

EVALUATING SMART COMMUNICATION AND MONITORING TECHNOLOGIES FOR HOSPITAL HYGIENE WORKFLOWS

Zaid Ali Shhedi ^{1*}

Alin Moldoveanu ²

Florica Moldoveanu ³

Cristian Taslitchi ⁴

Hesham Alabbassi ⁵

ABSTRACT

Hospitals receive many patients and visitors daily, and include a large number of medical staff members, thus, hospitals are eligible environments for infection transmission. The hospital acquired infection (HAI) is situated at the top of the reasons pyramid that lead to death. HAI means that a patient enters the hospital for some reason and gets infected because of another reason. Non compliance with hygiene protocols is a major cause of HAI. Therefore, the automatic monitoring of hospital workflows using the recent communication technologies is a vital factor for infection prevention. In this article, we highlight in details the technologies that could be investigated for monitoring the workflows in a hospital room. We describe the hospital room use case, and we analyze the suitability for each technology. The goal of this paper is to suggest a system for monitoring the clinical workflows and preventing the HAI. Nowadays, it became possible to perform efficient automated monitoring of hygiene related clinical workflows and we expect such solutions to become widely available within a few years.

KEYWORDS: *Hospital Acquired Infection (HAI), hand hygiene rules, medical workflows monitoring, hospital room, technological choices.*

1. INTRODUCTION

Nowadays, HAI is considered as a big challenge in current healthcare facilities, it leads to enlarging the mortality, expanding the patient stay in the hospital and thus raising the financial burden. Lack of training and guidelines, unsuitable airflow, contamination of equipment and surfaces, and especially contaminated hands are considered as the most popular HAI causes [1]. So using of smart technologies is a crucial factor for monitoring the hospital activities and thus combating the HAI.

^{1*} corresponding author, PhD Student, Doctoral School of Automatic Control and Computers, University POLITEHNICA of Bucharest, Splaiul Independentei 313, Bucharest, Romania, zaid.shhedi@yahoo.com

² Conf. dr. ing., Faculty of Automatic Control and Computers, University POLITEHNICA of Bucharest, Splaiul Independentei 313, Bucharest, Romania, alin.moldoveanu@cs.pub.ro

³ Prof. dr. ing., Faculty of Automatic Control and Computers, University POLITEHNICA of Bucharest, Splaiul Independentei 313, Bucharest, Romania, florica.moldoveanu@cs.pub.ro

⁴ PhD Student, Doctoral School of Automatic Control and Computers, University POLITEHNICA of Bucharest, Splaiul Independentei 313, Bucharest, Romania

⁵ PhD Student, Doctoral School of Automatic Control and Computers, University POLITEHNICA of Bucharest, Splaiul Independentei 313, Bucharest, Romania, al_abbassi2000@yahoo.com

In the last years, a wide variety of wireless communication technologies have become available, with a multitude of applications in all domains. Selecting the most suitable ones for a specific use case is an important challenge, since it requires a deep understanding of their base characteristics, specific advantages and drawbacks.

In this paper, we focus on identifying the most suitable technologies for implementing an important part of an automated monitoring system for preventing hospital acquired infections (HAI); which is the monitoring of the workflows related to room-level hygiene.

We will consider the basic case of a hospital room which contains two patient beds, a washing sink, and a toilet. It contains also a place dedicated for wounds and bandages, another one for used things, as well as air conditioning system. We try to automate the hygiene workflow through a monitoring system based on a group of recent technologies such as Bluetooth Low Energy (BLE), Near Field Communication (NFC), Radio Frequency Identification (RFID), ZigBee, and Wi-Fi.

2. OVERVIEW OF THE AVAILABLE BASE TECHNOLOGIES

2.1. Bluetooth Low Energy (BLE):

Definition: Bluetooth Smart (Bluetooth 4.0) is the latest version of the Bluetooth wireless technology published in 2010 [2], but it has totally different characteristics and purposes. BLE is a low cost, low bandwidth, and low power wireless technology [3]. Due to the fact that BLE sensors are with coin cell batteries that can live up to two years; BLE has a feature of low energy consumption [3], thus having the ability to deal with the power consumption problem[2], so it is considered as a promising choice for Internet of Things deployment [4], [5], [2], [6].

Concept and features: The operating range of the wireless devices stands on multiple factors; the obstacles and barriers, the environment, the device steering, the antenna design, the antenna size and the antenna broadcast Power and the used frequency. The dependable range of the BLE enabled device is 30m-50m line-of-sight, but the effective range, which is able to last the battery lifetime is between 2 & 5 meters [4]. Increasing transmission power leads to expanding the wireless device range, thereby increasing the consumption of resources such as battery lifetime. BLE has a wide spread that the number of electronic devices which include an integrated BLE chip will reach 2.9 billion by 2016 according to Bluetooth SIG (Bluetooth Special Interest Group) [2].

The working mechanism: A BLE device uses two mechanisms to communicate with other wireless devices within its broadcast range. The “**broadcasting**” way is broadcasting data -in one way connection- to any listening device capable of capturing this data within the sender device range. The other communication way of the BLE device is the “**connections**” way, which means establishing a secure encrypted connection between two BLE devices for exchanging data in both directions (the connection includes only the two devices) [4]. This way depends on the frequency hopping spread spectrum, which reduces the radio interference and may consume less power than the broadcasting way [4],[5].

The BLE device can be a master, a slave, or both, according to the application and to the communication requirements [4], but it can not play a role of client and server at the same time [6].

Devices that start the communication such as smart phones are called masters that each master device can communicate with many other devices known as slaves (small devices with constrained resources such as individual sensors). The BLE slave device can be connected to many masters at the same time (e.g. a smart phone connects to a lot of remote thermometers placed in some place) [4], [6]. The master device scans the three dedicated advertisement channels permanently, and when the slave advertises one of them, the master discovers the slave and then the communication is founded and data transfer begins. This is called asynchronous wake-up for both connector ends, and when the data transfer ends, they come back to the sleep mode again [5].

Advantages and drawbacks: Due to the rapidly growing in the smart device industry, which include BLE chips, that's a lot of manufacturing produce BLE equipped devices such as tablets and smart phones, BLE is well ahead of other competitor wireless technologies which are asynchronous. BLE products are cheaper and faster than other wireless technologies such as Wi-Fi, GSM, and ZigBee, and the communication does not require pairing before exchanging data. It is easy to use by, any person [6], and provides minimization, and ready reminding service [3]. BLE is fitted with small-size electronic products such as medical devices, and remote controllers. BLE can be considered as a solution of the power consumption problem of the wireless communications [2].

The main drawback of BLE is that the "Broadcasting" is not a secured way for exchanging data, especially the sensitive data that each listening device can receive the broadcasting data. But the "connection" way is considered as safe, that the data is exchanged over a secure encrypted link [4].

2.2. RFID Technology

RFID is one of the vital IoT technologies, which is based on the radio waves to build the communication between RFID readers and RFID tags. The main goal of RFID is to identify and track the everyday objects by means of tags [7].

RFID technology was firstly used in the military applications in the forties of the last century. Low cost RFID TAGS manufacturing appeared in the last decade of the twentieth century. Each of them consists of a small integrated circuit (IC) for storing and processing data, modulating and demodulating the (Radio Frequency) RF signal, the IC is connected to an antenna which is used for receiving and sending the RF signals [7].

RFID tags can store a little amount of data about the monitored object, in addition to small size applications, and they can be attached to or integrated into the daily things to provide them with interactive capabilities. RFID technology marks the daily life objects with unique identification numbers, so it facilitates the communication with those objects, and thus contributes to spread the Internet of Things [8]. RFID tags are either passive or active, passive tags are without power source, very cheap, and can survive and keep readable for a long time. RFID passive tags can operate at all RF frequencies, but active tags operate only at higher RF frequencies [7].

Working principle and components: The RFID system has two devices, **RFID reader** (interrogator), or a mobile phone provided with an NFC wireless interface from one hand and an **RFID tag** from the other hand. The reader could be individually or connected to a background database or provided with an interface for directing the obtained information to other systems. The communication between the reader and the system could be wired or wireless. Similarly to NFC, the RFID reader generates an RF field to operate the RFID tag (transponder) which does not have a power source. The passive tag can get the required power by means of the RF field signal and thus the IC inside the tag can boot up and send data. The RFID reader can read data stored into RFID tags placed within its range [7], [Syed, 2012].

The reader consists of a transceiver, a control unit decoder for interpreting data, and an antenna for broadcasting radio wave signals. When the tag is within the reader's range, it can absorb the required energy from the reader's electromagnetic field. The RFID operating range differs from a few CMs to a few meters. So the reader sends its requests and the tag receives the reader's requests and sends the data back, so that the RFID communication is done in a bidirectional half duplex way [7], [Syed,2012], [10] . Data stored in RFID tags can be encrypted and thus protected not to be stolen or modified by attackers, besides that making copies or original versions of RFID tags is too harder [7].

RFID advantages: It can operate without a line of sight; it has the ability to read from, write to and to modify the RFID tag's data. Each RFID tag has a unique code and a unique content, this singularity allows tracking each labeled object or product when it moves, which in turn can keep track theft cases or product loss [7] , [Syed,2012].

2.3. Near Field Communication (NFC)

Definition: NFC is one of the latest technologies which was introduced in the last ten years [Syed, 2012]. It is a wireless communication technology with a short range (0 to 20cm) high-frequency, quickly deployed, and low bandwidth and [Syed, 2012], [11]. NFC provides bidirectional communication between electronic devices in addition to the known mobile services. NFC offers new services to facilitate the daily life and can be considered as the best solution for the Internet of Things proliferation [3], [12], [11].

NFC Components: NFC system stands on three NFC devices:

- **NFC enabled mobiles** are the most effective and commonly used devices.
- **NFC reader** is an active NFC device that could be either **internal** included in an NFC enabled mobile phone and able to create its own radio frequency field, except when the NFC enabled mobile is in the standby or sleep mode [7]. Or **external**, such as a contactless POS (Point of Sale) device which operates as an NFC reader able to read data stored into an NFC enabled mobile phone close enough to it [7].
- **NFC tag:** which is an industrial passive RFID tag, easy to use, and able to store a little amount of data in addition to an exclusive identification number [7], [11].

Concept and communication mechanism: The NFC concept is based on integration of mobile devices, smart card interface, several contactless identification devices and

wireless technologies such as Bluetooth and Wi-Fi [7], [Syed, 2012]. At first, the contactless smart cards have emerged; nowadays mobile phones are available with NFC technology. Reader devices provided with NFC technology such a mobile phone can connect to RFID-tagged things in addition to contactless smart cards [7], [Syed, 2012].

The NFC communication is done between two mobile phones which support NFC technology, or between an NFC equipped mobile phone from one side and either an NFC reader or a tag from the other side by touching an NFC device to another one [7] . NFC technology does not allow more than two NFC enabled devices to communicate with each other at the same time and NFC allows people to interact with the surrounding ubiquitously [Syed, 2012]. NFC technology can operate in three **various modes**:

- **Reader/writer mode** means exchanging (reading and writing) data between an NFC mobile and an NFC tag [7].
- **Peer-to-peer mode** means exchanging data between two NFC supported mobile phones in a bidirectional half duplex communication [7].
- **Card emulation mode** is the most prevalent mode, so that the NFC enabled mobile phone can operate as a contactless card for payment and ticketing. The NFC mobile phone is activated by the RF field generated by RFID readers located in some places [7].

Advantages and disadvantages: Configuring wireless devices to operate with the wireless networks is not an easy work and takes time. NFC can be as a mediator between two wireless devices placed close to each other enabling them to exchange the required settings and to connect to wireless networks without needing to introduce their network parameters [Syed, 2012]. NFC technology can be integrated into many devices, and can be used for a huge variety of applications and services. NFC tags can be implanted into or fixed on everyday objects, that they have a small size, so NFC technology is adaptable.

The NFC mobile phone can provide an identification service, and access control. NFC provides implicit matching and fast communication, that the NFC mobile's application is activated routinely when discovering the matching pairs within its range and is communicated directly without the need for pairing as with Bluetooth. The NFC technology takes into account the users' privacy as in the case of using the NFC mobile phone as a credit card [Syed,2012], [7] , [12] .

NFC technology is deeply adapted with mobile phones that it does not affect the mobile battery as Bluetooth [13]. Due to the short communication range; NFC is considered as a high safe technology more than RFID. Thus, catching the signals during the communication is so difficult [Syed, 2012].

Unfortunately, RFID and NFC commercial applications are vulnerable to attacks, such as tag cloning and tag impersonation. Some attacks want to change the tag's content by displaying false information such as fake phone numbers, counterfeiting of person identities [14], or replacing the original tags by their own tags, so controlling the system as they want. Using cryptographic tags and authentication protocols can make the attacks more difficult. The readers are also vulnerable to theft, vandalism, impersonate the identity of the legal reader for obtaining the high importance information.

NFC Systems provide Benefits for a multitude of domains: that's regarding the transportation systems; passengers no longer need to use cash in order to buy tickets, and drivers no longer need to sell tickets, neither to use money or to make calculations, or even to check tickets in and out, so NFC is time-saving. Transport companies can save operating and maintenance costs that there is no longer a need for ticket dispensers or printing tickets, and it is easier to change the ticket's price or to apply discounts. NFC mobile phones can be used as electronic cards (credit or debit), thus, they provide flexibility that's users no longer have to carry a lot of cards which will not be lost or stolen as real ones. Proximity services enable the users to access services or sharing information simply by only tapping, touching, or waving their NFC enabled mobile phones. Borderless services: users who travel abroad with their NFC devices, do not need to use the new country's money, and they can get the tourist information from smart posters by using their NFC mobiles depending on the location-based services [Syed, 2012], [15].

Working principle: When two NFC enabled devices become within the required range; the active device (the initiator) which have its own power source generates an electromagnetic field to activate the other NFC device (the passive one), and thus the communication is founded [7]. The NFC device which receives the communication is called the target which can be either a passive device that gets its required power from the active device's electromagnetic field, or an active one that has its own power to respond. The NFC application which is installed in an NFC mobile phone is designed to boot up when this NFC mobile phone touches any other NFC device carries compatible data [7]. NFC tags and smart cards are always targets and passive devices [7], [9] and two NFC tags cannot build a communication and exchange data that they don't have power sources [7].

RFID - NFC Relation: NFC has been just a branch or an extension of RFID technology; it joins smart card technology interface and a reader into one device such as a mobile phone. This RFID son is a new wave of RFID, but it operates with a short range and different frequencies [7], [11]. NFC technology is able to interact with the RFID tags by means of our smart phones, or other readers and it adds further developments to the RFID technology by integrating of RFID technology into mobile phones. NFC enables billions of people to interact with the surroundings by means of RFID technology [Syed, 2012]. NFC reader which can read data stored in RFID tags allows downloading the readable information over the Internet and enable accessing services basing on the wireless communication technologies such as 3G, 4G, and Wi-Fi which are already embedded into mobile phones. NFC supports the RFID tag simulation mode, so that the mobile phone operates as an RFID tag, as if the phone holder is an object from the environment provided with an RFID tag [Syed, 2012]. As a closest brother or son to RFID; NFC can play a role of RFID cards or RFID readers.

2.4. ZigBee technology

Definition and concept: ZigBee is a low power wireless technology based on the IEEE 802.15.4 and developed by the ZigBee Alliance. It defines a set or a suite of high level communication protocols for battery-powered applications. ZigBee is low cost, [16], [17],

and low-data-rate, its effective range is between (10m – 70m) [18] , it is highly secure and highly reliable that it supports the mesh networking capability, ZigBee device has a high latency, and due to the communication consumes a little power [17], [16]. ZigBee is used for applications with long battery life, such as home automation, military applications, home based healthcare, and consumer electronics [17].

The maximum communication range of ZigBee is about 200m in open-air vicinity [18]. ZigBee is an optimal and an integrated solution for the commercial applications, especially the wireless sensor network applications [8], [16], [19], [20], [21].

ZigBee is a technology specified for Wireless Personal Area Networks (WPAN) and it is a global hardware and software standard for wireless network devices which operates in the mesh network structure with three frequencies 868 MHz, 915 MHz, and 2.4 GHz. These devices can send data over long distances by using of intermediate devices. ZigBee devices stay a very short time in the active mode and they keep in the sleep (power saving) mode for the rest of the time. ZigBee devices take only 30 ms or less to wake up, whereas Bluetooth devices take about 3 seconds, so the ZigBee device latency is high. ZigBee characteristics make implementing of a wireless ZigBee network easier than other standards such as IEEE 802.11 [7], [Syed, 2012], [21].

Advantages and Disadvantages: The IEEE 802.15.4 standard supports the possibility of encrypting the messages basing on the Advanced Encryption Standard (AES) [11]. The receiver can detect any modifications in the received message by means of the Message Integrity Code (MIC) which is contained in each coming message, so ZigBee has the possibility of data authentication [20]. In a wireless ZigBee network, intruders can get sensitive information from the network device memory, such as the security keys when these devices are not tamper-resistant nodes. But if the devices are tamper resistant; they can remove their sensitive information in order not to be stolen [20]. ZigBee nodes could stay alive for several years without the need to exchange their batteries. The ZigBee network can have thousands of tiny sensors and it is able to coordinate the communication between them easily, this is known as interoperability [16] .include

2.5. Wi-Fi communication technology

Definition: Wi-Fi is a high data rate and a long range technology dedicated to the Wireless Local Area Networks (WLANs), and based on the IEEE 802.11 standard. Wi-Fi is a wireless version of an Ethernet network developed and owned by Wi-Fi Alliance [7].

Advantages and drawbacks: Wi-Fi is a technology enabled of transmitting data for long distance with a high rate and a high power. So it is better and faster than other technologies that have the same frequency band. It is integrated in most of nowadays devices such as tablets, smart phones, printers, laptops and personal computers and allows these devices to access the Internet as they are within any Wi-Fi network range. Wi-Fi networks can provide a lot of services for users in local areas such as restaurants and other public places, they can be competitors or harmonious with other wired or wireless communication technologies available in the same place [16].

The main drawback about Wi-Fi is the high power consuming [3] , especially when Wi-Fi network is used by smart phones that it consumes their batteries quickly [6] , [18] . Wi-Fi

networks are almost everywhere and can cause coexistence interference to other technologies such as ZigBee and Bluetooth which operates with lower energy; that is because it runs with higher power and the same ISM 2.4GHz band [22]. Wi-Fi products manufacturers support security procedures proposed by IEEE 802.11 standards (802.11b/802.11i/WPA/WPA2). But Wi-Fi networks still have many shortcomings in security side. Some mechanisms were suggested to solve the problem such as access control which is not an optimal solution due to intruders can listen to the communication and steal the MAC addresses. Wi-Fi uses other security mechanisms such as authentication, encryption, decryption, confidentiality and integrity of data by exchanging encryption/decryption keys between stations. All the mentioned mechanisms do not provide a suitable solution and do not ensure a secure communication for Wi-Fi [16].

Table 1. Comparison of studied wireless technologies [7]

Parameter	NFC	RFID	Bluetooth	ZigBee	BLE
Flexibility	High	Low	High	High	High
Power Consumption	Low	No	High	Medium	Low
Security	High	High	Low	Low	Medium
Personalization	High	High	Medium	Low	Medium
Cost of tag	10 cent	10 cent	\$ 5	\$5	\$5

Table 2. Overview of studied wireless technologies [7]

Wireless Technology	Operating Frequency	Data Rate	Operating Range
802.15.4 ZigBee	2.4 GHz	250 kbps	70 m
802.15.1 Bluetooth 2.0	2.4 GHz	3 Mbps	10 m
802.11b/g Wi-Fi	2.4 GHz	54 Mbps	100 m
802.11a Wi-Fi	5 GHz	54 Mbps	100 m
NFC	13.56 MHz	106, 212, 424 kbps	0–4 cm
RFID	125–134 kHz (LF) 13.56 MHz (HF) 400–930 MHz (UF) 2.5 GHz and 5 GHz (microwave)	1–200 kbps	20 cm for passive 400 cm for active
BLE	2.4 GHz	1Mbit/s	30-50m 2-5m to last the battery lifetime

Table 3. Comparison of active tags and passive tags [7]

Parameters	Active Tags	Passive Tags
Power Source	Embedded power source	Power from RF field
Battery	Yes	No
Data Storage Capacity	High	Low
Manufacturing Cost	Expensive	Cheap
Operating Range	Long range	Up to a few meters
Signal Strength to Tag	Very low	Very high

3. HOSPITAL ROOM HYGIENE

The proposed use case has the goal to monitor, draw attention and increase consciousness about the importance of following the hygiene rules for reducing the HAI. The system is designed to monitor the possible breaching of hygiene rules inside a hospital room.

3.1. Use case description

Room layout: The considered room (Figure1) has two beds for patients separated by a suitable distance (at least 3 feet); a curtain can separate between the two beds; and the beds are placed perpendicular on the inner wall of the room versus to the entrance. A Hand washing sink is seated to the right wall, and so close to the entrance, that doctors and nurses should wash their hands directly when they enter the patient room. Each room has a small and closed place, dedicated to the treatment of wounds and changing the bandages to prevent the infection transmission within the room or outside. The room is provided with an air conditioning system to change the indoor air. A waste bin for unclean services is very close to the hand washing sink, so the used things such as head and face covers, masks, tissues, used towels and gloves can be disposed of directly through this bin. The waste bin is connected to the ground floor in order to prevent the transfer of contaminated purposes within the corridors of the hospital. The room also contains a toilet for the patients.

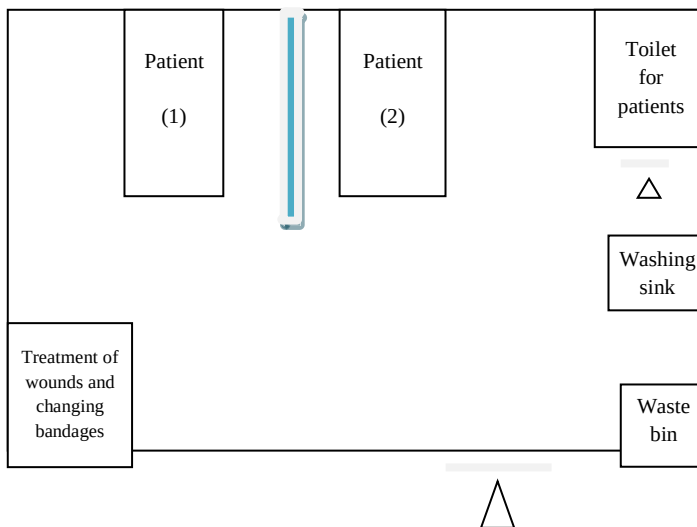


Figure 1. The room layout

Monitored events and rules: The events which must be monitored have the following sequence:

- The Physician's passing through the entrance; the system is able to recognize the physician's identity number while he is entering or leaving the room.
- The Physician's complying with the hand hygiene protocol at the washing sink before heading to the first patient.

- The first patient is treated while he is in his bed, but if this patient has wounds and needs to exchange the bandages, the physician accompanies the patient to the place of treating wounds and changing bandages. After finishing, the physician should go again towards the sink to sanitize his hands before progressing towards the second patient.
- The next patient will be treated in his bed if he is in recovery phase, or he will be accompanied to the place dedicated to changing the bandages. After finishing, and in both cases, the physician sanitizes his hands again before leaving the room.
- After any of the two patients uses the toilet, he should go to the sink to sanitize his hands.

3.2. Technological choices

We will choose the best technology for each monitored event type, based on the following criteria: operating mode and range, power consumption, security issues, cost, flexibility personalization.

Identifying persons passing the room entrance, we need to know the identity of people who are entering and leaving the room.

We use RFID technology for monitoring the physicians (doctors or nurses) entry and leaving into and out of the patient room for the following reasons:

- RFID is a technology dedicated for identification and tracking of people and daily objects and things by means of tags which can keep valid and readable for a long time and can store a unique identity number for each person.
- RFID has very low power consumption, a high personalization and a high security that the tag data is highly encrypted.
- The RFID does not need a line of sight to work like many other technologies,
- The RFID operating range (20 centimeters up to few meters) is very suitable for detecting the physician's ID when he passes through the entrance. These features make the RFID technology a good choice for monitoring the entrance.

NFC technology can also be used for monitoring the physician's passing into and out of the patient room for the following reasons:

- NFC is considered as a highly flexible technical solution; it is simple with only touching or waving one NFC device near the other.
- NFC performs a fast communication, so that the two NFC devices do not need pairing for establishing the connection as in other technologies such as Bluetooth.
- NFC provides a security higher than RFID, because the short distance communication prevents the attackers to catch the signal.
- NFC technology does not require a line of sight in order to operate and it has a high personalization that it takes into consideration the person's privacy.
- NFC also has low power consumption, so that when NFC technology is integrated into mobile phones or wrist bands, it does not consume high power.
- NFC can operate in three modes, so it enables finding solutions, and offers choices to solve problems.

Taking in consideration the hardware equipment, RFID, NFC tags has small sizes (around 0.5 mm²) so they can be integrated easily anywhere. They also are cheap and have a sufficient memory capacity (from kilobytes up to 1Mb and over) to be used.

At the washing sink, the physicians can interact with NFC technology very simply by only using their hands to move, wave or touch their NFC equipped devices close to other NFC equipped ones. At the sink we need to know if the physician complies with the hand hygiene rules or not. Implementing the NFC technology at the washing sink is a guaranteed solution because the NFC operating range is so short (0-4 cm), and will confirm that the hand washing event has been performed. This reason, in addition to the reasons mentioned earlier, makes the NFC technology a suitable solution.

BLE and ZigBee communication technologies face the obstacle problem that the signals spread in straight lines. When BLE uses the broadcasting way to perform the communication; it cannot be considered as a secured technology, that any listening device can capture the signal and steal the transmitted data. Regarding ZigBee technology; if one of the ZigBee nodes (devices) is not a tamper-resistant; then the sensitive information could be stolen. ZigBee and BLE tags have higher costs than RFID and NFC tags.

In the patient vicinity, We need to know exactly if the physician complies with the hand hygiene rules before and after treating each patient. In this case, each of NFC or RFID could also be a suitable solution due to their distinct features mentioned earlier, and that they are able to identify the physician's position, and which patient is being treated in real time. In our case, the complying with hand hygiene must be repeated three times:

- Before handling the first patient.
- After handling the first patient and before starting to treat the next one.
- After handling the second patient.

The idea of treating each patient also includes if any of them needed to go to the place dedicated for treating the wounds and changing the bandages.

When using the toilet, We need to know if the patient complies with the hand hygiene rules after using the toilet. Each of NFC or RFID technology is a suitable choice for monitoring this event due to the reasons mentioned earlier.

4. CONCLUSIONS

This paper focused on the hospital acquired infection as a big challenge of current hospitals. The most recent technologies have been reviewed in details; we demonstrated the concept, the work mechanism, the advantages and the drawbacks for each of them, with comparison tables show the characteristics and the features for each technology. The RFID-NFC relation was clarified precisely. We described a hospital room use-case, and we analyzed the events workflow of the patient room, which has to be monitored. In particular, we analyzed in details which technology is more suitable for each event and we concluded that RFID and NFC are the more suitable choices to be applied for monitoring the workflows due to their superiority over similar technologies especially in security, power consumption, cost, and operating mode aspects.

REFERENCES

- [1] Zaid Ali SHHEDI, Alin MOLDOVEANU, Florica MOLDOVEANU, "Traditional & ICT Solutions for preventing the Hospital Acquired Infection", 2015.
- [2] Zhe-Min Lin, Cheng-Hung Chang, Nai-Kuan Chou, and Yuan-Hsiang Lin, "Bluetooth Low Energy (BLE) Based Blood Pressure Monitoring System", 2014 International Conference on Intelligent Green Building and Smart Grid (IGBSG), IEEE, National Taiwan University of Science and Technology, Taipei, Taiwan, Department of Surgery, National Taiwan University Hospital, Taipei, Taiwan, DOI:10.1109/IGBSG.2014.6835225 23-25 April 2014, pp.1-4.
- [3] Hideki Matsuoka, Junbo Wang, Lei Jing, Yinghui Zhou, Yilang Wu, Zixue Cheng, "Development of A Control System for Home Appliances Based on BLE Technique" University-Business Innovation Centre, The University of Aizu Aizuwakamatsu, Fukushima, Japan, IEEE, 2014.
- [4] Kevin Townsend, Carles Cufi, Akiba, and Robert Davidson. "Getting Started with Bluetooth Low Energy Tools and techniques for low-power networking" Printed in the United States of America. Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, May 2014: First Edition.
- [5] Matti Siekkinen, Markus Hienkari, Jukka K. Nurminen, Johanna Nieminen. "How Low Energy is Bluetooth Low Energy? Comparative Measurements with ZigBee/802.15.4" WCNC workshop on Internet of Things Enabling Technologies Embracing Machine-to-Machine Communications and Beyond, 2012, Pp. 232-237.
- [6] Raphael Frank, Walter Bronzi, German Castignani, Thomas Engel, "Bluetooth Low Energy: An Alternative Technology for VANET Applications" *Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg*, raphael.frank@uni.lu, walter.bronzi@uni.lu, german.castignani@uni.lu, thomas.engel@uni.lu 2014 IEEE. pp. 104- 107.
- [7] Vedat Coskun, Kerem Ok and Busra Ozdenizci. "NEAR FIELD COMMUNICATION FROM THEORY TO PRACTICE", NFC Lab – Istanbul, ISIK University, Turkey. This edition first published 2012, C 2012 John Wiley & Sons Ltd, A John Wiley & Sons, Ltd., Publication.
- [8] ZigBee Specification 053474r17, Jan. 2008; available from www.zigbee.org, accessed 10-3-2015.
- [9] Syed A. Ahson and Mohammad Ilyas, "Near Field Communications Handbook", Edited by Taylor & Francis Group, Boca Raton London NewYork © 2012 by Taylor & Francis Group, LLC CRC Press is an imprint of Taylor & Francis Group, an Informa business. International Standard Book Number-13: 978-1-4200-8815-1 (eBook - PDF).
- [10] Finkenzeller, K. (2010) RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, JohnWiley & Sons, Ltd, ISBN: 978-0-470-69506-7.
- [11] Vishal Patil1, Nikhil Varma1, Shantanu Vinchurkar2, Bhushan Patil2 "NFC Based Health Monitoring And Controlling System", IEEE Global Conference on Wireless Computing and Networking (GCWCN), Department of Computer Engineering Sandip Institute of Technology and Research Center, Nasik, India, 2014. Pp 133-137.

- [12] Suk-Un Yoon, Shekhar Joshi, Seung-Seop Shim, "A New Simple Wi-Fi Direct Connection Method using NFC on Remote Control and DTV", 11th International Joint Conference on Computer Science and Software Engineering (JCSSE), IEEE, 2014, pp. 170-175.
- [13] Nurbek Saparkhojayev, Aigul Dauitbayeva, Aybek Nurtayev, Gulnaz Baimenshina," NFC-enabled Access Control and Management System", IEEE, 2014.
- [14] Mulliner, C. (2008) Attacking NFC Mobile Phones, EUsecWest 2008. Available at: http://www.mulliner.org/nfc/feed/collin_mulliner_eusecwest08_attacking_nfc_phones.pdf (accessed 10 July 2011).
- [15] NFC Forum, <http://www.nfc-forum.org/> (accessed 10 July 2011).
- [16] H. LABIOD *INT*, Evry, France ENST, Paris, France H. AFIFI C. DE SANTIS *INT*, Evry, France" WI-FI T M , BLUETOOTH T M , ZIGBEE T M A ND WIMAX TM", Published by Springer, 2007.
- [17] Prinslin.L Prof.V.Janani.M.E." Efficient Data Delivery in Mobility Aware ZigBee Wireless Networks", ICICES - S.A.Engineering College, Chennai, Tamil Nadu, India, IEEE 2014.
- [18] Firdaus, Ahriman, Rois Akbar, Eko Nugroho, "Wireless Sensor Networks for Microclimate Telemonitoring using ZigBee and WiFi", IEEE International Conference on Aerospace Electronics and Remote Sensing Technology (ICARES), 2014, pp 200-204.
- [19] Mohd Adib Sarijari^{1,2}, Mohd Sharil Abdullah^{1,2}, Anthony Lo¹ , Rozeha A.Rashid² "Experimental Studies of the ZigBee Frequency Agility Mechanism in Home Area Networks", 3rd IEEE International Workshop on Global Trends in Smart Cities goSMART 2014, Edmonton, Canada. Pp.711-717.
- [20] Shahin Farahani. "ZigBee Wireless Networks and Transceivers", Elsevier Ltd, 2008.
- [21] A. Mohammed Mian and Divyabharathi. R, "DESIGN AND SIMULATION OF ZIGBEE TRANSMITTER USING VERILOG", International Journal of Emerging Trends in Electrical and Electronics (IJETEE), March-2013.pp 22-26.
- [22] Wang, Qixin Wang, Guanbo Zheng, Zheng Zeng, Rong Zheng, and Qian Zhang," WiCop: Engineering WiFi Temporal White-Spaces for Safe Operations of Wireless Personal Area Networks in Medical Applications" IEEE TRANSACTIONS ON MOBILE COMPUTING, MAY 2014, pp 1145-1158.