Telecommunications in the ICT Age: From Research to Applications

Marco Baldi, Giovanni Cancellieri, Franco Chiaraluce, Adelmo De Santis, Ennio Gambi and Paola Pierleoni

Abstract The human society in the information age deeply relies on digital information processing, communication and storage. Photonic routing and switching is expected to be exploited in future all-optical networks. Channel coding is needed in order to protect information against natural disturbances, and modern coding schemes are able to reach the ultimate limits predicted by Shannon. On the other hand, post-quantum cryptography is necessary for assuring security against cyber attackers, possibly provided with quantum computers. Source coding, especially in video data compression, is recommended for optimizing the bandwidth usage. Spread spectrum systems can solve the problem of radio transmissions over common frequency bands. These technologies are of crucial importance for the evolution of networks and of the whole Internet, allowing people to interact each other and access information in the web. Nowadays, the conventional Internet of people has moved into the pervasive Internet of Things providing innovative services in a variety of application fields. In this respect, domotic systems, based on ambient and wearable sensors, appear of dramatic importance in the design of future assisted living protocols.

M. Baldi · G. Cancellieri · F. Chiaraluce (✉) · A. De Santis · E. Gambi · P. Pierleoni
Department of Information Engineering (DII), Università Politecnica delle Marche,
Via Brecce Bianche 12, 60131 Ancona, Italy
e-mail: f.chiaraluce@univpm.it

M. Baldi
e-mail: m.baldi@univpm.it

G. Cancellieri
e-mail: g.cancellieri@univpm.it

A. De Santis
e-mail: a.desantis@univpm.it

E. Gambi
e-mail: e.gambi@univpm.it

P. Pierleoni
e-mail: p.pierleoni@univpm.it

S. Longhi et al. (eds.), *The First Outstanding 50 Years of "Università Politecnica delle Marche"*, https://doi.org/10.1007/978-3-030-32762-0_4

1 Introduction

Digital signal procedures have replaced analog signal procedures in recent years. Such a transformation is clearly evidenced in the scientific production described below. Copper cables have been progressively substituted by optical cables in the transport network. Higher and higher radio frequencies have been employed in mobile telephony and subsequently in smart-phone services. Asymmetric Digital Subscriber Line (ADSL) and Very-high-bit-rate Digital Subscriber Line (VDSL) fixed connections linked users to central offices, up to the advent of a new organization in the access network. It is actually under deployment, being constructed on a completely passive support. This new infrastructure, called Passive Optical Network (PON), will guarantee an access speed up to several Gbit/s, by means of a solution named Fiber-To-The-Home. Since early seventies, relevant contributions to the study of telecommunication service availability in transport and access networks were produced, considering a micro-coaxial cable as a support [17]. Such technology was invented in Italy and gained some success around the world before the advent of optical fibres.

A telecommunication network is supported by a geographic infrastructure over which proper transmission protocols are implemented, according with the Open System Interconnection (OSI) 7-layer model, with particular attention to the first four layers. Any future evolution has to take into account that public services must be guaranteed to all the users with neutral access assurance. On such goals the true concept of Next Generation Network can be developed. This philosophy is a common element in what follows.

Such a digital revolution has implied significant advancements in various topics of the telecommunication world, that will be presented in the following sections. More precisely, the organization of the chapter is as follows. Section 2 deals with the study of optical transmission on multimode and monomode fibers. Optical switching and photon counting techniques are also discussed. Section 3 is devoted to reliable and secure digital transmissions. Channel error correcting codes are employed for assuring reliability and a secure physical layer is modelled against various types of cyber attacks. In particular, post-quantum cryptography based on proper codes is suggested for saving double-key cryptosystems from quantum computer threats. In Sect. 4 advanced systems for monitoring human activities in ambient assisted living are presented. They are based on TV signals, image recognition and data collection from distributed sensors. Section 5 is finally dedicated to interactions in wireless sensor networks, with particular attention to Internet of Things (IoT) applications.

2 Optics and Optical Communications

Research on optics and optical communications starts from an accurate description of the transmission medium and the electro-optical devices acting on it, then accounts for the systems and the networks which can be set up, finally faces the optimization in optical data packet routing and delivery. We can identify three main issues:

- multimode optical fibers and related optical sources with experimental measurements and tests;
- single-mode optical fibers and all-optical switching;
- optical networks and protocols.

All these aspects exploit the particular features which characterize an optical carrier for information transfer, which can be summarized in: high speed, good reliability, strong resilience against possible unauthorized information manipulation.

The study of time dispersion in multimode optical fibers has been exhaustively developed [20], considering also a proper diffusion equation for taking into account mode coupling [29]. Ray optics represents a valid model in order to simplify the description of optical power evolution along the fiber length on the trajectories imposed by a proper refractive index profile, when the propagating modes are in the order of some thousands [21, 24]. A double-α graded index profile has been proposed with the purpose of optimizing time dispersion performance [22]. This design solution is able to relax some construction trade-offs.

2.1 Multimode Optical Fibers and Related Optical Sources

The study of top-emitting Burrus type light-emitting diodes (LEDs) was developed, considering a model based on a circularly symmetric transmission line [30]. This theory is able to explain some well known phenomena regarding a time delay in the excitation of high-order modes in a multimode optical fiber [32]. Such process could induce remarkable performance degradation.

Measurement tests were carried out in cooperation with Centro Studi—Fondazione G. Marconi. They regarded modal differential attenuation, steady state reaching in loss contributions, the role of cables and joints [25], bandwidth evaluation in the frequency domain [26]. Transmission system designs, employing multimode fibers, have been treated when such links were firstly proposed in the transport network [28]. Different combinations of sources (LEDs or lasers) and detectors (PIN or avalanche photodiode (APD)) were compared. An exhaustive analysis of multimode fiber joints and in particular of their non-reciprocal behavior has been presented in those years [27].

2.2 Single-Mode Optical Fibers and All-Optical Switching

Single-mode optical fibers were modelled since 1985, with special attention to polarization mode dispersion [37], and effective cut-off wavelength of the first higher-order mode [31, 38]. Optical coherent transmissions and enhanced birefringence in order to select a single polarization have also been studied [23]. Spread spectrum systems at optical frequencies and photon counting procedures have been proposed [19].

Soliton propagation in single-mode fibers, exploiting the presence of a high peak power ultra-short optical pulse, has been described by means of non-linear temporal Schrödinger equation [33]. Very high speeds in the data flux appeared to be achievable.

Non-linear optics for modelling optical switching has been treated in the period 1985-89 with particular reference to four-wave mixing and optical frequency conversion [34]. Such type of devices has become commercially available products only very recently. All-optical spatial soliton coupling, in order to construct a polarization modulator, has been exploited [36].

2.3 Optical Networks and Protocols

Enhanced protocols were proposed for proper implementation on optical networks [15]. A multi-layered architecture has been introduced for future transport and access optical networks [16]. Graph theory and edge coloring have been exploited for the optimization of wavelength routing algorithms. Optical propagation and fiber communication systems were reviewed in a long invited paper devoted to show the state of the art in this important field of research and applications [35].

3 Reliability and Security of Digital Transmissions

Modern digital transmissions need to be reliable and secure. Reliability is related with the requirement to have a sufficiently low error rate at the receiver, in such a way the transmitted information is correctly interpreted and can be properly used. Security is related with the requirement to protect transmitted data from illicit interception, so preventing the possibility that unauthorized receivers can disclose the data. Reliability, obviously depends on the channel and the operation conditions. However, it can be usually improved by using well-designed error correcting codes. Commonly less known is the possibility to use error correcting codes also to achieve security, which can be done at the physical level, as occurs with the so-called *physical layer security* (PLS), or at higher level, as occurs with the so-called *code-based cryptography*. These issues will be discussed in the next sections.

3.1 Channel Coding

The invention of turbo codes in 1993 [14] has been a real breakthrough for the design and optimization of error correcting codes. By effectively exploiting codes concatenation and soft-decision decoding, turbo codes are able to approach the Shannon limit in several types of different channels. The distinctive feature of turbo codes is to present two distinct behaviors for the region of small signal-to-noise ratios (SNRs) and that of high SNRs. For small SNRs, that over the additive white Gaussian noise (AWGN) channel is typically expressed as the ratio between the energy per bit E_b and the one-side spectral density of thermal noise N_0, the error rate exhibits a waterfall behavior, which means it decreases by orders of magnitude with very small increase of E_b/N_0. For large SNRs, instead, performance is dominated by the code *minimum distance* d_{min} that, in case of linear codes, like turbo codes, is coincident with the minimum Hamming weight of codewords in the code: the larger d_{min} the better the performance. To determine d_{min} for a turbo code is often a a hard task. In [53] an algorithm based on the notion of constrained subcodes is proposed which permits the computation of d_{min} for large codes without set a constraint on the input sequence weight, the latter being a common shortcut to reduce complexity, which however produces only approximate results.

The original turbo code consisted of two recursive systematic convolutional codes, concatenated in parallel and with an interleaver between. But the turbo principle has inspired updating of many other, even classic, coding schemes that, thanks to the new idea have seen a significant improvement of the performance achievable. This is the case, for example, of product codes. In [42] the authors present a thorough analytical evaluation of extended Hamming product code performance in the low error rate regime, and a complete set of techniques covering all possible cases: normal, shortened, and punctured schemes.

Turbo-like codes have been rapidly included in many international standards. Among the first to address the adoption of the new schemes, there is the standard for telemetry (TM) synchronization and channel coding in space missions. Indeed, communication to and from a spacecraft or a probe travelling in the deep space is a privileged benchmark to test the effectiveness of an error correcting scheme. Valuable examples can be found in [18] where all relevant issues, including code rates, frame lengths, modulation formats, performance metrics, complexity, and others, are discussed for TM but also telecommand (TC) signals.

At present, the error correction scene is dominated by another instance of the turbo principle, which are the so-called low-density parity-check (LDPC) codes. These codes are characterized by the fact to have a parity-check matrix with a relatively small number of symbols 1. In this case, it is more proper to speak of belief propagation (BP) as the key algorithm for the decoder to reach a consensus about the estimated value of the received bits. In our research we have investigated several variants of LDPC codes including array convolutional LDPC codes [10], interleaved product LDPC codes [9], and others, up to the most recent spatially coupled LDPC convolutional codes [11] we are currently investigating. We have also proposed inno-

vative procedures to design quasi-cyclic low-density generator-matrix (QC-LDGM) codes [7] that, through the sparsity of the generator matrix, instead of the parity-check matrix, allow to have low complexity but also error floor performance better than that offered by other codes of the same class.

3.2 Physical Layer Security

Transmission security is often implemented at protocol layers higher than the physical one, by exploiting cryptographic techniques based on computation assumptions. Examples will be given in the next section. These schemes rely on the existence of one or more cryptographic keys that must be known by legitimate users and protected from eavesdroppers. On the contrary, when security is implemented at the physical layer, all receivers are perfectly aware of the encoding and transmission procedures, without the need of any shared secret. In this case, security is only based on the differences between the channels experienced by authorized and unauthorized users. On the other hand, exploiting these asymmetries often requires knowledge of the channel, while this assumption is not required in traditional cryptography. Therefore, physical layer security can be viewed as a substrate helping to reduce the complexity of cryptographic techniques at higher layers.

A well-known model to describe a PLS scenario is the so-called *wire-tap* channel, introduced by Wyner [83] in the 70's. According to this model, a transmitter (commonly named Alice), encodes a message vector into a codeword vector before transmitting it. Alice's transmission is received by a legitimate receiver (named Bob) and an eavesdropper (named Eve), and the channel that separates Alice from Bob is generally different from that between Alice and Eve. Therefore, the vector received by Bob is different from that gathered by Eve. Alice can adopt whatever randomization, encoding and modulation scheme, and both Bob and Eve are perfectly aware of the transmission technique she uses. On the other hand, because of the channels difference, the codeword vectors that Bob and Eve obtain after decoding can also be different. PLS is achieved when:

- Bob is able to reconstruct the original message.
- The message recovered by Eve has no significant correlation with the original message.

Over an AWGN channel, this explicitly means that the SNR value over Bob's channels must be sufficiently large to ensure a very small error rate for Bob (reliability constraint), while the SNR value over Eve's channels must be sufficiently small to ensure a very high error rate for Eve (security constraint). The error correcting code used in the system helps satisfying these constraints, but it is also required to reinforce the mechanism through the implementation of suitable supporting actions. A possibility consists in using systematic but punctured codes; in [3] we have shown that better results can be obtained by using instead non-systematic codes resulted by the application of a scrambling matrix.

The study of PLS requires to go beyond the error rate analysis, referring to concepts drawn from information theory. Though conceptually unquestionable, such an approach usually considers asymptotic conditions, that is, codes with infinite length and continuous modulations, which make difficult to evaluate concrete applicability of the proposed solutions. One of the merits of our research on this topic is the fact to have investigated more practical scenarios, by introducing security metrics working in the finite block length and discrete modulation regime. An example is in [5] where, additionally, the previous analyses on the wire-tap channel is extended by considering secret transmissions over parallel channels, under the assumption of knowing Bob's channel and having only a statistical description of the Eve's channel.

3.3 Post-quantum Cryptography

Contrary to PLS, cryptography acts at protocol layers higher than the physical one. The idea, in this case, is to convert ordinary plain text into unintelligible text, storing or transmitting data in a particular form, so that only those for whom they are intended can read and process them. Even if intercepted, encrypted data are useless for an attacker, since he is not able to disclose the information they contain. Obviously, this paradigm implies the availability of strong encryption methods, able to ensure, at least, computational security, that is, to guarantee that the secrets at the basis of the encryption procedures have a negligible probability to be discovered because of the limited (though possibly very large) computational capacity owned by the attackers.

Modern cryptography relies on the adoption of symmetric or asymmetric schemes. Focusing attention on the asymmetric solution, the secret is retained by only one of the parties (e.g., the receiver). From the secret key, another key is derived, which is publicly available (not secret) and from which the secret key cannot be derived. When the sender wishes to provide a message to the receiver he uses the public key. Only the owner of the latter, however, is able to decrypt the ciphered message, thanks to the secret key he knows. The roles of the public and private keys might be interchanged, but the general principle remains the same. Widespread examples of asymmetric systems are RSA (from the names of the inventors, Rivest, Shamir and Adleman) or the system based on discrete logarithms. Focusing attention on RSA, in short its security is based on the difficulty of finding the constituent factors in the product of two (very) large integer numbers. This problem is known to have a non-polynomial complexity, at least with conventional computational approaches.

RSA is used to secure web traffic, to ensure privacy and authenticity of email, to secure remote login sessions, and it is at the heart of electronic credit card payment systems. This scenario, however, is destined to change in the near future. In fact, recent advancements in the capabilities of quantum computers, while allowing to tackle significant computational problems in operating research and computational chemistry, also open an avenue to break the mathematical trapdoors on which current widely adopted asymmetric cryptography rely. The decoding of an error-affected codeword with a general linear error correcting code occupies a prominent place

among the most promising mathematical trapdoors withstanding an attack with a quantum computer. The use of a trapdoor based on decoding of a general linear code to build a public-key encryption scheme was pioneered in 1978 by Robert McEliece [56]. Such a cryptosystem has withstood around 40 years of cryptanalysis without seeing improvements in the computational effort required to break it beyond asymptotically vanishing terms. However, the large keypair sizes of McEliece's scheme, together with the non-negligible computational requirements still provide a hindrance for its use in tightly constrained embedded environments.

We have extensively worked on the subject and we have proposed variants of the McEliece's cryptosystem based both on classic families of codes, like Reed-Solomon codes [6], and on modern quasi-cyclic low-density parity-check (QC-LDPC) codes [4], obtaining significant reductions in the keypair sizes for a prefixed value of the security level. The most dangerous threat against code-based cryptosystems using QC-LDPC codes comes from reaction attacks. These attacks are able to recover the secret key by exploiting the inherent non-zero decryption failure rate (DFR) they exhibit and receiver's reactions upon decryption failures. In [75] we have proposed a special class of codes, known as monomial codes, which make reaction attacks not applicable, while in [8] we have applied countermeasures against non-profiled power consumption side channel attacks.

4 Signals and Systems

The results of the research activities in the TLC framework may be applied in very different contexts, due to the fact that all modern technologies are based on signals acquisition, elaboration and generation. In this section the research activities in the fields of ambient assisted living (AAL) systems, spread spectrum signals and coding of video signals are shown.

4.1 Unobtrusive Monitoring of Human Activities in Ambient Assisted Living

Population ageing is a growing phenomenon, especially in Europe, so researchers are developing active and assisted living solutions to promote ageing in place of elderly people. The objective of a research on active and assisted life is to develop tools with the aim of helping older people to live independently at home. In particular, human activity recognition algorithms can help to monitor aged people in home environments. One of the most critical issues for elderly people is represented by falls, and the development of fall risk estimation and fall detection tools can increase safety of elderly. The research focused on the developing of fall risk estimation and fall detection tools using data extracted from wearable, vision-based and radar-based

sensors. The interest in radar and RGB-D sensors is related to their capability to enable contactless and non-intrusive monitoring, which is an advantage for practical deployment and users' acceptance and compliance, compared with other sensor technologies, such as video-cameras, or wearables. Furthermore, the possibility of combining and fusing information from heterogeneous types of sensors is expected to improve the overall performance of practical fall detection systems [43, 46, 54], even if problems of synchronization arise [47]. However, the availability of skeleton joints simplifies the process of feature extraction from RGB-D frames, and this feature fostered the development of activity recognition algorithms using skeletons as input data, whose performances are evaluated on a large-scale dataset, through support vector machine (SVM) classification [44, 45]. Along with remote health monitoring, technological solutions remote assistance activities, like those related to chronical diseases, are of interest, and may be satisfied through a remote interaction with the patient, without a direct medical examination. Moving from these considerations, a system architecture is proposed for the provision of remote healthcare to the elderly, based on a blind management of a network of wireless medical devices, and an interactive TV set top box for accessing health related data [76, 81]. The selection of TV as the interface between the user and the system is specifically targeted to older adults. The idea is to create a unique interface towards both a cloud-based remote service for consulting of medical reports, provided by the regional Public Administration, and a personal local service that allows to collect and display data from biomedical devices, and to manage user's reminders for medicines [73]. With the use of enabling technologies, as near field communications, and a smart TV equipment, it is possible to effectively deliver telehealth services also to users who may be less familiar with technological devices, such as elder adults, or people living in rural communities [72]. However, the rapid growth of the IoT increases the interest in the application of this technology also in the domain of the environment assisted living. One major issue to address in this context is the identification of a suitable middleware able to leverage the potentialities offered by the IoT and, at the same time, ensure the necessary support to services and functions related to healthcare and personal assistance [50]. Due to its intrinsic nature, IoT may represent an 'integration platform' for AAL that includes features of home automation (energy management, safety, comfort, etc.) and introduces 'smart objects', to monitor activities of daily living and detect any abnormal behavior that may represent a danger, or highlight symptoms of some incipient disease, so overcoming the interoperability issues related to the interconnection of many different communication systems [74]. As a confirmation of remote monitoring effectiveness and usability, either from a patient's or a medical operator's perspective, an evaluation of a telemedicine approach has been performed by testing three remote health platforms, in a realistic scenario involving elder adults and medical operators (doctors and nurses), with the aim to evaluate the main positive and negative issues related to the system and service design philosophy each solution was built upon [79]. In the framework of an AAL solution, it may be of interest to evaluate if the user is spending too much time in a static condition, since this situation could denote an anomalous trend, possibly related to cognitive or physical conditions worsening. For such a kind of monitoring to be effective, the sensor technology

should be the less intrusive as possible, and should not require any specific action by the user. To this aim, a smart insole equipped with force sensors, that is able to classify different dynamic states (sitting, walking, standing, ...) and transmit related data to a supervising system is proposed in [49]. Preliminary experimental results confirm the effectiveness of the approach, in correctly detecting and classifying the user's activities [48].

4.2 Spread Spectrum Systems

Code division multiple access (CDMA) using direct sequence (DS) spread spectrum modulation provides multiple access capability essentially thanks to the adoption of proper sequences as spreading codes. The ability of a DS-CDMA receiver to detect the desired signal relies to a great extent on the auto-correlation properties of the spreading code associated to each user; on the other hand, multi-user interference rejection depends on the cross-correlation properties of all the spreading codes in the considered set. As a consequence, the analysis of new families of spreading codes to be adopted in DS-CDMA is of great interest. Results are provided about the evaluation of specific full-length binary sequences, the De Bruijn ones, when applied as spreading codes in DS-CDMA schemes, and their performance compared to other families of spreading codes commonly used, such as m-sequences, Gold, orthogonal variable spreading factor (OVSF), and Kasami sequences. While the latter sets of sequences have been specifically designed for application in multi-user communication contexts, De Bruijn sequences come from combinatorial mathematics, and have been applied in completely different scenarios. Considering the similarity of De Bruijn sequences to random sequences, the performance resulting by applying them as spreading codes are investigated. The results presented suggest that binary De Bruijn sequences, when properly selected, may compete with more consolidated options [77, 78, 82].

With the aim to propose new spreading waveforms able to increase the performance of CDMA systems, chaotic communication system and a spread spectrum system with similar features in terms of bandwidth and transceiver structure but based on more conventional Gold sequences are compared in the presence of noise and multipath contributions which degrade the channel quality. It is shown that, because of its more favorable correlation properties, the chaotic scheme exhibits lower error rates, at a parity of the bandwidth expansion factor [41]. A possible application of chaotic signals as an alternative to more conventional spreading schemes in direct-sequence spread spectrum (DS-SS) automotive radars is presented, being the radar a key component for road safety systems. Due to their very good correlation properties, chaotic sequences are potentially able to outperform previous options, like Gold codes, with regard to the detection probability and the number of available sequences. Numerical examples are given, in some typical scenarios and under severe operation conditions, due to the presence of interfering radars [51].

4.3 The Coding of Video Signals

Coding and encryption of video signal, to be used in video-communication systems, have been considered in the framework of a source coding activity. With the task to test the effects of the features implementation introduced by the video coding standard H.264, an extensive performance evaluation of spatial, temporal, and hybrid error concealment techniques was provided [58]. The quality of the recovered image was measured, and the comparison among the various schemes is developed, using the JM7.3 Reference Software, either in subjective or in objective terms [40]. The partial encryption of a bit stream was taken into account, with the aim to make the entire stream somehow useless for anyone that cannot decrypt its ciphered subset. The effects of the partial encryption was evaluated as a function of some H.264/AVC coding parameters, in order to obtain a moderate degradation of the video content, which can be appealing for commercial applications, like pay-per-view systems and others, without strictly focusing on security or cryptanalysis issues [80]. A chaotic algorithm which employed suitably arranged chaotic functions was presented for video encryption. The algorithm was implemented on a code which ensured real time transmissions, at 25 frames/s, of the images coming from a video camera. The efficiency of the algorithm was justified theoretically, and demonstrated through simulation examples. The algorithm permitted achievement of a high level of security with reasonable processing times [39].

5 Internet Evolution and the Internet of Things

The world of telecommunications has changed dramatically over the last 20 years, thanks to the combination of the digitalization of information and the unstoppable development of ICT technologies. The way in which today people communicate, get informed, entertain and interact with each other and with the surrounding environment is much more varied and rich than a few years ago. Communications are possible anywhere, with any device, on any channel, in a synchronized or non-synchronized way; they are traceable, lasting over time, personalized, multimedia and social. Furthermore, the disruptive effects of Internet diffusion has profoundly modified the global communication landscape. The Internet has been in concept in the 70s and its usage exploded about twenty year later when the World Wide Web application became broadly available with the arrival of the first commercial browser and server applications. Since that time, a huge quantity of contents and new applications have enriched the Internet, which has grown to reach more than 3.5 billion people. The Internet we experience every day is a complex combination of many elements such as transport networks, user devices, applications and services, held together by two main protocols: the Internet Protocol (IP) for the transport layer (including its control mechanisms: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)) and HyperText Transfer Protocol (HTTP) for the application layer. From the

so-called Internet of people, which we have known until today, we are experiencing a new revolution consisting of Smart Objects that become an integral part of the Internet environment to achieve the IoT paradigm. This trend is already underway as sensor networks connect to the Internet together with a large part of billions of mobile phones used worldwide. To this group, a myriad of devices of all kinds integrated into everyday life objects (home, office, portable, fixed and mobile sensors, etc.) will be added. The future of the Internet will be dictated by future applications and services scenarios, but the Internet is vital, continuously evolving, and it is difficult to predict its future. From a user perspective, the Internet has been transformed into a new media platform, as the nature of Internet traffic has changed from static data and text file transfer to streaming interactive media content (which is the main part of total Internet traffic). At the same time, the IoT provides a virtual view, via the IP, to a huge variety of real life Smart Objects, ranging from a car, to a seat, to a building, to trees in a forest. Its appeal is the ubiquitous generalized access to the status and location of any "thing" we may be interested in. To exploit this potential, telecommunications networks and services are taking a further step towards their transformation: from people and things to data connectors and the creation of associations between them through services for smart environments and more.

5.1 Wireless Sensor Networks and Smart Environments

In recent years, Wireless Sensor Networks (WSN) are becoming a very promising research field since they find application in many different areas. Thanks to what has been made possible by micro and nano-electronics, computing and communication technologies, over the next few years, billions of sensors will populate cities, homes, factories, devices and even clothes. Many of these will be integrated into devices with processing and communication capabilities, both wireless and wired, and many will become part of a new network layer, the sensor networks, characterized by the use of short-range, high-reconfigurability technologies, a certain dose of autonomy and very low power consumption. Nowadays, WSN are becoming even more a key element in networking and telecommunications especially with the advent of the IoT paradigm, where each single node of the WSN can obtain a unique IP address and it is potentially reachable from everyone, everything, and everywhere through the Internet. The IoT paradigm identifies a service model that makes possible to transform everyday life objects into Smart Object embedding computational capabilities, sensors, actuators and communication systems to detect and control a physical phenomenon or an event and exchange information about it with a cloud platform. The populations of the cities are already invested by these new phenomena. In fact, thanks to these sensors, the physical spaces of the cities are virtually filled with behavioral and environmental data in real time. In the so-called Smart Environment, a digital fabric overlaps with our physical world and extends to offer even richer experiences using the context of our environment to increase our capabilities. Explosive innovation and widespread adoption of smart and mobile devices, and the availability of rich

data sources are changing the cities in which we live, work and act. Thanks to an increasingly widespread computational capacity, urban spaces will be saturated with both visible and invisible means, which will collect and transmit information [55]. Smart Environment applications can be present in the most varied areas such as energy, ecology, transport, health and wellbeing, education, local government, security of the territory, cultural heritage, and tourism. Contextually, also our research studies about WSN and the IoT were successful applied and tested in a variety of case studies. Starting from the development and performance evaluation of protocols and complete architectures for IoT systems [57], we have demonstrated their potentiality in a series of application sectors such as environmental monitoring and control in the cultural heritage field [64], seismic and structural health monitoring [65], AAL [70], location services [69], e-Health systems [52, 67], and Wireless Body Sensor Network [1, 68]. In fact, the proposed IoT solutions can be used in many application fields with great success in terms of costs and resources optimization, variety of implemented features, level of customization and expandability of each solution.

5.2 Wireless Body Sensor Networks

The previous IoT architectures, based on WSN solutions, can simply allow the use of common web services in order to directly interact with each node belonging to the network, whether it is installed in the monitored environment or worn by a subject. In the field of Wireless Body Sensor Networks, we have developed wearable devices and network solutions useful for a series of real-time monitoring functions depending on the desired application and the placing site of the unit on a subject. We have studied and developed a conceptually simply device containing a 3-axes accelerometer, a 3-axes gyroscope and a 3-axes magnetometer, realizing an attitude heading reference system (AHRS). This AHRS provides the correct 3D orientation referred to the terrestrial axes through a special implemented orientation filter able to furnish the correct magnitudes evaluation starting from the raw data [59]. A typical application making use of a version of the previous device concerns the automatic falls detection in elderly. In fact, on the sensor board it can also be real time executed the automatic fall detection algorithm, handling the orientation data from the AHRS and the acceleration data from the tri-axial accelerometer [62]. Based on the excellent results achieved with the developed AHRS, a wearable sensor able to furnish the right altitude of a subject was subsequently proposed [63]. This device also embeds a barometric unit and implements an optimized data fusion algorithm for an extremely accurate fall detection, including a more effective discrimination of daily life activities from falls and a correct recognition of critical falls such as syncopes [60]. The AHRS has also been used as an aid to clinical diagnosis of Parkinson's disease (PD) [66]. The ability to objectively classify different types of tremor, specific for each patient and the evolutionary stage of the disease, through a simple, fast, low cost, and non-invasive instrumental examination is very useful for the diagnosis of the disease and for the study of its clinical course. The inertial sensors are embedded into a

special bracelet allowing the acquisition of the quantities of interest that, through appropriate algorithms, provide an objective and quantitative assessment of the type and severity of the observed tremor [12, 13]. This system is usable in clinical and diagnostic settings, but it can show its effectiveness also in patients home or hospital h24 monitoring. In fact, it is able to detect and objectively quantify PD events such as tremor and freezing of gait (FoG) and to transmit data of multitude of patients and make them available in the cloud.

So far, the history of the Internet has been incredibly successful in the development of technological innovations and telemedicine solutions are one of many examples in this regard. In such context, we have proposed innovative e-Health services for vital signs sharing based on the Web Real-Time Communication (WebRTC) technology that allows any person in a health emergency to remotely interact with the medical personnel [71]. Now, the challenge is to make the Internet able to provide an increasing quality of experience for the end-user and for those applications that will revolutionize our lives in the near future. The IoT is moving in this direction and it is also providing a valuable contribution to the growth of the tactile Internet. This term is used to refer to a data network with extremely low-latency in analogy to the human tactile system that works at extreme response speeds. In this regard, others experimental solutions have been proposed [2, 61] but the real challenge will be to develop data network able to deliver data within one millisecond latency. Such technology would enable previously unimaginable scenarios in automation and remote assistance and countless potential applications such as remote surgery, industrial control, high-precision agriculture, robotics, etc.

6 Conclusions

The transformation of research into practical applications is not always easy, and often requires several years. In this chapter, we have provided a survey for some of the most relevant challenges in this direction, in the field of telecommunications, clarifying the relationships between theory and applications. The main issues faced are summarized below. In communication technologies, information theory and channel coding, principles have to be implemented on proper electronic devices, whose cost does not prevent commercial success of the supported services. Similarly, the prediction of all-optical switches and spatial soliton behavior preceded their practical use by far. On the other hand, transmission security at physical level is a basic need for modern communications and the tools for assuring it are to be practically tested with proper attack simulation. Source coding, especially in video signals, and spread spectrum systems can make digital signals particularly efficient either in bandwidth saving or in interference managing. Monitoring of human activities is an enabling technology for ensuring population ageing preserving health and wellness. Practical solutions have been investigated attempting to insert them in suitable cloud-based protocols and interfaces. Internet evolution, up to the paradigm represented by Internet of Things, expresses a challenge in finding solutions which are reliable, scalable,

and low-cost. In particular, wireless sensor networks offer a great variety of opportunities for such evolution. Body sensors can reveal disease or accidents, especially for elder people, allowing accurate home control with acceptable cost and remarkable reliability. We have shown that all these topics have been properly addressed by the telecommunication group at the Polytechnic University of Marche.

References

1. Altepe C, Egi SM, Ozyigit T, Sinoplu DR, Marroni A, Pierleoni P (2017) Design and validation of a breathing detection system for scuba divers. Sensors 17(6):1349
2. Andreoli A, Gravina R, Giannantonio R, Pierleoni P, Fortino G (2010) SPINE-HRV: a BSN-based toolkit for heart rate variability analysis in the time-domain. In: Wearable and autonomous biomedical devices and systems for smart environment. Springer, pp 369–389
3. Baldi M, Bianchi M, Chiaraluce F (2012) Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: a security gap analysis. IEEE Trans Inf Forensics Secur 7(3):883–894
4. Baldi M, Bianchi M, Chiaraluce F (2013) Security and complexity of the McEliece cryptosystem based on quasi-cyclic low-density parity-check codes. IET Inf Secur 7(3):212–220
5. Baldi M, Chiaraluce F, Laurenti N, Tomasin S, Renna F (2014) Secrecy transmission on parallel channels: theoretical limits and performance of practical codes. IEEE Trans Inf Forensics Secur 9(11):1765–1779
6. Baldi M, Bianchi M, Chiaraluce F, Rosenthal J, Schipani D (2016) Enhanced public key security for the McEliece cryptosystem. J Cryptol 29(1):1–27
7. Baldi M, Bambozzi F, Chiaraluce F (2011) On a family of circulant matrices for quasi-cyclic low-density generator matrix codes. IEEE Trans Inf Theory 57(9):6052–6067
8. Baldi M, Barenghi A, Chiaraluce F, Pelosi G, Santini P (2018) LEDAkem: a post-quantum key encapsulation mechanism based on QC-LDPC codes. In: Lange T, Steinwandt R (eds) Post-quantum cryptography. PQCrypto 2018, vol 10786, pp 3–24, April 2018
9. Baldi M, Cancellieri G, Chiaraluce F (2012) Interleaved product LDPC codes. IEEE Trans Commun 60(4):895–901
10. Baldi M, Cancellieri G, Chiaraluce F (2014) Array convolutional low-density parity-check codes. IEEE Commun Lett 18(2):336–339
11. Battaglioni M, Tasdighi A, Cancellieri G, Chiaraluce F, Baldi M (2018) Design and analysis of time-invariant SC-LDPC convolutional codes with small constraint length. IEEE Trans Commun 66(3):918–931
12. Bazgir O, Frounchi J, Habibi SAH, Palma L, Pierleoni P (2015) A neural network system for diagnosis and assessment of tremor in Parkinson disease patients. In: Proceedings of Iranian conference on biomedical engineering (ICBME 2015). IEEE, pp 1–5
13. Bazgir O, Habibi SAH, Palma L, Pierleoni P, Nafees S (2018) A classification system for assessment and home monitoring of tremor in patients with Parkinson's disease. J Med Signals Sens 8(2):65
14. Berrou C, Glavieux A, Thitimajshima P (1993) Near Shannon limit error-correcting coding and decoding: turbo-codes. 1. In: Proceedings of the IEEE international conference on communications (ICC 1993), pp 1064–1070, May 1993
15. Borella A, Broglio D, Cancellieri G, Chiaraluce F (1993) Enhancements of DQDB protocol with ECBWB mechanism for fair access and multi-priority traffic management. Comput Commun 16(8):511–517
16. Borella A, Cancellieri G, Chiaraluce F (2001) Design techniques of two-layer architectures for WDM optical networks. Int J Commun Syst 14(2):171–188

17. Cacopardi S, Decina M, De Julio U (1973) Digital transmission at 34.304 Mbit/s on microcoaxial cable. In: Proceedings of the IEEE international conference on communications (ICC 1973), vol 6
18. Calzolari GP, Chiani M, Chiaraluce F, Garello R, Paolini E (2011) Channel coding for future space missions: new requirements and trends. Proc. IEEE 95(11):2157–2179
19. Cancellieri G (1989) Transmission efficiency in photon counting channels. IEEE Trans Commun 37(2):183–187
20. Cancellieri G (1978) Time-dispersion measurement in optical fibre by near- and far-field scanning technique. Electron Lett 14(15):465–467
21. Cancellieri G (1980) Mode coupling in graded-index optical fibres due to perturbation of the index profile. Appl Phys 23(1):99–105
22. Cancellieri G (1981) Exact evaluation of time dispersion in double-α profile fibres. Opt Commun 40(2):117–121
23. Cancellieri G, Chiaraluce F (1990) 2-PSK based binary sequences for optical coherent transmission. J Opt Commun 11(1):2–6
24. Cancellieri G, Fantini P (1981) Frequency-dependent steady-state distribution of optical power in multimode fibres. Opt Quantum Electron 13(3):229–239
25. Cancellieri G, Fantini P (1982) Optical fiber cabling processes: discussion of an optimization procedure. Appl Opt 21(15):2651–2652
26. Cancellieri G, Fantini P (1983) Mode coupling effects in optical fibres: perturbative solution of the time-dependent power flow equation. Opt Quantum Electron 15(2):119–136
27. Cancellieri G, Fantini P (1984) Time dispersion properties of cascaded multimode fiber links. IEEE Trans Microwave Theory Tech 32(8):929–935
28. Cancellieri G, Frosini F (1982) Discussion on equalization in optical fiber transmission systems. J Opt Commun 3(4):146–151
29. Cancellieri G, Mezzetti M (1979) Scanning technique for investigating optical fibre dispersion. Opt Quantum Electron 11(4):305–317
30. Cancellieri G, Mezzetti M (1980) Design parameters for reducing radiation confinement errors and the spatial dependence of the emission delays in light-emitting diodes. J Appl Phys 51(3):1813–1817
31. Cancellieri G, Orfei A (1985) Discussion on the effective cut-off wavelength of the LP11 mode in single-mode optical fibres. Opt Commun 55(5):311–315
32. Cancellieri G, Ravaioli U (1982) Baseband response of multimode optical fibers under different excitation conditions. J Opt Commun 3(1):13–18
33. Cancellieri G, Chiaraluce F, Gambi E (1994) Effects of EDFA construction parameters on soliton propagation in long-distance transmission systems. J Opt Commun 15(4):122–127
34. Cancellieri G, Chiaraluce F, Gambi E, Pierleoni P (1995) Coupled-soliton photonic logic gates: practical design procedures. J Opt Soc Am B 12(7):1300–1306
35. Cancellieri G, Chiaraluce F (1994) Recent progress in fibre optics. Prog Quantum Electron 18(1):39–95
36. Cancellieri G, Chiaraluce F, Gambi E, Pierleoni P (1996) All-optical polarization modulator based on spatial soliton coupling. J Lightwave Technol 14(3):513–523
37. Cancellieri G, Fantini P, Pesciarelli U (1985) Effects of joints on single-mode single-polarization optical fiber links. Appl Opt 24(7):964–969
38. Cancellieri G, Orfei A (1987) Asymptotic effective cutoff condition in single-mode optical fibers. J Lightwave Technol 5(2):199–205
39. Chiaraluce F, Ciccarelli L, Gambi E, Pierleoni P, Reginelli M (2002) A new chaotic algorithm for video encryption. IEEE Trans Consum Electron 48(4):838–844
40. Chiaraluce F, Ciccarelli L, Gambi E, Spinsante S (2004) Performance evaluation of error concealment techniques in H.264 video coding. In: Proceedings of the picture coding symposium (PCS 2004), pp 367–372
41. Chiaraluce F, Gambi E, Garello R, Pierleoni P (2002) Performance of DCSK in multipath environments: a comparison with systems using Gold sequences. IEICE Trans Fundam Electron Commun Comput Sci E85-A(10):2354–2363

42. Chiaraluce F, Garello R (2004) Extended Hamming product codes analytical performance evaluation for low error rate applications. IEEE Trans Wireless Commun 3(6):2353–2361
43. Cippitelli E, Fioranelli F, Gambi E, Spinsante S (2017) Radar and RGB-depth sensors for fall detection: a review. IEEE Sens J 17(12):3585–3604
44. Cippitelli E, Gambi E, Spinsante S, Flórez-Revuelta F (2016) Evaluation of a skeleton-based method for human activity recognition on a large-scale RGB-D dataset. In: Proceedings of the IET international conference on technologies for active and assisted living (TechAAL 2016), vol 2016
45. Cippitelli E, Gasparrini S, Gambi E (2016) Spinsante S (2016) A human activity recognition system using skeleton data from RGBD sensors. Comput Intelli Neurosci
46. Cippitelli E, Gasparrini S, Gambi E, Spinsante S (2016) An integrated approach to fall detection and fall risk estimation based on RGB-depth and inertial sensors. In: Proceedings of the ACM International Conference Proceeding Series, pp 246–253
47. Cippitelli E, Gasparrini S, Gambi E, Spinsante S, Wåhslény J, Orhany I, Lindhy T (2015) Time synchronization and data fusion for RGB-depth cameras and inertial sensors in AAL applications. In: Proceedings of the IEEE international conference on communication workshop (ICCW 2015), pp 265–270
48. De Santis A, Del Campo A, Gambi E, Montanini L, Pelliccioni G, Perla D, Spinsante S (2015) Unobtrusive monitoring of physical activity in AAL: a simple wearable device designed for older adults. In: Proceedings of the international conference on information and communication technologies for ageing well and e-health (ICT4AgeingWell 2015), pp 200–205
49. De Santis A, Gambi E, Montanini L, Raffaeli L, Spinsante S, Rascioni G (2014) A simple object for elderly vitality monitoring: the smart insole. In: Proceedings of the IEEE/ASME international conference on mechatronic and embedded systems and applications, conference proceedings (MESA 2014)
50. Del Campo A, Gambi E, Montanini L, Perla D, Raffaeli L, Spinsante S (2016) MQTT in AAL systems for home monitoring of people with dementia. In: Proceedings of the IEEE international symposium on personal, indoor and mobile radio communications (PIMRC, 2016), p 2016
51. Gambi E, Chiaraluce F, Spinsante S (2008) Chaos-based radars for automotive applications: theoretical issues and numerical simulation. IEEE Trans Veh Technol 57(6):3858–3863
52. Gambi E, Agostinelli A, Belli A, Burattini L, Cippitelli E, Fioretti S, Pierleoni P, Ricciuti M, Sbrollini A, Spinsante S (2017) Heart rate detection using microsoft kinect: validation and comparison to wearable devices. Sensors 17(8):1776
53. Garello R, Pierleoni P, Benedetto S (2001) Computing the free distance of turbo codes and serially concatenated codes with interleavers: algorithms and applications. IEEE J Select Areas Commun 19(5):801–812
54. Gasparrini S, Cippitelli E, Gambi E, Spinsante S, Wåhslén J, Orhan I, Lindh T (2016) Proposal and experimental evaluation of fall detection solution based on wearable and depth data fusion, vol 399. Advances in intelligent systems and computing
55. Incipini L, Belli A, Palma L, Ballicchia M, Pierleoni P (2017) Sensing light with LEDs: performance evaluation for IoT applications. J Imaging 3(4):50
56. McEliece RJ (1978) A public-key cryptosystem based on algebraic coding theory. DSN Progress Report, pp 114–116
57. Palma L, Pernini L, Belli A, Valenti S, Maurizi L, Pierleoni P (2016) IPv6 WSN solution for integration and interoperation between smart home and AAL systems. In: Proceedings of the IEEE sensors applications symposium (SAS 2016), pp 1–5, April 2016
58. Pasqualini S, Fioretti F, Andreoli A, Pierleoni P (2009) Comparison of H.264/AVC, H.264 with AIF, and AVS based on different video quality metrics. In: Proceedings of the IEEE international conference on telecommunications (ICT 2009). IEEE, pp 190–195
59. Pierleoni P, Belli A, Palma L, Pellegrini M, Pernini L, Valenti S (2015) A high reliability wearable device for elderly fall detection. IEEE Sens J 15(8):4544–4553
60. Pierleoni P, Belli A, Maurizi L, Palma L, Pernini L, Paniccia M, Valenti S (2016) A wearable fall detector for elderly people based on AHRS and barometric sensor. IEEE Sens J 16(17):6733–6744

61. Pierleoni P, Belli A, Concetti R, Palma L, Pinti F, Raggiunto S, Valenti S, Monteriù A (2018) A non-invasive method for biological age estimation using frailty phenotype assessment. In: Italian Forum of Ambient Assisted Living, pp 81–94, Springer
62. Pierleoni P, Belli A, Palma L, Pernini L, Valenti S (2014) A versatile ankle-mounted fall detection device based on attitude heading systems. In: Proceedings of the IEEE biomedical circuits and systems conference (BioCAS 2014), pp 153–156, Oct 2014
63. Pierleoni P, Belli A, Palma L, Pernini L, Valenti S (2014) An accurate device for real-time altitude estimation using data fusion algorithms. In: Proceedings of the IEEE-ASME international conference on mechatronic and embedded systems and applications (MESA 2014), pp 1–5, Sept 2014
64. Pierleoni P, Belli A, Palma L, Valenti S, Raggiunto S, Incipini L, Ceregioli P (2018) The Scrovegni chapel moves into the future: an innovative internet of things solution brings new light to Giotto's masterpiece. IEEE Sens J 18(18):7681–7696
65. Pierleoni P, Marzorati S, Ladina C, Raggiunto S, Belli A, Palma L, Cattaneo M, Valenti S (2018) Performance evaluation of a low-cost sensing unit for seismic applications: field testing during seismic events of 2016–2017 in central Italy. IEEE Sens J 18(16):6644–6659
66. Pierleoni P, Palma L, Belli A, Pernini L (2014) A real-time system to aid clinical classification and quantification of tremor in Parkinson's disease. In: Proceedings of the IEEE-EMBS international conference on biomedical and health informatics (BHI 2014), pp 113–116, June 2014
67. Pierleoni P, Pernini L, Belli A, Palma L (2014) An android-based heart monitoring system for the elderly and for patients with heart disease. Int J Telemed Appl 2014:10
68. Pierleoni P, Pernini L, Belli A, Palma L (2014) Real-time apnea detection using pressure sensor and tri-axial accelerometer. In: Proceeedings of the IEEE-EMBS international conference on biomedical and health informatics (BHI 2014), pp 513–516, June 2014
69. Pierleoni P, Pernini L, Belli A, Palma L, Maurizi L, Valenti S (2016) Indoor localization system for AAL over IPv6 WSN. In: Proceedings of the IEEE international symposium on personal, indoor, and mobile radio communications (PIMRC 2016). IEEE, pp 1–7
70. Pierleoni P, Pernini L, Belli A, Palma L, Valenti S, Paniccia M (2015) SVM-based fall detection method for elderly people using android low-cost smartphones. In: Proceedings of the IEEE sensors applications symposium (SAS 2015), pp 1–5, April 2015
71. Pierleoni P, Pernini L, Palma L, Belli A, Valenti S, Maurizi L, Sabbatini L, Marroni A (2016) An innovative WebRTC solution for e-Health services. In: Proceedings of the IEEE international conference on e-health networking, applications and services (Healthcom 2016). IEEE, pp 1–6
72. Raffaeli L, Spinsante S, Gambi E (2016) Integrated smart tv-based personal e-health system. Int J e-Health Med Commun 7(1):48–64
73. Raffaeli L, Gambi E, Spinsante S (2014) Smart tv based ecosystem for personal e-health services. In: Proceedings of the international symposium on medical information and communication technology (ISMICT 2014)
74. Rossi L, Belli A, De Santis A, Diamantini C, Frontoni E, Gambi E, Palma L, Pernini L, Pierleoni P, Potena D, Raffaeli L, Spinsante S, Zingaretti P, Cacciagrano D, Corradini F, Culmone R, De Angelis F, Merelli E, Re B (2014) Interoperability issues among smart home technological frameworks. In: Proceedings of the IEEE/ASME international conference on mechatronic and embedded systems and applications, conference proceedings (MESA 2014)
75. Santini P, Baldi M, Cancellieri G, Chiaraluce F (2018) Hindering reaction attacks by using monomial codes in the McEliece cryptosystem. In: Proceedings of the IEEE international symposium on information theory (ISIT 2018), pp 951–955, June 2018
76. Spinsante S, Gambi E (2012) Remote health monitoring by osgi technology and digital tv integration. IEEE Trans Consum Electron 58(4):1434–1441
77. Spinsante S, Gambi E (2013) De Bruijn binary sequences and spread spectrum applications: a marriage possible? IEEE Aerosp Electron Syst Mag 28(11):28–39
78. Spinsante S, Andrenacci S, Gambi E (2011) Binary De Bruijn sequences for DS-CDMA systems: analysis and results. EURASIP J Wireless Commun Netw 1:2011

79. Spinsante S, Antonicelli R, Mazzanti I, Gambi E (2012) Technological approaches to remote monitoring of elderly people in cardiology: a usability perspective. Int J Telemed Appl
80. Spinsante S, Chiaraluce F, Gambi E (2005) Masking video information by partial encryption of H.264/AVC coding parameters. In: Proceedings of the European signal processing conference (EUSIPCO 2005), pp 838–841
81. Spinsante S, Gambi E (2012) Remote health monitoring for elderly through interactive television. BioMed Eng Online 11
82. Warty C, Mattigiri S, Gambi E, Spinsante S (2013) De Bruijn sequences as secure spreading codes for wireless communications. In: Proceedings of the international conference on advances in computing, communications and informatics (ICACCI 2013), pp 315–320
83. Wyner AD (1975) The wire-tap channel. Bell Syst Tech J 54(8):1355–1387