a wireless network the initial access of a user implies the exchange of a encryption key from the base station (BS) to the mobile terminal (MS). This private key is sent by BS by using a public key, during the initial period of authentication. Once the user is authenticated, he'll use the private key to encode its information. The weak point is the authentication period and the exchanging of the private key. An unwanted third listener could steel the private key during that period. In a future full-wireless world, where the user is seen to be always connected and immerse in multiple wireless networks, the problem of secure authentication throughout different wireless systems is a hard task to be provided by a procedure. To solve this problem, a new approach is here proposed. The main idea is to render intrinsically secure the physical link by modulating using the noise loop as discussed in the above sections.

Let us assume hereby that a third unwanted user is listening the transmission of terminal 1. The terminal 3 can be supposed, without loss of generality, to have a different propagation delay $\tau_{p3} \neq \tau_p$ and an independent thermal noise process $n_3(t) \neq \{n_1(t), n_2(t)\}$. The terminal 3 tries to demodulate the information bit b_2 coming from terminal 2 to terminal 1 by using a receiver scheme similar to the one depicted in Fig. 6. The best choice of the unwanted user is to perform a correlation $y_1(t)y_1(t - 2\tau_{p3})$ and decide on the sign of its mean value $E[y_1(t)y_1(t - 2\tau_{p3})]$.

The mean value of the $2\tau_{p3}$-shifted correlation $\bar{y}_1(t)\bar{y}_1(t - 2\tau_{p3})$ can be derived to be

$$E[\bar{y}_1(t)\bar{y}_1(t - 2\tau_{p3})] = \begin{cases} \frac{b_1^k b_2^k \sigma_n^2 (\alpha_1\alpha_2)^k (1+\alpha_2^2)}{1-\alpha_1^2\alpha_2^2} & \text{if } \tau_{p3} = k\tau_p,\ k \in \mathcal{N} \\ 0 & \text{if } \tau_{p3} \neq k\tau_p,\ k \in \mathcal{N} \end{cases} \tag{9}$$

Another important result can be highlighted here: the decision variable of the third unwanted party depends on the multiplication of the information bits b_1 and b_2, both unknown at the unwanted listener.

In the best case (for user 3), i.e., when $\tau_{p3} = k\tau_p$, the decision variable of the third user is $z_3 = \frac{b_1^k b_2^k \sigma_n^2 (\alpha_1\alpha_2)^k (1+\alpha_2^2)}{1-\alpha_1^2\alpha_2^2} = b_1^k b_2^k \bar{z}_3$.

This result means exactly that the third unwanted listener is not able at all to demodulate the information exchanged between user 1 and 2. This impossibility is intrinsic in the modulation method at physical layer level.

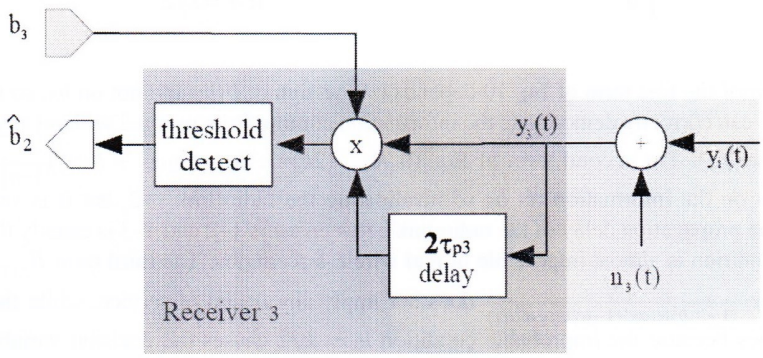


Fig. 6 Receiver scheme for the third unwanted listener. The unwanted user n.3 tries to demodulate the signal exchanged between legal user n.1 and n.2 by using the scheme depicted in this figure. In particular, we supposed that the user n.3 tries to demodulate the bit coming from user n.2, without loss of generality. The receiver scheme is similar to the one used by user n.1 (see Fig. 5)

Due to the fact that the third unwanted party experiences a different delay $\tau_{p3} \neq \tau_p$ and a different noise process $n_3(t) \neq n_1(t) \neq n_2(t)$, the delayed (shifted) autocorrelation of the receiving signal has no possibility to take the knowledge of the information bit b_2 or, symmetrically, b_1. In fact, the decision variable is permanently zero (that implies a probability of error equal to 1/2) or, in the lucky case, the decision variable is always dependent on the product between the unknown information bits $b_1 \cdot b_2$ and hence to know an information stream (for example b_2) is mandatory to know the other b_1.

8 Denial of Service

Another very important task for wireless security is the avoidance of the denial of service by an unwanted third user. A third user could insert into the communication system and although it is not able to correctly detect the information exchanged between the two legal users, it could actively trying to communicate (in some ways) aiming to disturb/deny the radio link between the legal users.

We have studied the case of a third unwanted user which actively starts a communication (using the noise loop itself) with one of the legal user. The scheme provides that the user n.3 (unwanted) tried to actively connect to the user n.1 in order to demodulate or deny the communication between legal user n.1 and n.2.

The user n.3 tries to disturb as much as possible the radio link between legal users n.1 and n.2 by actively starting a noise loop modulated communication towards user n.1. The scheme of the system in this case is reported in Fig. 7.

We aim to extract the decision variable of user n.1 $R_{y_1 y_1}(2k)$ in order to see if the legal user n.1 suffers from the presence of the unwanted user n.3 communication. By solving the system we finally obtain

$$R_{y_1 y_1}(2k) = \begin{cases} b_1 b_2 \frac{\alpha_1 \alpha_2 (1+\alpha_2^2+\alpha_3^2)(1+\alpha_1^2\alpha_3^2-\alpha_1^2\alpha_2^2)}{(1-\alpha_1^2\alpha_2^2-\alpha_1^2\alpha_3^2)^2}\sigma_n^2 & \text{if } h \neq k,\ h \neq 2k,\ h \neq k/2 \\ b_1\alpha_1(b_2\alpha_2 + b_3\alpha_3)\frac{\sigma_e^2}{1-\alpha_1^2\alpha_2^2-\alpha_1^2\alpha_3^2} & \text{if } h = k \\ b_1 b_2 \alpha_1 \alpha_2 \frac{\sigma_e^2}{(1-b_1 b_3 \alpha_1 \alpha_3)(1-\alpha_1^2\alpha_2^2-\alpha_1^2\alpha_3^2)} & \text{if } h = 2k \\ 0 & \text{if } h = k/2 \end{cases} \tag{10}$$

The sign of the first term of Eq. 10 depends on the sign of $b_1 b_2$ and not on b_3, so the legal user n.1 can correctly demodulate the information coming from user n.2 without any disturb from user n.3. The second term of Eq. 10 $R_{y_1 y_1}(2k) = b_1\alpha_1(b_2\alpha_2 + b_3\alpha_3)\frac{\sigma_e^2}{1-\alpha_1^2\alpha_2^2-\alpha_1^2\alpha_3^2}$ depends on the information bit b_3 so invalidating the radio link 1–2, but it is valid only when the propagation delay of the radio link between users 1–2 and 1–3 is exactly the same. This condition is almost impossible in real wireless scenarios. The third term $R_{y_1 y_1}(2k) = b_1 b_2 \alpha_1 \alpha_2 \frac{\sigma_e^2}{(1-b_1 b_3 \alpha_1 \alpha_3)(1-\alpha_1^2\alpha_2^2-\alpha_1^2\alpha_3^2)}$ does not imply any denial of service, while the fourth term does because the improbable condition $h = k/2$ causes the decision variable to be zero. The presence of two very particular points which can cause denial of service (DoS) should not create panic because those situations are incredibly improbable and moreover the two legal users, once the noise loop modulation is started, can exchange a locally generated additional delay in order to avoid such dangerous situations.

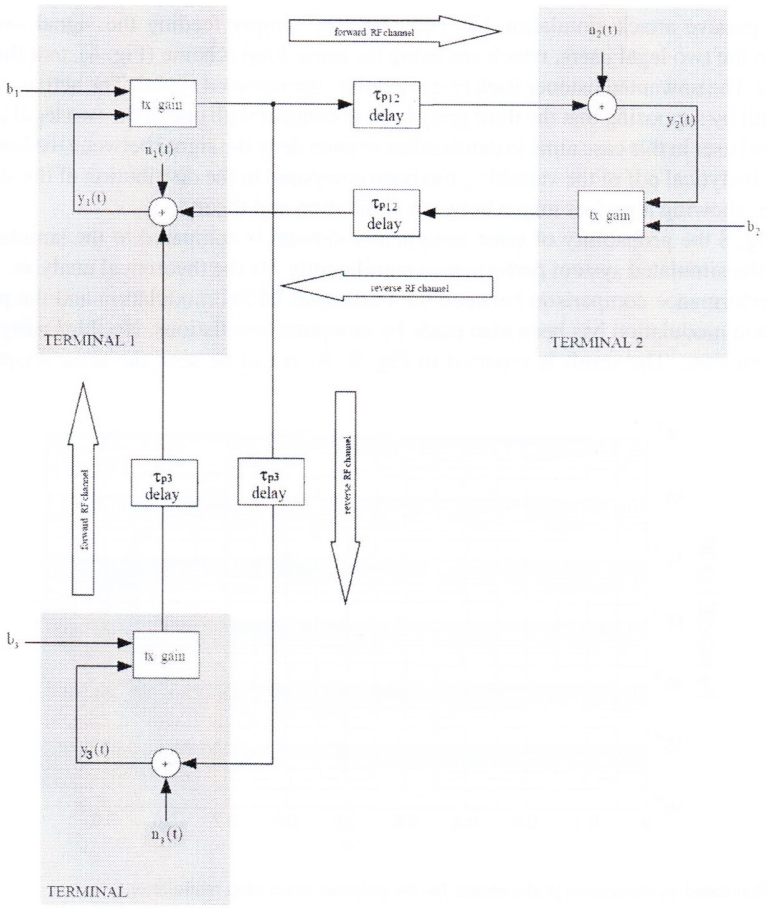


Fig. 7 Loop scheme for the third unwanted user: active attack case. The scheme shows the user n.3 which tries to actively connect to user n.1 in order to demodulate or deny the communication between legal user n.1 and n.2.

9 Simulation Results

The noise loop depicted in Fig. 4 has been also implemented by using MATLAB-Simulink software. In particular, both the passive attack (the third unwanted user trying to simply demodulate the data exchanged by the two legal users and the active attack (the third unwanted user now actively transmits into the radio link of the two legal user in order to deny the service or demodulate the information have been simulated as they should be in the real.

The simulation results have been compared to the analytical results previously illustrated. Simulations have been run with the following parameters:

- a ratio between the bit time and the propagation delay equal to $\frac{T_b}{\tau_p} = 10$,
- a thermal noise variance $\sigma_n^2 = 0.125$,
- a propagation delay for the third unwanted user τ_{p3} randomly chosen in the interval $(\tau_p, 5\tau_p)$ following a uniform distribution,
- a number of bit equal to 80,000 and
- 100 Monte Carlo runs for each simulation.

The passive attack simulation has been built by simply feeding the signal exchanged between the two legal users, which are using the noise loop scheme (Fig. 4), to a third party receiver. The unwanted listener tried to demodulate the received signal. The active attack has been built by supposing that the third party tried to connect with one of the two legal user. The unwanted user in this case aims to demodulate or even deny the signal between the legal users.

The analytical pdf of the variable z has been compared to the distribution of the simulated vector z, showing a perfect match between simulation and theory.

In Fig. 8 the probability of error analytically derived is compared to the simulated one. Again, the simulated system performance significantly fits the theoretical analysis.

A performance comparison between the traditional BPSK modulation and the proposed noise loop modulation has been also made by computer simulations. No third party is present in this case. The result is reported in Fig. 9. As it can be seen the noise loop scheme

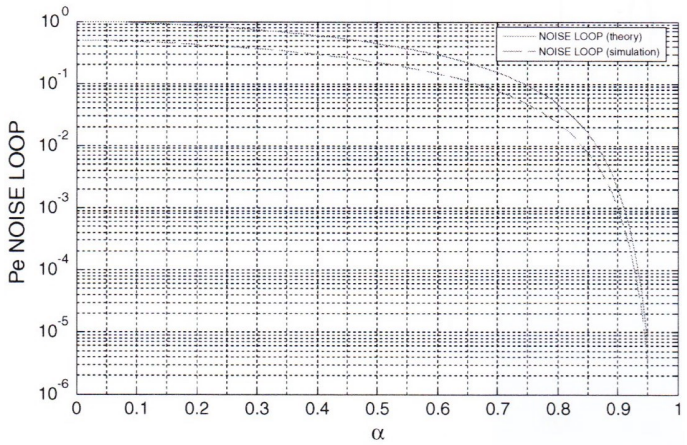


Fig. 8 Simulated vs theoretical performance for the propose noise loop modulation

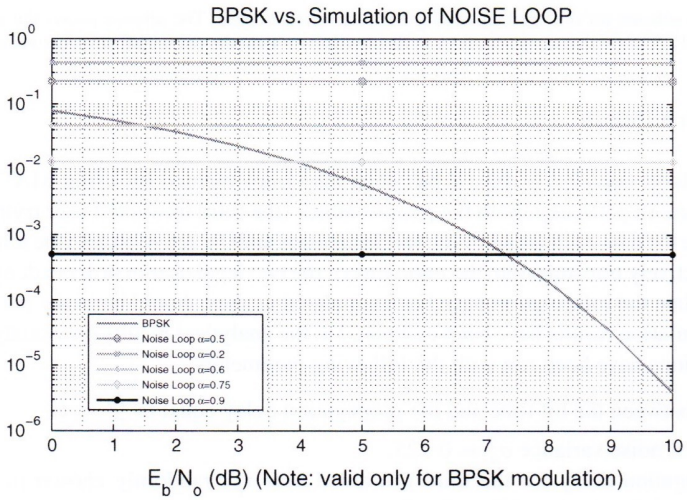


Fig. 9 Simulated performance comparison between the traditional BPSK and the proposed noise loop modulation. Note that noise loop scheme is independent of the noise power, but depends only of the noise loop gain α

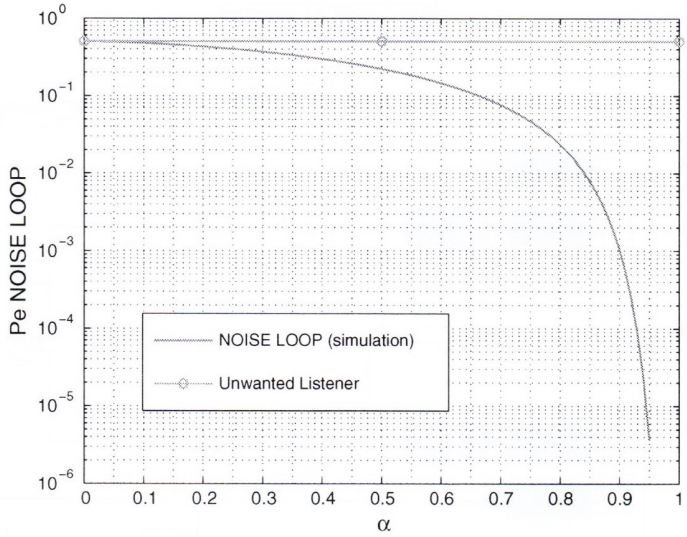


Fig. 10 Simulated performance comparison between the probability of error of the legal user using noise loop modulation, e.g. user n.1, and the third unwanted listener, user n.3

has a probability of error independent by the thermal noise power. Moreover, increasing the noise loop gain α the performance of the noise loop scheme can overcome the traditional modulations for low SNRs.

When a third party is present in the system, it can be passive or active. If passive, it simply stores the signal exchanged between the two legal users and tries to demodulate it. In Fig. 10 the probability of error of the third party receiver is reported. The user n.3 experiences a constant probability of incorrect decision equal to $4.5 \cdot 10^{-1}$ that means the impossibility of detection of the symbols. On the contrary, the legal user, e.g. user n.1, has a decreasing probability of error with the noise loop gain α.

As it can be seen a third unwanted listener experiences an almost constant probability of error $P_{e3} \simeq 0.5$ for antipodal signalling, as depicted in Fig. 10. A probability of error equal to 0.5 means a probability of correct detection of the information equal to 0.5, that in the case of BPSK modulation (bit $b = \pm 1$ with probability 0.5) of the information means a total uncertain, i.e., a perfect SCC or information-theoretic secrecy.

When the third party is active, it transmits its unwanted signal towards one of the two legal user in order to deny the service or degrade the demodulation of the signal by the other legal receiver.

The performance of the legitimate receiver has been simulated with and without the active attacker. The results show that an active attacker does not cause the performance degradation of the legal user, i.e., no denial of service is possible.

10 FPGA Implementation

The proposed TX/RX scheme has been implemented on a Xilinx Virtex II FPGA to evaluate the real computational complexity and to prove the validity of data detection on a fixed point signal processing system. The transmission, reception and baseband processing branches for two terminals have been implemented in VHDL using Xilinx System Generator tool. The

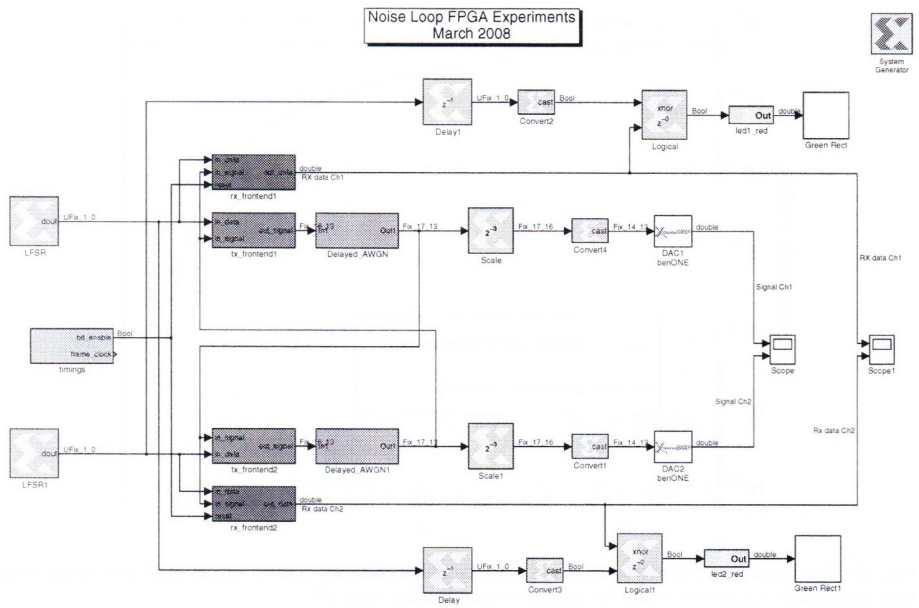


Fig. 11 FPGA implementation: Simulink model of noise-loop transmission chain

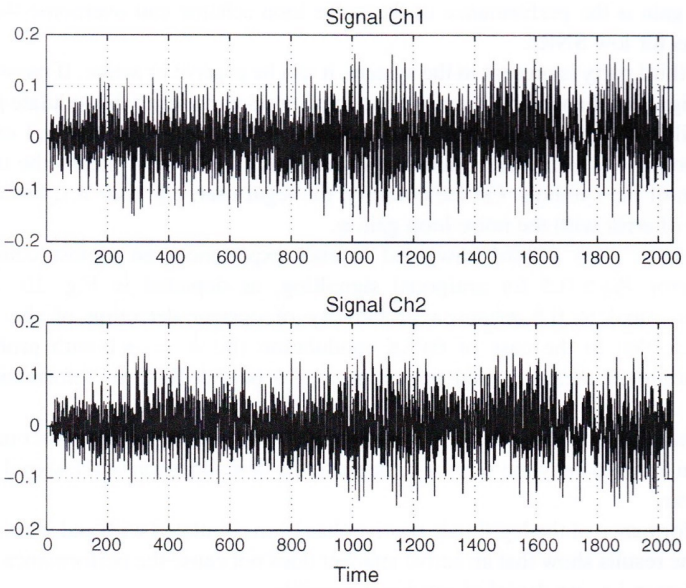


Fig. 12 FPGA implementation: baseband signals for forward and reverse channel

Matworks Simulink model of the implemented chain is represented in Fig. 11. The model includes two PN-sequence generators to emulate the transmitted data from both terminals, a timing section, the TX and RX frontends, a delayed AWGN emulator, and other performance evaluating blocks. The baseband signal generated by the two noise-loop terminals are represented in Fig. 12 for both forward and reverse channels (respectively Ch1 and Ch2). The

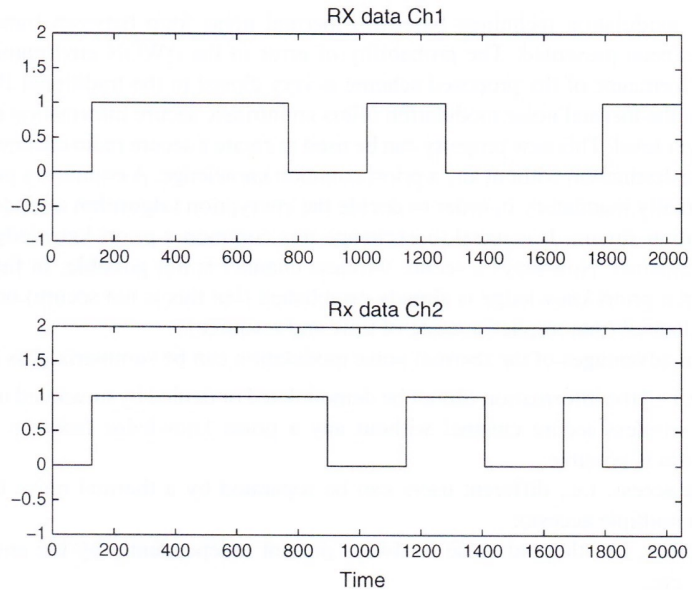


Fig. 13 FPGA implementation: detected data from both receivers

Table 1 FPGA utilization (total and fraction of Xilinx Virtex II xc2vp30-5ff1152 resources)

FPGA resource	TX module	RX module
Multipliers (MULT)	1 (0.7%)	3 (2.2%)
Look-up tables (FGs)	136 (0.4%)	42 (0.1%)
Arithmetic logic (CYs)	75 (0.2%)	40 (0.1%)
Storage Elements (DFFs)	68 (0.2%)	165 (0.6%)

detected data is reported in Fig. 13. No visible correlation can be found with the baseband signal of Fig. 12, confirming the assumptions made in the theoretical sections of this work.

The complexity of the proposed implementation is reported in Table 1. As shown both the transmitter and receiver blocks use a very small portion of the used FPGA, though framing and synchronization have not been addressed yet.

11 Conclusions

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 manufacturers 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 users position.

A novel modulation technique based on thermal noise loop between transmitter and receiver has been presented. The probability of error in the AWGN environment showed that the performance of the proposed scheme is very closed to the traditional BPSK transmission, but the thermal noise modulation offers an intrinsic secure information exchange at physical layer level. This new property can be used to create a secure radio channel between a source and a destination without any a priori common knowledge. A common a priori knowledge 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 main advantages of the thermal noise modulation can be summarized as follows:

- security, i.e., the information cannot be demodulated or denied by unwanted users; moreover, a wireless secure channel without any a priori knowledge between source and destination is possible;
- multiple access, i.e., different users can be separated by a thermal noise basis (noise division multiple access);
- applicability, i.e., thermal noise is always present independently by the environments, devices, etc.

References

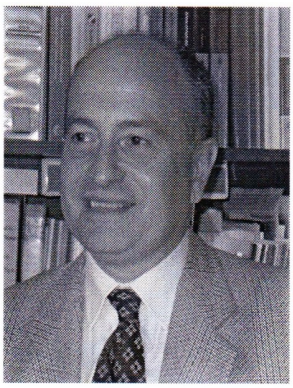
1. Shannon, C. (1949). Communication theory of secrecy systems. *Bell System Technical Journal, 29*, 656–715.
2. IEEE 802.16-2004. (2004). IEEE standard for local and metropolitan area networks part 16: Air interface for fixed broadband wireless access systems.
3. ANSI/IEEE Std 802.11. (1999). Wireless LAN medium access control (MAC) and physical layer (PHY) specifications.
4. IEEE Std 802.11i. (2004). Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, amendment 6: Medium access control (MAC) security enhancements.
5. IEEE Std 802.15.1. (2005). IEEE standard local and metropolitan area networks–part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs).
6. Kent, S., & Seo, K. (2005). Security architecture for the internet protocol, internet engineering task force, RFC 4301.
7. Bennett, C. H., & Brassard, G. (1984). *Proceedings of IEEE international conference on computers systems and signal processing, Bangalore, India*, pp. 175–179
8. Hero, A. O., III. (2003). Secure space-time communication. *IEEE Transactions on Information Theory, 49*(12), 3235–3249.
9. Maurer, U. (1993). Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory, 39*(3), 733–742.
10. Wyner, A. D. (1975). The wire-tap channel. *Bell System Technical Journal, 54*(8), 1355–1387.
11. Csiszar, I., & Korner, J. (1978). Broadcast channels with confidential messages. *IEEE Transactions on Information Theory, 24*(3), 339–348.
12. Sharbaf, M. S. (2009). Quantum cryptography: A new generation of information technology security system, information technology: New generations. ITNG '09. Sixth international conference on, 27–29 April, pp. 1644–1648.
13. Wilson, R., Tse, D., & Scholtz, R. A. (2007). Channel identification: Secret sharing using reciprocity in ultrawideband channels. *IEEE Transactions on Information Forensics and Security, 2*(3), 270–275.
14. Hyungjin, K., & Villasenor, J. D. (2008). Secure MIMO communications in a system with equal numbers of transmit and receive antennas. *IEEE Communications Letters, 12*(5), 386–388.
15. Li, X., & Ratazzi, E. P. (2005). MIMO transmissions with information-theoretic secrecy for secret-key agreement in wireless networks. IEEE military communications conference (MILCOM'2005) Atlantic City, NJ, Oct. 17–20.

16. Mohammadi, M. S. (2009). MIMO minimum leakage—physically secure wireless data transmission, application of information and communication technologies. AICT 2009. International Conference on, 14–16, pp. 1–5.

Author Biographies

L. Mucchi (lorenzo.mucchi@unifi.it) received the M.S. Degree (Laurea) in Telecommunications Engineering from the University of Florence (Italy) in 1998 and the Ph.D. in Telecommunications and Information Society in 2001. His main research areas are spread spectrum techniques (UWB, CDMA, etc.), cooperative communication systems, cognitive radio, wireless security, MIMO and diversity techniques and multi-satellite communications. He has published a chapter in 3 international books, 13 papers in international journals and 55 papers in international conferences during his research activity. Lorenzo Mucchi is also a full member of the Institute of Electrical and Electronics Engineers (IEEE).

L. S. Ronga [IEEE S89-M94-SM04] received his M.S. degree in electronic engineering in 1994 and his Ph.D. degree in telecommunications in 1998 from the University of Florence, Italy. In 1997 joined the International Computer Science Institute of Berkeley, California, as a visiting scientist. In 1998 obtained a post-doc position in the engineering faculty of the University of Florence. In 1999 he joined Italian National Consortium for Telecommunications, where he is currently head of research. He has been leader of national and international research groups. He authored over 50 papers published in international journals and conference proceedings. He has been editor of EURASIP Newsletter for 4 years.



E. Del Re was born in Florence, Italy, since 1975 he has been with the Department of Electronics Engineering of the University of Florence, Florence, Italy, first as a Research Assistant, then as an Associate Professor, and since 1986 as Professor. His main research interest are digital signal processing, mobile and satellite communications and communication networks, on which he has published more than 150 papers, in international journals and conferences. He is the head of the Digital Signal Processing and Telematics Laboratory of the Department of Electronics and Telecommunications of the University of Florence. He is a member of the Executive Board of the Italian Interuniversity Consortium for Telecommunications (CNIT). Professor Del Re is a Senior Member of the IEEE.