2015 Eight International Workshop on Selected Topics in Mobile and Wireless Computing

Bluetooth Smart: An Enabling Technology for the Internet of Things

Shahid Raza⋆, Prasant Misra†, Zhitao He⋆, Thiemo Voigt⋆‡
⋆SICS Swedish ICT Stockholm, Sweden
‡Uppsala Universitet, Uppsala, Sweden
{shahid, zhitao, thiemo}@sics.se
†Robert Bosch Centre for Cyber Physical Systems, Indian Institute of Science, Bangalore, India
prasant.misra@cps.iisc.ernet.in

***Abstract*—The past couple of years have seen a heightened interest in the Internet of Things (IoT), transcending industry, academia and government. As with new ideas that hold immense potential, the optimism of IoT has also exaggerated the underlying technologies well before they can mature into a sustainable ecosystem. While 6LoWPAN has emerged as a disruptive technology that brings IP capability to networks of resource constrained devices, a suitable radio technology for this device class is still debatable. In the recent past, Bluetooth Low Energy (LE) - a subset of the Bluetooth v4.0 stack - has surfaced as an appealing alternative that provides a low-power and loosely coupled mechanism for sensor data collection with ubiquitous units (e.g., smartphones and tablets). When Bluetooth 4.0 was first released, it was not targeted for IP-connected devices but for communication between two neighboring peers. However, the latest release of Bluetooth 4.2 offers features that makes Bluetooth LE a competitive candidate among the available low-power communication technologies in the IoT space. In this paper, we discuss the novel features of Bluetooth LE and its applicability in 6LoWPAN networks. We also highlight important research questions and pointers for potential improvement for its greater impact.**

Keywords*—*Bluetooth Smart, Bluetooth 4.2, Low Energy, Internet of Things, Research Challenges

I. Introduction

The Internet of Things (IoT) is envisioned as a large scale network of physical devices. The IoT is a vision wherein anything in the physical world can be digitally represented and connected together. It is largely being driven by the trends in data/device proliferation, networking, cloud and community computing. The current assumption here is of a few hundreds of connected devices in any given localized physical space; however, we would soon be witnessing an immense proliferation of such devices on the scale of tens of thousands. Of the many possible design directions to achieve such scale and densities at affordable costs, a very interesting one suggests piggybacking on existing and widely adopted standards and techniques; and using a combination of 'really' cheap sensing/networking platforms and highly functional gateways (possibly themselves mobile). Pushing down the cost would potentially result in devices that are much more constrained in terms of energy and communication capabilities than the current state-of-the-art.

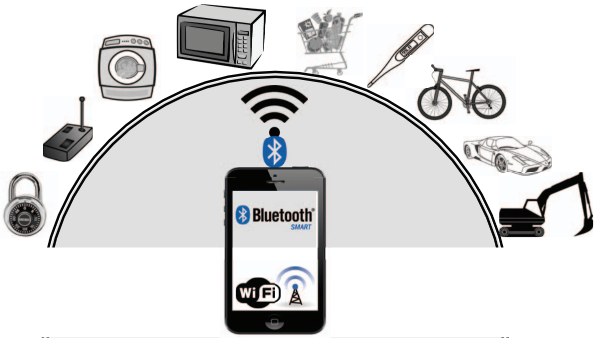


Fig. 1: A network architecture showing smartphone-connected Bluetooth Smart devices.

Of the few available energy and communication constrained technologies, Bluetooth Low Energy (LE)[1] - specified in Bluetooth v4.0 - is an appealing alternative. Bluetooth LE, in addition to combining a standardized communication technology designed for low-power systems and a new sensor-based data collection framework, offers easy integration with most handheld devices (such as smartphones and tablets), something that conventional wireless sensor networks are still working towards. Figure 1 shows a network architecture of Bluetooth LE-enabled IoT devices accessed through a smartphone.

[1] Bluetooth LE is marketed as Bluetooth Smart

978-1-4673-7701-0/15/$31.00 ©2015 IEEE

In this paper, we discuss the novel attributes of Bluetooth LE that make it an enabling technology for the IoT. The latest Bluetooth 4.2 release [1] has many new features such as IP profile, government-scale[2] security, and enhanced privacy, which make Bluetooth LE a disruptive technology for the IoT. This paper also highlights open research challenges and limitations of Bluetooth LE. In order to take full advantage of Bluetooth LE in the IoT, issues such as Bluetooth Smart mesh, multicasting, secure broadcast, open hardware and open source software, and provision of 6LoWPAN capabilities in smartphones should be addressed. Last but not least, we discuss implementing Bluetooth Smart for IoT devices.

The rest of the paper is organized as follows. We describe novel Bluetooth LE features and implications of those in the IoT in Section II. In Section III, we discuss available Bluetooth LE implementations and their suitability in the IoT. Section IV presents open research challenges in the Bluetooth LE-connected IoT. Finally, Section V concludes this paper.

II. Bluetooth 4.2: Novel Features and Implications

Until Bluetooth 4.1, the primary target applications of Bluetooth in connection mode consisted of a pair of consumer devices communicating with each other over a low-power radio such as a TV and remote control, a smart watch and smartphone, and a headset and music player. Applications using the Bluetooth LE broadcast mode can use the communication from different nearby Bluetooth LE dongles and provide a set of new functionalities such as localization. Bluetooth 4.1 offers no significant differences over Bluetooth 4.0 that enable widespread use in new domains. In contrast, the new Bluetooth 4.2 [1] has novel features that make Bluetooth LE a promising enabling technology for the IoT.

Bluetooth 4.2 was realized in December 2014, and from then on, it is being pushed as a protocol for the IoT. In this section we highlight the features that make Bluetooth LE one of the most favorable technologies to be used in constrained devices in the IoT. Above all, the Bluetooth LE out-of-the-box support in most smartphones eliminates the need of gateways such as 6LoWPAN border routers [2] to connect Bluetooth LE devices with the Internet. This means that we can easily use any Bluetooth LE supported smartphone as a Bluetooth LE gateway to the Internet. Bluetooth 4.2 is not yet supported in smartphones but most high-end smartphones already have support for 4.1; therefore, we expect 4.2 upgrade to be available in new smartphones soon.

A. Internet connectivity: Internet Protocol Support Profile

Though it is compatible with Bluetooth 4.1, the Internet Protocol Support Profile (IPSP) [3] is released with Bluetooth 4.2. IPSP provides support to an IPv6-enabled Bluetooth *central* and a *peripheral* to discover each other and establish a link-layer connection. Bluetooth LE Generic Attribute Profiles (GATT) helps to discover if IPSP is supported and the Bluetooth LE L2CAP Credit Based Flow Control Mode is used to exchanged data. Over GATT, the IP Support Service (IPSS) is used to determine support for the IPSP's *Node* role [3] . Though there were previous efforts to connect Bluetooth LE devices with the Internet [4], Nieminen et. al in an IETF draft [5] discuss the standardized way of transmitting IPv6 packets over Bluetooth LE. They explain the use of 6LoWPAN techniques and the linkage between 6LoWPAN and Bluetooth LE. They adapt the 6LoWPAN header compressed mechanism over Bluetooth LE; however, propose not to use 6LoWPAN fragmentation, rather rely on the Bluetooth L2CAP fragmentation mechanisms.

The above two standard documents explain the use of Bluetooth LE in 6LoWPAN networks that are integral part of the IoT. In Figure 2 we shows the protocol stacks in constrained devices in a Bluetooth LE-connected IoT infrastructure. In order to support 6LoWPAN-compressed Bluetooth LE communication, both the node side and the smartphone side must implement the 6LoWPAN header compression mechanisms, in addition to the Bluetooth LE standard. Currently, smartphones have no out-of-the-box support for the 6LoWPAN standard. In order to take full advantage of 6LoWPAN over Bluetooth LE, we expect that with the Bluetooth 4.2 upgrade smartphones would include the support for 6LoWPAN. For the node side, many implementations of 6LoWPAN and Bluetooth LE already exist; for example the Contiki OS (an operating system for the IoT) supports 6LoWPAN [6] and Bluetooth LE [7].

Upcoming Bluetooth GATT service called the HTTP Proxy Service (HPS) and RESTful APIs will further complement the connectivity of Bluetooth LE devices with the Internet. In the IoT domain, Constrained Application Protocol (CoAP) [8] is more lightweight and suitable for constrained devices than HTTP. We hope that the Bluetooth 4.2 will be extended with something

[2] Specified by NIST in Federal Information Processing Standards (FIPS)

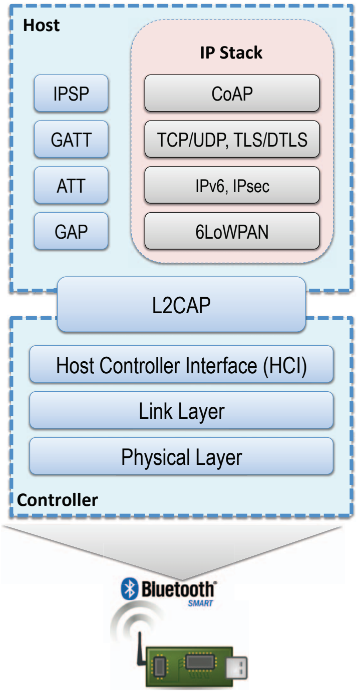


Fig. 2: Software stack in resource-constrained sensor devices in a Bluetooth LE-connected IoT setup.

called CoAP Proxy Service or similar; or rather define a generic proxy service that can be extended with different web protocols for example CoAP, HTTP, MQTT, WebSockets, etc. Recall from Figure 2 that IPSS can already be used to run CoAP or other web protocols in the Bluetooth LE-connected IoT. For seamless IP experience, rather than proxy services, we prefer using IPSS and IP/6LoWPAN all the way to Bluetooth LE gateways.

B. Enhanced security

To improve energy efficiency, Bluetooth LE initially has weaker security compared to standard Bluetooth [9]. Unlike Bluetooth 4.1 and earlier releases, Bluetooth 4.2 comes with a strong security that brings the level of Bluetooth LE security equal to the standard Bluetooth. For key management, Bluetooth 4.2 is equipped with the industrial scale asymmetric Elliptic Curve Cryptography (ECC) with FIPS recommended elliptic curves. It also uses FIPS's approved AES-CCM cryptography for message encryption. Currently, the security features in the Bluetooth 4.2 provides security between two neighboring devices. This link-layer security can protect wireless links against passive eavesdropping, and in some cases, Man-in-the-Middle (MITM) attacks depending on the availability of a display/keyboard to the device.

In an IoT setting it is sometimes important that the communication between a source and destination is secured End-to-End (E2E). This eliminates the need of trusted gateways. For example, in an e-health application, a patient's privacy can be protected from untrusted intermediaries if the communication is secured E2E between wearable medical devices and a remote doctor equipment. We see a possibility to enable E2E security in the Bluetooth LE-connected IoT using the IPSS/IPSP and then running Internet security protocols such as lightweight IPsec/IKE [10] or DTLS [11]. Figure 2 depicts these settings.

C. Enhanced privacy

Personal privacy in the current Internet is already daunting; and in the IoT, consisting of everyday smart objects around humans, it will be even more challenging. Primarily due to the lack of interest from big industry players, the technological standards for privacy preservation is almost non-existence. Bluetooth LE, on the other hand, includes the privacy feature since Bluetooth 4.0. Bluetooth 4.2 comes with enhanced privacy features (discussed below) that consumes even less power, which increases the chances of adopting Bluetooth LE as a technology for low-power IoT devices.

Since Bluetooth 4.0, Bluetooth LE supports frequent changing of Bluetooth device address (called private address) to limit the ability to track Bluetooth LE devices over a period of time. A Bluetooth LE device that wants to establish a connection with another device must be able to resolve private addresses that are generated using the resolving identify key (IRK) shared during the bonding process. In addition to the private address resolution in the *Host* (supported in Bluetooth 4.1), Bluetooth 4.2 adds private address resolution in the *Controller*. Furthermore, Bluetooth 4.2 supports white list of private addresses at the Controller. This means that the Controller at the link-layer can resolve and generate private addresses without involving the Host, and can accept and reject incoming request consulting the white list. This significantly reduces the frequency of waking up the Host (i.e. Bluetooth LE chips) and hence consumes less power. When the Host is involved, for example when the Controller cannot stored all IRKs, the device filtering must be disabled, which results in higher power consumption.

D. Enhanced Packet Capacity and Speed

One of the prominent features of Bluetooth 4.2 is increased Bluetooth LE packet capacity, almost 10 times compared with the Bluetooth 4.1 LE (from 27 bytes to 251 bytes). Also, data throughput in Bluetooth 4.2 LE is increased up to 2.5 times. This increased capacity facilitates efficient communication and opens new possibilities of Bluetooth LE usages. For example, due to the increased packet size, IP communication became efficient in Bluetooth LE devices. Further usage of increased capacity are: fast and frequent firmware updates, ability to run Internet security and communication protocols, and fast uploading of sensor data logs to the computing backend (a computer, a smartphone, or a cloud).

Thanks to the increased packet size and throughput, it is possible to run IoT security (such as Datagram TLS), routing (such as RPL [12]), and networking (such as IPv6) protocols on top of Bluetooth LE. In IEEE 802.15.4-based 6LoWPAN networks [13], a device has to perform packet fragmentation and assembly when the MTU size is more than 127 bytes, resulting in higher energy consumption. This get worse when IEEE 802.15.4 security is enabled because encryption and integrity protection is applied on each fragment rather than on each packet [14]. In Bluetooth LE-enabled 6LoWPAN networks, we can even bundle different messages (e.g. DTLS handshake flights [11]) 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.

III. Implementing Bluetooth Smart for IoT Devices

According to the Bluetooth standard, a minimal implementation of a Bluetooth LE device covers the four lowest layers and associated protocols, as well as the Security Manager and the Attribute Protocol. The Host Controller Interface (HCI) provides a natural programming interface that roughly divides functionality into application on the host and system services on the controller, and facilitates development of interoperable hosts and controllers. The actual implementation of a Bluetooth LE device on a commercial system-on-chip, however, involves fine-grained HW-SW co-design that balances performance, power consumption 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 [15]. In spite of the binary form of the provided Bluetooth LE controller firmware, register-level details disclosed in datasheets by certain vendors leave the door open to ambitious developers who want to experiment with their own Bluetooth LE implementation [16] [17].

The low power, low data rate nature of Bluetooth LE simplifies requirements for radio traffic monitoring, which in turn simplify protocol debugging and fault diagnosis; On the other hand, simpler PHY and link layers render packets and connections quite susceptible to eavesdropping by a malicious attacker. The open source Ubertooth project has developed low cost hardware and free software for Bluetooth LE traffic sniffer and injector [18]. Using Ubertooth, Ryan has demonstrated an effective attack against the weak key-exchange protocol used by Bluetooth LE [19].

With the connection-free broadcast mode, Bluetooth LE has potential for vast deployment of extremely low complexity wireless sensors. The Apple iBeacon is a location service based on broadcast-only Bluetooth LE devices [20]. A Bluetooth LE broadcast is no more complex than a short advertisement packet sent at 1 Mbps using GFSK modulation by any 2.4 GHz radio. Hobbyists have successfully used the low cost Arduino and nRF24L01+ radio to create Bluetooth LE broadcast [21]. We have ourselves ported Contiki OS to a Renesas RL78G14-based platform and generated Bluetooth LE broadcasts using nRF24L01+ [22].

IV. Open Research Challenges

Though Bluetooth Smart offers feature that makes it a technology for the IoT, there are still open research issues that need to the solved before we can utilize its full potential. We discuss these open research issues and their importance in the IoT realm.

A. Bluetooth Smart Mesh

Bluetooth Smart is constrained by factors such as shorter transmission range, limited coverage and support for only (one-hop) peer-to-peer communication. It is here that the wireless mesh networking technology[3] can enable Bluetooth Smart to significantly expand its coverage range.However, re-factoring a Bluetooth network into a mesh arrangement has many challenges.

The networking foundations of Bluetooth are rooted in a *Piconet* (master-slave) architecture. Bluetooth v4.1

[3] A wireless mesh is a peer-to-peer, multi-hop wireless network where participating network elements cooperate to route packets.

brings a fundamental change to this model by introducing the *Scatternet* topology that enables a master node of one or several slave nodes to simultaneously be a slave of another node. While the foundations of a multihop topology can be witnessed in this new standard, yet the inherent piconet based asymmetric network model does not allow nodes to seamless communicate without establishing a master-slave connection.

Mesh networking is an integral part of the IoT. Many applications rely on mesh capabilities to deliver seemless IoT experience; for example smart lighting and HVAC in smart homes, process automation in industrial environments, connected smart vehicles in smart cities, environment monitoring, etc. The Internet Engineering Task Force (IETF) has already standardized IoT protocols to support mesh capabilities in constrained environments. For example, RPL [12] is a routing protocol for the IoT that supports mesh networking. Bluetooth Smart does not support mesh networking yet, but its need is seriously felt in the Bluetooth community. Therefore, a new Bluetooth Smart Mesh WG has been formed to standardize the mesh capabilities. This work is still in its inception stage and welcomes different proposals for future Bluetooth Smart mesh.

B. Securing the Bluetooth Smart Mesh

Bluetooth offers security services at the link (by LE Security Mode 1) and ATT (by LE Security Mode 2) layers for protecting the information exchange between two connected devices. The fundamental building block of Bluetooth security is the concept of *pairing* wherein devices generate and distribute keys. The pairing process comprises *three* phases: *one*, devices (interested to connect with each other) agree on the mode of operation for the second phase; *two*, generation of the short term key (STK); and *three*, distribution of (upto) three 128 bit keys: 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 the ATT layer, and identity resolving key (IRK) that is used to generate a private address on the basis of a device public address. The message exchange required for distributing the LTK, CSRK or IRK is encrypted using STK.

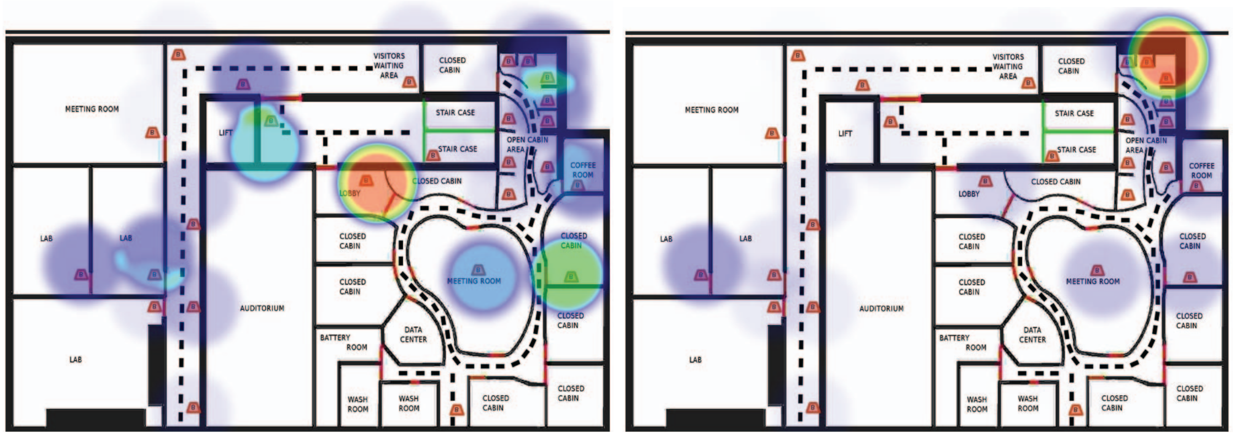
Bluetooth Mesh poses a number of challenges if an attempt is made to use the security mechanisms *already* present in Bluetooth. Mesh topologies, in general, would consist of large number of nodes that will want to network with a large segments of neighboring node, and these neighbors will change over time. Also, external network elements (such as smartphones) would need to communicate with any part of the meshing infrastructure. Therefore, Bluetooth's security that is designed to secure a single point-to-point connection will not scale well for accommodating the system dynamics that occur in mesh arrangements.

C. Secure Bluetooth Smart Broadcast

Master-slave, in the form of a piconet, is the de facto network model of Bluetooth. However Bluetooth v4.0 introduced a new feature in the form of an 'advertisement' (configurable through the broadcast/peripheral mode). This new mode offers unidirectional communication between two or more Bluetooth devices using advertising events, thereby achieving a communication solution without entering into a bonded connection (as required by Classic Bluetooth devices). Such a loose coupled manner of data transfer is undoubtedly more energy efficient; but also unearths other limitations. Bluetooth broadcast mechanisms are highly vulnerable to a range of security threats such as packet injection attacks.

We demonstrated the effect of a packet injection attack on a Bluetooth LE based indoor location system [23] for a regular office environment. This experimentation space was instrumented with a set of 26 beacon units. The beacons were configured to broadcast advertisement packets at an interval of 750 ms and at their lowest transmit power of -23 dB. For our evaluation, 10 people carried Android smartphone running the location service for about 6 hours. Proximity events were streamed to the Cloud service that aggregated the data from all 10 mobile units and generated a real-time location heat map of people in the office space. During the experimentation period, a packet injection attack was launched on the location sensing system by impersonating a benign beacon with a malicious one. The malicious beacon was placed in the same zone as the benign beacon so as to tag it with the same context, but was configured to broadcast Bluetooth LE packet at an interval of 100 ms and at a higher transmit power of -6 dB. While under a normal situation (as expected), the regions of high interest to people were observed to be meeting rooms, the office front desk and cubical spaces; the situation gets entirely flipped under the attack scenario where it appears that people are mostly interested in gathering at one office corner.

Applications based on Bluetooth Smart (such as an iOS app that is strictly based on the broadcast mode1) can provide custom designed security protocols at the application layer. Such a solution has interoperability issues across different vendors. Unfortunately, Bluetooth 4.2 still restricts the broadcast packet size to 31 bytes, which limits the use of a sophisticated broadcast



(a) *System under normal conditions*

(b) *System under attack conditions*

Fig. 3: **Heat map of the movement of people in the indoor environment.** *(a) shows the ground truth results, while (b) shows the impact of a packet injection attack on the location results.*

authentication protocol such as Tesla [24]. For a strong Bluetooth LE broadcast security it is important that the size of Bluetooth LE broadcast packet should also be increased. It is important to note that the Bluetooth LE broadcast is not a reliable communication mechanism meaning that the broadcaster has no way of knowing whether the data actually reaches any observers at all. This is yet another research challenge to solve before we have a secure and reliable Bluetooth LE broadcast.

D. Secure Bluetooth Smart Multicast

Multicasting or group communication is an important feature in 6LoWPAN networks. Features, such as 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. Rahman et al. [25] present group communication in the IoT and discusses different use cases.

In a Bluetooth piconet there is one active master and up to 7 active slaves. At each time instant there is only a pair of nodes communicating: the master and one slave. Even though upto 254 slaves are supported, all slaves from 8 to 254 must remain inactive. The traditional Bluetooth piconet is not efficient for multicasting because data can reach the slave nodes *only* sequentially. Besides inactive slave nodes need to be brought online before they can receive the multicast data for piconet with more than 8 slaves. 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.

E. Open Source Bluetooth Smart

Bluetooth Smart, as a technology, gives system designers a low power wireless communications standard that allows devices to communicate with one another in a manufacturer-independent manner. Existing Bluetooth stacks are proprietary and/or closed[4], and hence do not offer the flexibility for researchers and designers to experiment. Also the current licensing terms hinders wider Bluetooth LE adaptability by new IoT startups without paying heavy licensing fees. An open source Bluetooth stack with BSD license will be a great leap towards getting the wider community involved and also expedite the Bluetooth Mesh vision.

A minimal functional 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.

F. Novel Applications of Bluetooth Smart

The latest additions to the Bluetooth standard (such as broadcasting modes) makes it a very attractive communication primitive for crowd-source sensing. Crowdsourcing has become an increasingly common way to

[4] BlueZ (http://www.bluez.org) is open source but has GNU General Public License and mainly targeted for Linux-based standard Bluetooth devices.

collect open data from the general public. It refers to the process of collecting observational data from the public (crowd) who are near the phenomena that is observed, using widely available tools or devices, and performing analysis on top of the data.

Going beyond amateur data collection or by specific interest groups, there has been growing recognition that crowd-sourcing can be an efficient way to collect large scale data in real-time with limited infrastructure capability. A distribution transformer beaconing its vital health parameters, a pollution sensor spreading air quality parameters, etc., are potential applications wherein the Bluetooth Smart technology can help to drastically reduce the cost of the monitoring and measurement infrastructure. Remember that the Bluetooth LE broadcast is insecure (Section IV-C); therefore, in order to use it in sensitive applications we must first develop a secure Bluetooth LE broadcast.

Summary: Bluetooth Smart is becoming ready to significantly contribute to the Ericsson's and Cisco's vision of 50 billion connected devices in the year 2020. To take full advantage of Bluetooth LE in the IoT and to enable innovations using the Bluetooth LE technology, there are open research challenges that should be addressed. We have identified and discussed the following issues and challenges in this paper: *(i)* a secure and reliable multi-hop communication in Bluetooth LE-connected 6LoWPAN networks, *(ii)* securing the currently available broadcast communication, *(iii)* a secure group communication in Bluetooth LE-connected 6LoWPAN networks, *(iv)* open source and open licensed Bluetooth LE software stack for resource-constrained IoT devices, *(v)* open Bluetooth LE hardware with register-level details disclosed in datasheets, *(vi)* support for 6LoWPAN header compression in smartphones and Bluetooth LE gateways, and *(vii)* empirical evaluation of IoT protocols (RPL, CoAP, Datagram TLS, IPsec, 6LoWPAN) over Bluetooth LE.

V. Conclusions

Bluetooth Low Energy is the lightweight variant of the standard Bluetooth protocol targeted for low-power resource-contained devices. The latest release of Bluetooth adds new capabilities in Bluetooth LE that make it a suitable technology for low-power devices in the Internet of Things. We have discussed these novel features and how they help building the Internet of Things. Though the latest Bluetooth Smart release already contains features that can be used to connect Bluetooth LE devices with the Internet, there are still missing important features that should be included in Bluetooth LE before we talk full advantage of Bluetooth LE in the Internet of Things. We have discussed these open issues and research directions in this paper and highlighted new opportunities that these novel features can bring.

In future, we plan to address some of the proposed challenges and implement and evaluate our solutions on real Bluetooth LE hardware platforms.

Acknowledgment

This research has been funded by VINNOVA Sweden for SICS Swedish ICT.

References

[1] Bluetooth SIG. Bluetooth Specification Version 4.2 [Vol 0]. Bluetooth Specification, December 2014. [https://www.bluetooth.org/en-us/specification/adopted-specifications Online; accessed 12-7-2015].

[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] T. Savolainen, K. Kerai, F. Berntsen, J. Decuir, R. Heydon, V. Zhodzishsky, and E. Callaway. Internet Protocol Support Profile. Bluetooth Specification, December 2014.

[4] H. Wang, M. Xi, J. Liu, and C. Chen. Transmitting ipv6 packets over bluetooth low energy based on bluez. In *Advanced Communication Technology (ICACT), 2013 15th International Conference on*, pages 72–77. IEEE, 2013.

[5] J. Nieminen, T. Savolainen, M. Isomaki, B. Patil, Z. Shelby, and C. Gomez. IPv6 over Bluetooth Low Energy. Working Draft, 2015.

[6] A. Dunkels, B. Gronvall, and T. Voigt. Contiki - a lightweight and flexible operating system for tiny networked sensors. In *29th Annual IEEE International Conference on Local Computer Networks*, 2004.

[7] P.R. Narendra. Comparison of link layer of BLE and 802.15.4 - Running on Contiki OS. Master's thesis, KTH Royal Institute of Technology, Stockholm, Sweden, September 2014.

[8] Z. Shelby, K. Hartke, and C. Bormann. The Constrained Application Protocol (CoAP). RFC 7252 (Proposed Standard), June 2014.

[9] M. Ryan. Bluetooth: With low energy comes low security. In *Presented as part of the 7th USENIX Workshop on Offensive Technologies*, Berkeley, CA, 2013. USENIX.

[10] S. Raza, S. Duquennoy, A. Chung, D. Yazar, T. Voigt, and U. Roedig. Securing communication in 6LoWPAN with compressed IPsec. In *7th International Conference on Distributed Computing in Sensor Systems (DCOSS'11)*, Barcelona, Spain, 2011.

[11] 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.

[12] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550, March 2012.

[13] J. Hui and P. Thubert. Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks. RFC 6282, September 2011.

[14] S. Raza, S. Duquennoy, J. Höglund, 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.

[15] Texas Instruments. CC26xx Contiki Port, 2015. [https://github.com/contiki-os/contiki/pull/974 Online; accessed 3-7-2015].

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

[17] Nordic Semiconductor. nRF52832 datasheet, 2015.

[18] Project Ubertooth, 2015. [http://ubertooth.sourceforge.net Online; accessed 3-7-2015].

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

[20] Apple iBeacon, 2015. [https://developer.apple.com/ibeacon Online; accessed 3-7-2015].

[21] Faking Bluetooth LE, 2013. [http://dmitry.gr/index.php?r=05.Projects&proj=11.%20Bluetooth%20LE%20fakery Online; accessed 3-7-2015].

[22] 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.

[23] P. Misra, S. Raza, V. Rajaraman, J. Warrior, and T. Voigt. Poster abstract: Security challenges in indoor location sensing using bluetooth le broadcast. In *The 12th European Conference on Wireless Sensor Networks (EWSN 2015))*, Porto, Portugal, February 2015.

[24] A. Perrig, R. Canetti, J. D. Tygar, and D. Song. The tesla broadcast authentication protocol. *CryptoBytes*, 5(2):2–13, August 2002.

[25] A. Rahman and E. Dijk. Group Communication for the Constrained Application Protocol (CoAP). RFC 7390 (Experimental), October 2014.