WARWICK
THE UNIVERSITY OF WARWICK

Original citation:
Katzis, Konstantinos, Jones, Richard W. and Despotou, George (2017) Totally connected healthcare with TV white spaces. In: Mantas, John and Hasman, Arie and Gallos, Parisis and Househ, Mowafa S. , (eds.) Informatics Empowers Healthcare Transformation. Studies in Health Technology and Informatics, 238. IOS Press, pp. 68-71. ISBN 9781614997801

Totally Connected Healthcare with TV White Spaces

Konstantinos KATZIS[a,1], Richard W. JONES[b] and Georgios DESPOTOU[c]
[a] *Depatment of Computer Science and Engineering, European University Cyprus, CY*
[b] *School of Engineering, University of Warwick, U.K.*
[c] *Institute of Digital Healthcare WMG, University of Warwick, U.K.*

Abstract. Recent technological advances in electronics, wireless communications and low cost medical sensors generated a plethora of Wearable Medical Devices (WMDs), which are capable of generating considerably large amounts of new, unstructured real-time data. This contribution outlines how this data can be propagated to a healthcare system through the internet, using long distance Radio Access Networks (RANs) and proposes a novel communication system architecture employing White Space Devices (WSD) to provide seamless connectivity to its users. Initial findings indicate that the proposed communication system can facilitate broadband services over a large geographical area taking advantage of the freely available TV White Spaces (TVWS).

Keywords. Wearable Medical Devices, Body Area Networks, TVWS

Introduction

Future communications envisage a plethora of wireless, connected, sometimes ‘smart’ devices that will communicate in real time with each other. This is referred to as the ‘Internet of Things’. These devices are expected to be part of our daily lives, interfacing not only with humans, but also with other devices known as machine to machine communications [1]. IoT enabled medical devices are expected to form a smart environment that is characterized by polymorphic requirements in terms of latency, throughput, reliability, speed, power, security, etc. generating enormous amounts of new, unstructured real-time data. 5G is expected to provide connectivity to such devices including a wide range of Wearable Medical Devices (WMD) [2]. When considering broadband connections, one might think the fastest the better. Nevertheless, some of these devices / users might not necessarily require a ‘gigabit experience’ but lower data-rates to maintain longer battery life and reliability. WMD requirements, are application specific but there are a common set of constraints in size, power and functionality since they are all going to be carried by humans. The location of the WMD, data rate, frequency and regulatory standards all influence the design complexity and power dissipation of telemetry links. The design of antenna is very demanding with the major challenges being miniaturization, low-power consumption to aid the energy efficiency of the MD (especially in the case of Implanted Medical Devices). Patch antennas are generally used because of their flexibility in design, conformability and shape [4]. For those that they do need the high data-rate experience, delivering higher capacities and speeds requires better cell densification and access to new, broader carriers in new spectrum. So how can 5G network address all these devices singlehanded? For the time being and perhaps for the next few years, part of the capacity growth can be gradually addressed by the ageing 3G/4G based systems, but by 2020, 5G technologies will have to be operational. Nokia [4] and Ericsson [5] introduced a number of new services and use cases that will drive the technology such as mobile broadband, mobile media, IoT, etc. Based on these use-cases, it has been deduced that 5G networks will be have to somehow fulfill the 5 major parameters and these are: throughput, capacity, number of devices, cost, latency and reliability. This contribution proposes a novel long-range communication system architecture which is using unlicensed frequencies (470-700MHz) to provide internet connectivity to WMDs. The approach to identifying the challenges included a digital library search, as well as review of the main standard applicable to TVWS which is IEEE 802.22. The authors picked a representative sample from the results, based on their experience. The literature used the keywords "wearable + medical + device + IoT" and "wearable + medical device + TV white spaces". The papers were reviewed by the authors for examples or discussion on the interaction between security design features.

1. Wearable Medical Devices – Operation parameters and requirements

Advances in electronics, sensors and IoT technology, has inspired the design of new medical devices, shaping the new generation of Body Area Networks (BAN) and healthcare. Wearable Medical Devices (WMDs) and Implanted Medical Devices (IMDs) can be considered part of the BAN and expected to generate data, communicate it, aggregate it, and analyze it providing constant health monitoring for the patients. This enables the healthcare system to sustain detailed long-term health records of patients and help the doctors make the correct diagnosis. Current wireless technologies used for connecting various medical sensors are: Bluetooth, ZigBee, WiFi, RFID, IEEE 802.15.6, etc [6]. As the number of applications increases, existing wireless technologies will not be able to cope with the fast-evolving sensors. For example, the data-rates supported by the current standards might not be able to cope with future sensors which will generate larger volumes of data. Furthermore, security is already an issue for some of the standards such as RFID and ZigBee [7],[8]. This means that great caution must be taken when using them in a healthcare environment.

2. Current and future Mobile Networks – Providing services to WMDs

Remote monitoring for large numbers of patients will require high bandwidth, reliable communication links, large coverage area and high quality of service when deploying future mobile communication systems. Today, the main wireless cellular mobile network technologies that can be used to provide substantial coverage and data-rates for wireless medical devices are 3G: WCDMA, CDMA2000, EVDO and 4G: Long Term Evolution (LTE). Nevertheless, these types of wireless networks cannot provide direct connectivity to WMDs and IMDs devices since these are usually low power, high frequency devices usually operating in the Industrial Scientific Medical (ISM) bands. Furthermore, it will be expensive for the patient to keep all devices connected transmitting through these networks. Future 5G systems will bring in paradigm shift in remote patient monitoring and tracking but probably at a high cost. It is expected that it will form the new technology of choice for applications that require very high capacity as well as very low latency. Nevertheless, 5G networks is promising high bandwidth (1gbps per user) and coverage for its users with sub-1ms latency needed to support the time-critical applications in emergency applications such as healthcare.

3. TV White Spaces for Connecting Wearable Medical Devices?

WMDs and IMDs are considered highly demanding due to the nature of the data exchanged, depending on the mission and safety critical process control data. They therefore require robust, low latency, reliable and highly available wireless links while interference must be mitigated in an interference-prone radio-busy radio environment. What we are proposing here is a communication system architecture that will connect all WMDs and IMDs to the healthcare system in a secure way while guaranteeing the polymorphic requirements of each application. As part of this system, a device – called Body Sensor Managing Device (BSMD) is introduced to locally communicate with the WMDs and IMDs through the BAN, while it will transmit the data to the internet through unlicensed TV White Space (TVWS) spectrum employing the IEEE 802.22 communication standard also known as WiFar (see fig.1). Users carrying their BSMD equipment, are expected to move through the 802.22 cellular network and connect to the closest base-station to achieve internet access. The IEEE802.22 cellular network, to avoid causing / receiving interference to the incumbent devices (see fig 1), sensing-assisted spectrum databases (SASDs) are used where they offer an efficient solution for certain scenarios, eliminating the need for wireless network operations and management in a complex, interference-prone local or indoor environment when used in the context of self-configuration [12]. Since healthcare has very strict operational requirements it is imperative to employ dynamic spectrum management, relying on the information collected and managed by such databases in order to ensure incumbent protection, co-existence and interference management as well as fine-grained adaptation to available spectrum.

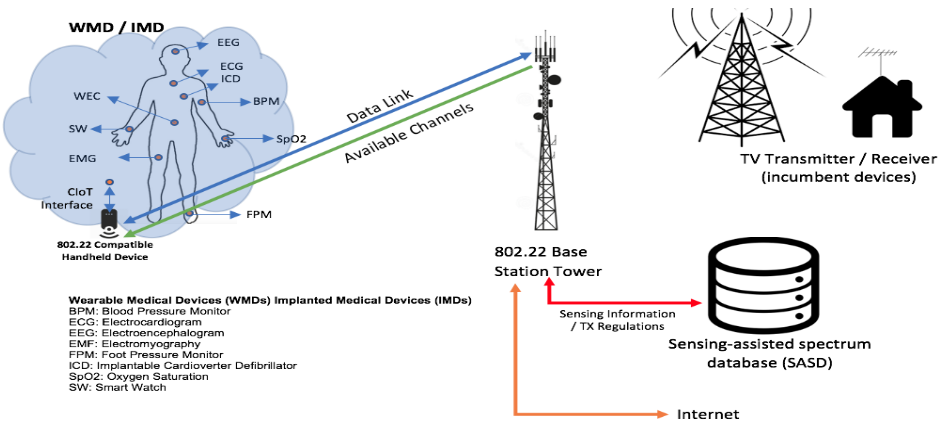

Figure 1 Proposed architecture connecting WMDs and IMDs to the internet using WiFar (IEEE 802.22)

4. Discussion

Medical sensors in/on human body will become vital part of our lives and in some cases mandatory (possibly by our life insurance). In order to provide seamless connectivity in large geographical areas, a novel type of network is proposed where all these sensors communicate with our BSMD through the BAN and all data generated is transferred in real time using the freely available TVWS spectrum using IEEE802.22 cellular type of network. Our proposed system requires substantial work in a number of research topics in order to become operational. First topic is the convergence of the numerous lightweight networking protocols that the current WMDs are using. Furthermore, the antenna design for our BSMD device must be designed to address the issue of propagation losses especially in highly populated cities. BSMD should also ensure that it establishes low-power communication with the sensors forming the BAN in order to extend their lifetime. Finally, it is important that the system's performance is tested for availability, reliability and throughput to assess the capability of our system architecture to support critical medical devices.

Our proposed architecture can be used as a reference point for future work and for redefining the way WMDs operate as well as pave the road for a new fully connected and highly integrated healthcare system that will process the data generated by the WMDs and IMDs and transmitted by our BSMD device.

References

[1] Rushanan, M. et al. *SoK: Security and privacy in implantable medical devices and body area networks*. In Proceedings of the 2014 IEEE Symposium on Security and Privacy. IEEE CS, 524–539.

[2] A. Pantelopoulos and N. G. Bourbakis, *A Survey on Wearable Sensor-Based Systems for Health Monitoring and Prognosis*, in IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. **40**, no. 1, pp. 1-12, Jan. 2010.

[3] A. Kiourti, K. A. Psathas, J.R. Costa, C.A. Fernandes, K. S. Nikita, *Dual-band implantable antennas for medical telemetry: a fast design methodology and validation for intra-cranial pressure monitoring*. **141**, (2013), 161-183.

[4] Nokia Networks, *FutureWorks 5G use cases and requirements*, White paper - 5G Use Cases and Requirements, Retrieved, April 13, 2017, http://networks.nokia.com/sites/default/files/document/5g_requirements_white_paper.pdf

[5] Erik Ekudden, Head of Technology Strategies, *Ericsson, talks about 5G use cases*, 5G Use Cases, Retrieved, April 23, 2017, http://www.ericsson.com/news/150708-5g-user-cases_244069645_c?query=5g

[6] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain and K. S. Kwak, *The Internet of Things for Health Care: A Comprehensive Survey*, in IEEE Access, vol. 3, no. , pp. 678-708, 2015.

[7] Zillner, T., *ZigBee Exploited, The good, the bad and ugly*, cognosec, August 2015, Mandalay Bay, USA, Retrieved, April 29, 2017, https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf

[8] RFID Hacking Tools, Retrieved, April 29, 2017, https://www.bishopfox.com/resources/tools/rfid-hacking/attack-tools/

[9] Haykin, Simon, *Cognitive radio: brain-empowered wireless communications*, Selected Areas in Communications, IEEE Journal on, vol.23, no.2, pp.201,220, Feb. 2005

[10] Qihui Wu; Guoru Ding; Yuhua Xu; Shuo Feng; Zhiyong Du; Jinlong Wang; Keping Long, *Cognitive Internet of Things: A New Paradigm Beyond Connection*, Internet of Things Journal, IEEE , vol.1, no.2, pp.129,143, April 2014, doi: 10.1109/JIOT .2014.2311513

[11] P. Vlacheas, R. Giaffreda, V. Stavroulaki, et al, *Enabling smart cities through a cognitive management framework for the internet of things*, IEEE Communications Magazine, June 2013.

[12] B. Bochow, O. Holland and K. Katzis, *Spectrum sensing infrastructure support for IEEE 1900.6b sensing-assisted spectrum databases*, 2016 IEEE Conference on Standards for Communications and Networking (CSCN), Berlin, 2016, pp. 1-6., doi: 10.1109/CSCN.2016.7785179