Bluetooth Low Energy: A Survey

Shamsaa Hilal Al. Hosni
Sohar University

ABSTRACT
Bluetooth Low Energy (BLE) is a wireless technology with low power that is designed to be embedded into a number of devices to monitor their applications. It is considered as power friendly where it enables devices to consume less power while running on a long period of time. The most interesting thing with BLE is its capability to work on applications already installed on smartphones and tablets without any difficulty. This capability will provide developers with a proper solution to enable the technology on billions of devices which are already on the market. This paper describes the concept of BLE technology, its architecture and the used applications. The established security structure on BLE is also described to show BLE performance on devices.

General Terms
Link manager protocol, Telephony Control and Signaling Layer, Service Discovery Protocol, Logical link control adaption protocol Physical layer, application layer, Bluetooth low energy Architecture , piconet , GAP ,Security, and Algorithms .

Keywords
Bluetooth Low Energy, architecture, security

1. INTRODUCTION
Nowadays, wireless communication technologies become as one of the most famous technology that used in various fields and techniques. One of the wireless communication technologies is Bluetooth technology, which enhance to communicate easily without cables connections in short range with a good communication performance according to the applications types and devices types. Bluetooth was released by Ericsson in 1994 (Bijoy Kumar, 2014).During 1998, Ericsson, Nokia, and Intel grouped together to make a special interest group (SIG).In 1999 ,the first Bluetooth V1.0 standard was released in manufacturers fields that used low –power devices like "mice ,heart rate monitors, and home security sensors " (Roy want, 2013). Bluetooth V1.0 and Bluetooth V.3 high speed consider as "classic Bluetooth" which used (79 1MHZ) channel on the (2.4) GHZ ISM(Industrial Scientific Medical) band with frequency leaping sequence randomly (Vilegas, 2012). In June 2011, Bluetooth v4.0 was released by the Bluetooth special interest group (SIG). Actually Bluetooth v4.0 is the newest version in the Bluetooth technology that has ultra -power energy feature which is 2.4 GHZ RF band. (SEMICONDUCTOR, 2011) .BLE (Bluetooth low Energy) developed as an enhancement and compatible to the classic Bluetooth ,where BLE "designed as a low-power solution for control and monitoring applications" (Carles Gomez, 2012).Its system designed to transmit small packets of data ,with less power and cost ,that will be run for a year on tiny and coin cell batteries (li, 2012).BLE is the basis of smart devices ,which can be used in several new devices that use a small power ,coin batteries like watches, toys ,sports & fitness ,health care, mice and many applications as discussed later in this paper. BLE has many features such as :"ultra –low peak ,ultra-low cost plus small size for accessories and human interface devices(SEMICONDUCTOR,2011),implementation cost is very low and has a secured system with multi-vendor interoperability .as mentioned previously, classic Bluetooth used 79 frequency hopping but BLE used 40 channels on 20 MHZ spacing (Roy want, 2013).for more technical details about the Bluetooth low energy see section IV .Also, there will be a compression between BLE and classic Bluetooth in section VII .In 2012 IETF 6LoWPAN working group (WG) acknowledged the importance of BLE for the internet of things ,where, they established a specification that enhance to transmit IPV6 packets over BLE (Carles Gomez, 2012).Furthermore, Bluetooth low energy network topology is star topology (SIG, 2014).By the recent improvements in Bluetooth technology ,Bluetooth used by 9 billion devices ,where BLE is predicted to be used in 2.9 billion devices per year by 2016 (Ryan, 2014) and by 2020 ,according to ABI research ,30 billion devices will generate into the internet of things ecosystem powered by Bluetooth smart (Ritcher, 2014).

2. BLUETOOTH ARCHITECHURE OVERVIEW
Bijoy et al. (Bijoy Kumar Mandal, 2014) clarified Bluetooth technology architecture as shown in figure (1) has several layers and protocols that differ between their functions .From the lower layer of the Bluetooth architecture, consist of:

1. Radio Frequency (RF) layer

Radio Frequency is a physical wireless layer that is the air interface used ISM range to reduce the collisions between devices and well-matched with other countries ISM band. In order to spread the energy in ISM range ,the radio used a frequency hopping and split the range into (79MHZ)band ,"starting at 2.402GHZ and stopping at 2.480HZ" (Bijoy Kumar Mandal, 2014).

2. Baseband layer

By base band layer, data packet is sending and managing through the radio layer, where the baseband communicate between devices. Bluetooth devices connected to another device to create a simple network called "a piconet" .this Bluetooth network has the major role to state each device either as master, slave, or standby as clarify in the following state:

2.1. *Master*: the Bluetooth device is the prompter of devices communications. Where, the Bluetooth device master is responsible to set the time and publish its clock to the slave and fit out the device hope frequency at which time.

2.2. *Slave: all devices that are connected to another devices state as slave device. The Bluetooth device which is connected directly to the master and getting the data or sending data to master device is called "active slave ". But, the device which is not active and not sending or receiving data is called "passive slave ".*

2.3. *Standby*: devices that are not connected to the master when searching for another device, the device investigate the

Bluetooth device and create a Bluetooth link .so far the device will be in a low power mode which will save power.

3. *Link manager protocol (LMP):*
Link manager protocol is a protocol that is responsible to control the radio link between devices, which manage the security and authentication between Bluetooth devices.

4. *Logical link control and adaption protocol (L2CAP):*

The L2CAP function is to exchange data packets between higher layer protocols over the base band.

5. *Radio Frequency Communication Protocol (RFCOMM)*
(RFCOMM) is made up the L2CAP layer, where, it has the Bluetooth serial connection that transport data for the upper level services, through the baseband layer.

6. *Service Discovery Protocol (SDP)*
SDP identify the service for Bluetooth devices and determine the supported services for each device.

7. *Telephony Control and Signaling Layer (TCS)*
TCS is managed the data call and control the speech between devices, where its signals passed through L2CAP.

8. *Application layer*
This layer holds the user applications. RFCOMM protocol cooperates with the application to create a rivalled serial connection.

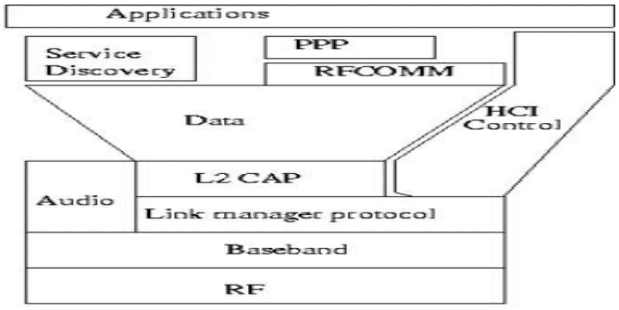

Figure 1: Bluetooth architecture (Bijoy Kumar, 2014)

3. BLUETOOTH LOW ENERGY ARCHITECTURE

This section defines the Bluetooth low energy architecture as shown in figure(2) which consists of three basic layers: controller, host and applications .Each layer has a specific function and protocol, comparing to the classic Bluetooth architecture BLE structure shared it in the application layer. First layer: controller layer which contains physical layer, link layer, and direct test mode. Second layer is the Host layer which runs on an application processor then functions in the upper level that consists of several protocols which are Logical link and adaption protocol (L2CAP), the attribute protocol (ATT), security manager protocol (SMP), generic attribute profile (GATT) and generic access profile (GAP).There is a host controller interface (HCI) acts as an BLE RF has two types of channels :advertising channels and data channels . advertising channel is used to discover devices ,to start the connection between devices and to spread broadcast while data channels is used to bidirectional communication between connected Bluetooth devices. There are three advertising channels 1,6 and 11 which are used to reduce the frequencies overlapping with IEEE 802.11 as shown in figure(4)(Carles Gomez,2012).

interface and as communication point between the controller and the host layer. Lately, the third layer is applications layer not define by Bluetooth specification (Carles Gomez, 2012).

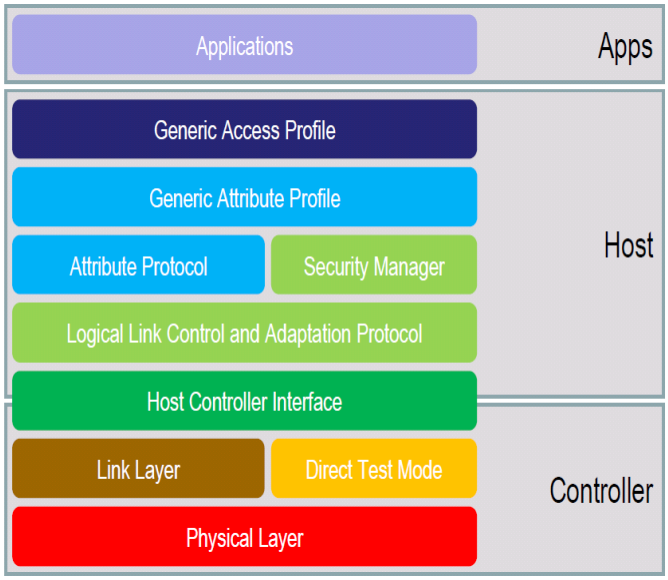

Figure 2: Bluetooth Low Energy Architecture (Ryan, 2014)

Now let's clarify each layer and protocol functions briefly.

1. Physical layer: BLE travels in 2.4 GHZ ISM band ,and has better range where it express 40 radio frequency channels on 2 MHZ channel spacing (see figure 3)this feature obtains it to be cheap and simple radio chips (SIG, 2014).

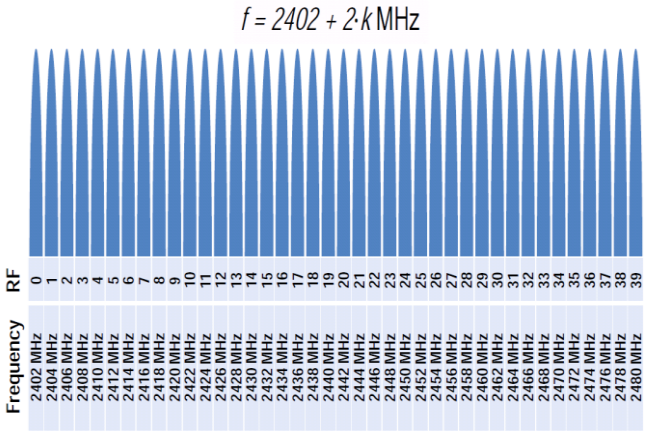

Figure 3: Bluetooth Low Energy technology uses 40 channels (SIG, 2014)

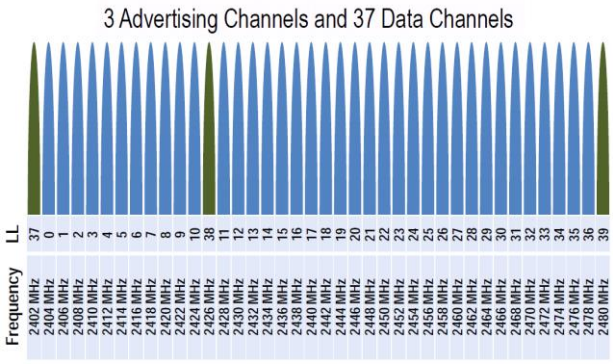

Figure 4: advertising channels (SIG, 2014)

2. Link layer: it takes the physical packets in the radio band, and manages packets timing for sending and receiving packets (Vilegas, 2012).In addition, it used to stop-and –wait movement control device founded on acknowledgments as well as error recovery is provided (Carles Gomez, 2012).

3. L2CAP: it is responsible for multiplexing and segmenting the data packets for the upper level layers ATT, SMP, and link layer signaling as well as recollect packets from the controller before they transmit to the higher levels.L2CAP has 23 bytes as payload size where the data packets from the upper layer protocol cannot exceed this size .

4. ATT :is responsible to provide a communication for a small data packet over L2CAP channel (SEMICONDUCTOR, 2011).the attribute protocol can be discovered, ,read or write by other device because it has a pair values or attributes that stored and managed by GATT .However, the client can send a request to the server to contact server's attributes ,in the other hand ,the server can send notification or indications to the client (SIG, 2014)

5. GATT: is used to determine the ATT framework and the conversation of packets that contains a value and properties (characteristics) between devices (Carles Gomez, 2012)see figure (5).GAP device support GATT services and user define (Roy want, 2013).

6. Security: BLE provide a secure environment for data exchange between devices, where the supported services can be exchange either in "LE security mode 1or LE Security mode 2" (Carles Gomez, 2012). These two modes operate the security purpose in link layer and ATT layer. Link layer use "Cipher Block chaining –message authentication code algorithm and 128-bit AES block cipher "in order to support encryption and authentication process. Also, BLE support privacy feature that permits the device to send and receive by using a private address (Carles Gomez, 2012).

7. GAP and Application profiles :GAP is located in the upper layer of BLE stack which is promit the client-server connection between services (Roy want, 2013).where ,it manages and sets the roles for the discovery devices and it is responsible to determine the modes and methods to perform a secured connection.GAP with enhancement from controller plays four roles:"broadcaster,observer,peripheral and central".A device can broadcast data through advertising channel,then the observer receives the data from the broadcaster .whereas, the central role is implementing to a dvice that manages multi-connections,and peripheral role created for a simple devices that used a single connection with a device in the central role.

Applicaation profile is located in the highest layer of BLE structure is definited how application should deal and operated which's specified by SIG . Application profile acts as intermediary between devices from various manufacturers (Carles Gomez, 2012).

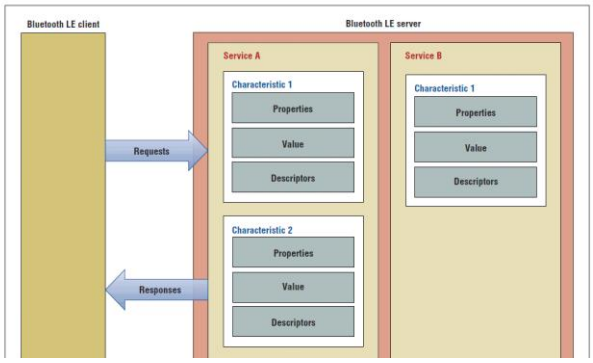

Figure 5: The Bluetooth LE Attribute protocol, implemented by Generic Attribute (GATT) services containing characteristics (Roy want, 2013)

4. BLUETOOTH LOW ENERGY TECHNICAL DETAILS

Technical details as mentioned in Bluetooth special interest group site (SIG, 2014) summarized at following: Bluetooth low energy allow to data transfer at 1Mbps that used sniff-sub rating to perform ultra-low duty cycle. It communicates with other versions of Bluetooth technology in high rate that overcome the interference in 2.4 GHZ. When it has any actions the host operates with the controller and then return back to sleep mode until next action for saving power and achieve low power consumption. Its data transfer latency is very low around 3ms in a range over 100 meters. BLE has adaptive Frequency Hopping, 24 bit CRC here appears its robustness. Furthermore, it has a high security Full AES-128 encryption using CCM.BLE technology improved for one to one connection it can be client-server connection ,and its allow one to many connection by using a star topology as shown in figure 6.

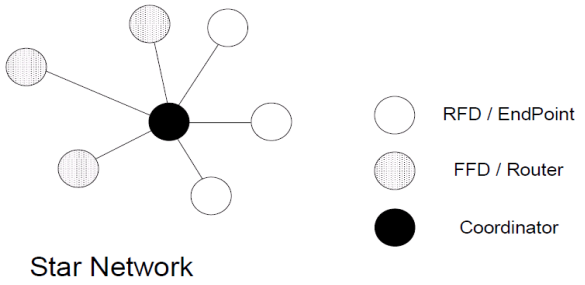

Figure 6: BLE used star topology (SIG, 2014)

5. BLUETOOTH LOW ENERGY APPLICATIONS & ITS DEVELOPMET

Bluetooth low energy is designed to run in several applications in new devices, especially for devices that search for low power consumption where it was the most problems that classic Bluetooth faced (Nilsson, 2014). According to the BLE features it comes very popular and more require in industrial world. It's low cost and simple use carries most of fields to use it, where the newest device comes with Bluetooth implementations that could be benefit for more vendors .Also, they can use the service for years by using a coin cell batteries that's make their maintenance easier (Vilegas, 2012).The following parts show the uses of Bluetooth low energy :

1) Smart Energy

Nowadays many smart phones is able to connect with each other by implementing Bluetooth v4.0, where Apple was the first in the market which installed Bluetooth v4.0 in their devices, then others like Android, RIM Blackberry ,Symbian, and windows phone 7(li, 2012).the smart phones can be used to communicate with people in a smart way by the help of Bluetooth low energy features like the study done by Antonio(Antonio J. Jara, 2014) that clarifies how smart phone can make the life easier ,secure, with a high performance where the number of sensors are increased that predict by 2020 (50-100)billion devices will be connecting all thing around the user that called Internet of Things. There is a challenge to determine the interaction between the human and the object. They analyzed the human behavior in big smart cities that include smart glass or smart watches, and could be using heart wearable sensor. Also, one of the interesting applications is hand-free call system that used in most new cars and trucks (Ritcher, 2014).BLE found in home sensors that perform a security purpose, like the nearness alarm that could be used for child safety devices that will make an alarm to the parent when the children move a way .another application indoor sensor application which can be used in a big building and broadcast information even without GPS signal like in airport building that can inform the passenger the air time and gates .etc. (SEMICONDUCTOR, 2011).

2) Health and wellness

By the growth of BLE uses, it allows to the user to check and use medical models like monitor heart rate, and blood pressure at home just by connecting to their smart phones (li, 2012). Shiwei Luan et al. (Shiwei Luan, 2014) developed a Para educator (para) glove for disabled children to enhance them to track with some behavior by using their fingers where each finger has a special function then it will be recorded by a microcontroller that is established in glove which is responsible to send data to their smart phone by using wireless technology which is BLE. According to ABI research (114%) growth rate millions of smart Bluetooth devices going to enable remote health care devices from 2012 to 2018.there are several medical devices which is available in the market like "blood glucose monitors, pulse oximeters, heart rate monitors, asthma inhalers and stethoscopes" (Ritcher, 2014).In the markets may found some devices that monitor a diabetic person's sugar level which is not supported for the Bluetooth low energy that suffer dangerous situation because it comes off its beeps ,while the diabetic devices that has BLE it will be more effective and never stop because it measure the sugar level and send it back to the central application located on the internet (Vilegas, 2012).

3) Sport and fitness

Bluetooth low energy used in sport and fitness field. Where, the person can use his/her smart phone which is supported BLE like in Android has S Health application that count user walk hours and reference him with the exercise and his weight loss and organize a schedule for his sport and his food with calorie measurement for eaten food anytime and anywhere and distance covered .as well as it monitor the heart rate and sleep hours (Samsung, 2014).Some materials that comes with BLE chip used in sport like the running shoes ,heart rate monitor and sport watch that track an athlete's vitals during their trial and transmit their events to their cell phone to share their location and map with others (Vilegas, 2012).

4) Entertainments

BLE could be used for entertainment sector where it has a small coin cell battery that can be implemented in many types of toys. For example, it can be seen in racing car toy, robot device that can be controlled remotely, and MP3 player remote control (SEMICONDUCTOR, 2011).

6. SECURITY AND PERFORMANCE

Bluetooth low energy has many ways of security that make it difficult to attack and provide a high secure environment to its services. Where BLE used "AES-128 with CCM encryption engine" (Robin Heydon, 2014).BLE security uses key generation, encryption, signed data and privacy feature as the security methods. Where the key generation is execute by the host in each connected device that can upgrade its algorithm easily without changing the controller. BLE use different keys like "confidentially of data and devices authentication, authentication of unencrypted data and device identity" (SIG, 2014).Where during pairing operation only one link key is used between devices.in the other hand, in the encryption sector it use AES-CCM cryptography perform in the controller. (Counter Mode Cipher Block Chaining Message authentication Code) (Robin Heydon, 2014).BLE enables sending the authenticated data through unencrypted ATT in a trusted area. That occur by signing data with "connection Signature Resolving key (CSRK)".Each sending data should contain a signature, where, the receiver has to identify and confirm the signature if its' from trusted source. The signing and a counter establish a message authentication code to protect message from replay attack. Privacy feature is supported by BLE technology that changes the address of data on the frequent basis to avoid the attack during a specific time (SIG, 2014).In order to discover and connect with other devices BLE uses only three channels, which makes its performance high efficiency in low power consumption which takes to link only milliseconds. (7.5ms) is the latency period for a slave that depends on the master period how often it send the message and it receive the message from the slave. Comparing to the classic Bluetooth, BLE has the best link budget around 3db.Conseqently, BLE unit can provide the range from 200 to 300 without any increase in the power amplifier (Nilsson, 2014).

7. CLASSIC BLUETOOTH TECHNOLOGY VS. BLUETOOTH LOW ENERGY TECHNOLOGY

Bluetooth has made a paradigm shift in design .Where, Bluetooth v2.0 EDR and Bluetooth 3.0 Hs were designed with faster data transmitting. Bluetooth v4.0 (low energy) was designed with lower power consumption but it is not designed to stream large amount of data.it sends short data in a short distance. There are two types of BLE devices dual mode which is backwards compatible with previous Bluetooth

technology versions. Single mode supports BLE 4.0. Dual mode devices perform high date rate streaming but not benefit from the low power consumption of BLE. Whereas classic Bluetooth is connection oriented .The following table I clarify the main differences between BLE and classic Bluetooth (ConnectBlue, 2014).

Table 1: classic Bluetooth technology vs. bluetooth low energy (ConnectBlue, 2014)

	Classic Bluetooth technology	Bluetooth low energy technology
Data payload throughput (net)	2 Mbps	~100 kbps
Robustness	Strong	Strong
Range	300m	250m
Local system density	Strong	Strong
Large scale network	Weak	Good
Low latency	Strong	Strong
Connection set-up speed	Weak	Strong
Power consumption	Good	Very strong
Cost	Good	Strong

8. OPEN ISSUES

Mike Ryan (Ryan, 2014) asserts in his study: "Bluetooth: with low energy comes low security "where, his discussion was underlie Bluetooth low energy privacy.as mention in section VI BLE perform the encryption using 128 bit AES which seem complexity. As BLE devices transmit over channel by using 2.4 GHz hops where it uses one channel to send or receive a packet. They implement a sniffer on the Unbetroth platform where, they clarified the requirement that should know to sniff connection are" hop interval, hop increment, access address and CRC unit". Unbetroth is a USB that come with an RF, CC2400 radio chip, which can monitor BLE channel at any period of time. They introduce a technique to eavesdropping on BLE. Therefore, they establish an attack touching the key exchange protocol, which offer a way to any attack .They resulted with a security limitation in BLE. In general Bluetooth security seeks to secure disabling discovery and enabling discovery in trusted communication .They mention as many employees serve in any organization they could use several types of applications via Bluetooth technology. Which can be attacked easily that will affect the organization server or their profiles. They show how the Bluetooth devices can be attacked easily by the hackers as well as, there are some open sources and tools that are available help them to simply attack any Bluetooth device. Here some examples of attacks that are able to attack Bluetooth devices are:" BlueSnarf, BlueSnarf++, Blue Jacking, and Hello Moto" (Dr. Ashley L. Podhradsky, 2012).Rolf and Bill (Saltstein, 2012) have mention some limitations in BLE when comparing with the classic Bluetooth .Their discussion was in the power consumption and the coin cell batteries. Where data transfer over below 100 kb/s, as a huge data are sending in the same period it will lose its power saving as the transmitting process is completed. The power consumption average depends on the application type itself.

9. CONCLUSION

As rapid growth of technology as it need a daily improvement for its techniques. One of the improvement technologies is Bluetooth low energy which is a wireless communication that enhance for several devices to communicate in a short range with low power consumption. A performance evaluation on energy consumption, latency, picante size, and throughput of this technology is provided as well as exploring their potential and impacts on the application. All three mainly depends on the connection Interval and connection Slave Latency parameters which in turn have to be evaluated in a wise way to successfully meet the application requirements (Dr. Ashley L. Podhradsky, 2012). In addition, a deep understanding of what is happening on the backend beyond running existing sniffing tools and their affect in sniffing the Bluetooth traffic which summarizes that the Bluetooth version 4.0 is considered as a highly secured protocol and developing it will continue and overcome any associated vulnerabilities and really obvious that this technology gives new markets opportunity's for devices that require both low cost components and low power wireless connectivity. Like any other technology, there are various implementation challenges and issues may lead to low performance of BLE. It still formulates a strong contributing low-power wireless technology in connecting a huge amount of new devices to the Internet of Things.

10. REFERENCES

[1] N. SEMICONDUCTOR, "Bluetooth low energy wireless technology backgrounder," NORDIC SEMICONDUCTOR 2011, 2011.

[2] S. C. T. P. Y. C. W. L. Z. Youcong Ni, "A Profile for Step Data Transmission based on Bluetooth Low Energy," 2013.

[3] N. H. Robin Heydon, "CSR," 2014. [Online]. Available: www.csr.com. [Accessed 2014].

[4] J. Vilegas, "Bluetooth low Energy version 4.0," Bluetooth smart ready, 2012.

[5] B. s. L. Roy want, "Bluetooth LE Finds its Niche," smartphones, vol. 12, no. 04, pp. 12-16, 2013.

[6] R. Nilsson, "Bluetooth Low Energy: the best media for sensors and actuators?," Industrial Ethernet Book, no. 67 / 40, 24 11 2014.

[7] J. o. a. j. Carles Gomez, "overview and Evaluation of Bluetooth low Energy :An emerging low-power wireless technology," Sensors, p. 11, 12 9 2012.

[8] B. Y. a. l. x. a. Y. li, "Bluetooth low energy (BLE) based mobile electrocardiogram monitoring system," shenyang, 2012.

[9] D. B. T.-h. K. Bijoy Kumar, "A Design Approach for Wireless Communication Security in Bluetooth Network," International Journal of Security and Its Applications, vol. 8, no. No.2, pp. 341-352, 2014.

[10] M. Ryan, "ubertooth," 2014. [Online]. Available: http://ubertooth.sourceforge.net/. [Accessed 11 2014].

[11] S. Ritcher, "NO strings attached," A TWICE SUPPLEMENT, 2014.

[12] B. SIG, "Bluetooth," 2014. [Online]. Available: http://www.bluetooth.com/Pages/what-is-bluetooth-technology.aspx. [Accessed 05 Nov 2014].

[13] B. SIG, "Bluetooth special interest-training resources," 2014. [Online]. Available: https://www.bluetooth.org/en-us/training-resources/technology. [Accessed 5 Nov 2014].

[14] Y. B. D. G. Antonio J. Jara, "Mobility management in Bluetooth Low Energy," 2014.

[15] I. S. M. D. G. P. P. I. M. a. S. W. I. M. Shiwei Luan, "A Paraeducator Glove for Counting Disabled-Child Behaviors thatIncorporates a Bluetooth Low Energy Wireless Link to a Smart Phone," 2014.

[16] Samsung, "S health," 2014. [Online]. Available: http://content.samsung.com/mobile/us/contents/aboutn/sHealthIntro.do. [Accessed 26 oct 2014].

[17] C. C. C. Dr. Ashley L. Podhradsky, "Managing Bluetooth Risks in the Workplace," London, 2012.

[18] P. R. R. R. S. S. L. E. Helmut H. Strey, "Bluetooth Low Energy Technologies for Applications in Health Care:Proximity and Physiological Signals Monitors," 2013.

[19] Aislelabs, "Byte light," 2014. [Online]. Available: http://blog.bytelight.com/post/953918898/the-limitation-of-bluetooth-le-with-battery-drain-ana-accuracy. [Accessed Nov 2014].

[20] R. N. a. B. Saltstein, "Bluetooth low Energy vs. classic bluetooth:choose the best wireless technology for your application," MDE medical Electronics Design, 2012.

[21] ConnectBlue, "Bluetooth Low Energy Technology," 2014. [Online]. Available: http://www.connectblue.com/technologies/bluetooth-low-energy-technology/. [Accessed 15 NOV 2014].

[22] T. S. R. M. Baris Aksanli, "Benefits of Green Energy and Proportionality in High Speed Wide Area Networks Connecting Data Centers," 2012