An Overview on the Internet of Things for Health Monitoring Systems

Mobyen Uddin Ahmed(✉), Mats Björkman, Aida Čaušević, Hossein Fotouhi, and Maria Lindén

Mälardalen University, Västerås, Sweden
{mobyen.ahmed,mats.bjorkman,aida.causevic,hossein.fotouhi,
maria.linden}@mdh.se

Abstract. The aging population and the increasing healthcare cost in hospitals are spurring the advent of remote health monitoring systems. Advances in physiological sensing devices and the emergence of reliable low-power wireless network technologies have enabled the design of remote health monitoring systems. The next generation Internet, commonly referred to as Internet of Things (IoT), depicts a world populated by devices that are able to sense, process and react via the Internet. Thus, we envision health monitoring systems that support Internet connection and use this connectivity to enable better and more reliable services. This paper presents an overview on existing health monitoring systems, considering the IoT vision. We focus on recent trends and the development of health monitoring systems in terms of: (1) health parameters and frameworks, (2) wireless communication, and (3) security issues. We also identify the main limitations, requirements and advantages within these systems.

1 Introduction

According to the Eurostat population projection, by 2030 just in the European Union, the percentage of elderly people (65 years old and older) will increase with 6.1 %, compared to 2008, with the assumption that the growth will continue in the future [11]. At the same time, we are facing the problem of birth rates that are below the level needed for a sustained population. This results in a growing need for healthcare, and reduces the ability to financially support it. In 2008, four persons of working age were supporting one person aged 65 or older, while projection shows that by 2030 the number of working persons will decrease to 2.5. This calls for less expensive solutions in healthcare that will utilize the benefits of modern technology, providing distance monitoring of elderly, and avoiding hospitalization when it is possible.

Technical advances in physiological sensing devices and wireless connectivity provided by the IoT can enable dramatic changes in the ways health monitoring and remote healthcare will be performed in the future. However, for such changes to take place, the enabling technologies must be employed with the well-being

B. Mandler et al. (Eds.) IoT 360° 2015, Part I, LNICST 169, pp. 429–436, 2016.
DOI: 10.1007/978-3-319-47063-4_44

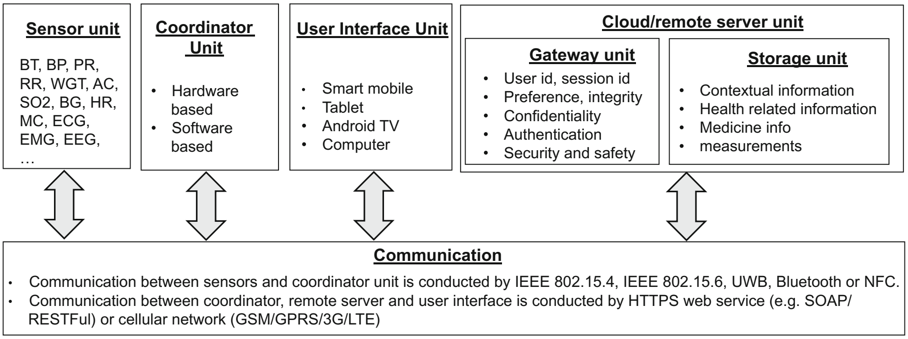

Sensor unit
BT, BP, PR, RR, WGT, AC, SO2, BG, HR, MC, ECG, EMG, EEG, …
Coordinator Unit
Hardware based
Software based
User Interface Unit
Smart mobile
Tablet
Android TV
Computer
Cloud/remote server unit
Gateway unit
User id, session id
Preference, integrity
Confidentiality
Authentication
Security and safety
Storage unit
Contextual information
Health related information
Medicine info
measurements
Communication
Communication between sensors and coordinator unit is conducted by IEEE 802.15.4, IEEE 802.15.6, UWB, Bluetooth or NFC.
Communication between coordinator, remote server and user interface is conducted by HTTPS web service (e.g. SOAP/RESTFul) or cellular network (GSM/GPRS/3G/LTE)

Fig. 1. A system-level framework for health monitoring systems.

of the patient in focus, since neither individuals nor society would accept IoT solutions that mismatch the standards of current best practice in healthcare.

IoT for health monitoring systems can enable new possibilities not available to patients today, especially to those not ill enough to be admitted to a hospital. By providing low-cost solutions to in-home monitoring, IoT can enable monitoring of such patients, enabling early detection of signs of deteriorating health, allowing for earlier responses and treatment. In order for in-home monitored patients to feel safe and secure when staying at their homes, the IoT solutions used must guarantee safety and security at a more technical level. Hence, one important focus of this overview is the security of the health monitoring systems studied.

In this paper, we are targeting health monitoring issues by considering the IoT vision. Section 2 provides an overview on the relevant parameters and frameworks. In Sect. 3, we explain the most common wireless standards and technologies for remote health monitoring. Section 4 continues with relevant security issues and challenges in this area. Finally, we conclude the paper in Sect. 5.

2 Parameters and Frameworks for Health Monitoring

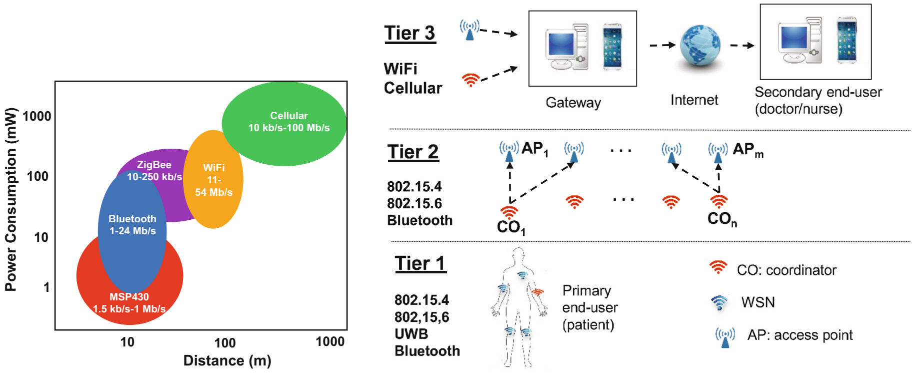
Remote health monitoring systems support monitoring a number of physiological parameters. Most common parameters included in health monitoring systems are vital signs, such as: Body Temperature (BT), Blood Pressure (BP), Pulse Rate (PR), and Respiratory Rate (RR) [2,4]. Beside these parameters, there are some other parameters defined as; Weight (WGT), Activity (AC), Oxygen Saturation (SO2), Blood Glucose (BG), Heart Rate (HR), and Medication Compliance (MC) [26]. Some systems facilitate remote monitoring of Electrocardiography (ECG) and Electromyography (EMG) [24], while few are looking forward to develop electroencephalogram (EEG) [25]. Some health parameters are measured sparsely, such as BP, BG, WGT, BT, while HR, PR, RR. EEG, EMG and ECG are measured continuously at specific time periods. There are different ways for sensor data management, considering IoT and most common components that are presented in a block diagram — see Fig. 1.

Main components in health monitoring systems are: (1) sensor unit, (2) coordinator unit, (3) remote server unit, (4) user interface unit, and (5) communication unit. A sensor unit contains a set of sensors for different health parameters that typically are battery powered, together with a microcontroller for data processing, and an antenna for communication purposes. According to the literature, most of the systems use commercially available and CE[1] certified sensors, while few of them use sensors that are under development within academia. The coordinator unit is developing in two directions; (1) hardware direction, and (2) software direction. The main hardware parts are processor, memory, radio and relevant sensor(s) [19], while the software direction is an application, performing on a host platform, e.g. an Android operating system that collects different measurements from sensors [2,4]. A remote server is placed in the cloud, which usually consists of a Gateway and a storage. The Gateway that delivers data from one wireless domain to another, focuses on security, safety and privacy issues, and it manages users and user requests in term of data management. The storage stores all user related information together with health measurements. Moreover, it also provides import and export facilities, while enabling data encryption. Most of the existing user interfaces are implemented either for smartphones or tablets [2,24,26], or in laptop-based platforms [25], with exception of a smart TV-based implementation [19]. The data communication is considered in two aspects: local and global. The local communication is between sensor and coordinator units, which is normally obtained by either Bluetooth [13] or IEEE 802.15.4, which will be further discussed in Sect. 3. The global communication provides connection between the coordinator, remote server and user interface and is established via either HTTPS web service (e.g. SOAP/RESTFul) or cellular networks. In [3], the authors proposed a generic system-level framework for health monitoring systems, where they tried to combine several available techniques.

3 Wireless Communication in Health Monitoring

The use of wireless sensing devices on the human body is attracting the healthcare and wireless communities. However, there are still many open issues that need further investigation within the wireless domain. For instance, which wireless technologies and standards are appropriate enablers for different healthcare scenarios? Is it feasible to employ multiple Low-Power Wireless Network (LPWN) technologies in a healthcare system? How can health monitoring systems provide IoT requirements? In this section, we investigate various wireless technologies and their main features, followed by providing a generic system model for the health monitoring applications.

[1] The CE marking is the manufacturers' declaration that the product meets the necessary requirements.



(a) (b)

Fig. 2. Wireless communication for healthcare: (a) comparing different wireless technologies in terms of transmission power, transmission range and data rate, and (b) categorizing wireless technologies at each tier.

LPWN contains a group of wireless standards/technologies that support low-power radios, such as IEEE 802.15.4 (ZigBee [5]), IEEE 802.15.1 (Bluetooth [13]), IEEE 802.15.6 (UWB), Radio Frequency Identification (RFID) [21], and IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) [22]. Internet Protocol (IP)-based LPWNs are becoming increasingly important for many applications. From the aforementioned LPWN standards/technologies, 6LoWPAN supports IPv6 over IEEE 802.15.4 based networks that guarantees some security levels. The IP-based addressing provides smooth integration of LPWNs within other wireless technologies, such as WiFi and cellular network. This integration provides the possibility of connecting sensing devices to cloud-based services, allowing extensive information processing for early diagnosis.

The use of LPWNs for critical applications is very challenging. LPWNs operate at a very low data rate and transmission power, aiming at a prolonged lifetime. Figure 2(a) shows a comparison of power consumption of wireless transceivers and a microprocessor in different wireless systems. The maximum transmission power of a regular LPWN device (e.g. TelosB with MSP430 microprocessor [7]) is 1 mW, while in WiFi access points is in the range of 30 mW to 800 mW and in cellular networks from 500 mW in smartphones to $\approx 10^5$ mW in base stations. Providing reliable data transmission between sensing devices with extremely low-power radios in a noisy environment is very challenging. This requires considering various parameters, such as link quality estimation, time synchronization, collision avoidance and mobility management when designing a data communication protocol.

There are various system architectures for communication in different health monitoring applications [16,17,27]. In this paper, we present a generic system that covers all the related works — see Fig. 2(b). It shows three tiers based on using appropriate wireless technologies. *Tier* 1 requires LPWNs for communicating between sensing devices and the coordinator[2]. One of the sensing devices or an additional device is usually devised to collect data from all sensors. This level of communication consists of multiple physiological sensing devices that are capable to sample the vital signs, process data and communicate through a wireless medium. These devices should be carefully placed on the human body by either direct attachment on the body skin, or placing in special clothes, or implanting inside the body. *Tier* 2 provides the possibility of communication between coordinators and fixed set of sensor nodes, known as Access Points (APs) [8,9]. This would benefit elderly people by avoiding the necessity of holding smartphones for collecting data. Finally, *Tier* 3 is devised for relaying data from LPWN toward the secondary end-user for further processing. In this level, health monitoring systems gain from the existing WiFi and cellular infrastructure.

4 Security in Health Monitoring

In pervasive healthcare that assumes an IoT-based environment, it is important to ensure basic security services such as: *privacy* (patient identity protection); *confidentiality* (protecting medical information of patients, as well as medical staff information); *integrity* (protection of data alternation during the transmission by any adversary); *authentication* (making sure that the data is sent from a trusted source); *data freshness* (preventing an adversary to capture transmitted data and later replay it, causing possible confusion in the system); etc. These services are required by existing legislatives such as European directive 95/46 [18] on data protection and HIPAA [6] in the United States, and should ensure guarantees of patient's safety and privacy. IEEE 802 has established a working group for standardization of Wireless Body Area Networks (WBAN) that produced IEEE 802.15.6 standard [12]. The standard establishes foundation for low-power in-body/on-body nodes to serve a number of different applications, including health monitoring application in a secure and safe way.

Any security mechanism in sensor-based systems should be fit with existing system requirements such as energy efficiency, memory restrictions, minimum possible computational and communication resource consumption, fast operation mode in order to avoid any delays of critical data, and high level of scalability. One has to bear in mind that the growth in number of connected devices in IoT brings larger number of possibilities for attacks on personal data. Also, communication is extended far outside of local networks, which requires strong authentication and authorisation protocols to be defined. The existing security-related solutions in many cases are not able to cope with all these requirements to their full extend and therefore more research in this area is required.

There is a number of research projects that aim at addressing security-related challenges. In [23], authors address patient's privacy as one of the main challenges when providing efficient and effective service in e-healthcare. Haque et al.

[2] The coordinator is a regular sensor device that is assigned for collecting data from other sensors.

describe open security issues in pervasive computing and emphasise the importance and the role of strong authentication in pervasive environments that is applicable to healthcare in IoT [14]. In [15], authors describe an authentication mechanism based on correct calculation of a Message Authentication Code, that is used to identify data as being sent by a trusted participant. As a way to achieve data confidentiality a light-weight data encryption model is proposed [20]. Garcia-Morchon et al. describe a security framework that combines strong security primitives such as public-key cryptography with light-weight cryptographic primitives, providing a trade-off between security, availability and efficiency that is followed by privacy-aware user identification in the system [10]. Nguyen et al. describe challenges and limitations of existing secure communication protocols for IoT [1]. They provide a novel classification of existing protocols based on their bootstrapping approach to establish a secure communication channel, and point out the performance challenges with respect to the use of these protocols.

5 Conclusions

This paper presents an overview on health monitoring systems in a daily life considering the IoT for health. Here, we reviewed the main aspects related to health, focusing on recent trends and development of the health monitoring systems through IoT. A number of recent health monitoring systems have been reviewed in terms of health parameters, frameworks, wireless communication and security issues. We presented the motivation for considering the IoT for interoperability between different devices, networks and applications. According to the observations, the development and the trend of the research on IoT in the area is growing, however, many issues are not tackled yet. Considering unreliable links in LPWNs and coexistence of interference from high-power wireless networks working in the same frequency band, risk factor analysis and user evaluation, based on primary and secondary end-users, can extend the study, which is our future focus.

Acknowledgments. This work is funded by Knowledge Foundation's research profile Embedded Sensor System for Health (ESS-H) and the distributed environment Ecare@Home.

References

1. Survey on secure communication protocols for the internet of things. Ad Hoc Netw. (2015)
2. Ahmed, M.U., Banaee, H., Loutfi, A., Rafael-Palou, X.: Intelligent healthcare services to support health monitoring of elderly. In: HealthyIoT (2014)
3. Ahmed, M.U., Björkman, M., Lindén, M.: A generic system-level framework for self-serve health monitoring system through internet of things (iot). In: pHealth (2012)

4. Ahmed, M.U., Espinosa, J.R., Reissner, A., Domingo, À., Banaee, H., Loutfi, A., Rafael-Palou, X.: Self-serve ict-based health monitoring to support active ageing. In: HEALTHINF (2015)
5. Alliance, Z.: Zigbee specification (2006). http://zigbee.org/
6. Congress, U.S.: Health insurance portability and accountability act (1996). http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm
7. Crossbow Technology, Inc.: Telosb datasheet, December 2014. http://www.willow.co.uk, http://www.willow.co.uk/TelosB_Datasheet.pdf
8. Fotouhi, H., Moreira, D., Alves, M.: mRPL: boosting mobility in the internet of things. Elsevier Ad-Hoc Netw. **26**, 17–35 (2015)
9. Fotouhi, H., Zuniga, M., Alves, M., Koubaa, A., Marrón, P.: Smart-HOP: a reliable handoff mechanism for mobile wireless sensor networks. In: Picco, G.P., Heinzelman, W. (eds.) EWSN 2012. LNCS, vol. 7158, pp. 131–146. Springer, Heidelberg (2012)
10. Garcia-Morchon, O., Falck, T., Heer, T., Wehrle, K.: Security for pervasive medical sensor networks. In: 6th Annual International on Mobile and Ubiquitous Systems: Networking Services, MobiQuitous 2009 (2009)
11. Giannakouris, K.: Population and social conditions, regional population projections europop2008: most eu regions face older population profile in 2030. Eurostat: Statistics in focus (2010)
12. Group, W.W.P.A.N.W.W.: Ieee standard for local and metropolitan area networks - part 15.6: wireless body area networks (2012). http://standards.ieee.org/about/get/802/802.15.html
13. Haartsen, J.C.: The bluetooth radio system. IEEE Pers. Commun. **7**, 28–36 (2000)
14. Haque, M.M., Ahamed, S.I.: Security in pervasive computing: current status and open issues. Int. J. Netw. Secur. **3**, 203–214 (2006)
15. Kumar, P., Lee, Y.D., Lee, Y.D.: Secure health monitoring using medical wireless sensor networks. In: NCM (2010)
16. Liang, X., Li, X., Barua, M., Chen, L., Lu, R., Shen, X., Luo, H.: Enable pervasive healthcare through continuous remote health monitoring. IEEE Wirel. Commun. **19**, 10–18 (2012)
17. Mitra, U., Emken, B.A., Lee, S., Li, M., Rozgic, V., Thatte, G., Vathsangam, H., Zois, D.S., Annavaram, M., Narayanan, S., et al.: Knowme: a case study in wireless body area sensor network design. IEEE Commun. Mag. **50**, 116–125 (2012)
18. European Parliament and of the Council: Directive 95/46/ec of the european parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
19. Parra, J., Hossain, M.A., Uribarren, A., Jacob, E.: Restful discovery and eventing for service provisioning in assisted living environments. Sensors **14**, 9227–9246 (2014)
20. Rekha, N.R., PrasadBabu, M.: Secured framework for pervasive healthcare monitoring systems. IJSCAI **2**, 39–47 (2013)
21. Roberts, C.M.: Radio frequency identification (RFID). Elsevier Comput. Secur. **25**, 18–26 (2006)
22. Shelby, Z., Bormann, C.: 6LoWPAN: The Wireless Embedded Internet. Wiley, Chichester (2011)
23. Sun, J., Fang, Y., Zhu, X.: Privacy and emergency response in e-healthcare leveraging wireless body sensor networks. IEEE Wirel. Commun. **17**, 66–73 (2010)
24. Tomasic, I., Avbelj, V., Trobec, R.: Smart wireless sensor for physiological monitoring. Stud. Health Technol. Inform. **211**, 295–301 (2014)

25. Xavier, B., Dahikar, P.: A perspective study on patient monitoring systems based on wireless sensor network, its development and future challenges. Int. J. Comput. Appl. **65**, 35–38 (2013)
26. Yang, G., Xie, L., Mantysalo, M., Zhou, X., Pang, Z., Da Xu, L., Kao-Walter, S., Chen, Q., Zheng, L.R.: A health-iot platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box. IEEE Trans. Ind. Inform. **10**, 2180–2191 (2014)
27. Yuce, M.R.: Implementation of wireless body area networks for healthcare systems. Elsevier Sens. Actuators A: Phys. **162**, 116–129 (2010)