Machine-to-Machine Communications for e-Health Applications

Elli Kartsakli, *Member, IEEE,* Aris S. Lalos, *Member, IEEE,*
Angelos Antonopoulos, *Member, IEEE,* Stefano Tennina, *Member, IEEE,*
Marco Di Renzo, *Member, IEEE,* Luis Alonso, *Member, IEEE,*
and Christos Verikoukis, *Senior Member, IEEE*

Abstract

The emerging technology of Machine-to-Machine (M2M) communications is bringing a paradigm shift in healthcare delivery. A broad range of e-Health applications can be conceived, with considerable benefits for both patients and healthcare providers. Many technological challenges have to be met, however, to ensure the widespread adoption of e-Health solutions in the future. In this context, we aim to provide a comprehensive overview on M2M systems for e-Health applications from a wireless communication perspective. We provide an overview of the candidate wireless technologies that are suitable for different parts of the M2M system architecture and then show how these technologies are seamlessly integrated to provide an end-to-end e-Health solution. In particular, we discuss end-to-end solution designs and testbed implementations, we present the key security and privacy challenges associated with the sensitive nature of medical data and we summarize the most recent research projects dedicated to e-Health applications.

Index Terms

Machine-to-Machine (M2M), e-Health, WBAN, M2M Area Network, M2M Communications Network, IEEE 802.15.6, end-to-end communications

Elli Kartsakli and Aris S. Lalos are with the Department of Signal Theory and Communications (TSC) of the Technical University of Catalunya (UPC), Spain (e-mail: {ellik, aristeidis.lalos@}@tsc.upc.edu).

Angelos Antonopoulos and Christos Verikoukis are with the Telecommunications Technological Centre of Catalonia (CTTC) (e-mail: {aantonopoulos, cveri}@cttc.es).

Stefano Tennina is with the WEST Aquila srl, University of L'Aquila, Italy (email: tennina@westaquila.com).

Marco Di Renzo is with the Laboratory of Signals and Systems (L2S), Univ Paris-Sud (Paris), France e-mail:(marco.direnzo@lss.supelec.fr).

I. Introduction

Machine-to-Machine (M2M) communications is an emerging technology that envisions the interconnection of machines without the need of human intervention. The main concept lies in seamlessly connecting an autonomous and self-organizing network of M2M-capable devices to a remote client, through heterogeneous wired or wireless communication networks. An intelligent software application is usually employed at the remote client to process the collected data and provide the end user with a set of smart services and a practical interface. Although the idea of telematics and telemetry applications is not new, the widespread use of Internet, along with the trend for ubiquitous connectivity, especially via wireless communication systems, have placed M2M systems on the spotlight of attention for both academia and industry.

The increasing interest on M2M communications poses significant challenges that need to be met. A key issue to be handled is the large number of devices that must be supported in an M2M network, since market predictions estimate that the number of M2M-enabled devices with Internet connectivity will reach up to 50 billion by the end of 2020 [1]. Regardless of the exact figures, the growth rate is impressive, and major efforts are required to provide scalable solutions that support the increasing number of devices with diverse characteristics and requirements. Another challenge stems from the multitude of technical solutions that can be employed in M2M systems. Depending on the application deployment, different approaches may be adopted for the interconnection of M2M devices, such as wired or wireless technologies, short-range or long-range communications, and solutions based on existing open communication standards or proprietary technologies.

The above challenges stress the imperative need for standardization of M2M communications [2]. To this direction, the European Telecommunications Standards Institution (ETSI) has established the M2M Technical Committee which aims to provide an end-to-end view of M2M standardization, focusing on the interoperability of M2M devices with existing standards. In July of 2012, ETSI and six other major standards development organizations (ARIB and TTC of Japan, ATIS and the TIA of the USA, CCSA of China, and TTA of Korea) joined their efforts in the oneM2M initiative, under the goal of creating a single universal standard for M2M communications [3]. This global standardization effort is crucial to enable the integration of heterogeneous technologies in order to achieve seamless end-to-end connectivity, removing potential barriers to market growth.

The penetration of M2M solutions for monitoring and remote control in a wide range of markets, including building and industrial automation, security and surveillance, smart metering, energy management, and transportation, generates great business opportunities. The application of M2M enabling technologies to the healthcare sector, in particular, is expected to be one of the major M2M market drivers: market projections forecast that more than 774 million health-related devices with M2M connectivity will be available by 2020, yielding a total revenue of 69 billion euros in that year [4].

The use of information and communication technologies to facilitate and improve healthcare and medical services, often referred to by the term e-Health, is bringing a shift to healthcare delivery. The M2M paradigm in the context of e-Health involves the use of appropriate sensor devices on patients to enable the remote monitoring of vital signals, the early detection of critical conditions and the remote control of certain medical treatments [5]. The medical sensors, placed in the vicinity of, or inside, the human body, are usually interconnected through a short-range wireless technology, thus forming a Wireless Body Area Network (WBAN). An M2M-enabled gateway node collects all the sensory data from the WBAN and forwards them to a remote online server, where processing and integration with medical-related software applications take place. The connection of the gateway to the Internet is generally based on long-range communication access technologies for Wireless Local/Metropolitan Area Networks (WLANs/WMANs).

The emerging application scenarios are numerous, including the active management of diseases such as diabetes (e.g., by measuring blood sugar levels and controlling the insulin dosage accordingly), the support for independent aging to the elderly (e.g., by tracking their medication intake and their activity level) and the monitoring of personal fitness activities to improve health and well-being (e.g., by logging health and fitness indicators during workouts) [5]. Overall, e-Health can offer significant benefits for both patients and healthcare providers, reducing the cost of healthcare services while ensuring enhanced quality, efficiency, flexibility in healthcare delivery.

In the recent years, the research community has been motivated by the diversity of applications, the promising benefits and the potential market opportunities of e-Health M2M solutions. The main technological challenges for M2M communications, the most representative usage models and the status of global standardization efforts are discussed in [6]. Focusing on the emerging M2M technologies for e-Health applications, a technical discussion on the communication network design is given in [7], but generally most of the related work adopts a high-level approach. In [8], some interesting challenges from the network perspective are identified, while interoperability issues and recent standardization efforts are presented in [9]. On a different level, a lot of research activity has been focused on the body area domain, on the design of medical sensor devices [10] and on the main advances and challenges in the field of WBANs [11]–[14].

In this chapter, we aim to provide a comprehensive overview of M2M systems for e-Health applications from a wireless communication perspective. We discuss different aspects of the M2M ecosystem in the healthcare domain, focusing mainly on the end-to-end connectivity: First, the high-level ETSI architecture for M2M systems and the key elements for a healthcare application scenario are described in Section II. Section III provides an overview of the enabling wireless communication technologies that can be employed in M2M systems, focusing on both open communication standards and proprietary solutions. Then, in Section IV, we offer an end-to-end perspective of M2M systems for e-Health, focusing on the integration and convergence of different communication technologies, through both theoretical approaches and testbed implementation, and presenting the key security challenges that arise. The survey of existing works in the field of M2M communications for e-Health is completed by a summary of current research projects in Section V, whereas some concluding remarks are given in Section VI.

II. M2M Network Architecture

In the recent years, ETSI has been actively engaged in the development of a standard for M2M systems, with the objective to ensure interoperability between the diverse M2M components and the already existing technologies. To this direction, ETSI proposes a high-level horizontal architecture, dividing the system into three domains: *i*) the device and gateway domain, where the M2M devices communicate with a gateway through short-range area networks, *ii*) the network domain that connects the gateway to the applications through long-range access and core communication networks, and *iii*) the application domain, where various application services are defined depending on the use case [15].

Figure 1 illustrates an example of the M2M system architecture for wireless healthcare applications. The ETSI architecture consists of five key elements that are described below [15], [16]:

- The *M2M devices*, which are devices capable of transmitting data autonomously or after receiving a data request. In the context of healthcare applications, the M2M devices are principally low-power medical sensor or actuator devices with embedded wireless communication modules.
- The *M2M Area Network*, also known as capillary network, which is a short-range network that provides connectivity between the M2M devices and the gateway. In the considered scenario, the area network will also be referred to as WBAN, given that the M2M devices are deployed near or within the human body.
- The *M2M Gateway*, which acts as a proxy between the M2M devices (interconnected through the WBAN) and the network domain. Practically, the gateway must be a portable device with advanced processing capabilities and multiple radio interfaces, able to operate in technologies employed by both the WBAN and the communication network. Typical examples of M2M gateways include smartphones, Personal Digital Assistants (PDAs) and smart watches.
- The *M2M Access Communication Network*, which connects the M2M gateway to the the M2M application server via the Internet.
- The *M2M Application Server*, which is the middleware layer that provides data to the specific business applications.

III. Enabling Wireless Technologies: Standards and Proprietary Solutions

The ETSI M2M architecture framework, described in the previous section, defines two levels of wireless connectivity: *i*) short-range connectivity within the M2M area network (WBAN), and *ii*) long-range connectivity within the M2M access communication network. In this section, we give an overview of the key enabling technologies for each type of network.

A. M2M Area Network

The main requirements for the candidate WBAN technologies are short-range connectivity, low-power operation and Quality of Service (QoS) provisioning to support real-time monitoring and critical events in e-Health applications. The presented technologies are classified into two categories: *i*) open communication standards that ensure interoperability and compatibility among different vendors, and *ii*) proprietary solutions available in the market that are tied to

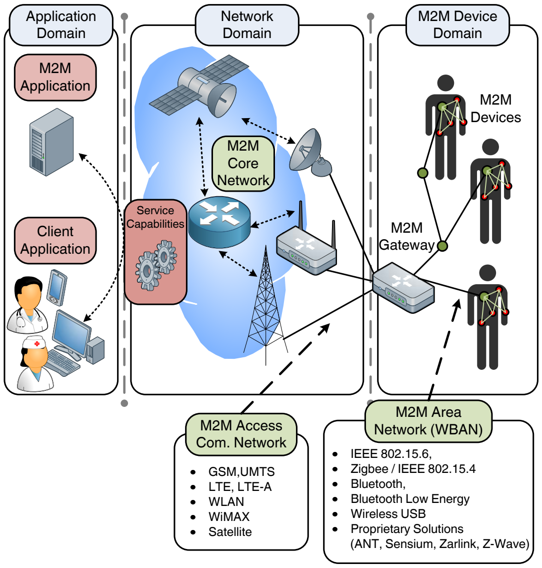

Fig. 1. Simplified M2M architecture for wireless connectivity in healthcare application scenarios

specific vendors. Here, we briefly describe the most prevalent available technologies in both categories, giving particular emphasis on the IEEE 802.15.6 standard defined specifically for WBAN communications. The main technical features of the presented technologies for M2M area networks are summarized in Table I.

1) Open Standards: **Bluetooth** (http://www.bluetooth.com) is an industrial standard for short-range wireless communications. The lower layers of the Bluetooth protocol stack, namely the Physical (PHY) and the Medium Access Control (MAC) layers, are specified in the **IEEE 802.15.1** standard [18], whereas a number of application profiles are defined at the upper layers to support application-specific tasks. Bluetooth operates at the unlicensed 2.4 GHz Industrial, Scientific and Medical (ISM) band, using spread spectrum and frequency hopping transmission techniques. It is mainly intended for peer-to-peer connections or small ad hoc networks formed by a master and up to seven slave devices. In the context of e-Health, Bluetooth defines a specific profile for healthcare and fitness applications, called Health Device Profile. The latest version of the Bluetooth standard includes **Bluetooth Low Energy**, a technology that enhances energy efficiency by providing ultra-low power operation and reliable point-to-multipoint data transfer between M2M devices.

ZigBee (http://www.zigbee.org) is a protocol stack widely applied in remote control and sensor

Technology		Frequency Band	Data Rate	Range (m)	Modulation	Topology
Open Standards	**Bluetooth Low Energy**	2.4 GHz ISM	1 Mbps	10	GFSK	star
	WUSB	3.1-10.6 GHz UWB	48-53 Mbps	3-10	MB-OFDM	star
	ZigBee	868 MH, 915 MHz, 2.4 GHz ISM	250 Kbps	30-100	O-QPSK	P2P, tree, star, mesh
	IEEE 802.15.6	Multiple, including 402-405 MHz MICS, 900 MHz ISM, 2.4 GHz ISM, and 3.1-10.6 GHz UWB	100 Kbps– 12 Mbps	~ 3	Multiple, including $\pi/2$-DBPSK, $\pi/4$-DQPSK, and IR-UWB On-Off	extended star
Proprietary Solutions	**ANT**	2.4 GHz ISM	1 Mbps	10-30	GFSK	P2P, mesh tree, star
	Sensium	868-915 MHz	50 Kbps	5-25	BFSK	star
	Zarlink	402-405 MHz MICS 433-434 MHz	$200-800$ Kbps	2	2FSK/4FSK	P2P
	Z-Wave	900 MHz ISM	9.6-40 Kbps	30	GFSK	mesh

TABLE I

ENABLING WBAN TECHNOLOGIES FOR E-HEALTH APPLICATIONS [9], [17].

applications. ZigBee defines the application, the security and the network layer specifications and is built on top of the PHY and MAC layers defined by the **IEEE 802.15.4** standard [19]. It mainly operates at the unlicensed 2.4 GHz ISM band, employing direct sequence spread spectrum techniques for interference tolerance. ZigBee defines the Personal Health and Hospital Care profile (PHHC), ensuring device interoperability for secure and reliable monitoring of non-critical healthcare services, such as chronic disease management, obesity and aging.

Wireless Universal Serial Bus (WUSB) is a short-range, high-bandwidth wireless radio communication standard that operates at the frequency range of 3.1-10.6 GHz [20]. WUSB is placed among the first candidates to be commercially available for short-range high-speed wireless interfaces, offering reliable and fast point-to-point links with a security level similar to wired communications. At its latest version, WUSB is expected to offer the same functionality as the standard wired USB devices, without the cabling restrictions.

The above technologies share some weaknesses when applied to e-Health scenarios, mainly due to the fact that they have been designed with different target applications in mind. Bluetooth, for example, has limited scalability and QoS support and is not very energy-efficient. Bluetooth Low Energy reduces power consumption but the scalability and QoS are still an issue. ZigBee, on the other hand, is energy-efficient and scalable but provides lower data rates, whereas WUSB can only support to peer-to-peer connection topologies.

In an effort to overcome these limitations and tackle the specific requirements of WBANs, the **IEEE 802.15.6** standard has recently been issued for short-range wireless communications in the vicinity of, or inside, the human body. A key characteristic of IEEE 802.15.6 is that it supports operation at very low transmission powers, as well as macroscopic and microscopic power management through hibernation and sleep modes, respectively, in an effort to increase battery lifetime and comply with the safety regulations limits on the Specific Absorption Rate (SAR) level for in-body communications. It also provides QoS guarantees for the prompt delivery of alarms in emergency situations and employs robust security mechanisms to provide privacy and confidentiality protection of the medical data.

The standard provides specifications for the PHY and the MAC layers. With respect to the PHY layer, three different technologies are supported: *i*) the Narrowband (NB) PHY, which introduces low control overhead, very low peak power consumption and robustness against interference, *ii*) the Ultra-Wideband (UWB) PHY, based on a technology for transmitting information over a large bandwidth, offering high performance, robustness, low complexity and ultra-low power operation, and *iii*) the Human Body Communications (HBC) PHY, which uses the human body as a means of propagation for the data transmission. Operation at multiple frequency band is supported, starting from the Medical Implant Communications Service (MICS) band of 402-405 MHz, reserved for medical implant communication, up to the unlicensed 2.4 GHz ISM band.

With regard to the MAC layer, IEEE 802.15.6 defines eight levels of user priorities, with level 0 corresponding to the lowest priority class and level 7 being assigned to the highest priority traffic for emergency situations or medical implant event reports. The WBAN operates in an extended star topology, with all nodes connected directly, or through a single relay node, to the coordinating node, denoted as the hub. The standard considers both contention-based and contention-free channel access.

Two random access schemes for contention-based access are supported, namely Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) and slotted Aloha. The standard also supports three contention-free access modes that require centralized control from the WBAN hub: *i*) improvised access, which is a polling scheme for immediate of future allocation for both uplink and downlink, *ii*) scheduled access, which are periodic allocations for uplink, downlink or bidirectional transmissions that are negotiated between the nodes and the hub during the association phase, and *iii*) unscheduled access, which is a best-effort version of the scheduled access.

As far as security is concerned, the standard defines 3 different connectivity levels: *i*) unsecured communication, *ii*) authentication only, and *iii*) authentication and encryption.

2) Proprietary Solutions: Apart from the open communication standards, some proprietary solutions for WBANs are also available in the market. **ANT** (http://www.thisisant.com) is a wireless networking protocol and embedded system solution, operating at the 2.4 GHz ISM band, originally designed for general purpose wireless sensor networks. It provides ultra-low power consumption, low latency and simplicity in implementation, while limited QoS support and low data rates are its main drawbacks. The next generation of ANT, named **ANT+** protocol, focuses on the seamless interoperability between sensors and monitoring devices of different manufacturers (e.g., heart rate sensors with smart watches) and defines various health and fitness device profiles.

Sensium (http://www.toumaz.com) is an ultra-low power platform designed for healthcare and lifestyle management applications. The Sensium platform integrates various sensor devices with a processing unit and a low-power transceiver operating at 900 MHz. A master-slave topology is considered, where slave sensor nodes periodically send data to the Sensium platform that processes them and forwards them to a monitoring device through a gateway.

Zarlink (http://www.zarlink.com) has designed a series of ultra-low power transceivers for medical implants, operating at the 402-405 MICS band. The Zarlink devices achieve extremely low power consumption, by spending most of their time in a deep sleep mode and being woken up by special wake-up signals transmitted at the 2.4 GHz band. Their drawbacks are low data rates and limited QoS provisioning.

Z-Wave (http://www.z-wave.com) is a proprietary protocol designed for home control and monitoring. It provides low-power interconnection of home devices such as lights, thermostats and door locks to provide a smart living environment. It operates at the 900 MHz band, thus avoiding interference from most short and medium range wireless technologies (operating at the 2.4 GHz band), but offers very low data rates.

B. M2M Access Communication Network

The M2M access communication network requires medium or long-range wireless technologies with high data rate capabilities. Hence, wireless technologies for WLANs and WMANs are the main candidates: the first provide connectivity within a limited area, either indoors (e.g., a house or a hospital ward) or outdoors (e.g., a public hotspot), whereas the latter offer ubiquitous connectivity to an extended coverage area. Since the key employed technologies are widely used and well known, they are briefly stated next:

- The **IEEE 802.11** specification [21] for the PHY and the MAC layers, commonly referred to as **WiFi**, is the predominant technology adopted in WLANs for the 2.4 GHz and 5 GHz ISM bands.
- The **IEEE 802.16** standard [22], commonly known as **WiMAX**, defines a broadband access technology for WMANs, offering high rates and QoS provisioning.
- **Long Term Evolution (LTE)** and its evolved version **LTE-Advanced (LTE-A)**, are 3rd Generation Partnership Project (3GPP) mobile communications standards for high data rates and spectral efficiency.

IV. End-to-End Solutions for M2M Communication: Connectivity and Security

The goal of an e-Health application is to provide a bridge between the patient and the medical personnel. Hence, the M2M system must provide end-to-end connectivity, connecting the medical sensor devices via the M2M gateway to the Internet, and ultimately to the application server. Since standardization efforts on M2M communications are still underway, there are many different approaches to achieve end-to-end connectivity. However, despite their differences, most approaches partly follow the system architecture shown in Figure 2.

In this section, we examine end-to-end solutions for M2M communications, as well as security and privacy issues pertinent to e-Health applications. In particular, we first discuss theoretical works that focus on the high-level integration of WLAN/WMAN access communication technologies with WBANs. Then, we give some practical examples of end-to-end solutions by presenting testbed implementations for healthcare monitoring. Finally, we identify security and privacy issues that arise in M2M communication scenarios and are particularly related to the sensitive medical data handled by e-Health services.

A. Technology Integration for M2M Communications

The integration of different wireless technologies into a unified end-to-end solution for e-Health applications is an interesting topic that has attracted a lot of attention in the research community. Since there is no unique solution to this problem, in this section we present different approaches proposed in the literature. Some works identify the key challenges and application scenarios for the seamless integration of different technologies, while others provide analytical frameworks for end-to-end performance evaluation.

The work published in [23] studies the challenges concerning the deployment of a WiFi-based network within a healthcare facility such as a hospital unit. Practical guidelines for the design, dimensioning and the installation of the network, as well as appropriate validation methods, are provided, in order to satisfy the specific e-Health application requirements.

In [24], a two-tier network architecture is considered. The lower tier consists of the WBAN, where multiple sensor devices worn by a single patient are connected to a coordinating node by employing the CSMA/CA access mode of IEEE 802.15.4. At the upper tier, multiple WBAN coordinators (corresponding to multiple patients) located within a specific area, for example a hospital ward, communicate with an Access Point through WiFi. End-to-end packet delay and access time have been modeled as a function of the number of coexisting WBANs. An extension of this work in [25] has introduced service differentiation to prioritize high-rate data streams (e.g., electroencephalography (EEG) data) over low-rate streams (e.g., electrocardiography (ECG) data). The idea is to provide contention-free access to the high-priority data flows, whereas maintain CSMA/CA access for the lower priority nodes.

In [26], the authors discuss the feasibility of employing a hybrid network based on WiFi and WiMAX technologies as the access communication network in an M2M system for e-Health services. The integration of the two technologies poses several challenges, mainly related to QoS provisioning, connection admission control, scheduling, and mobility management through seamless vertical handovers. The envisioned heterogeneous deployment scenario considers nodes with either single (WiFi or WiMAX) or dual radio interface and aims to provide wireless connectivity between different subnetworks, including WBANs, home care networks, mobile patients and networks of healthcare providers (such as intranets of hospitals, clinics, drugstores, etc.).

Another remote monitoring scheme that provides ubiquitous connectivity for mobile patients has been presented in [27]. In the proposed scheme, a patient-attached monitoring device collects the WBAN data, classifies them as high-priority (e.g., critical data such as blood pressure, pulse rate and heart rate) or normal priority (e.g., ECG signal) and forwards them towards the e-Health provider through an heterogeneous WiFi/WiMAX access communication network. The access technology is selected depending on the patient's location, considering that WiFi hotspots cover only specific (mainly indoor) locations and WiMAX has a wider (outdoor) coverage. In addition, two types of connections are provided by the network operator: *i*) low-cost reserved connections, allocated to patients for given amounts of time (e.g., weeks); and *ii*) high-cost on-demand connections, employed when the available bandwidth for reserved connections is not enough to cover the traffic load. The authors approach this e-Health scenario from the service provider's side, who has to buy in advance a certain number of reserved connections from the network operator to serve a given number of patients. Stochastic programming techniques are used to determine the optimal number of reserved connections for each wireless technology in order to minimize the provider's cost.

As far as LTE-based solutions for healthcare applications are concerned, the relevant works in the literature are limited. The impact of 4G communication technologies on e-Health and the emerging challenges are discussed in [28]. In [29], a mapping between the QoS requirements of e-Health services and the existing service classes defined by 3GPP standards is proposed, aiming to provide guidelines for network operators. A cross-layer design for QoS of medical video streaming over mobile WiMAX (IEEE 802.16e) and High-Speed Packet Access (HSPA)[1] and a comparison between the performance of the two technologies is proposed in [30], opening

[1] HSPA technology is a precursor to LTE.

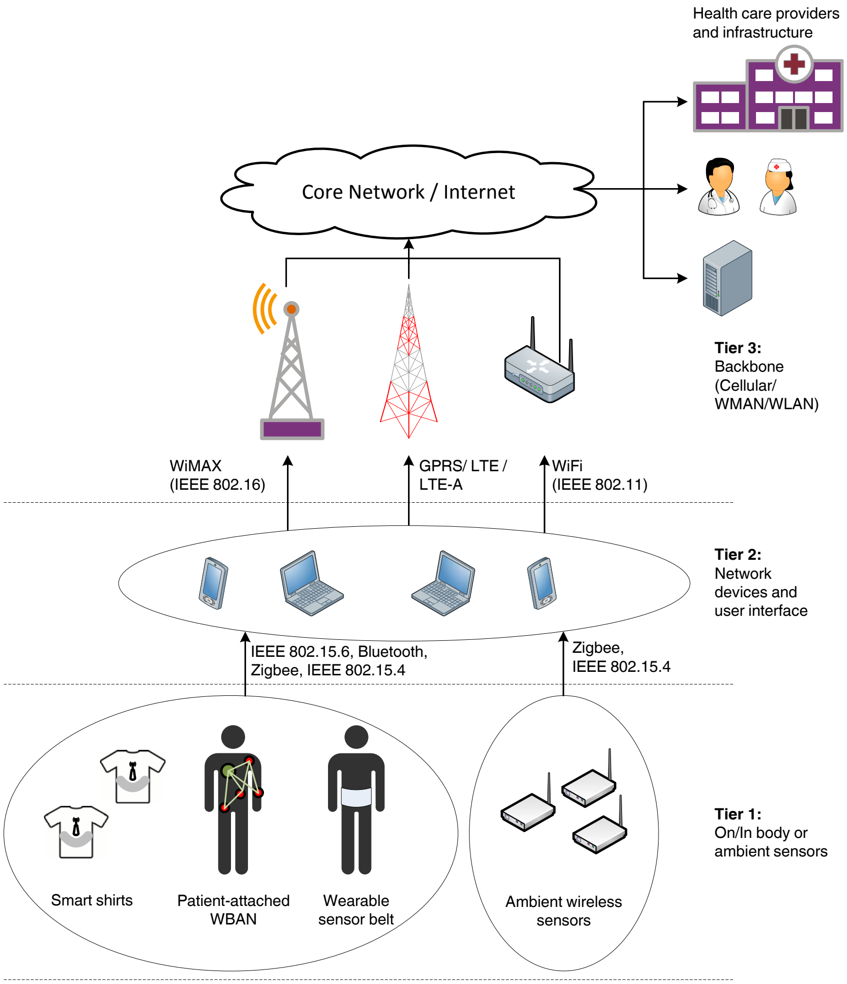

Fig. 2. Architecture of remote patient monitoring system for WiFi/WiMAX heterogeneous scenario (adapted from [27])

the road to further investigation on LTE-based e-Health applications.

B. Testbed Implementation of M2M Solutions

Research on end-to-end connectivity is not limited to a theoretical-only level. During the last years, research efforts have been devoted to the actual implementation of M2M networks. In this section, we present the most representative examples of implemented end-to-end solutions for e-Health applications.

In [31], the authors introduce a new file format for the transfer of sensory data and implement a pilot testbed for an end-to-end patient monitoring application. Their contribution is twofold.

First, they present an enhanced version of a standard protocol for communication among ECG devices, by proposing an adaptive data structure that can handle multiple vital signals, as well as data for positioning, allergies and demographic information on patients. The definition of a standardized data structure is an important step towards the integration of the medical data measured by the WBAN sensors with various e-Health information systems for monitoring or administrative purposes, belonging to hospitals, individual care-givers, home-care, etc. Second, they implement a testbed of an M2M healthcare application for the remote monitoring of patients suffering from heart problems. The patient is equipped with a WBAN formed by a number of wearable sensors, a Global Positioning System (GPS) device and a PDA. The PDA aggregates the sensory and geolocation data, as well as any additional information inserted manually by the patient, and plays the role of the M2M gateway. On the one hand, it employs Bluetooth technology to communicate with the WBAN nodes and, on the other hand, it has mobile ADSL capabilities to forward the data to the remote server located at a hospital facility. To the other end of the system, a portable data acquisition system is considered, consisting of a medical monitor device, a GPS and a laptop with Internet connectivity. Finally, a software application has been developed for the processing and visualization of the data retrieved by the healthcare provider. The pilot testing of the proposed solution on real patients has revealed some very interesting conclusions. From the doctors' perspective, the use of the M2M e-Health system has been an overall positive experience, facilitating the patient monitoring and the collection of data. The patients, on the other hand, have given a more neutral evaluation. Even though they have generally been satisfied by the experience, they have shown more concerns on the wearability of the sensors, the user friendliness of the software application and the data collection process.

A two-tier architecture is considered in [32] to implement a remote monitoring application for patients with Chronic Obstructive Pulmonary Disease (COPD). Bluetooth is used as the WBAN technology for the communication between the sensors and the coordinating node (e.g., a PDA). Apart from the Bluetooth network interface, the coordinating node can support two additional long-range wireless technologies for Internet connectivity with a remote medical server: cellular GPRS and WiFi. The authors perform an interesting experiment by measuring system performance metrics of these two upper-tier technologies. The study clearly shows that GPRS and WLAN have complementary power and delay profiles: the energy consumption of GPRS is low but high delays may be observed, whereas WiFi has higher energy cost but lower delays. Based on the observed results, the authors provide guidelines for the design of an adaptive protocol that switches between the two long-range technologies depending on the scenario: *i*) WiFi is the recommended technology, when available, especially in emergency situations due to the low data latency. In these cases, the GPRS interface should remain on but at an idle state, employed only to receive incoming calls if needed. *ii*) if the WiFi connection is not available, the WiFi network interface should be switched off completely and GPRS should be employed for communication.

In some works, ambient sensor networks for environmental monitoring are employed in conjunction with WBANs, in order to provide additional information on the patient's environment, such as temperature, humidity and light conditions. Along this line, a three-tier network architecture is proposed in [33], for the remote monitoring of elderly or chronic patients in their residence. The lower tier consists of two systems: *i*) a patient-worn fabric belt, which integrates the medical sensors and is equipped with a Bluetooth transceiver; and *ii*) the ambient wireless sensors that form a ZigBee network and are deployed in the patient's surroundings (e.g., in the patient's home or a nursing house). In the middle tier, an ad hoc network of powerful mobile computing devices (e.g., laptops, PDAs, etc.) gathers the medical and ambient sensory data and forwards them to the higher tier. The middle-tier devices must have multiple network interfaces: Bluetooth and ZigBee to communicate with the lower tier and WLAN or cellular capabilities for connection with the higher layer. Finally, the higher tier is structured on the Internet and includes the application databases and servers that are accessed by the healthcare providers. The study involves a real implementation of the proposed architecture and tackles several security issues that arise along the three tiers. The proposed framework offers a flexible and secure solution for the monitoring of multiple patients that can be applied to different scenarios, including home, hospital and nursing home environments.

Sensor networks can also be employed for patient localization purposes. In [34], the authors propose a system architecture based on two independent subsystems for the monitoring and location tracking of patients within hospital environments. The healthcare monitoring subsystem consists of smart shirts with integrated medical sensors, each equipped with a wireless IEEE 802.15.4 module. The location subsystem has two components: *i*) a deployment of wireless IEEE 802.15.4 nodes that are installed in known locations within the hospital infrastructure and broadcast periodic beacon frames; and *ii*) IEEE 802.15.4 end devices, held by the patients, that collect signal strength information from the received beacons. Both subsystems transmit their respective data (i.e., medical sensory data and signal strength information) to a gateway through an IEEE 802.15.4-based ad hoc distribution network. The gateway has wired Internet connectivity and forwards the data to the management server and the monitoring e-Health application. The proposed system has been tested with success in a hospital, achieving high reliability, sufficient battery lifetime of the sensors and real-time data reconstruction. In terms of usability, the obtained feedback of the medical personnel has been taken into account to improve the software interface.

C. Security and Privacy Issues

Despite the great potential for improving the quality of life, the introduction of M2M e-Health solutions raises considerable security and privacy challenges, mainly due to the confidential nature of the medical data exchanged in healthcare environments. The remaining of this section discusses the main security challenges, along with the most representative solutions proposed in the literature.

1) Challenges: In order to preserve the confidentiality of sensitive medical data, international organizations oblige the healthcare providers to follow specific privacy rules [35], [36], by setting strict civil and criminal penalties to punish any sensitive data leakage. Hence, a plethora of research surveys has been recently released [37]–[42], focusing mainly on the M2M area network. In this context, the security framework is divided into two slightly overlapping parts: *i*) *Data Security*, and *ii*) *Data Privacy*. The former deals with the secure data storage and transfer through the (usually wireless) medium, while the latter tackles access rights and secrecy issues related to the patient's private information, including among others identity, time and location.

The requirements for the schemes of the first class do not substantially differ from the general requirements of wireless networks. However, the application of traditional security methods in M2M area networks is not straightforward, due to the intrinsic characteristics of wireless sensor devices, such as small size, restricted computational capabilities and limited energy resources. In particular, the main issues concerning security are:

- Data Integrity: The broadcast nature of M2M area networks enables adversary users to intervene in the transmissions, posing high risks in emergency life-critical events. Therefore, proper data integrity mechanisms have to be put in place to ensure that the received data have not been altered.

- Data Authentication: In healthcare environments, the authentication of the transmitted data is essential to guarantee and verify whether the received packets come from a trusted source.
- Data Availability: The medical data and information have to be available upon any-time request, without being hampered by Denial-of-Service (DoS) attacks.
- Data Freshness: In the e-Health domain, data freshness is of crucial importance, since it indicates that the received physiological patient signals are up-to-date and not simply replayed by malicious users.

On the other hand, on ensuring privacy, the following fundamental requirements have to be considered:

- Data Confidentiality: As mentioned above, health data are generally subject to ethical and legal obligations of confidentiality, thus offering substantial protection from malicious eavesdropping, which is further facilitated by the broadcast wireless nature.
- User Authentication: User authentication is a strong prerequisite in healthcare environments so as to prevent unauthorized users from gaining access to sensitive medical information.
- User Localization: The location privacy is one very important aspect in M2M area networks. Concealing the patient's location precludes malicious users to claim legitimate coordinates in the network, while hindering any false signals that create confusion with regard to the patient's real physical location.

Apart from the aforementioned commonplace security requirements, new challenges are posed by the M2M concept which includes the interconnection of different technologies, as well as the data storage in multiple different physical locations. Considering the importance and the criticality of medical data, we will provide a brief an overview of the security-related research conducted in the e-Health domain, providing useful insights on issues that arise either in the M2M area network or in the whole end-to-end system.

2) Approaches: Several cryptographic schemes have been already proposed in the literature, trying to provide effective solutions for data integrity, authentication and confidentiality. Most schemes provide encrypting capabilities based on a secret key shared among nodes, either in software [43] or hardware level [44], [45]. In addition, notable advances have been observed in the implementation of Elliptic Curve Cryptography (ECC) [46], [47], which has emerged as a promising alternative to RSA-based algorithms, guaranteeing the same level of security, while employing a much smaller key size. To overcome the limitations of traditional symmetric cryptography in wireless networks, biometrics [48], [49] exploit particular physiological values of the patient's body in order to provide efficient cryptographic techniques in WBANs, thus gaining significant ground in healthcare environments.

Apart from the important technological achievements with regard to cryptography, several other works deal with privacy issues, motivated by the challenges that arise on the higher tiers of the network architecture due to the involvement of many different entities in end-to-end approaches. Narayanan and Gunes [50] present an information protection framework against unauthorized access in cloud provisioned multi-tenant healthcare systems. The term multi-tenant explicitly refers to the plethora of authorities that need access to the sensitive medical data, including hospitals, clinics, pharmacies, professionals and, in some cases, the patients themselves. The authors propose an improved access control scheme for cloud instances by extending the well-known Task-Role-Based Access Control Model [51] to include adaptive user roles and tasks in order to support multi-tenant cloud applications.

Similar issues about guaranteeing user privacy across several providers and organizations are also addressed in [52], [53]. In particular, the work in [52] aims at extending the traditional service-oriented architecture framework to define a flexible policy-based approach for defining and monitoring streaming event data based on a general publish/subscribe model in business-to-business healthcare networks. The policy-based framework presented in this paper is a specific part of a comprehensive information system, named Palliative Information System, designed to support day-to-day homecare delivery for palliative care patients.

A preliminary approach to address security and privacy issues is presented in [53]. In emergency scenarios, the "on-the-fly" network integration as well as the information exchange among different entities are of paramount importance. However, the achievement of these goals is complicated, since each domain may correspond to a different authority. The proposed solution supports medical device integration and authentication among networks of different providers, dealing with interoperability challenges by using open standards like ISO/IEEE 11073-20601 ([54]), Device Profile for Web Services and Bluetooth Health Device Profile for medical data transmission. Their solution claims to ensure cost-effectiveness, simplicity and emergency support through sharing devices among authorities and dynamically reintegrating them in case of network alteration. Moreover, a new DPWS-based security model is described, without, however, considering scope crucial parameters such as trusting and key distribution among the authorities.

Finally, it is worth noting the importance of guaranteeing an undisclosed location for the nodes (and consequently for the patient) in healthcare scenarios. Although location information is necessary in sensor networks, it can evolve in a serious threat in case that security and privacy restrictions are not met. To this end, many works in the literature have set the focus on designing effective secure localization methods [55], [56] and the interested reader may further refer to [57] for a complete guide to secure localization schemes in sensor networks.

V. Existing Projects

The aim of this section is to present an overview of the most recent and relevant research funded projects for e-Health applications.

HEALTH@HOME (Health at Home) (www.aal-europe.eu/projects/healthhome) aims to provide an end-to-end solution for the remote monitoring of cardiovascular and respiratory patient parameters. The data are continuously gathered through an automatic processing system and are accessed by the responsible medical personnel. A typical client/server architecture is adopted, where the client side is a residential gateway located at the patient's home, able to collect data from the biomedical sensors through wireless Bluetooth links. The most significant measured signals are ECG, SpO2, weight, blood pressure, chest impedance, respiration and body posture. The measured data are sent through the gateway to a server located at the health service facilities that is integrated with the Hospital Information System. The gateway communicates with the server through ADSL as the primary transmission channel, or mobile broadband (i.e., GSM/GPRS/UMTS) as the secondary (backup) data channel. Alarms are sent by Short Message Service (SMS) directly to the physicians, the patients' relatives and their caregivers. The HTTPS protocol addresses the security issues in the communication between the gateway and the server through a certificate validation process. The proposed solution has been tested on 30 patients during monitoring periods of at least one month and has received positive feedback by both patients and medical personnel, as a reliable, user-friendly means of remote control and management of acute conditions.

IS-ACTIVE (Inertial Sensing Systems for Advanced Chronic Condition Monitoring and Risk Prevention) (www.is-active.eu) provides a person-centric healthcare solution for elderly people that suffer from Chronic Obstructive Pulmonary Disease (COPD). The project aims to provide real-time support to users in order to monitor, self-manage and improve their physical condition by encouraging physical activity through visual feedback and real-time motivational cues. Since motion sensing is one of the main goals of IS-ACTIVE, inertial sensor nodes (accelerometers and gyroscopes) and sensor nodes that measure physiological data (heart rate, oxygen saturation, etc.) are employed. The nodes form a WBAN and report the sensory data to a central gateway, connected by cable to a computer. The node communication takes place at the 2.4 GHz ISM band, while two operation modes are adopted: *i*) low-power, low data rate IEEE 802.15.4 compatible implementation, for long-term sensing and monitoring, e.g., for activity level monitoring applications, and *ii*) high data rate, real-time motion capture via the proprietary FastMAC networking protocol, for short term, detailed sensory data acquisition, e.g., for algorithm design and evaluation.

HELP: Home-based Empowered Living for Parkinson Disease Patients (www.aal-europe.eu/projects/help) targets at designing a health monitoring system able to control disease progression and to mitigate Parkinson Disease (PD) symptoms, thus improving the quality of life of affected elderly people. Although it provides an end to end solution that employs M2M communication for monitoring patients with PD, its aim is to design a control system for a subcutaneous infusion pump that administers the exact required drug dose according to the patients' level of activity without focusing in communication issues. This system is composed of the following components: *i*) an intra-oral electronic drug delivery device with miniaturized, non-invasive and removable design, *ii*) an external pump that delivers higher amounts of drug, *iii*) a WBAN to gather information on the user environment to detect blockades, *iv*) a telecommunication and services infrastructure to analyze and transfer data exchanged between the user and the automated system, and *v*) a remote care unit for patient supervision.

WiserBAN (Smart miniature low-power wireless microsystem for Body Area Networks) (www.wiserban.eu) objective is to improve personal sensing capabilities by using tiny, unobtrusive, long-lifetime radio microsystems for WBAN sensor nodes, such as hearing aids, cardiac implants, insulin pumps and cochlear implants. Particular emphasis is given on: *i*) sensor miniaturization for both implantable and wearable based WBANs, *ii*) the sensor data processing efficiency compared to microprocessors used in WBAN radios, and *iii*) the development of a flexible/reconfigurable and low-power radio baseband system. To meet the aforementioned requirements, WISERBAN proposes a highly integrated microsystem that includes radio and antenna and data processing units. Two RF blocks in 65 nm CMOS technology that operate in the 2.4 GHz and the 402-405 MHz MICS band are implemented, along with reconfigurable PHY and MAC layer protocols. Apart from the key medical related use cases, WiserBAN has an ambitious exploitation plan with possible applications in home energy management, smart grids and even military communication scenarios.

CAALYX-MV: Complete Ambient Assisted Living Experiment - Market Validation (www.caalyx-mv.eu) goal is to provide an end to end solution that is focused on improving the elder's quality of life. The proposed solution is composed of: *i*) a home system capable of monitoring and controlling social and health status of elder people and providing them with some tools and services to support their daily activities, *ii*) a roaming system that comprises a smart textile shirt able to measure specific vital signs, detect falls and communicate emergencies, and *iii*) a care system for the monitoring of individuals by family, caretakers and health services. All sensors in the WBAN are wearable, measure different parameters such as motion, blood pressure and heart rate, and communicate using Bluetooth links with a mobile phone. The sensory data are sent through standard low-cost networking equipment to a GPS-enabled smart phone (3G/UMTS) that runs a completely autonomous software application. The application continuously analyzes sensor data in order to identify problematic conditions and promptly alert the care system. The proposed system will be validated through 3 pilot programs that will test the usability and acceptability of the system by the users (both patients and caregivers) and will evaluate the reliability and detection accuracy of health problems in the monitored patients.

Help4Mood (http://www.help4mood.info/site/default.aspx) aims at developing an end-to-end system to help the recovery of people with major depression. The system is designed to be used together with other forms of therapy, such as self-help, counseling or medication. The main components include: *i*) a personal monitoring system to keep track of important behavior aspects, comprised of sensors for both user activity and sleep monitoring, *ii*) an interactive virtual agent asking patients about their health and well-being and providing a portal to trusted health information, and *iii*) a decision support system handling the virtual agent to allow its customization to the individual needs of the person with depression.

The sensor devices communicate by using a proprietary low-power RF network protocol named SimpliciTI [58] over Bluetooth. To increase energy efficiency and reliability, the system adopts the idea of cooperation between nodes, achieved through the slight modification of the MAC protocol.

EXALTED (EXpAnding LTE for Devices) (http://www.ict-exalted.eu/) is a project that focuses on developing a new scalable network architecture to support the most challenging requirements for future wireless communication systems. Its aim is to provide secure, energy-efficient and cost-effective M2M communications for low-end devices. Motivated by the inability of LTE Releases 8, 9 and 10 to serve a multitude of low data rate devices in an energy-, spectrum- and cost-efficient way, EXALTED proposes improvements that can be easily integrated in the new LTE-M backbone. The LTE-M extension aims to fulfill the specific energy, spectrum, cost, efficiency constraints of M2M communications, by proposing improvements on the PHY, MAC, Radio Link Control, Packet Data Convergence Protocol and the Radio Resource Control layers of LTE. Security issues for LTE-M networks are also addressed. Finally, proof-of-concept of the proposed techniques will be provided through the implementation of a realistic testbed.

WSN4QoL: Wireless Sensor Networks for Quality of Life (http://www.wsn4qol.eu/) is a project focused on wireless communication technologies for e-Health applications. The main objectives of WSN4QoL are: *i*) to provide a protocol stack architecture, which can accommodate a variety of protocols, algorithms and sensor devices for healthcare applications, *ii*) to develop reliable, energy-efficient, interference-robust communication protocols and algorithms, *iii*) to develop distributed localization protocols that meet the constraints imposed by WBANs in health care scenarios, and *iv*) to propose effective and efficient security solutions for the proposed communication protocols. The proposed protocols and algorithms will be integrated in healthcare commercial devices, in order to evaluate the performance improvements in realistic environments.

To conclude, TABLE II provides a comparison among the main characteristics of the projects presented here. Summarizing, even though the objectives of all M2M health related projects are different, some common goals can be identified: - reliable communication of data, both at a WBAN level as well as an end to end level - accurate detection of alarms to avoid unnecessary hospitalizations and detect emergencies - wearability, user friendliness etc...

VI. Concluding Remarks

This chapter has provided an overview of M2M systems for e-Health applications from a wireless communication perspective. After describing the high-level ETSI M2M system architecture, we presented the key candidate technologies that can be employed at different parts of the system,

TABLE II

SUMMARY OF EXISTING PROJECTS ON E-HEALTH APPLICATIONS

Project	**Main Application**	**M2M Area Net. Technology**	**M2M Com. Net. Technology**	**End to End**	**Real World Validation**	**Security Issues**
HEALTH@HOME	CVD	Bluetooth	ADSL	✓	✓	✓
IS-ACTIVE	Fall detection	Bluetooth	UMTS	✗	✓	✗
HELP	Parkinson disease	Bluetooth	–	✓	✓	✗
WISERBAN	Healthcare sensors	IEEE 802.15.6	–	✗	✗	✗
CAALYX-MV	Independent living	Bluetooth	3G UMTS / WiFi	✓	✓	✓
Help4Mood	Depression management	Bluetooth/SimpliciTI	ADSL	✓	✓	✓
EXALTED	Technology-oriented	–	LTE-M	✗	✓	✓
WSN4QoL	Communication-oriented	IEEE 802.15.6	–	✗	✓	✓

to provide short-range interconnection of the sensor devices, as well as long-range Internet connectivity. We, then, focused on end-to-end connectivity in M2M systems. After discussing the integration challenges between diverse communication technologies, we have highlighted different design approaches for end-to-end connectivity through examples of practical testbed implementations for healthcare services. Security and privacy challenges pertinent to e-Health have also been addressed. Finally, a list of recent research projects in the context of e-Health has been given, with emphasis on the different technical solutions adopted in each project.

Summarizing, the presented works and projects study different aspects of M2M systems for healthcare delivery, ranging from solving technical communication problems to the implementation of close to market solutions. Despite their differences, several common goals can be identified, that can serve as guidelines for the design of successful end-to-end e-Health applications: *i*) miniaturization and enhanced wearability of the sensor devices, to provide unobstructive monitoring that will not interfere with normal life activities of the patients, *ii*) reliable two-way communication protocols, that guarantee the prompt and successful delivery of data from the medical sensors to the medical personnel, as well as the reception of medical feedback at the patient, *iii*) accurate detection of emergency situations to ensure timely medical intervention in life threatening events. In addition, it is important to maintain a low probability of false positive alarms, to avoid unnecessary hospitalizations and interventions, *iv*) advanced security mechanisms to guarantee confidentiality and privacy of the medical data, and *v*) user friendly and easy to learn application interfaces, to ensure the successful adoption of the e-Health solutions, given that patients are often elderly people not familiar with the use of technology. Furthermore, the visualization of the monitored data must be done in a clear and helpful way for both the patient and the healthcare providers.

ACKNOWLEDGEMENTS

This work has been funded by the research projects ESEE (324284), WSN4QoL (286047) and GEOCOM (TEC2011-27723-C02-01).

REFERENCES

[1] OECD Report, "Machine-to-Machine Communications: Connecting Billions of Devices," *OECD Digital Economy Papers*, vol. 192, Jan. 2012. available online at: http://dx.doi.org/10.1787/5k9gsh2gp043-en.

[2] K. Chang, A. Soong, M. Tseng, and Z. Xiang, "Global Wireless Machine-to-Machine Standardization," *IEEE Internet Computing*, vol. 15, pp. 64–69, Mar.–Apr. 2011.

[3] "oneM2M global Partnership Project," July 2012. http://www.onem2m.org/.

[4] Machina Research, "Machine-to-Machine (M2M) Communications in Healthcare 2010-20," May 2011.

[5] ETSI, "Machine to Machine Communications (M2M): Use Cases of M2M Applications for eHealth," *Draft TR 102732 v0.4.1*, Mar. 2011.

[6] G. Wu, S. Talwar, K. Johnsson, N. Himayat, and K. Johnson, "M2M: From mobile to embedded internet," *IEEE Communications Magazine*, vol. 49, pp. 36–43, Apr. 2011.

[7] K.-C. Chen, "Machine-to-Machine Communications for Healthcare," *Journal of Computing Science and Engineering*, vol. 6, pp. 119–126, June 2012.

[8] X. Shen, "Emerging technologies for e-healthcare [Editor's Note]," *IEEE Network*, vol. 26, pp. 2–3, Sept. - Oct. 2012.

[9] A. Aragues, J. Escayola, I. Martinez, P. del Valle, P. Munoz, J. Trigo, and J. Garcia, "Trends and challenges of the emerging technologies toward interoperability and standardization in e-health communications," *IEEE Communications Magazine*, vol. 49, pp. 182–188, Nov. 2011.

[10] J. Ko, C. Lu, M. Srivastava, J. Stankovic, A. Terzis, and M. Welsh, "Wireless sensor networks for healthcare," *Proceedings of the IEEE*, vol. 98, pp. 1947–1960, Nov. 2010.

[11] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. Leung, "Body Area Networks: A Survey," *Mobile Networks and Applications*, vol. 16, pp. 171–193, Apr. 2011.

[12] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wireless Networks*, vol. 17, pp. 1–18, Jan. 2011.

[13] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," *Computer Networks*, vol. 54, pp. 2688–2710, Oct. 2010.

[14] M. Patel and J. Wang, "Applications, challenges, and prospective in emerging body area networking technologies," *IEEE Wireless Communications*, vol. 17, pp. 80–88, Feb. 2010.

[15] ETSI, "Machine to Machine Communications (M2M): Functional Architecture," *Technical Specification TS 102690 v1.1.1*, Oct. 2011.

[16] Enrico Scarrone, "The ETSI M2M standard as enabler of a global market," in *11th edition of the M2M Forum*, May 2012. available online at: http://www.m2mforum.com/eng/images/stories//scarroneopening.pdf.

[17] H. Cao, V. Leung, C. Chow, and H. Chan, "Enabling Technologies for Wireless Body Area Networks: A Survey and Outlook," *IEEE Communications Magazine*, vol. 47, pp. 84–93, Dec. 2009.

[18] "IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Personal Area Networks (WPANs)," *IEEE Std 802.15.1-2005 (Revision of IEEE Std 802.15.1-2002)*, June 2005.

[19] "IEEE Standard for Local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)," *IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006)*, June 2011.

[20] "Wireless Universal Serial Bus Specification 1.1," Sept. 2010.

[21] "IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," *IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-2007)*, Mar. 2012.

[22] "IEEE Standard for Air Interface for Broadband Wireless Access Systems," *IEEE Std 802.16-2012 (Revision of IEEE Std 802.16-2009)*, pp. 1–2542, June 2012.

[23] S. Baker and D. Hoglund, "Medical-Grade, Mission-Critical Wireless Networks [Designing an Enterprise Mobility Solution in the Healthcare Environment]," *IEEE IEEE Engineering in Medicine and Biology Magazine*, vol. 27, pp. 86–95, Mar.–Apr. 2008.

[24] J. Misic and V. Misic, "Bridging between IEEE 802.15.4 and IEEE 802.11b networks for multiparameter healthcare sensing," *IEEE Journal on Selected Areas in Communications*, vol. 27, pp. 435–449, May 2009.

[25] J. Misic and V. Misic, "Bridge performance in a multitier wireless network for healthcare monitoring," *IEEE Wireless Communications*, vol. 17, pp. 90–95, Feb. 2010.

[26] Y. Zhang, N. Ansari, and H. Tsunoda, "Wireless telemedicine services over integrated IEEE 802.11/WLAN and IEEE 802.16/WiMAX networks," *IEEE Wireless Communications*, vol. 17, pp. 30–36, Feb. 2010.

[27] D. Niyato, E. Hossain, and S. Camorlinga, "Remote patient monitoring service using heterogeneous wireless access networks: architecture and optimization," *IEEE Journal on Selected Areas in Communications*, vol. 27, pp. 412–423, May 2009.

[28] R. S. H. Istepanaian and Y.-T. Zhang, "Guest Editorial Introduction to the Special Section: 4G Health – The Long-Term Evolution of m-Health," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, pp. 1–5, Jan. 2012.

[29] L. Skorin-Kapov and M. Matijasevic, "Analysis of QoS requirements for e-health services and mapping to evolved packet system QoS classes," *International Journal of Telemedicine and Applications [Special issue on healthcare applications and services in converged networking environments]*, vol. 9, pp. 1–18, Jan. 2010.

[30] A. Alinejad, N. Philip, and R. Istepanian, "Cross-Layer Ultrasound Video Streaming Over Mobile WiMAX and HSUPA Networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, pp. 31–39, Jan. 2012.

[31] G. J. Mandellos, M. N. Koukias, I. S. Styliadis, and D. K. Lymberopoulos, "e-SCP-ECG+ protocol: an expansion on SCP-

ECG protocol for health telemonitoring – pilot implementation," *International Journal of Telemedicine and Applications [Special issue on healthcare applications and services in converged networking environments]*, vol. 2010, pp. 1–17, Jan. 2010.

[32] K. Wac, M. Bargh, B.-j. Van Beijnum, R. Bults, P. Pawar, and A. Peddemors, "Power- and delay-awareness of health telemonitoring services: the mobihealth system case study," *IEEE Journal on Selected Areas in Communications*, vol. 27, pp. 525–536, May 2009.

[33] Y. Huang, M. Hsieh, H. Chao, S. Hung, and J. Park, "Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks," *IEEE Journal on Selected Areas in Communications*, vol. 27, pp. 400–411, May 2009.

[34] G. López, V. Custodio, and J. Moreno, "LOBIN: E-Textile and Wireless-Sensor-Network-Based Platform for Healthcare Monitoring in Future Hospital Environments," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, pp. 1446–1458, Nov. 2010.

[35] Office for Civil Rights, United State Department of Health and Human Services, "Medical Privacy - National Standards to Protect the Privacy of Personal Health Information." available online at:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html.

[36] The Data Protection Directive, "EU Directive 95/46/EC." available online at:
http://www.dataprotection.ie/viewdoc.asp?m=&fn=/documents/legal/6aii-1c.htm#1.

[37] P. Kumar and H.-J. Lee, "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2011.

[38] T. Dimitriou and I. Krontiris, "Security issues in biomedical wireless sensor networks," in *Proc. of the 1st International Symposium on Applied Sciences on Biomedical and Communication Technologies (ISABEL 2008)*, pp. 1–5, Oct. 2008.

[39] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, "Security and Privacy for Implantable Medical Devices," *IEEE Pervasive Computing*, vol. 7, pp. 30–39, Jan. 2008.

[40] E. Weippl, A. Holzinger, and A. M. Tjoa, "Security aspects of ubiquitous computing in health care," *e & i Elektrotechnik und Informationstechnik*, vol. 123, pp. 156–161, 2006. 10.1007/s00502-006-0336.

[41] D. Kotz, "A threat taxonomy for mHealth privacy," in *Proc. of the 3rd International Conference on Communication Systems and Networks (COMSNETS 2011)*, pp. 1–6, Jan. 2011.

[42] S. Avancha, A. Baxi, and D. Kotz, "Privacy in mobile technology for personal healthcare," *ACM Computing Surveys*, vol. 45, pp. 3:1–3:54, Dec. 2012.

[43] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in *Proc. of the 2nd international conference on Embedded networked sensor systems (SenSys 2004)*, pp. 162–175, ACM, 2004.

[44] M. Healy, T. Newe, and E. Lewis, "Efficiently securing data on a wireless sensor network," *Journal of Physics: Conference Series*, vol. 76, no. 1, 2007.

[45] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S. Lin, and J. Stankovic, "ALARM-NET: Wireless sensor networks for assisted-living and residential monitoring," tech. rep., Department of Computer Science, University of Virginia, Tech. Rep. CS-2006-1,, 2006.

[46] A. Liu and P. Ning, "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks," in *Proc. of the International Conference on Information Processing in Sensor Networks, (IPSN 2008)*, pp. 245–256, Apr. 2008.

[47] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab, "NanoECC: testing the limits of elliptic curve

cryptography in sensor networks," in *Proc. of the 5th European Conference on Wireless sensor networks (EWSN 2008)*, (Berlin, Heidelberg), pp. 305–320, Springer-Verlag, 2008.

[48] F. M. Bui and D. Hatzinakos, "Biometric methods for secure communications in body sensor networks: resource-efficient key management and signal-level data scrambling," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, pp. 1–16, Jan. 2008.

[49] K. K. Venkatasubramanian and E. K. S. Gupta, "Security for pervasive health monitoring sensor applications," in *Proc. of the 4th International Conference on Intelligent Sensing and Information Processing (ICISIP 2006)*, pp. 197–202, Dec. 2006.

[50] H. Narayanan and M. Gunes, "Ensuring access control in cloud provisioned healthcare systems," in *Proc. of IEEE Consumer Communications and Networking Conference (CCNC 2011)*, pp. 247–251, Jan. 2011.

[51] S. Oh and S. Park, "Task-role-based access control model," *Inf. Syst.*, vol. 28, pp. 533–562, Sept. 2003.

[52] B. Eze, C. Kuziemsky, L. Peyton, G. Middleton, and A. Mouttham, "Policy-based Data Integration for e-Health Monitoring Processes in a B2B Environment: Experiences from Canada," *Journal of theoretical and applied electronic commerce research*, vol. 5, pp. 56 – 70, 04 2010.

[53] A. Kliem, M. Hovestadt, and O. Kao, "Security and Communication Architecture for Networked Medical Devices in Mobility-Aware eHealth Environments," in *Proc. of IEEE First International Conference on Mobile Services (MS 2012)*, pp. 112–114, June 2012.

[54] "ISO/IEC/IEEE Health informatics–Personal health device communication–Part 20601: Application profile–Optimized exchange protocol," *ISO/IEEE 11073-20601:2010(E)*, pp. 1–208, 1 2010.

[55] N. Labraoui and M. Gueroui, "Secure range-free localization scheme in Wireless sensor networks," in *Proc. of the 10th International Symposium on Programming and Systems (ISPS 2011)*, pp. 1–8, Apr. 2011.

[56] J. Jiang, G. Han, L. Shu, H.-C. Chao, and S. Nishio, "A novel secure localization scheme against collaborative collusion in wireless sensor networks," in *Proc. of the 7th International Wireless Communications and Mobile Computing Conference (IWCMC 2011)*, pp. 308–313, July 2011.

[57] A. Srinivasan and J. Wu, "A Survey on Secure Localization in Wireless Sensor Networks," in *Encyclopedia of Wireless and Mobile Communications* (B. Furht, ed.), CRC Press, Taylor and Francis Group, Boca Raton, London, 2008.

[58] "Simpliciti protocol stack." www.ti.com/tool/simpliciti.