ where τ_p is the channel delay between terminal 1 and 2

6 Performance Analysis on Ideal AWGN Channel

The term in (4) represents the instantaneous decision metric for the mutual information term to be estimated: $\hat{b_1}\hat{b_2}$. The performance of the proposed receiver in terms of bit error probability is related to the first and second order statistics of (4). The distribution of the unpredictable noise process, however, is no longer Gaussian.

The pdf of the stochastic process $Z = X \cdot Y$, where $X \in \mathcal{N}(\mu_x, \sigma_x)$ and $Y \in \mathcal{N}(\mu_y, \sigma_y)$, is a zero-order modified K-Bessel function:

$$p_Z(z) = \int_{-\infty}^{+\infty} p_{XY}\left(y, \frac{z}{y}\right)\frac{1}{|y|}dy = \frac{e^{\frac{z\rho}{\sigma^2(1-\rho^2)}}}{2\pi\sigma^2\sqrt{1-\rho^2}}\int_{-\infty}^{\infty}\frac{e^{\frac{1}{\sigma^2(1-\rho^2)}\left(-\frac{z^2}{2y^2}-\frac{y^2}{2}\right)}}{|y|}\mathrm{d}y$$

$$= \frac{e^{\frac{z\rho}{\sigma^2(1-\rho^2)}}}{\pi\sigma^2\sqrt{1-\rho^2}}K_0\left(\left|\frac{z}{\sigma^2(1-\rho^2)}\right|\right) \tag{6}$$

where $K_0(\cdot)$ is the second kind modified Bessel function of order zero and $\sigma = \sigma_x = \sigma_y$ is the standard deviation of the Gaussian processes. In our system, where $x = y_1(t)$ and $y = y_1(t - 2\tau_p)$, it is easy to derive that $\rho = b_1 b_2 \alpha_1 \alpha_2$.

The decision term in (4) is characterized by a probability density function defined by (6). The mean value of the decision variable (4) is

$$E[y_1(t)y_1(t-2\tau_p)] = b_1 b_2 \alpha_1 \alpha_2 \frac{\sigma_n^2(1+\alpha_2^2)}{1-\alpha_1^2\alpha_2^2} \tag{7}$$

where $\sigma_n^2 = var[n_1(t)] = var[n_2(t)]$ is the variance of the thermal noise processes involved in the loop. The relation between σ_n and σ is

$$\sigma^2 = var[y_1(t)] = var[y_1(t-2\tau_p)] = \frac{\sigma_n^2(1+\alpha_2^2)}{1-\alpha_1^2\alpha_2^2}$$

For the sake of simplicity, let us assume hereby that $\alpha_1 = \alpha_2 = \alpha$, assumed that $0 < \alpha < 1$.

Supposing a binary antipodal signalling (BPSK) modulation, the receiver 1 demodulates the bit b_2 by deciding on the sign of the decision variable $d = b_1 \cdot s$ where $s = E[z] = E[y_1(t)y_1(t-2\tau_p)] = b_1 b_2 |\rho| \sigma^2$. Thus, an error occurs when $d > 0$ but $b_2 = -1$ and $d < 0$ but $b_2 = 1$.

Due to the symmetry of the pdfs, the total probability of error P_e for the receiver terminal 1 can be written as

$$P_e = P_e(\alpha) = 2\int_{\alpha^2}^{\infty}\frac{e^{\frac{-\alpha^2 z'}{1-\alpha^4}}}{\pi\sqrt{1-\alpha^4}}K_0\left(\left|\frac{z'}{1-\alpha^4}\right|\right)dz' \tag{8}$$

As a first important result, it can be highlighted that the probability of error does not depend on the noise variance but only on the loop gain α.

7 Eavesdropping

The main scope of an intrinsic secure communication is to provide that an unwanted third party is not able at all to demodulate the information exchanged by terminal 1 and 2. Normally this security is provided by complex cryptography and procedures at higher layers level. In