DOI: 10.2478/bhee-2017-0004

Review scientific paper/Pregledni naučni rad

TOWARDS SAFETY, SECURITY AND RELIABILITY OF DATA COMMUNICATION IN IOT AAL APPLICATIONS

IZAZOVI I MOGUĆA RJEŠENJA ZA SIGURNU I POUZDANU KOMUNIKACIJU U IOT AAL SISTEMIMA

Aida Čaušević[1], Maryam Vahabi[1], Hossein Fotouhi[1], Mats Björkman[1], Kristina Lundqvist[1]

Abstract: Internet of Things (IoT) Ambient Assisted Living (AAL) systems are expected to enable the next generation healthcare, in the era of increased number of elderly and disabled people.

IoT AAL is assumed to enable healthcare in the comfort of patients' own homes, and keep the cost of the healthcare within economically acceptable range. In this paper, we focus on a health monitoring system consisting of a number of sensing devices, cloud services, remote hospital offices connected via communication infrastructure (e.g., WiFi, cellular networks, etc.) aiming at providing safe, secure, reliable and time-efficient services.

We identify challenges related to guaranteeing these properties and provide a brief description of our approach that enables reasoning about reliable and time-efficient communication, and outline an approach for risk analysis of safety and security properties.

Keywords: IoT, AAL, safety, security, reliable communication

Sažetak: Očekuje se da će Internet of Things (IoT) Ambient Assisted Living (AAL) sistemi omogućiti novu generaciju zdravstvene usluge i njegu starijih osoba (65 godina i starijih) i biti u stanju, na kvalitetan način, odgovoriti na njihove potrebe u eri konstantnog povećanja broja osoba ove životne dobi. Smatra se da će IoT AAL omogućiti zdravstvenu njegu u njihovim domovima, istovremeno zadržavajući troškove unutar ekonomski prihvatljivih granica. U ovom radu fokus je na zdravstevnim sistemima za praćenje starih osoba na daljinu koji se sastoji od velikog broja senzora, cloud usluga, bolničkih ureda koji komuniciraju putem komunikacijske infrastrukture (WiFi, mobilne mreže, itd.), a sve s ciljem obezbjeđivanja sigurne i pouzdane (engl. safe and secure) usluge unutar vremenski prihvatljivih okvira.

U ovom radu smo identificirali izazove vezane za garanciju pomenutih svojstava ovakvih sistema, te dali kratak opis našeg pristupa koji će omogućiti analizu vremena odziva, te pouzdanosti ovakvih sistema. Osim toga, ukratko je opisan pregled našeg pristupa za analizu sigurnosnih (engl. safety and security risk analysis) svojstava ovakvih sistema.

Ključne riječi: IoT, AAL, sigurnost, pouzdana komunikacija

INTRODUCTION

According to the UN report on the world population aging, it is estimated that the world population of elderly (60 and older) will grow by 56% between 2015 and 2030, and by 2050 the global population of elderly is projected to more than double its size in 2015[1]. Given this, it might be a challenging task to provide cost-efficient, personalized, reliable and good quality of healthcare for elderly people in the future.

[1]http://www.un.org/en/development/desa/population/publications/pdf/ageing/WPA2015_Report.pdf

[1]Mälardalen University Västerås, Sweden
aida.causevic@mdh.se, maryam.vahabi@mdh.se, hossein.fotouhi@mdh.se, mats.bjorkman@mdh.se, kristina.lundqvist@mdh.se

Paper submitted: October 2017 Paper accepted: November 2017

In healthcare, Internet of Things (IoT) is foreseen to enable a variety of services, including health monitoring systems in the context of Ambient Assisted Living (AAL) [1]. IoT provides connectivity of different types of objects (i.e., sensors, mobile phones, cloud services, etc.), enabling efficient data collection and management of these objects.

The main idea is to build, operate, and manage the physical world throughout pervasive networking, data accumulation, different types of analysis, optimization [2]. AAL is a novel technology discipline that exploits the potential of emerging communication technologies to keep elderly people active, independent and safe in their daily life. It is expected that AAL will enable people to live and age with good life quality and support elderly in their current activities, enabling continued participation and engagement at home and in the community, and last but not least improving the cost-effectiveness and quality of healthcare [3].

The novelties provided by IoT AAL are seen as promising solutions to make both economical and societal impact in the near future. IoT AAL approach is expected to guarantee better life conditions, reliable and secure communication with their physicians over Internet, more safety for elderly people using innovative technologies and services. Systems like this are assumed to be continuously connected to the Internet, and therefore no longer closed, but open solutions. Network technologies as they are now, are unable to support a large number of low-power devices that interact with the physical world, people, and cloud. Some of these challenges include scalability, multi-tenancy, reliability, safety and security [4].

An IoT AAL system is an example of a safety-critical system. In many cases, it contains open network interfaces that make it possible for malicious intruders to pose different types of threats to the system. This might produce interruption in service delivery and introduce hazardous and life-threatening events to patients. It is obvious that ensuring the safety in isolation without security consideration is no longer enough. According to [5], poor quality of system availability, safety, and data integrity can lead to inappropriate emergency assistance and potentially causing fatal consequences for elderly citizens relying on home-based personal healthcare systems. Our intention is to explore the nature of interdependencies between the safety and security properties in IoT AAL applications, and acquire knowledge needed to enable joint risk analysis in our proposed framework.

In this paper, we address the communication challenges related to the IoT AAL system. Wireless communication is considered as the main component of the system communication infrastructure as it provides flexibility to the elderly movement. According to the lossy nature of the wireless links, the communication is highly fragile and unreliable, e.g., a data packet may drop due to a poor link quality. Network security is another challenge that must be considered [6]. These issues put big challenges to guarantee a satisfactory level of safety in IoT AAL systems.

This paper provides a discussion on challenges in modern IoT AAL systems with the main focus on communication, safety and security issues. We map identified challenges and issues to our proposed IoT AAL framework model that will be used for modelling and analysis of communication related properties, as well as risk analysis in our future work.

1. WORKING EXAMPLE: A MODEL OF A HEALTH MONITORING SYSTEM

Let us assume an IoT model of AAL system depicted in Figure 1. We assume two types of users: *a primary end-user*, defined as an elderly person or a patient that carries sensors, and *a secondary end-user*, a physician, whom analyses and makes decisions based on the provided information. In our model, an elderly person carries four types of sensors: motion, pulse, blood pressure, and ECG sensor, to record measurements. The attached sensors might have low and high sampling rates based on their requirement. It is possible to collect all the measurements at a coordinator, which might be embedded within a Gateway device. Smart phones, tablets and personal computer (PC) can be used as Gateways to transmit measurements to an external network. Both the Gateway and PC are equipped with an application that acts as a decision support system with the purpose to aggregate the data, dismiss the potential noise and incomplete/incorrect data. Aggregated data is then transmitted via high-speed data links to the cloud or emergency room (ER) in case of an alarm state. It is important to point out that we assume existence of a high priority alarm link towards ER in case a patient is in an emergency state.

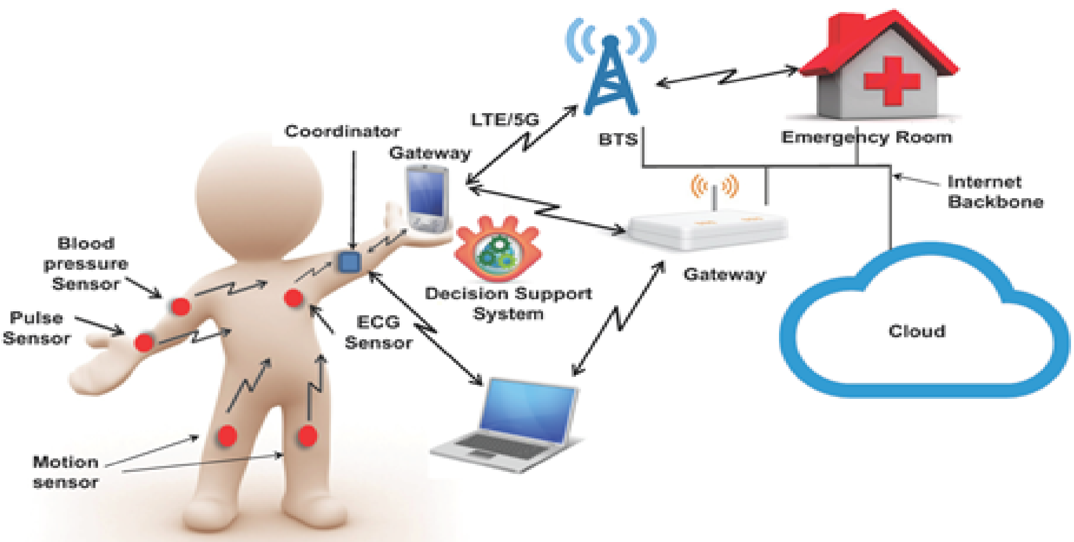

Figure 1: Proposed AAL framework model

1.1. Infrastructure of the proposed AAL model

In the model depicted in Figure 1, it is possible to employ various wireless technologies throughout the network. However, used network technologies must answer application requirements, while providing acceptable level of quality of service. To select appropriate technologies, it is essential to identify IoT AAL requirements, and get advantages of most recent technological advancements. An option couls be the future generation of wireless and mobile broadband network (5G), which will provide the infrastructure for billions of devices, while enabling the capacity to support all applications. Also, software-defined networking (SDN) and network functions visualization (NFV) will play important roles, especially in terms of a new network topology. The concept of SDN provides more flexibility in the network implementation by establishing a re-configuration policy at the controller level [7]. The controller discovers the actual network topology through an interface to the network infrastructure, and implements high level network management. Any entity of the infrastructure has a flow table that stores the rules for the received data flow. The rules are introduced and updated by the controller based on application requirements.

Considering the commercial-off-the-shelf (COTS) physiological devices, the most common radios for health monitoring devices are IEEE 802.15.4, Bluetooth (and its related family, i.e., BLE), and WiFi. However, to the best of our knowledge there is no restriction from health organizations and International Telecommunication Union for radio regulation. Thus, vendors are producing variety of devices, where each of them might support different standards. System designer should take advantages of all possible radios, and devise a network that fulfils requirements. For instance, it is recommended to employ ZigBee radio to achieve longer lifetime with low-sampling frequency measurement. Bluetooth radio is usually used for transmitting stream of packets with higher data rate. WiFi radio with higher channel bandwidth is used for forwarding huge amounts of data. We expect that future IoT AAL systems should support various low-power radios to enable various health monitoring applications.

2. CHALLENGES

The fundamental function in an IoT AAL is sensing an alert and sending an alarm message using different types of communication channels within given time. A large number of messages is being interchanged and these messages change in format, type, and size before sent to different parts of the system. It is also important to be able to filter/aggregate messages when needed, to decide when to transfer and how to transfer, taking into consideration the dependability requirements for a reliable IoT AAL system, as well.

There are various challenges that have been identified including communication challenges in different domains. These challenges are even more severe in wireless medium, where devices have no dedicated channel for data transmission, especially when employing low-power wireless radios with unreliable links. Therefore, we introduce some of the main challenges that play the major role in designing the wireless infrastructure of the IoT AAL system.

Low-power radios are prone to ***interference*** from other radios that are operating in the same frequency band. The ISM band is shared among most wireless radios, such as in ZigBee, Bluetooth, and WiFi. This increases the probability of packet losses for radios with lower transmission power. Next, current systems are equipped with various radios and technologies, creating ***heterogeneity*** in terms of hardware and software. It is important to provide network interoperability, seamless connectivity between various hardware devices and transmit packets through different network technologies. An IoT AAL system may consist of several health monitoring applications running in parallel. Some of the examples of these applications are fall detection, heart monitoring, sleep monitoring, etc. Each of these applications provide different types of traffic based on their sampling interval. Moreover, sensors are battery powered, and it is necessary to consider energy efficiency strategies in order to prolong network lifetime. ***Network management*** is a challenging topic in IoT AAL, where it targets traffic management, resource management, scalability, and on-the-fly programming of sensors. Each health monitoring application has a set of requirements that should be considered in the network design. This quality of service requirements is known as network ***reliability*** in terms of packet delivery ratio, and ***timeliness*** in terms of latency and end-to-end delay.

2.1. Safety and security in IoT AAL

In systems like IoT AAL, it is important to be able to guarantee safety and security of the system. It is often assumed that providing ***secure communication links*** between sensing devices, remote servers and cloud services is enough. However, there are a number of challenges along the way of ensuring secure IoT AAL systems. Wearable sensors deployed in IoT AAL are small and come at the price of low-power supply, which makes them incapable to carry out large computations and to store larger amounts of data. Therefore, cryptographic mechanisms used to enable secure communication links should be as light-weight as possible [8-13]. Managing ***identity and authentication*** in IoT AAL systems is a challenge, as we have multiple devices in need to recognize each other to create trustable services on demand [14]. We might even count on dynamic interactions in which network could be unaware of devices communicating with each other in advance. Since many devices manage sensitive information, ***privacy*** in terms of data protection and a user personal information protection is crucial to establish.

IoT AAL systems in general are examples of safety-critical systems and while designing such systems it is crucial to avoid possible risks (i.e., unintentional system threats) that might endanger the system and put human life into the danger. On the other hand, in the context of IoT, we have to think about an intentional system misuse and sabotage. We are challenged by the fact that in IoT system, safety can be influenced by security threats, providing new risks or causing the same risks to appear due to security-related cause. Examples of such interplay are insulin and drug infusion pumps that have been exposed to intentional threats and caused system safety risks. Due to this US FDA[2] has provided guidance on how to address cyber-security to assure safety of medical devices. Based on this, and similar findings it is evident that assuring the safety of the system and not taking security threats into consideration is not sufficient anymore.

3. OUR APPROACH

Our approach is twofold: (i) providing an analyzable model of an IoT AAL example presented in Figure 1, and (ii) analyzing safety risks, security threats, and their interdependencies on a given model. We are planning to develop the preliminary model in OMNeT++[3], by considering various wireless technologies, and evaluate system reliability and timeliness. To improve reliability, we are planning to implement some redundancy approaches both in wired and wireless parts of the system to increase the packet delivery rate. The next step will be to model a cloud server with unpredictable processing delay and to evaluate system performance. Furthermore, a new design for network management is needed such that the better performance can be achieved by adapting the system based on available resources. The parameters of the model are then added into a safety and security analysis for further investigation on possible risks for patients' life. In our safety and security work, we start with assumption that no human life will be ever endangered in our system. In doing so, we need to provide the definition of our IoT AAL system, identifying the boundaries and scope of the risk and threat reasoning, relying on the information provided by the network simulator. Next, we will cater an initial hazard analysis w.r.t. safety and security relations in our model. Further, risks identified in the previous step should be classified within a suitable classification scheme in order to extract their severity. Finally, we will provide recommendations on the suitable risk and threat reduction measurements.

[2]https://www.fda.gov/Safety/MedWatch/SafetyInformation/SafetyAlertsforHumanMedicalProducts/ucm456832.htm
[3]http://www.omnetpp.org

4. CONCLUSIONS

In this paper, we present our ongoing work on designing a reliable, safe and secure IoT AAL system, taking into consideration various wireless technologies. Our aim is to be able to address open questions such as interference, heterogeneity, network management and timeliness, as well as safety and security related issues provided that our system is a complex IoT system that includes communication infrastructure. In the next step we aim at implementing proposed model and analyze described system requirements.

ACKNOWLEDGMENT

This work is funded by the Swedish Knowledge Foundation (KKS) throughout research profile Embedded Sensor System for Health (ESS-H), the distributed environments E-care@home, and Research Environment for Advancing Low Latency Internet (READY)

REFERENCES

[1] L. Mainetti, L. Patrono, A. Secco, I. Sergi: An IoT-aware AAL system for elderly people, SpliTech, 2016
[2] D. Metcalf, S. T. J. Milliard, M. Gomez, M. Schwartz: Wearables and the internet of things for health: Wearable, interconnected devices promise more efficient and comprehensive health care, IEEE Pulse, 2016
[3] A. S. Hwang, J. I. Cameron, K. N. Truong, E. Lindqvist, L. Nygård, A. Mihailidis: Co-designing ambient assisted living environments: Unravelling the situated context of informal dementia care, IBioMed Research International, 2015
[4] R. Alur, E. D. Berger, A. W. Drobnis, L. Fix, K. Fu, G. D. Hager, D. P. Lopresti, K. Nahrstedt, E. D. Mynatt, S. Patel, J. Rexford, J. A. Stankovic, B. G.Zorn: Systems computing challenges in the internet of things, CoRR, 2016
[5] G. N. Rodrigues, V. Alves, R. Silveira, and L. A. Laranjeira: Dependability analysis in the ambient assisted living domain: An exploratory case study, Journal of Systems and Software, 2012
[6] J. P. Walters, Z. Liang, W. Shi, V. Chaudhary: Wireless sensor network security: A survey, Security in distributed, grid, mobile, and pervasive computing, 2007
[7] C. J. Bernardos, A. De La Oliva, P. Serrano, A. Banchs, L. M. Contreras, H. Jin, J. C. Zúñiga: An architecture for software defined wireless networking, IEEE wireless communications, 2014
[8] S. L. Keoh, E. Lupu, M. Sloman: Securing body sensor networks: Sensor association and key management, IEEE PerCom, 2009
[9] S. M. K.-u.-R. Raazi, H. Lee, S. Lee, Y.-K. Lee: Bari+: A biometric based distributed key management ap-

proach for wireless body area networks, Sensors, 2010

[10] H.Wang, H. Fang, L. Xing, M. Chen: An integrated biometric-based security framework using wavelet-domain hmm in wireless body area networks, IEEE ICC, 2011

[11] P. Nie, J. Vähä-Herttua, T. Aura, A. Gurtov: Performance analysis of hipdiet exchange for wsn security establishment, Q2SWinet. ACM, 2011

[12] R. Sankar, X. Le, S. Lee, D. Wang: Protection of data confidentiality and patient privacy in medical sensor networks, in Implantable Sensor Systems for Medical Applications, Woodhead Publishing, 2013

[13] P. Porambage, A. Braeken, A. Gurtov, M. Ylianttila, S. Spinsante: Secureend-to-end communication for constrained devices in IoT-enabled ambient assisted living systems, WF-IOT, 2015

[14] P. Mahalle, S. Babar, N. R. Prasad, R. Prasad: Identity Management Framework towards Internet of Things (IoT): Roadmap and Key Challenges, Berlin, Heidelberg: Springer Berlin Heidelberg, 2010

BIOGRAPHY

Aida Čaušević is a researcher at Mälardalen University. She has received her PhD from Mälardalen University in 2014. Her main research interest are formal methods and safety-critical systems, especially related to the safety and security interdependencies. She is currently running a nationally funded project SAFSEC-CPS, but is also involved in several other projects both EU and nationally funded such as: ESS-H, SafeCop, RAASS, CloSS. She has served as an organizer at conferences such as: HealthyIoT 2015 and Medicinteknikdagarna 2017. She is a program committee member for Embedded Conference Scandinavia.

Maryam Vahabi is a Postdoctoral researcher at the Mälardalen University. She has received her PhD from University of Porto, Portugal. During her PhD studies, she was working as a researcher at CISTER/INESC-TEC research institute. Her main research interests are on Internet of Things, wireless communication, cyber physical systems and software defined networking. She was involved in many European projects as well as Portuguese national funded (FCT) projects.

Hossein Fotouhi is an assistant professor at the Mälardalen University. He completed his PhD in Electrical and Computer Engineering at University of Porto, Portugal. He was a researcher at CISTER/INESC-TEC during his PhD. His main research areas are wireless communication, sensor networks, IoT and Fog Computing. He is currently involved in several projects such as ESS-H, ecare@home, READY and FiC. He was program committee of: WFCS 2016, ETFA 2016, IOTBD 2016, MobiApps 2016, DPNoC 2016, SNCNW 2016, and serving as session chair at HealthyIoT 2015, SCNNW Workshop 2016 and COMPSAC 2017, and local chair and publicity chair of HealthyIoT 2016.

Mats Björkman is Professor in Computer Communication at Mälardalen University since 2001. He received his MSc in Computer Science in 1986 from Uppsala University, and his PhD in Computer Systems in 1993 also from Uppsala University. Previously, Mats has worked as a researcher at the Swedish Institute of Computer Science (SICS) in Stockholm, Sweden, and at the University of Arizona in Tucson, Arizona. He is involved in several national and EU funded projects such as: CAMI, ESS-H, FiC, Ready and industrial graduate schools such as ITS-ESS-H and ITS-EASY.

Kristina Lundqvist serves as the Professor of Dependable Software Engineering at the School of Innovation, Design and Engineering at Mälardalen University. Her research group on Safety-critical engineering focuses on bridging the gap between the theoretical foundations of dependability and industrial software development practices of complex dependable systems. Additionally, Prof. Lundqvist is the Director of the ITS-EASY industrial research school. She received a Ph.D. in Computer Systems from Uppsala University in 2000. Prior to coming to Mälardalen University in 2007, she served on the faculty of the Department of Aeronautics and Astronautics at Massachusetts Institute of Technology (MIT).