Bluetooth Protocol Stack: Bluetooth Specification Version 4.2

As a potential solution for Internet of Internet of Things

Ehsan-Ul-Haq, Muhammad (1st *Author*)
1098587
ehsan-ul-haq@hotmail.com

Malik, Manan (2nd *Author*)
1098312
manan.maqbool@gmail.com

***Abstract (Auth.1)*—Bluetooth Special Interest Group (SIG) officially announced Bluetooth version 4.2 in December 2014 and it brought quite a lot of revolutionary changes in the Bluetooth Low Energy or LE for short -a subset of Bluetooth version 4.0 stack. The past couple of years have seen a high interest in the idea of connecting everything to the internet known as Internet of Things (IoT), which has also exaggerated the underlying technologies well before they can mature in a sustainable ecosystem. The idea has also brought IPv6 based Low Power Personal Area Networks (6LoWPAN) as disruptive technology, that brings IP capabilities to the network of resource constrained devices, but a suitable radio technology for this device class is still debatable. When Bluetooth 4.0 was first released, it was not targeted for IP-connected devices, but for the communication between two neighboring peers. However, the latest release of Bluetooth 4.2 offers features that makes Bluetooth LE suitable, and competitive candidate among available low power radio technologies in IoT space. In this paper, we will discuss newly added features of latest release and its applicability in 6LoWPAN networks. We will also highlight some future research challenges and improvements for its broader impact.**

Keywords—Special Interst Group, Bluetooth 4.2, Low Energ, Internet of Things, Low Power Personal Area Networks, Research Challenges

I. INTRODUCTION (AUTH. 1)

The name Bluetooth comes from the king of Denmark Harald Blåtand translated as Harald Bluetooth in English (940-986 BC), who united Denmark and Norway. Today, Bluetooth is known as open standard to allow connectivity and collaboration between disparate products and industries.

The man behind this technology was Sven Mattison in Lund, an engineer who in mid 90s, working along with other engineers at Ericsson, built a wireless communication standard that connects devices over a certain distance. The technology was first launched in May 1998, under the name of Bluetooth, to great expectations. Since then, a number of Bluetooth versions have been released. They come with different specifications to offer different options to the users. Moreover, all the updated versions of Bluetooth are backward compatible. Special Interest Group (SIG) of Bluetooth technology, is the governing body for the development and standardization of the protocol, released Bluetooth version 1.2 in the year 2003.

Figure 1: Smartphone connected to Bluetooth enabled smart devices

It is also known as Basic Rate (BS) Bluetooth with theoretical max data rate of 721 Kbps. Later, after one year it released version 2.0 to abolish radio frequency interference by using frequency hopping technique and also added security against tracking and snooping. Version 2.1 was released in 2007, which provided more data transmission rate, with Enhanced Data Rate (EDR) for about 2.178 Mbps, more security, less power consumption, and improved pairing system using Secure Simple Pairing (SSP) was introduced. Then in 2009, Bluetooth 3.0 High Speed (HS) came out with the ability to use Wi-Fi connections, and max data rate of 24 Mbps by using 802.11 link in the physical layer. After that, in 2010 and 2011 smarter versions of Bluetooth 4.0 & 4.1 known as Bluetooth Low Energy (LE) were introduced respectively. Which are really low power consuming versions, with strong power management skills. In addition to combining a standardized communication technology designed for low power systems and a new sensor based data collection framework, Bluetooth LE also offers easy integration with most handheld devices (such as smartphones and tablets), something that conventional wireless sensor networks are still working towards.

In recent years the idea of Internet of Things (IoT) is gaining lot of attention. IoT is referred as large scale network of physical devices, where anything in the physical world can be digitally represented and connected. The idea is

largely driven by the trends in data/device proliferation, networking and cloud computing. In this paper we discuss the latest Bluetooth 4.2 release and its many new features such as IP profile, enhanced privacy and government-scale security[1], which make Bluetooth LE a disruptive technology for the IoT. The paper also highlights future research challenges and limitations of Bluetooth LE. For example, In order to take full advantage of Bluetooth LE in IoT, we need to address issues such as, Bluetooth Smart mesh, multicasting, secure broadcast, open source hardware and software and provision of 6LoWPAN in smartphones.

The organization of the rest of the paper is as follows. We describe newly added features of Bluetooth LE 4.2 in Section II. In Section III, we discuss its available implementations and suitability for IoT. Section IV describes research challenges in Bluetooth LE-connected IoT. In the end, Section V concludes the paper. Figure 1 shows a scenario of Bluetooth LE implemented for IoT enabled devices

II. BLUETOOTH 4.2: NEW FEATURES AND THEIR SIGNIFICANCE (AUTH.1)

Bluetooth 4.2 was first introduced in December 2014. Until Bluetooth 4.1, it was only targeted for the low-power radio communication between pair of devices such as headset and music player, smart watch and smart phone or TV and remote control. In contrast Bluetooth 4.2 has novel features which makes it promising for IoT. In this section we will highlight the newly added features and discuss about what makes it front runner for communication between constrained devices in IoT [1]. Moreover, Bluetooth LE out-of-box support in most smartphones makes it possible to use Bluetooth LE supported smartphone as a gateway to the internet. Anyhow, the necessity of 6LoWPAN border router gateways for internet connection can still not be totally eliminated because of the situations where a smart phone can't be available all the time. Following are some novel features of Bluetooth 4.2 [2].

A. Flexible internet conectivity (Auth. 1)

It is estimated that in 2020, about 28 billion devices will be connected to the internet, keeping this in mind, the most important feature included in Bluetooth 4.2 is the internet connectivity. A newly created profile (a formal specification that defines Bluetooth based wireless communication between devices) known as Internet Protocol Support Profile (IPSP) is designed to enable IPv6 for Bluetooth. Which also means IoT devices would be able to talk directly to the internet by 6LoWPAN border router gateway.

IPSP provides a support to an IPv6 enabled Bluetooth *central* and *peripheral* to discover and establish connection in link-layer. Bluetooth LE Generic Attribute Profiles (GATT) helps to discover if IPSP is supported or not. Over GATT, IP Support Service (IPSS) is used to determine support for IPSP's *Node* role [3].

[1] Federal Information Processing Standards (FIPS) specified by NIST

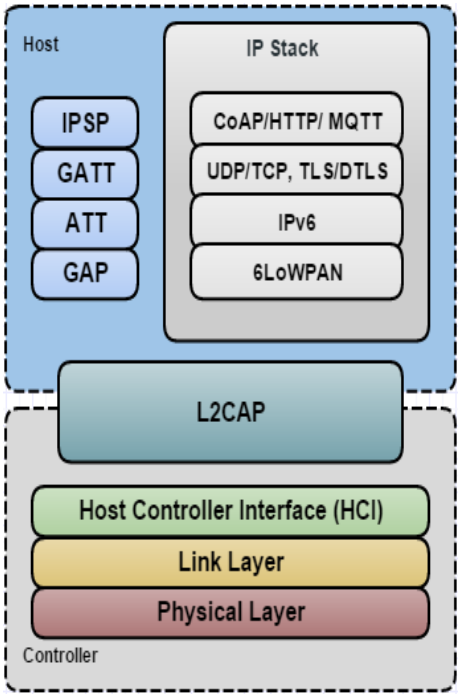

Figure 2: Bluetooth Low Energy Protocol Stack Version 4.2

The Logical Link Control and Adaption Layer Protocol L2CAP resides in the data-link layer and provides connectionless and connection oriented services to upper layer protocols with protocol multiplexing, segmentation and reassembly capability. IETF has discussed a standardized way of transmitting IPv6 packets over Bluetooth LE in its RFC 7668. They explain to use 6LoWPAN techniques and adaption of compressed header mechanism over Bluetooth LE.

Moreover, they prefer to rely on L2CAP fragmentation mechanism over 6LoWPAN fragmentation [4]. With the help of GATT, the HTTP Proxy Service HPS allows a device to expose HTTP web services and RESTful APIs further comment on the connectivity Bluetooth LE devices with the internet [4]. Constrained Application Protocol CoAP, is a light weight web application layer protocol that is especially tailored for devices with the limited resources. HTTP and CoAP share common set of request methods: GET, POST, PUT and DELETE [5]. The reason CoAP is suited for limited devices is that it can work on UDP and instead, it implements its own lightweight, simple, but not fully featured reliability mechanism. Only problem with CoAP is that it is not yet widely spread as HTTP. But, we hope that Bluetooth 4.2 will extend something called CoAP proxy service or similar. Fig. 2 illustrates IPSS can already be used to run CoAP or other web protocols in Bluetooth connected IoT.

B. Enhanced Privacy (Auth. 1)

Bluetooth 4.2 comes up with industry leading privacy measures that lowers the power consumption and builds upon government-grade privacy features of Bluetooth specification. The new privacy features put control back into

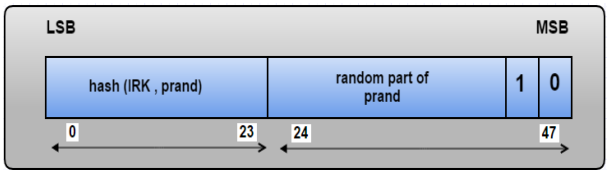

Figure 3: Bluetooth Low Energy RPA format

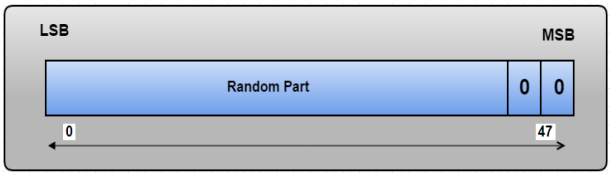

Figure 4: Bluetooth Low Energy NRPA format

the hands of consumer by making it difficult for eavesdroppers to track a device through its Bluetooth connection without permission. For example, when you are shopping in a retail store with a beacon, you can't be tracked unless you've enabled the permission to engage with your device.

The privacy feature introduced in Bluetooth 4.1 changes the device private address on a frequent basis over period of time, such that adversary can't connect a static Bluetooth LE address to a specific device. In Bluetooth core specification 4.1, the host Bluetooth LE device can generate 48 bit RPA or NRPA using the resolving identifying key IRK shared during the bonding process. Fig. 3 and 4 show the format of RPA and NRPA. After receiving the generated RPA, the peer device does the exhaustive search in bond database for specific IRK.

The IRK is used to identify the device which generated the RPA. In connection mode, a BLE device follow a specific rule to generate a 48 bit NRPA and distribute to a device. Next time, the peer device can use the NRPA to reconnect to the known BLE device. In Bluetooth 4.2, the private address resolution is also included in the *Controller* and it also manages the white list of private addresses there. Which makes it possible to resolve and generate private addresses without involving host and accept and reject the requests based on white list, which significantly reduces the frequency of waking the host and consumes less energy [6].

C. Enhanced Security (Auth. 2)

Security Manager Layer in the BLE Stack is in fact responsible for Key generation and device pairing). ATT is adjacent layer to SM, employed for small packet sizes and for exposing the attributes including Key generation. Bluetooth Low Energy (LE) initially has weaker security in the earlier releases, with the release of Bluetooth version 4.2 security level is considerably strong enough. It allows some of the tightest security in the industry with 128-bit AES data encryption. To make sure the communication over Bluetooth with its low energy feature (BLE V4.1 and earlier) is always secure and protected, the Bluetooth Core Specification provides several features to cover the encryption, trust, data integrity and privacy of the user's data [20].

a) Pairing

The pairing mechanism is the process where the parties involved in the communication exchange their identity information to set up trust and get the encryption keys ready for the future data exchange. In version 4.0 and 4.1 of the core specification, Bluetooth with its low energy functionality uses the Secure Simple Pairing model (referred to as LE Legacy after the Bluetooth 4.2 release), in which devices choose one method is followed i.e. Passkey entry and Out of Band (OOB) based on the input/output capability of the devices. In Bluetooth version 4.2, the numeric comparison method is added to the traditional methods and the Elliptical Curve Hellman-Diffie (ECDH) algorithm is introduced for key exchange in this process [20].

b) Key Generation

Key generation in Bluetooth with LE v4.2 is performed by the Host on each low energy device independent of any other. Key generation in BR/EDR is performed in the Controller. When using Bluetooth LE Secure Connections, the following keys are exchanged between master and slave: Connection Signature Resolving Key (CSRK) for Authentication of unencrypted data, Identity Resolving Key (IRK) for Device Identity and Privacy In LE Secure Connections, the public/private key pair is generated in the Host and a Secure Connection Key is generated by combining contributions from each device involved in pairing [6].

c) Encryption

Encryption in Bluetooth with low energy uses AES-CCM cryptography. Like BR/EDR, the LE Controller will perform the encryption function. This function generates 128-bit encrypted Data from a 128-bit key and 128-bit plaintext Data using the AES-128-bit block cypher as defined in FIPS-1971 [21].

d) Signed Data

Bluetooth has ability to send authenticated data over an unencrypted transport (i.e. communication channel is not encrypted. This is accomplished by signing the data with a CSRK. The sending devices place a signature after the Data Protocol Data Unit (PDU). The receiving device verifies the signature and, if the signature is verified, the Data PDU is assumed to come from the trusted source [21].

The goal of the low energy security mechanism is to protect communication between devices at different levels of the stack. Currently two neighboring devices are being protected by BLE V4.2; Link Layer security can protect against passive eavesdropping and in some cases man-in-the-middle (MITM) attacks.

D. *Enhanced Packet Capacity and Speed (Auth. 2)*

In Bluetooth version 4.1 and earlier, the most important drawback was that BLE operating at low speed data transfer. With the advent of version 4.2, Bluetooth SIG announced an increase in both the transmission rate by 2.5 times and the size of the transmitted packet by 10 times. Figure 6 and 7 are related to each other shows that the data rate increased because the size of the transmitted packet has increased. If we observe the Link Layer of the stack and it's PDU (protocol data unit) data channel: Each PDU contains a 16-bit header. So, the header in the version 4.2 is different from the header in the version 4.1. The header of version 4.2 contains label RFU (Reserved for Future Use)-field. As name depicts this abbreviation is reserved for future use and is filled with zeros. As we see the last 8 bits of the header are different. It is easy to calculate that the Length field in version 4.1 may contain values in the range from 0 to 31, and version 4.2 in the range from 0 to 255. If we subtract the value of the maximum length of the MIC field (4 octets), we obtain that useful data can be 27 and 251 octets for version 4.1 and 4.2 respectively. In fact, the maximum n umber of data is even less because in the payload are also overhead L2CAP (4 octets) and ATT (3 octets), but it shall not be considered. Thus, the size of transmitted user data has increased about 10 times.

Thanks to the up gradation of packet size and data rate in Bluetooth v4.2, it has enabled IP based communication and hence opens the doors for IoT security (such as Datagram TLS), routing (such as RPL) and networking (such as IPv6) protocols on top of Bluetooth LE. According to IEEE802.15.4 based 6LoWPAN networks [9], more energy is consumed as a device has to perform packet fragmentation and assembly whenever the MTU size is more than 127 bytes. This gets worse when IEEE 802.15.4 security is enabled because encryption and integrity protection is applied on each fragment rather than on each packet [10]. In Bluetooth LE-enabled 6LoWPAN networks, different messages can be merged together (e.g. DTLS handshake flights [8]) in a single packet, which makes Bluetooth LE more energy efficient, fast, and reliable (due to reduced packet losses) compared to IEEE 802.15.4-based 6LoWPAN networks [17].

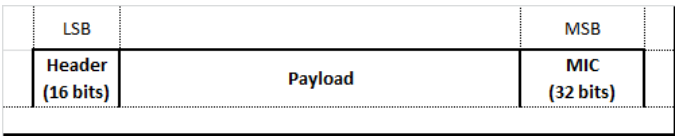

Figure 5: Bluetooth Low Energy PDU Channel

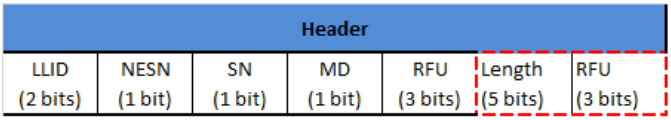

Figure 6: Bluetooth Low Energy version 4.1 Header

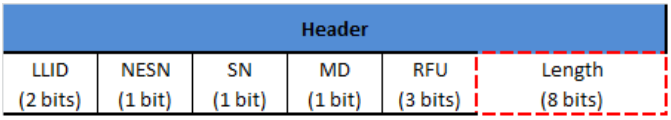

Figure 7: Bluetooth Low Energy version 4.2 Header

III. IMPLEMENTING BLUETOOTH SMART FOR IOT (AUTH. 2)

2016 could be the year for the Internet of Things and for the implementation of IoT devices companies are focusing to this concept with Intel is leading the charge, with a group dedicated to creating consumer and other devices that are connected to the Internet. Implementation of Bluetooth LE as per the Bluetooth standard requires at least the four lowest layers of the Bluetooth protocol stack inclusive of the Security Manager (SM) and the Attribute Protocol. The Host Controller Interface (HCI) offers Programming interface which approximately divides the functionality into application which runs on the host and system services on the controller. This also provides development of exchangeable hosts and controllers [17].

In 2013, Intel introduced the Quark, a low-power system on a chip for wearables. The Quark features a tiny battery, along with a motion sensor, Bluetooth, and battery-charging capabilities [Ref: Intel.com]. The real time implementation of BLE device requires a balanced design of software and hardware that results in low power consumption, better performance and programmability. "Whereas a controller API is usually provided along with host-side software to the developer as source code, the controller is implemented as firmware that has exclusive access to the radio. The tight integration of the firmware binary and the PHY layer is conducive to performance optimization and low power operation conducted by the chip vendor. The close-source nature of the firmware libraries provided by major vendors, however, becomes a disincentive to innovations by third parties. This has not stopped the vibrant IoT community from integrating some of these chips with open-source embedded operating systems and tools, e.g. the late port of TI CC2650 to Contiki OS [17]". As Bluetooth LE firmware is in binary form still many vendors has make register-level details open source for developers to code it according to their new ideas and hence inventing self-owned new implementation of Bluetooth LE [11] [12].

The implementation of Bluetooth LE is also simpler as the requirements include low power and low date rate which leads to simple protocol debugging and fault diagnosis. This simplicity has one open loop that the packets and connections are susceptible to eavesdropping for malicious attacker since of the simpler Physical and Link Layers. For Bluetooth LE sniffer and injectors an open source project called Ubertooth has developed a low cost hardware and free software [13]. Ryan has practically explained, using the

Ubertooth, an operative attack against the weak key exchange protocol used by Bluetooth LE [14].
Simplest Wireless sensors could be deployed using Bluetooth LE utilizing the connection-free broadcast mode [15]. Broadcast feature of Bluetooth LE is exactly the same as of an advertisement packet being sent at 1Mbps using GFSK modulation by any radio of 2.4 GHZ frequency. Many developers have developed Bluetooth LE broadcast feature using low cost Arduino and nRF24L01+radio [16].

IV. FUTURE RESEARCH CHALLENGES (AUTH. 1)

In order to have broader impact of Bluetooth, there are certain research challenges that need to be solved to utilize it to its full potential. Following are few major challenges in this regard.

A. Bluetooth Smart Mesh (Auth. 1)

Mesh networking is a key architecture for IoT in which each node of network can accept and forward data to neighboring node, allowing a network to scale more easily by just adding new nodes. This is more cost effective and easier to implement than having to use additional gateway devices or access points which often need more extensive planning to avoid clashing frequencies.

Bluetooth on the other hand is fundamentally a point to point connection, linking to a terminal such as a smartphone or to an access point such as iBeacon or Eddystone. Which is basically a Piconet (master-slave) architecture. Bluetooth 4.1 brings a change in this architecture and introduces Scatternet topology that enables a master node to be a slave for another node or vice versa. So, the Scatternet absolutely makes the multi-hop connection possible. Yet, it does not inherently change the Piconet based asymmetric topology model, where a relay node can receive/relay a message in data channels only after establishing a master-slave connection with a corresponding transmitter/receiver. This challenge calls for innovative solutions to overcome these constraints [7].

Short range IoT devices in a capillary network, such as Bluetooth LE devices, can be connected to internet by capillary gateway. Nevertheless, the short transmission range for such devices with a single hop network topology prevents the use case of IoT applications from running over a large number of devices. BLE mesh enables these use case by providing peer-to-peer and robust multi-hop connectivity for a large number of local Bluetooth LE devices. This way, IoT application data can be exchange between any local Bluetooth LE and internet through the mesh network and a gateway [7].

The Bluetooth SIG recently launched a study group to examine the subject of mesh networks with a view of defining an industry standard mesh protocol. When the process completes, this will be a big news for manufacturers and developers

B. Security Issue in Bluetooth Smart Mesh (Auth. 1)

The Bluetooth security, designed to secure a single point-to-point connection, does not scale well to accommodate mesh architecture. Mainly, Bluetooth implements its security at ATT and Link Layer for the protection of information exchange between two connected devices. Fundamental block of the Bluetooth security lies in the concept of pairing. The pairing comprises of three phases: first, agreement on the mode of operation; second generation of short term key (STK); third, distribution of long term key (LTK) that is used for link layer encryption and authentication, connection signature resolving key (CSRK) that is used for data signing performed at ATT layer, identity resolving key (IRK) for private address generation on the basis of device public address. So the whole process requires the exchange of LTK, CSRK, IRK or STK.

This security mechanism was designed by keeping in mind the communication between two nodes. But, a mesh scenario consists of large number of nodes, they will try to communicate with neighboring nodes and these neighboring nodes will keep changing over time. Therefore, current Bluetooth security doesn't scale well to accommodate mesh architecture and there is a need to review the Bluetooth's security mechanism.

C. Security issue in Loosely Coupled Communication (Auth.1)

With the advent of Bluetooth LE 4.0, SIG introduced a new mode in form of an advertisement. This new mode offers unidirectional communication between two or more Bluetooth devices using advertisement events, thereby achieving a communication solution without entering into a bonded connection. This kind of loosely coupled communication manner is undoubtedly more energy efficient but more vulnerable to a range of security threats such as packet injection attacks.

Applications based on Bluetooth Smart can provide custom security protocols at application layer, but such solution has interoperability issue across different vendors. Moreover Bluetooth 4.2 still restricts broadcast packet size to 31 bytes, For strong Bluetooth LE broadcast security, it is important that the size of broadcast packet should also be increased. Moreover, in this type of communication mechanism broadcaster doesn't have any way of knowing whether the data is actually reached any observer or not. Which is indeed another research challenge.

D. Secure Bluetooth Smart Multicast (Auth. 2)

"Multicast is sending a message to multiple destination nodes with one network invocation" RFC 7390. It is a group communication in which data or information is shared to a group. It is an essential feature of 6LoWPAN networks. Features like synchronous ON/OFF of smart light bulbs or requesting the capacities of a group of nodes in a 6LoWPAN network are important for different IoT applications.

Generally there is one active master and up to 7 active slave in Bluetooth pico-net. At a time only two nodes can communicate i.e. the master and one of the slaves. Although maximum of 254 slaves are supported by one master, all

slaves from 8 to 254 must remain inactive. The older version of Bluetooth piconet is not efficient for multicasting because data can reach the slave nodes only sequentially. For multicasting in a piconet having slaves more than 8, all inactive slave nodes need to be brought online before they can receive the multicast data. “Therefore multicasting is tedious task in this model of operation. Efficient ways of secure group communication in Bluetooth LE-connected 6LoWPAN networks is an open research challenge” [17].

E. Open Source Bluetooth Smart (Auth. 2)

Bluetooth Smart is a communication technology which allows different devices from various vendors to communicate to each other with low power consumption. Currently Bluetooth stacks are not open source and developers do not have the opportunity to experiment on the stack. Moreover all new comers in the field of IoT have to pay licensing fees of Bluetooth LE. An open source Bluetooth stack with Berkeley Software Distribution (BSD) license could attract more brains and also speedup the Bluetooth Mesh vision.

“A nominal well-designed Bluetooth stack should have at least four components: (1) physical data transport layer for a connected Bluetooth physical baseband transceiver, (2) HCI layer for the establishment and management of physical connections, (3) L2CAP layer for the establishment and management of logical channels within an established connection, and (4) one Bluetooth Services on top of the L2CAP layer to implement functionality such as the Service Discovery Protocol (SDP) to expose local device functionality and interact with remote devices” [17].

F. Novel Applications of Bluetooth Smart (Auth. 2)

With the advent of Bluetooth LE Wireless sensor networks (WSNs) are becoming a global technology. WSNs are a group of spatially distributed sensing nodes with low maintenance requirements, which can automatically monitor environmental parameters and cooperatively transfer the data through a gateway to a main database using wireless networking [18]. One application for WSNs is the monitoring of noise levels around construction sites to determine the noise pollution levels for surrounding residents, businesses and amenities. Such technology is currently required at London Bridge Station [19].

Bluetooth LE has momentum to organize communication between various devices used in applications which are still ideas such as smart grids, smart meters, smart houses, smart healthcare systems, smart industry, etc. Bluetooth could play an important role for all data communicating under way projects in which low power consumption and low cost is the main requirement.

V. CONCLUSIONS (AUTH. 2)

In the light of all the facts we have discussed it can be concluded that no doubt Bluetooth LE V4.2 is the main stream communication standard for Internet of Things (IoT) upcoming innovations due to the high data rate and speed plus low power consumption features. We have discussed these novel features and how they help building the Internet of Things and wireless sensors networks (WSNs). Bluetooth Open source stack would be a great help in achieving the novel inventions.

REFERENCES

[1] Bluetooth SIG. Bluetooth Specification Version 4.2 [Vol 0].Bluetooth Specification, December 2014. [https://www.bluetooth.com/specifications/adopted-specifications].

[2] N. Kushalnagar, G.Montenegro, and C. Schumacher. IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. RFC 4919, August 2007.

[3] Bluetooth SIG: Bluetooth Specification Version 4.2 [Vol 1]. Adopted Specifications, ISPS December2014.

[4] J. Nieminen, T. Savolainen, M. Isomaki. IPv6 over Bluetooth Low Energy: Bluetooth LE Packet Size and MTU. RFC 7668, October 2015

[5] Constrained Application Protocol (CoAP), IETF RFC 7252 [https://tools.ietf.org/html/rfc7252]

[6] Bluetooth Specification Version 4.2 [Vol 3, Part H] 3.6.1 Key Distribution and Generation

[7] Ericsson Research Blog: [http://www.ericsson.com/research-blog/internet-of-things/bluetooth-smart-mesh-make-sense-iot]

[8] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt. Lithe: Lightweight Secure CoAP for the Internet of Things. Sensors Journal, IEEE, 13(10):3711–3720, 2013.

[9] J.HuiandP.Thubert.Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks. RFC 6282, September 2011.

[10] S. Raza, S. Duquennoy, J. H¨oglund, U. Roedig, and T. Voigt. Secure Communication for the Internet of Things - A Comparison of Link-Layer Security and IPsec for 6LoWPAN. Security and Communication Networks, Wiley, 7(12):2654–2668, December 2014

[11] Nordic Semiconductor. nRF51822 datasheet v3.0, September 2014

[12] Nordic Semiconductor. nRF52832 datasheet, 2015

[13] Project Ubertooth, 2015. [http://ubertooth.sourceforge.net Online; accessed 3-2-2016

[14] M. Ryan. Bluetooth: With low energy comes low security. In WOOT, 2013.

[15] Apple iBeacon, 2015. [https://developer.apple.com/ibeacon Online; accessed 3-2-2016

[16] S. Sridhar, P. Misra, and J. Warrior. Cheepsync: A time synchronization service for resource constrained bluetooth low energy advertisers. In Proceedings of the 14th International Conference on Information Processing in Sensor Networks, IPSN ’15, pages 364–365, New York, NY, USA, 2015. ACM.

[17] Shahid Raza, Prasant Misra, Zhitao He and Thiemo Voigt “Bluetooth Smart: An Enabling Technology for the Internet of Things,” 2015 Eight International Workshop on Selected Topics in Mobile and Wireless Computing

[18] F. Akyildiz and I. Kasimoglu, "Wirless Sensor and Actor Networks: Research

[19] Challenges," Ad Hoc Networks, vol. 2, no. 4, pp. 351-367, 2004. Josie Hughes, Jize Yan* and Kenichi Soga “DEVELOPMENT OF WIRELESS SENSOR NETWORK USING BLUETOOTH LOW ENERGY (BLE) FOR CONSTRUCTION NOISE MONITORING,” INTERNATIONAL JOURNAL ON SMART SENSING AND INTELLIGENT SYSTEMS VOL. 8, NO. 2, JUNE 2015

[20] BLUETOOTH SPECIFICATION Version 4.2 [Vol 1, Part A] 5.4.2 Key Generation •

[21] BLUETOOTH SPECIFICATION Version 4.2 [Vol 3, Part H] 3.6.2 Encryption Information, 3.6.6 Signing Information