Work-in-Progress: Communication and security trade-offs for wearable medical sensor systems in hospitals

Jori Winderickx
imec-COSIC and ES&S - KU Leuven
Leuven, Belgium
jori.winderickx@kuleuven.be

Pierre Bellier
Microsys lab, Montefiore - ULiège
Liège, Belgium
pbellier@uliege.be

Patrick Duflot
CHU de Liège
Liège, Belgium
pduflot@chuliege.be

Dorothée Coppieters
Microsys lab, Montefiore - ULiège
Liège, Belgium
d.coppieters@ulg.ac.be

Nele Mentens
imec-COSIC and ES&S - KU Leuven
Leuven, Belgium
nele.mentens@kuleuven.be

ABSTRACT

This paper describes an important first step in the development of a custom wearable health platform that allows the end-to-end secure monitoring of six vital parameters. We explore the impact of wireless network protocols and security schemes on the energy consumption of the wearable device. The results show that the energy efficiency is comparable to existing systems that support far less sensor data and that compromise on end-to-end security.

ACM Reference Format:
Jori Winderickx, Pierre Bellier, Patrick Duflot, Dorothée Coppieters, and Nele Mentens. 2019. Work-in-Progress: Communication and security trade-offs for wearable medical sensor systems in hospitals. In *2019 International Conference on Embedded Software (EMSOFT'19), October 13–18, 2019, New York, NY, USA*. ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3349568.3351548

1 INTRODUCTION

The system analyzed in this work is a custom waterproof wearable device communicating with a local hospital server. It is used to monitor six vitals: hearth rate, blood pressure variation, breathing rate, oxygen saturation, skin temperature and human activity. These vitals are compiled by the local server using the raw signals wirelessly transmitted from the wearable device. The following raw signals are measured: the electrocardiogram (ECG), the photoplethysmogram in three wavelengths (PPG), bio impedance (BioZ), the temperature (T), and the 3-axes accelerometer (ACC). Maximizing the lifetime of the wearable is the primary goal of this work. The battery should at least last for a day, such that it can be swapped by the medical staff daily. The secondary goal is to ensure a high level of security for the communication. To achieve both goals, the impact on the energy consumption of the wireless network protocol and the security architecture are explored. Different network protocols and security schemes are evaluated, and, the system is validated using a PoC implementation.

2 RELATED WORK

A lot of healthcare projects and platforms have already been devised, as analyzed by Javdani et al. [1]. From these projects, the CodeBlue [3] and MEDiSN [2] project are the most popular. The considered platforms often focus only on one sensor, e.g. ECG for CodeBlue and ECG or pulse oximetry (PO) for MEDiSN. Furthermore, security is either partially neglected or not sufficiently provided. However, regulations like the General Data Protection Regulation (GDPR) [4], state that medical data need to be protected.

3 SYSTEM MODEL

Two entities are considered: the wearable device and the local server. Both operate within the network of the hospital. The wearable has a wireless communication interface to transmit the raw data of the sensors to the local server. In total, 33 kB of raw data is sent every 10 seconds. The local server is connected using the wired Ethernet infrastructure of the hospital. The wearable device and local server are interconnected using a set of gateways and routers.

3.1 Wireless communication trade-offs

Many protocols have been designed to enable wireless communication between devices. For the system at hand, the Wireless Local Area Network (WLAN) and Wireless Personal Area Network (WPAN) protocols are the most suitable because the wearable devices operate within the hospital (limited range) and produce a sizable amount of data (high throughput). Therefore, only BLE, ZigBee and Wi-Fi are further explored, as detailed in Table 1. Additionally, an efficiency parameter is calculated, representing the amount of raw data sent in comparison to the total packet size including overhead (see Equation 1).

Table 1: Wireless network protocols for indoor application.

Features	BLE	ZigBee	Wi-Fi
Data rate (Mbps)	1-3	0.250	54-150
Max active devices	8	65000	2007
TX (μW/kb)	3.7-88.8	108.2-435.6	3.8-465
RX (μW/kb)	3.6-72.6	129.3-369.6	3.1-120.8
Idle current (μA)	2-200	0.7-2.5	690
Max payload (B)	339	102	1500
Max overhead (B)	158/8	31	58
Efficiency	94.46%	76.67%	96.28%

$$\text{Efficiency} = \frac{Ndata}{Ndata + (Npackets * Noverhead)} \qquad (1)$$

EMSOFT'19, October 13–18, 2019, New York, NY, USA

ACM ISBN 978-1-4503-6924-4/19/10…$15.00
https://doi.org/10.1145/3349568.3351548

The most optimal protocol for the targeted system is Wi-Fi. First, it scores best in terms of the efficiency parameter. Furthermore, less gateways are required than in BLE to support a realistic setup where lots of wearable devices are used. Next, Wi-Fi's large throughput is best suitable for the amount of raw data. Finally, an extensive Wi-Fi infrastructure is often already implemented in hospitals.

3.2 Security trade-offs

A high level of security must be used for the communication channel between the wearable device and the local server. The four following properties are identified: entity authentication, data origin authentication, confidentiality, data integrity.

Using the ciphersuites of the Transport layer Security (TLS) protocol as a reference, the four candidates below can provide the four required cryptographic properties. However, ciphersuite (1) is added as a reference since it is often used in constrained environments but it does not provide Perfect Forward Secrecy (PFS). PFS prevents previous sessions from being compromised if a current session is compromised.

(1) TLS_PSK_WITH_AES_128_GCM_SHA256
(2) TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256
(3) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
(4) TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

4 PROOF-OF-CONCEPT IMPLEMENTATION

The wearable device will communicate using the Wi-Fi network. Since it is IP-based, the TCP protocol is used to provide reliable communication. Next, TLS is chosen and it is ideal for securing TCP. Finally, in terms of application protocol, the proven and lightweight messaging transport of the MQTT protocol is chosen.

The wearable device is a custom platform which consists of the following elements: the sensors, the MSP432P4011 as application microcontroller (MCU) and the CC3120 as network processor (NWK). The MCU collects the raw data and sends it wirelessly using the NWK. The NWK can provide the entire stack up to the MQTT protocol. To implement the MQTT protocol, a software implementation was used on the MCU. Furthermore, the chosen ciphersuites are tested using two different methods. Ciphersuites (1) and (2) are implemented using the Mbed TLS library on the MCU and Ciphersuites (3) and (4) using the Secure Socket feature of the NWK.

To compare the ciphersuites, the energy required to establish a secured communication channel (session) is estimated. The performance of the calculations and transmission cost were taken into account. The lightest protocol is, as expected, Ciphersuite (1), using about 1.5 mJ to establish a session. In second place, Ciphersuite (4) uses about 32 mJ. It outperforms the other ciphersuites because of the RSA hardware accelerator present in the NWK. In third place, Ciphersuite (2) consumes about 53 mJ. It uses the efficient PSK based authentication and the more expensive public-key cryptography for key establishment. Finally, Ciphersuite (3) requires the most energy, about 147 mJ.

The energy consumed to establish a session is negligible in comparison to the total energy required. A session does not need to be established for each raw data packet, and, we have chosen to utilize a session lifetime of one day. In total, the wearable uses about 698.2 mJ to measure and transmit the data in one period of raw data collection (10 seconds). Given that each day the wearable will reconnect and establish a new session with the local server, the energy required for setting up a secured communication takes almost zero percent of the energy budget of the wearable with a lifetime of one day.

The average power consumption of our platform is also compared in Table 2 to the related work described in Section 2. Our platform is measured using the Keithley 2000 Ammeter. Given the large range of vitals and consequently the larger amount of data, the platform performs about 20% to 33% better and 6 to 12 times worse than the highest and lowest consuming platforms. Using a battery of 400 mAh, our platform has a lifetime of about 19 hours.

Table 2: Comparison of average power and lifetime estimation of related platforms. Lifetime is calculated using a 400 mAh battery.

Project	Vitals	Power (mW)	Lifetime (days)	End-to-end security
CodeBlue [3]	PO	87.78	0.63	no
MEDiSN [2]	ECG	11.29	4.87	no
	PO	105.30	0.52	no
Samie et al. [5]	ECG	5.87	9.36	no
This work	ECG, PPG, BioZ, ACC, T	**69.82**	**0.79**	**yes**

5 CONCLUSION

A secure wearable health monitoring device intended for real-life use in a hospital with a multitude of sensors is under development. It is used to monitor six vital parameters: heart rate, blood pressure variation, breathing rate, oxygen saturation, skin temperature and human activity (intensity and posture). As a first step in the development process, trade-offs with respect to end-to-end security and wireless communication are evaluated with the goal of maximizing the energy efficiency and thus the battery lifetime. The selected wireless communication protocol and ciphersuite lead to a battery lifetime of 19 hours, assuming a 400 mAh battery. Our solution outperforms related work in terms of energy efficiency, taking into account that it supports a much higher number of vital parameters.

ACKNOWLEDGMENTS

This work was funded by the WearIT4Health project which is carried out under Interreg V-A Euregio Meuse-Rhine and is supported by the European Union and the European Regional Development Fund and with financial support of the province of Limburg - Belgium.

REFERENCES

[1] H. Javdani and H. Kashanian. 2018. Internet of things in medical applications with a service-oriented and security approach: a survey. *Health and Technology* 8, 1-2 (2018), 39–50.

[2] J. Ko, R. P Dutton, J. H. Lim, Y. Chen, R. Musvaloiu-E, A. Terzis, G. M Masson, T. Gao, W. Destler, and L. Selavo. 2010. MEDiSN: Medical Emergency Detection in Sensor Networks. *ACM Transactions on Embedded Computing Systems* (2010), 1–29.

[3] D. Malan, T. Fulford-Jones, M. Welsh, and S. Moulton. 2004. CodeBlue : An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care. In *International Workshop on Wearable and Implantable Body Sensor Networks*. WIBSN'04, 3.

[4] European Parliament. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* 679 (2016), 88.

[5] F. Samie, L. Bauer, and J. Henkel. 2015. An approximate compressor for wearable biomedical healthcare monitoring systems. In *2015 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS)*. IEEE, 133–142.