Volume 3, Issue 3, July 2016 ISSN: 2348-8565 (Online)

International Journal of Modern Engineering and Research Technology

Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

Secure Data Transfer Over Bluetooth Based on Speed

Pradeep Vishwakarma
M. Tech. Research Scholar
IPS Academy
Indore (M.P.), [INDIA]
Email: aloysious.vpradeep1@gmail.com

Leeadhar Chourasiya
Head of the Department
Department of School of Computers (SOC)
IPS Academy
Indore (M.P.), [INDIA]
Email: hod.soc@ipsacademy.org

Abstract

In our world of embedded electronics hackery, Bluetooth serves as an excellent protocol for wirelessly transmitting relatively small amounts of data over a short range (<100m). We use it to create a DIY HID Computer Keyboard. Or, with the right module, it can be used to build a homebrew, wireless MP3-playing speaker. This tutorial aims to provide a quick overview of the Bluetooth protocol. These days it feels like everything is wireless, and Bluetooth is a big part of that wireless revolution. Bluetooth embedded into a great variety of consumer products, like headsets, video game controllers, or (of course) trackers. It's perfectly suited as a wireless replacement for serial communication interfaces. We'll examine the specifications and profiles that form its foundation, and we'll go over how Bluetooth compares to other wireless protocols.

Keywords:*—Bluetooth, serial communication interfaces, pairing, piconets.*

I. Introduction

The Bluetooth protocol operates at 2.4GHz in the same unlicensed ISM frequency band where RF protocols like ZigBee and WiFi also exist [1]. There is a standardized set of rules and specifications that differentiates it from other protocols. If you have a few hours to kill and want to learn every nook and cranny of Bluetooth, check out the published specifications, otherwise here's a quick overview of what makes Bluetooth special. Bluetooth low energy wireless technology is an open low energy, short range radio technology

Key Benefits

- Low power consumption
- Small size
- Connectivity to mobile phones
- Low Cost
- Robust, efficient
- Multi-vendor interoperability
- Global availability, license free

II. Bluetooth Pairing

When Bluetooth devices come in range with each other, an electronic conversation takes place to determine whether the devices in range are known or whether one needs to control the other. Most Bluetooth devices do not require any form of user interaction for this to occur [2]. If devices within range are known to one another, the devices automatically form a network– known as a pairing. Two devices interacting in an authentication procedure are referred to as the claimant and the verifier. The verifier is the Bluetooth device validating the identity of another device. The claimant is the device attempting to prove its identity. The authentication verification scheme is depicted in Figure 1.

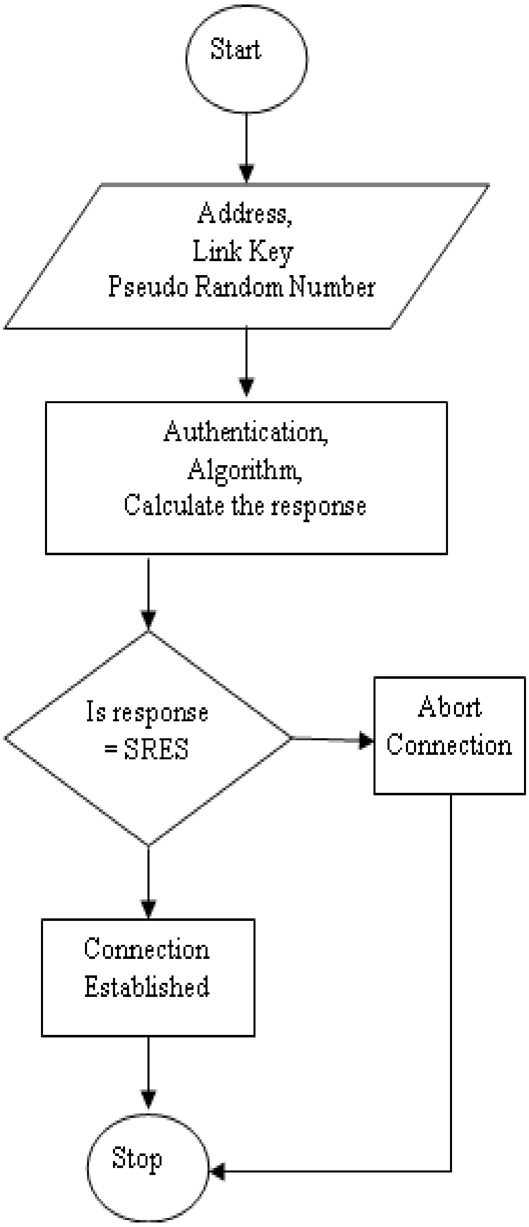

Figure 1: Existing Authentication Process

Serial Communication – Bluetooth is like a RF version of serial communication.

Hexadecimal – Bluetooth devices all have a unique address, which is usually presented as a hexadecimal value.

III. How Bluetooth Works

The Bluetooth protocol operates at 2.4GHz in the same unlicensed ISM frequency band where RF protocols like Zig Bee and WiFi also exist [3]. There is a standardized set of rules and specifications that differentiates it from other protocols. If you have a few hours to kill and want to learn every nook and cranny of Bluetooth, check out the published specifications, otherwise here's a quick overview of what makes Bluetooth special [4].

Access network technologies

The access network, whose length ranges from a few hundred meters to several miles, includes all the devices between the backbone network and the user terminals [5]. It is thus aptly called "the last mile". Because the backbone network usually used optical fibre structure with a high transmission rate, the access network has become the bottleneck of the entire network system. As shown in Figure 2, due to the open property of wireless channels, conflicts will happen in time, space or frequency dimension when the channel is shared among multiple users [6]. The function of access network technologies is to manage and coordinate the use of channels resources to ensure the interconnection and communication of multiple users on the shared channel.

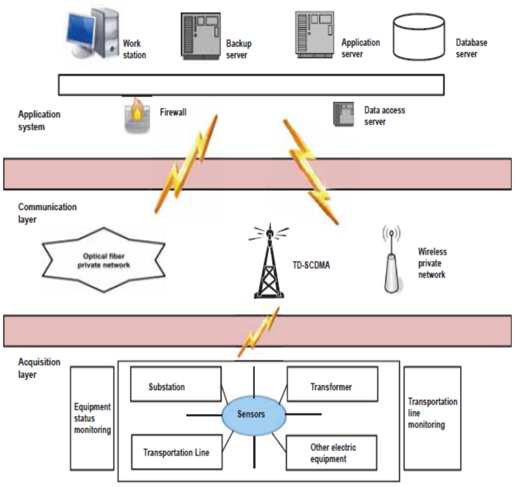

Figure 2 : Working of blue tooth in different fields

Masters, Slaves, and Piconets

Bluetooth networks (commonly referred to as **piconets**) use a master/slave model to control when and where devices can send data. In this model, a single master device can be connected to up to seven different slave devices. Any slave device in the piconet can only be connected to a single master [7]. Figure 3 is a pictorial depiction of above discussion.

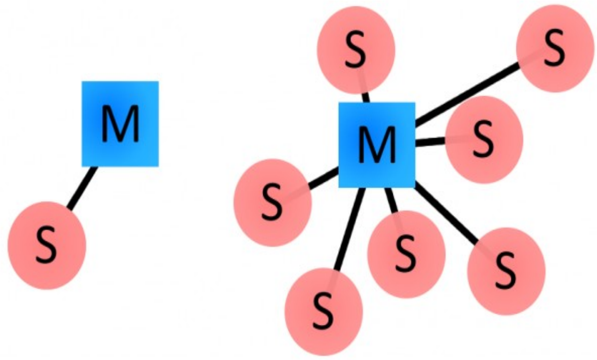

Figure 3 examples of Bluetooth master/slave piconet topologies.

The master coordinates communication throughout the piconet. It can send data to any of its slaves and request data from them as well [8]. Slaves are only allowed to transmit to and receive from their master. They can't talk to other slaves in the piconet.

Characteristic features of WSNs

A WSN can generally be described as a network of nodes that cooperatively sense and control the environment, enabling interaction between persons or computers and the surrounding environment. WSNs nowadays usually include sensor nodes, actuator nodes, gateways and clients [9]. A large number of sensor nodes deployed randomly inside of or near the monitoring area (sensor field), form networks through self-organization [10]. Sensor nodes Monitor the collected data to transmit along to other sensor nodes by hopping. During the process of transmission, monitored data may be handled by multiple nodes to get to gateway node after multihoprouting, and finally reach the management node through the internet or satellite (Figure 4).It is the user who configures and manages the WSN with the management node, publish monitoring missions and collection of the monitored data [11].

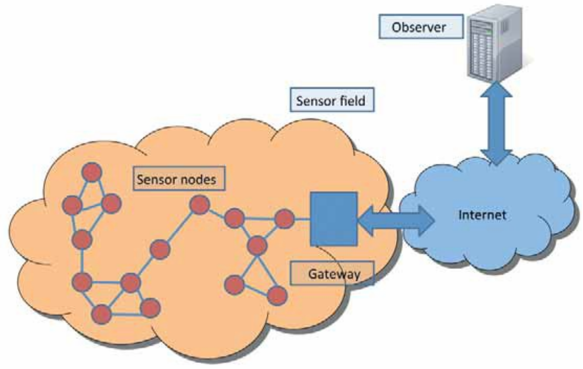

Figure 4: Wireless sensor networks

IV. Bluetooth Addresses and Names

Every single Bluetooth device has a unique 48-bit address, commonly abbreviated BD_ADDR. This will usually be presented in the form of a 12-digit hexadecimal value [12]. The most-significant half (24 bits) of the address is an organization unique identifier (OUI), which identifies the manufacturer. The lower 24-bits are the more unique part of the address [13,14].

This address should be visible on most Bluetooth devices as shown in figure 5. For example, on this RN-42 Bluetooth Module, the address printed next to "MAC NO." is 000666422152:

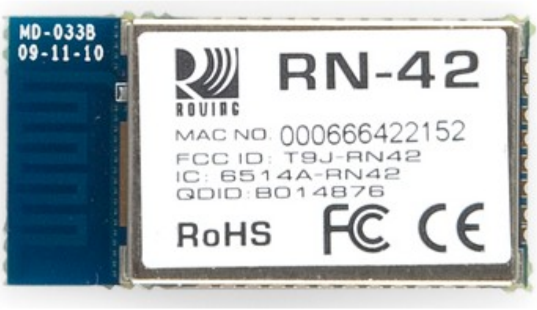

Figure 5: Address in blue tooth device

The "000666" portion of that address is the OUI of Roving Networks, the manufacturer of the module. Every RN module will share those upper 24-bits. The "422152" portion of the module is the more unique ID of the device.

According to on World [15], wireless devices to be installed in industrial fields will increase by553 % between 2011 and 2016 when there will be24 million wireless-enabled sensors and actuators, or sensing points, deployed worldwide. Among these, 39 % will be used for new applications that are only possible with wireless sensor networking [16].By 2014, the number of WSN devices will account for 15 % of the entire industrial measurement and control equipment sensing points, and 33 % by2016. Data has been shown in following Figure 6.

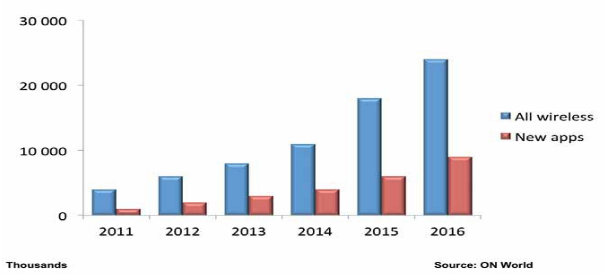

Figure 6: Global installed industrial wireless sensing points

Bonding and Pairing

When two Bluetooth devices share a special affinity for each other, they can be bonded together. Bonded devices **automatically establish a connection** whenever they're close enough. When I start up my car, for example, the phone in my pocket immediately connects to the car's Bluetooth system because they share a bond. No UI interactions are required. Bonds are created through one-time a process called **pairing [17]**. When devices pair up, they share their addresses, names, and profiles, and usually store them in memory. The also share a common secret key, which allows them to bond whenever they're together in the future. Pairing usually requires an **authentication process** where a user must validate the connection between devices. The flow of the authentication process varies and usually depends on the interface capabilities of one device or the other. Sometimes pairing is a simple "Just Works" operation, where the click of a button is all it takes to pair (this is common for devices with no UI, like headsets) [18]. Other times pairing involves matching 6-digit numeric codes. Older, legacy (v2.0 and earlier), pairing processes involve the entering of a common PIN code on each device. The PIN code can range in length and complexity from four numbers (e.g. "0000" or "1234") to a 16-character alphanumeric string.

V. Connection Process

Creating a Bluetooth connection between two devices is a multi-step process involving three progressive states:

Inquiry – If two Bluetooth devices know absolutely nothing about each other, one must run an inquiry to try to **discover** the other. One device sends out the inquiry request, and any device listening for such a request will respond with its address, and possibly its name and other information.

Paging (Connecting) – Paging is the process of forming a connection between two Bluetooth devices. Before this connection can be initiated, each device needs to know the address of the other (found in the inquiry process).

Connection – After a device has completed the paging process, it enters the connection state. While connected, a device can either be actively participating or it can be put into a low power sleep mode.

Active Mode – This is the regular connected mode, where the device is actively transmitting or receiving data.

Sniff Mode – This is a power-saving mode, where the device is less active. It'll sleep and only listen for transmissions at a set interval (e.g. every 100ms).

Hold Mode – Hold mode is a temporary, power-saving mode where a device sleeps for a defined period and then returns back to active mode when that interval has passed. The master can command a slave device to hold.

Park Mode – Park is the deepest of sleep modes. A master can command a slave to "park", and that slave will become inactive until the master tells it to wake back up [19].

Low Cost IP Interconnection Technology

The design of early sensor networks commonly used internal addresses to manage the sensor network nodes. The address length was relatively short and suitable for implementing in low-power embedded sensor network nodes. However, the internal address management method is not compatible with the IP method of the internet, which increased the difficulty of interacting between the sensor network nodes and the traditional IP network nodes. Therefore, there is a need to resolve [20].

Power Classes

The transmit power, and therefore **range**, of a Bluetooth module is defined by its power class. There are three defined classes of power, shown in Table 1:

Table 1 transmit power of power classes

Class Number	Max Output Power (dBm)	Max Output Power (mW)	Max Range
Class 1	20 dBm	100 mW	100 m
Class 2	4 dBm	2.5 mW	10 m
Class 3	0 dBm	1 mW	10 cm

Some modules are only able to operate in one power class, while others can vary their transmit power.

VI. Bluetooth Profiles

Bluetooth profiles are additional protocols that build upon the basic Bluetooth standard to more clearly define what kind of data a Bluetooth module is transmitting. While Bluetooth specifications define how the technology *works*, profiles define how it's *used*.

The profile(s) a Bluetooth device supports determine(s) what application it's geared towards. A hands-free Bluetooth headset, for example, would use headset profile (HSP), while a Nintendo WiFi Controller would implement the human interface device (HID) profile. For two Bluetooth devices to be compatible, they **must support the** same **profiles**. Let's take a look at a few of the more commonly-encountered Bluetooth profiles [21].

Hands-Free Profile (HFP) and Headset Profile (HSP)

Those Bluetooth earpieces that makes important business guys look like self-conversing wackos? Those usually use headset profile (HSP) or hands-free profile (HFP).HFP is used in the hands-free audio systems built into cars. It implements a few features on top of those in HSP to allow for common phone interactions (accepting/rejecting calls, hanging up, etc.) to occur while the phone remains in your pocket [22]

Advanced Audio Distribution Profile (A2DP)

Advanced audio distribution profile (A2DP) defines how audio can be transmitted from one Bluetooth device to another. Where HFP and HSP send audio to and from both devices, A2DP is a one-way street, but the audio quality has the potential to be *much* higher. A2DP is well-suited to wireless audio transmissions between an MP3 player and a Bluetooth-enabled stereo [23].

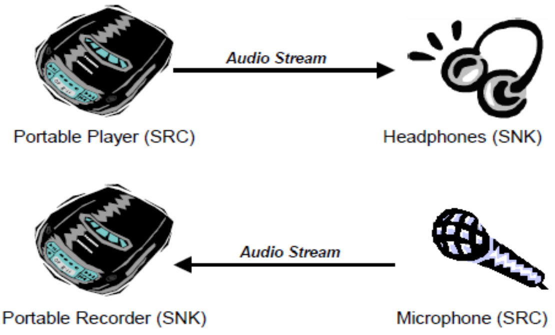

Figure 7: A2DP example configurations. Image from A2DP specification (v1.3).

Most A2DP modules support a limited set of audio codecs. In the least they'll support SBC (sub band codec), they may also support MPEG-1, MPEG-2, AAC, and ATRAC.

A/V Remote Control Profile (AVRCP)

The audio/video remote control profile (AVRCP) allows for remote controlling of a Bluetooth device. It's usually implemented alongside A2DP to allow the remote speaker to tell the audio-sending device to fast-forward, rewind, etc [24].

Serial Port Profile (SPP)

If you're replacing a serial communication interface (like RS-232 or a UART) with Bluetooth, SPP is the profile for you. SPP is great for sending bursts of **data** between two devices Figure 7. It's is one of the more fundamental Bluetooth profiles (Bluetooth's original purpose was to replace RS-232 cables after all). Using SPP, each connected device can send and receive data just as if there were RX and TX lines connected between them. Two Arduinos, for example, could converse with each other from across rooms, instead of from across the desk.

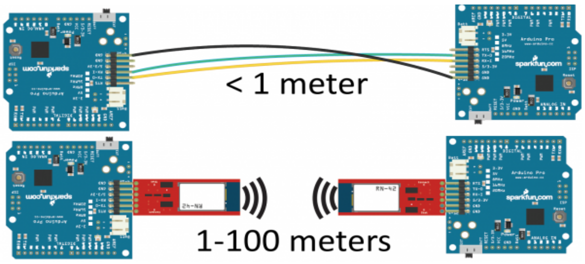

Figure 7: SPP for a blue tooth

VII. Wireless Comparison

Bluetooth is far from the only wireless protocol out there. You might be reading this tutorial over a WiFi network. Or maybe you've even played with ZigBees or XBees. Let's compare and contrast.

Table 2 : Some common wireless version and its comparison with blue tooth

Name	**Bluetooth Classic**	**Bluetooth 4.0 Low Energy (BLE)**	**ZigBee**	**WiFi**
IEEE Standard	802.15.1	802.15.1	802.15.4	802.11 (a, b, g, n)
Frequency (GHz)	2.4	2.4	0.868, 0.915, 2.4	2.4 and 5
Maximum raw bit rate (Mbps)	1-3	1	0.250	11 (b), 54 (g), 600 (n)
Typical data throughput (Mbps)	0.7-2.1	0.27	0.2	7 (b), 25 (g), 150 (n)
Maximum (Outdoor) Range (Meters)	10 (class 2), 100 (class 1)	50	10-100	100-250
Relative Power Consumption	Medium	Very low	Very low	High
Example Battery Life	Days	Months to years	Months to years	Hours
Network Size	7	Undefined	64,000+	255

Bluetooth isn't the best choice for every wireless job out there, but it does excel at short

-range cable-replacement-type applications. It also boasts a typically more convenient connection process than its competitors (ZigBee specifically).

ZigBee is often a good choice for monitoring networks – like home automation projects. These networks might have dozens of wireless nodes, which are only sparsely active and never have to send a lot of data.

BLE combines the convenience of classic Bluetooth, and adds significantly lower power consumption. In this way it can compete with Zigbee for battery life. BLE can't compete with ZigBee in terms of network size, but for single device-to-device connectivity it's very comparable. WiFi is probably the most familiar of these four wireless protocols. We're all pretty familiar with what purpose it's best for: Internet. It's fast and flexible, but also requires a lot of power. For broadband Internet access it blows the other protocols out of the water. The fight is on for wireless device-to-device networking supremacy between a refreshed incumbent, Bluetooth 4.0, and a newcomer, Wi-Fi Direct. Both specifications are promising to make it easier for you to quickly transfer pictures, files and other data between two wireless devices such as your Smartphone and laptop without the need for a Wi-Fi network or USB cable [25].

VII. Resources

Here are some more great reads, if you want to learn more about Bluetooth:

- ***Palo wireless Bluetooth Tutorial*** – Great in-depth look at how Bluetooth works on every layer. If you're interested in getting an overview of the protocols behind Bluetooth, check this out.
- ***Bluetooth.org Specifications*** – Thousands of pages covering the specifications of every Bluetooth version and profile known to mankind.
- ***Althos Bluetooth Tutorial*** – This is a well done beginner tutorial presented in slide form.

The Wi-Fi Alliance originally announced the Wi-Fi Direct specification in December, promising speedy data transfers over long distances between two devices. On Monday, the alliance said it has started certifying Wi-Fi Direct products that should hit store shelves before the end of the year. Meanwhile, the Bluetooth Special Interest Group announced in July that it would soon start certifying Bluetooth 4.0 devices. Just like Wi-Fi Direct, Bluetooth 4.0 is promising speedy device-to-device transfers over long distances, and Bluetooth 4.0 devices should also hit the market in the coming months. Can Wi-Fi Direct and Bluetooth 4.0 complement each other or will one crush the other in a wireless specification battle for the ages? Only time will tell. Until then, here's a quick look at the major highlights of Bluetooth 4.0 and Wi-Fi Direct. Bluetooth 4.0 is an upgrade from Bluetooth 3.0 that includes a power-saving feature called "Low-Energy Technology." Basically, Bluetooth 4.0 is three Bluetooth specs in one. Bluetooth 4.0 not only uses the new low-energy technology, but also relies on high-speed data transfers introduced in Bluetooth 3.0 and so-called classic Bluetooth technology found in older Bluetooth specifications. The tricky thing is that Bluetooth 4.0's low-energy technology is not compatible with existing Bluetooth devices. However, that doesn't mean your new Bluetooth 4.0-equipped Smartphone wouldn't be able to work with a Bluetooth 2.1 headset. It means that a device that only uses Bluetooth's low-energy technology wouldn't be able to talk to an older Bluetooth device. Let's say you have a Bluetooth pedometer that only has Bluetooth 4.0's low-energy feature baked in (and not the other parts of the Bluetooth 4.0 spec). You wouldn't be able to transfer via

Bluetooth the pedometer's data to an older laptop equipped with Bluetooth 2.1.It should be pointed out, however, that manufacturers could incorporate low-energy technology into a newer device using Bluetooth 2.1 or Bluetooth 3.0. So the backward compatibility problem only affects older Bluetooth devices, and not the actual Bluetooth specifications [26].

Bluetooth 4.0 vs. Wi-Fi Direct: Speed

Wi-Fi Direct promises device-to-device transfer speeds of up to 250Mbps, while Bluetooth 4.0 promises speeds similar to Bluetooth 3.0 of up to 25Mbps. Both Bluetooth 4.0 and Wi-Fi Direct use the 802.11 networking standard to reach their maximum speeds. But whether Bluetooth or Wi-Fi Direct speeds will run as fast as promised in the real world remains to be seen. In other words, don't believe the hype and keep an eye on independent data speed tests to see how each specification performs [27].

Security

Bluetooth 4.0 is using AES 128-bit encryption, while Wi-Fi Direct relies on WPA2 security, which uses AES 256-bit encryption. Both forms use key-based encryption and authentication methods, and both offer enough security for the average consumer. Although users will usually interface directly only with the upper layers of the Bluetooth Low Energy protocol stack, it’s probably best to begin with a basic overview of the complete stack, which provides a solid foundation to understanding how and why things operate the way they do. A complete single-mode BLE device is divided into three parts: controller, host, and application. Each of these basic building blocks of the protocol stack is split into several layers that provide the functionality required to operate [28].

Application

The application, like in all other types of systems, is the highest layer and the one responsible for containing the logic, user interface, and data handling of everything related to the actual use-case that the application implements. The architecture of an application is highly dependent on each particular implementation. Following is the status of wireless sensor using shown in figure it has been diminished due to the greater use of blue tooth. [29]

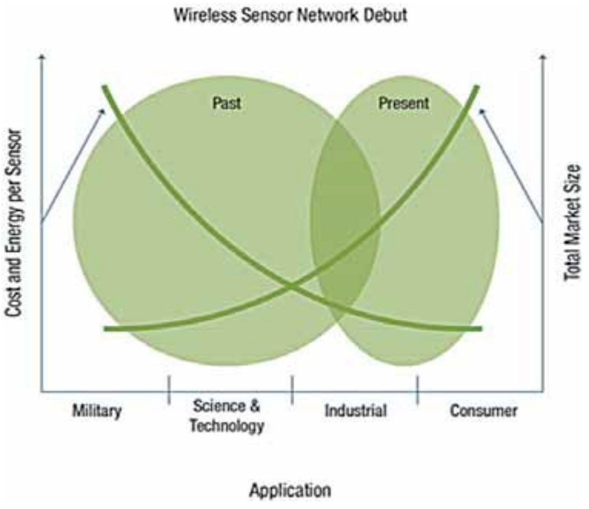

Figure 8: Data showing use of wireless at different time spans in different industries

VIII. Conclusion

If an unknown device wants to make connections or request for a service, then proper authentication is followed by authorization and encryption. We propose that the authentication process should be such that pairing will be become a secure manner but some complexity is remain here. In this process it takes a little time to start communication. IoT offers a way for different elements in social services to relate and connect with each other through the internet: man, equipment, and social service resources. Thanks to IoT, on one hand, the service providers can obtain information about people’s demands and provide them tailored and high-quality services. The Bluetooth address is a public parameter that is unique to each device. This address can be obtained through a device inquiry process. The link key is a secret entity. The pseudo random challenge is designed to be different on every transaction. The random number is derived from a pseudo-random process within the Bluetooth device.

REFERENCES:

[1] William Stallings," Network Security Essentials Applications & Standards", Pearson ed., 2001, pp 4-15.

[2] A. Laurie. "Serious flaws in bluetooth security lead to disclosure of personal Data", 2003

[3] Armknecht "An Algebraic attack on the Bluetooth Key Stream Generator", 2004

[4] Gehrmann, J. Persson, B. Smeets. "Bluetooth Security" Artech House, Inc... 2004

[5] ZigBee 2012, *ZigBee specification overview*. Available from: http://www.zigbee.org/Specifications/ZigBee/GreenPower.aspx

[6] Bluetooth Low Energy. Wikipedia: The Free Encyclopedia. 31 July 2014 at 05:16. Available from: http://en.wikipedia.org/wiki/Bluetooth_low_energy

[7] ZigBee Alliance. http://zigbee.org/Home.aspx

[8] IEC 62591, Industrial communication networks Wireless communication network and communication profiles WirelessHART™.

[9] IEEE Std 802.11™-2012, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Computer Society, March 2012.

[10] Uimer, C. *Wireless Sensor Networks*. Georgia Institute of Technology, 2000. Available from: www.craigulmer.com/portfolio/unlocked/000919_sensorsimii/wireless_sensor_networks.ppt

[11] Pister, K. and Doherty Y, L. *TSMP: Time synchronized mesh protocol*. [C]. Proceedings of the IASTED International Symposium, Distributed Sensor Networks (DSN 2008), 2008, pp. 391398. Available from: http://robotics.eecs.berkeley.edu/~pister/publications/2008/TSMP%20DSN08.pdf

[12] Shelby, Z. and Bormann C. *6LoWPAN: The wireless embedded Internet*. New York, NY, USA: John Wiley & Sons Ltd, 2009. Available from: http://elektro.upi.edu/pustaka.elektro/Wireless%20Sensor%20Network/6LoWPAN.pdf

[13] Sensinode. Available from: www.sensinode.com\\EN\\products\\software.html

[14] 6LoWPAN Sub1GHz Evaluation kit. Texas Instruments. Available from: www.ti.com/tool/CC-6lOWPAN-DK-868

[15] IEC/PAS 62734, Industrial communication networks – Field bus specifications – Wireless systems for industrial automation: process control and related applications.

[16] IEC 62601, Industrial communication networks – Field bus specifications – WIA-PA communication network and communication profile.

[17] IEEE Std 802.15.4e-2012, Local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sub layer. April 2012.

[18] IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs). IEEE 802.15.5 WPAN Mesh Networks. http://grouper.ieee.org/groups/802/15/pub/Meeting_Plan.html. May 2005.

[19] GainSpan, Low Power Wi-Fi Modules and Embedded Software, Product Photography, Available from: http://www.gainspan.com/news/media_kit

[20] IEEE Std 802.11s-2011, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 10: Mesh Networking, IEEE Computer Society, September 2011.

[21] Ang, R.J., Tan, Y.K. and Panda, S.K. Energy harvesting for autonomous wind sensor in remote area. 33rd Annual IEEE Conference of Industrial Electronics Society (IECON'07), Taipei, Taiwan, 2007.

[22] Tang, L. and Guy C. *Radio frequency energy harvesting in wireless sensor networks*. International conference on communications and mobile computing, 2009, pp. 644648.

[23] Courtesy of Shenyang Institute of Automation, Shenyang, China, 2014.

[24] FP7 Exalted consortium, *D3.3 – Final report on LTE-M algorithms and procedures*, project report, July 2012. Available from: http://www.ict-exalted.eu/fileadmin/documents/Exalted_WP3_D3.3_v1.0.pdf

[25] Ashton, K. That 'Internet of Things' Thing. In the real world, things matter more than ideas. RFID Journal, 22 June 2009. Available from: http://www.rfi djournal.com/articles/view?4986

[26] Broring, A. et al. New generation sensor web enablement. Sensors, 11, 2011, pp. 26522699. ISSN 1424-8220. Available from: doi:10.3390/s110302652

[27] Sensei. Integrating the physical with the digital world of the network of the future. Available from: http://www.sensei-project.eu/

[28] Chong, C.-Y. and Kumar, S. P. Sensor networks: Evolution, opportunities, and challenges. Proceedings of the IEEE 91(8), 2003, pp. 1247-1256.

[29] Kumar, S. and Shepherd, D. Sensit: Sensor information technology for the war fighter. Proceedings of the 4th International Conference on Information Fusion (FUSION'01), 2001, pp. 3-9.

* * * * *