Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 11, November-2016

Bluetooth Protocol in Internet of Things (IoT), Security Challenges and a Comparison with Wi-Fi Protocol: A Review

Mukhtar Ahmad Sofi
M.Tech (Computer Science & Engineering)
Pondicherry University
Pondicherry

***Abstract*--There has been a growing interest, over the past few years, in the Internet of Things (IoT), cutting across various industries, ranging from public transport to academia etc. This paper gives an overview of the current state of Bluetooth and Wlan(Wi-fi) technology. This study covers some facets aside from a brief introduction to the principles of the technology, major current and envisaged fields of application. It addresses an overview of the technologies in terms of services. The open communications environment makes wireless transmissions more vulnerable than wired communications to malicious attacks, including both the passive eavesdropping for data interception and the active jamming for disrupting legitimate transmissions. Therefore, this paper is motivated to examine the security vulnerabilities and undercurrents imposed by the inherent open nature of wireless communications.**

Keywords: IoT, Bluetooth, Vulnerabilities, undercurrents

I. INTRODUCTION

The Internet of Things (IoT) is imagined as a large-scale network of physical devices in which the Internet extends into the real world enclasping everyday objects that scale from a single constrained device up to massive cross-platform deployments of embedded technologies and cloud systems connecting in real-time.. Physical devices are no longer isolated from the virtual world, but can be handled remotely and can act as physical access points to Internet services.As with new ideas with enormous potential, the optimism of IoT has also enlarged the underlying technologies well before they can mature into a sustainable ecosystem. With numerous standards available spreading over multple frequency bands, using dfferent communication protocols, choosing the right wireless connectivity technology for an IoT application can be a quite challenging.

Wireless networks such as cellular networks, wireless lan, wireless sensor networks, Bluetooth, ZigBee, Rfid(Radio frequency identification) etc has played a significant role in Internet of things(IoT) enabling physical devices share the necessary data. According to Abi Research forecasting, in global wireless connectivity market, Bluetooth will be in 60% of total devices by 2021. The mobile phone market will account for less than 45% total Bluetooth shipments by this time as Bluetooth Smart continues to grow and branch into new verticals. Bluetooth Smart will be in 16% of devices by this time, with strong growth in smart home and beacon applications, in addition to a significant presence in the connected home and wearable space[22]. Wi-Fi will see its most significant growth in IoT across various industries. However, by 2021, mobile phones will still account for 55% of the Wi-Fi-enabled device market. the growing trend to develop multiprotocol connectivity system on chips (SoCs), will create new opportunities in various areas of the IoT market[22]. In this paper, we review the predominant wireless technologies Wi-Fi(Wireless fidility) and BLE(Bluetooth low energy) , discuss their security challenges, technological principle and security challenges. In addition, a comparison of Wi-fi and Bluetooth in terms of services has been discussed.

II. A SURVEY OF CONNECTION TECHNOLOGIES IN INTERNET OF THINGS (IoT)

In Internet of things era , the physical devices exchange or share information automatically without manual input which takes place through some communicaton technologies which are described below.

A) Bluetooth

Bluetooth [1]. is a short-range, low-power, IEEE open standard for implementing wireless personal area networks. Bluetooth operates in the globally unlicensed 2.4GHz short-range radio frequency spectrum meant for short-range communications devices suitable to substitute for cables for printers, faxes, joysticks, mice, keyboards, and so on. The devices can also be used for communications between portable computers, act as bridges between other networks, or serve as nodes of adhoc networks. This range of applications is known as wireless personal area network (WPAN). 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. According to the Analyst firm ABI Research, the Bluetooth smart home devices will show a 75 percent growth rate between 2016 and 2021.
Bluetooth 4.2 was realized in December 2014, and from then on, it is being pushed as a protocol for the IoT. Bluetooth LE eliminates the need of gateways such as 6LoWPAN border

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 11, November-2016

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. According to Bluetooth Special Interest Group(SIG), Bluetooth 5, releasing in the late 2016 or in early 2017 includes significantly increased range, speed, and broadcast messaging capacity. Extending range will deliver robust, reliable Internet of Things (IoT) connections that make full-home and building and outdoor use cases a reality[3]. Higher speeds will send data faster and optimize responsiveness. Increasing broadcast capacity will propel the next generation of "connectionless" services like beacons and locationrelevant information and navigation[3].

1. Basic Operation

When a Bluetooth device is powered on, it may try to operate as one of the slave devices of an already running master device. It then starts listening for a master's inquiry for new devices and responds to it. The inquiry phase lets the master know the address of the slave; this phase is not necessary for very simple paired devices that are granted to know each other's address. Once a master knows the address of a slave, it may open a connection toward it, provided the slave is listening for paging requests. If this is the case, the slave responds to the master's page request and the two devices synchronize over the frequency hopping sequence, which is unique to each piconet and decided by the master. Bluetooth predefines several types of connection, each with a different combination of available bandwidth, error protection, and quality of service. Once a connection is established, the devices can optionally authenticate each other and then communicate. Devices not engaged in transmissions can enter one of several power and bandwidth-saving modes or tear down the connection. Master and slave can switch roles, which may be necessary when a device wants to participate in more than one piconet.

2. Protocol overview

Bluetooth protocol not only defines a radio interfac but allows devices to find each other and advertise the services they offer. The Bluetooth MAC protocol is designed to facilitate the construction of adhoc networks without the need for manual configuration, cables, or wired infrastructure. It is based not on distributed contention resolution, as in traditional wireless LANs, but on a master slave mechanism. A Bluetooth piconet consists of one master and up to seven slaves. The master allocates transmission slots1 (and therefore, channel bandwidth) to the slaves in the piconet[4]. Bluetooth radio model uses low power radio transceivers o range from 10m to 100m that operate at a frequency of 2.45GHZ. The available radio band of 83.5 Mhz is divided into 79 channels of 1MHz width each [7]. Bluetooth utilizes one channel per time and the channel is switched 1600 times per minute regarding to a channel hopping scheme derrived from the piconet master device address[5].

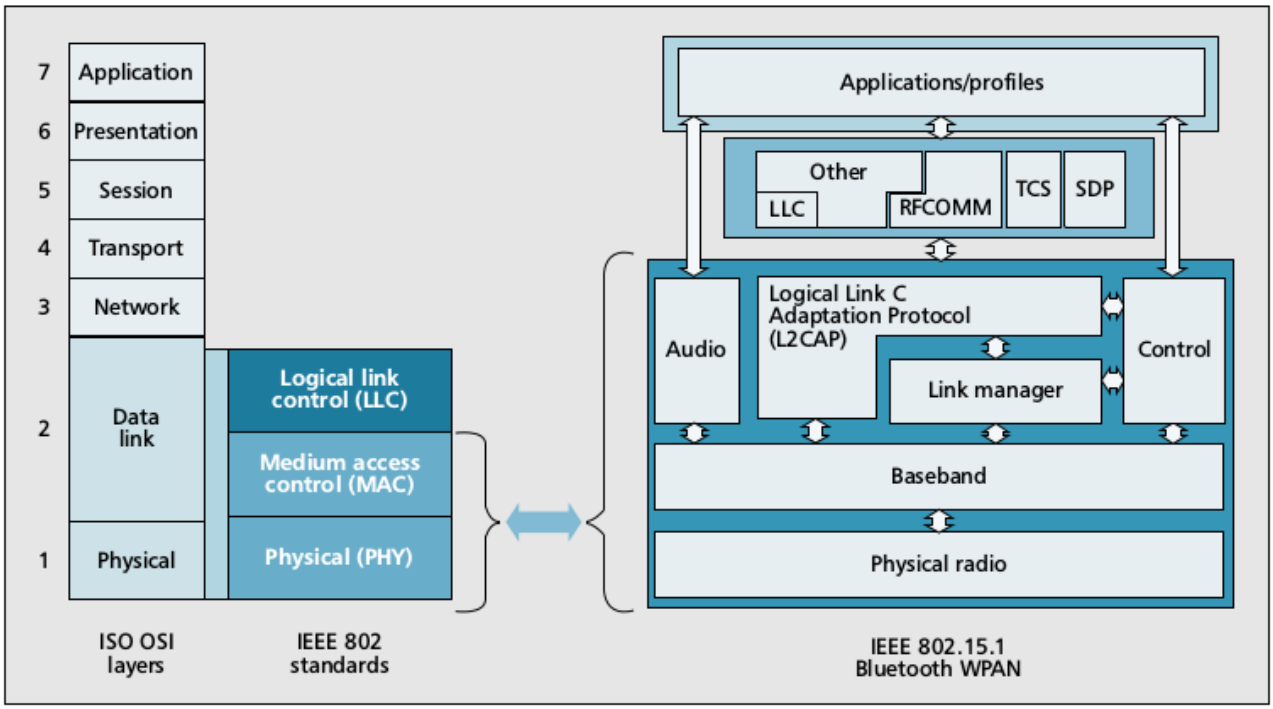

Figure 1: Basic diagram of Bluetooth protocol stack

3. Baseband Layer

Bluetooth uses synchronous connection oriented(SCO) and Asynchronous connectionless (AL) links to establish a connection among devices. SCO provides a circuit switched connection between the master and slave by establishing a point to point and symmetric dedicated link between two devices thereby providing guaranteed delay and bandwidth to transmit average quality voiceand music by the use of link mangement protocol. On th other hand, ACL provides a packet switched connection between the mastr and slave and establishes a poin to multipoint and asynchronous link between two devices an is suitable for non real time data transmission. This means that, applications requiring different QoS parameters cannot be supplied.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 11, November-2016

There are two different ACL link packets: 1) DMx which the payload is encoded and 2) DHx whichthe payload is unprotected. The value of x stands for the number of slots that is required to transmit the packet. DMx types are DM1, DM3 and DM5, which includes forward error correction (FEC), cyclic redundancy check (CRC) code and automatic repeat request (ARQ). The payload header is one or two bytes long, depending on packet type and its specification such as logical channel, user payload length and flow control [6]. Table 1 summarizes the ACL packet characteristics [6]:

Type	Payload	CRC	FEC	Symmetric max rate(kbps)	Forward Asymmetric max rate(kbps)	Backward Asymmetric max rate(kbps)
DM1	0-17	YES	2/3	108.8	108.8	108.8
DM2	0-121	YES	2/3	258.1	387.2	54.4
DM5	0-224	YES	2/3	286.7	477.8	36.3
DH1	0-27	YES	NO	172.8	172.8	172.8
DH3	0-183	YES	NO	390.4	585.6	86.4
DH5	0-339	YES	NO	433.9	723.2	185.6

Table1: Characteristics of ACL packets

4. Bluetooth Specification and features

Bluetooth is a wireless communication technology for short-range communications[7]. First released in 1998, Bluetooth was designed for low power consumption and moderate data transfer rates over short ranges. The Bluetooth Special Interest Group is an industry consortium that specifies and licenses the technology. Major specification versions and release dates are as follows[1][2][3][6][7]:

Bluetooth Version	Release Date	Features
Bluetooth 1.0	1999	Many issues including interoprabiliy
Bluetooth v1.1	2002	Registered as IEEE Standard 802.15.1 , uses non-encrypted channels, includes Signal Strength Indicator (RSSI)
Bluetooth v1.2	2005	backward compatible with 1.1, Faster Connection and Discovery, Adaptive frequency-hopping spread spectrum (AFH), Higher transmission speeds up to 721 kbit/s, Extended Synchronous Connections (eSCO), Host Controller Interface (HCI), Flow Control and Retransmission Modes for L2CAP.
Bluetooth v2.0 + EDR	2004	Enhanced Data Rate (EDR) about 3 Mbit/s, Faster Connection and Discovery, Adaptive frequency-hopping spread spectrum (AFH), Extended Synchronous Connections (eSCO), Host Controller Interface (HCI), Flow Control and Retransmission Modes for L2CAP.
Bluetooth v3.0 + HS	2009	data transfer speeds of up to 24 Mbit/s, L2CAP enhanced modes, Unicast connectionless data, and enhanced power control.
Bluetooth v4.0	2010	Bluetooth low energy (BLE), includes Classic Bluetooth, Bluetooth high speed and Bluetooth Low Energy protocols. support for the Generic Attribute Profile (GATT), and Security Manager (SM) services with AES Encryption.
Bluetooth v4.2	December 2014	extend the features of Bluetooth Low Energy to allow low-power IP connectivity over Bluetooth with a new profile which supports IPv6 and 6LoWPAN. Overall speed increasing by 2.5 times over previous implementations, Suitable in Inernet of things(IOT)[8]
Bluetooth v5	June 2016	promises quadruple the range and twice the speed of Bluetooth 4.2,

Table 2 : Bluetooth versions and features

5. Security Vulnerabilities In Bluetooth

In this section, we present a systematic review of various security vulnerabilities and weaknesses encountered in Bluetooth. Bluetooth hacking has gained a lot of momentum these days. With the release of new version blue tooth (4.0), some of these threats have been taken care of. One must member that this protection is available automatically only to Bluetooth products that supports the latest version. The other products that have been in use that are based on legacy versions of Bluetooth still are vulnerable to attacks. As there are many different threats present, classifying these threats becomes very important. Classification can help in determining threat severity, measures that could be taken to avoid them and taking inputs for the next version to avoid this threat by design[9][10][11][12][13][14][15].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 11, November-2016

Attack Type	Threats	Purpose	Threat level
Surveillance	Blueprinting, bt_audit, redfang, War-nibbling, Bluefish, sdptool, Bluescanner, BTScanner	observe and gather information about the device and its location	Low
Range Extension	BlueSniping, bluetooone, Vera-NG	extend the device range so that attacks could be conducted from far way distance	Low
Man In The Middle	BT-SSP-Printer-MITM, BlueSpooof, bthidproxy	place a device between two connected devices. All the information sent through the channel are available to the device in between.	High
Denial Of Service	Battery exhaustion, signal jamming, BlueSYN, Blueper, BlueJacking, vCardBlaster	Deny resources to a target by saturating the communication channel.	Medium
Obfuscation	Bdaddr, hciconfig, Spooftooph	hide the attacker's identity.	Low
Fuzzer	BluePass, Bluetooth Stack Smasher, BlueSmack, Tanya, BlueStab	submit non standard input to get different results.	Medium
Malware	BlueBag, Caribe, CommWarrior	carry out attacks typically using self replicating form of software.	Medium
Unauthorised Direct data access	Helomoto, Bloover, BlueBug, BlueSnarf, Unauthorized BlueSnarf++, BTCrack, Car Direct Data Whisperer, HeloMoto, btpincrack	gather private information in an unauthorized manner.	High
Sniffing	FTS4BT, Merlin, BlueSniff, HCIDump, Wireshark, kismet	capture the Bluetooth traffic in transit.	Medium

Table 3: Bluetooth Attack classification with threat levels

6. 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.

i. Bluetooth Smart Mesh
ii. Securing the Bluetooth Smart Mesh
iii. Secure Bluetooth Smart Broadcast
iv. Secure Bluetooth Smart Multicast
v. Open Source Bluetooth Smart
vi. Novel Applications of Bluetooth Smart

B) Wi-Fi (Wireless fidility)

Wi-Fi so called Wireless Fidelity is based on the IEEE 802.11 family of standards and is primarily a local area networking (LAN) technology designed to provide in-building broadband coverage providing data rate of 54 Mbps and typically provide indoor coverage over a distance of 100 meters.All wireless devices that join a Wi-Fi network, they form a basic service set (BSS). A BSS is a set of wireless stations(STAs), whether mobile, portable or fixed controlled by a single coordination function (CF) that determines when a STA transmits and when it receives.

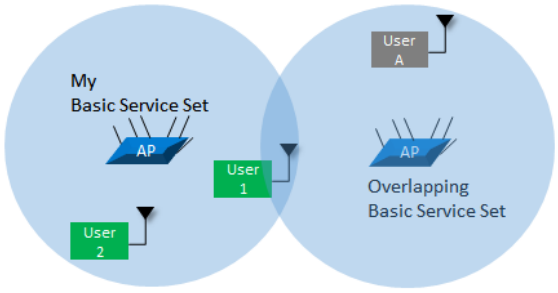

Figure 2: Basic Building Block of a Wi-fi

WiFi has become the de facto standard for last mile broadband connectivity in homes, offices,
organisations and public hotspot locations. A variety of algorithms and new techniques has been added to wi-fi over the years to ensure security , nevertheless, Security has been one of the major deficiencies in WiFi, though better encryption systems are now becoming available. In IoT, with battery-powered physical devices, The IEEE 802.11 standard has established itself as one of the most popular wireless technologies offering connectivity, thereby allowing the low power physical devices remain connected for longer times due to their energy efficient design.

1. Wifi Specification and Features

The 802.11 family consists of a series of half-duplex over-the-air modulation techniques that use the same basic protocol. 802.11-1997 was the first wireless networking standard in the family, but 802.11b was the first widely accepted one, followed by 802.11a, 802.11g, 802.11n, and 802.11ac. Other standards in the family (c–f, h, j) are service amendments that are used to extend the current scope of the existing standard, which may also include corrections to a previous specification[16][17].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 11, November-2016

Standard	Description	Year	Bandwidth(MHz)	modulation
IEEE 802.11	WLAN; up to 2 Mb/s; 2.4 GHz	1997	22	DSSS,FHSS
IEEE 802.11a	WLAN; up to 54 Mb/s; 5 GHz	1999	20	OFDM
IEEE 802.11b	WLAN; up to 11 Mb/s; 2.4 Ghz	1999	22	DSSS
IEEE 802.11g	WLAN; up to 54 Mb/s; 2.4 GHz	2003	20	OFDM
IEEE 802.11e	New coordination functions for QoS	2003	20	OFDM
IEEE 802.11f	Inter-Access Point Protocol recommendation for communication between access points to support roaming clients	2003	20	OFDM
IEEE 802.11n 802.11p,802.11r, 802.11s,802.11u	100+ Mbps standard improvements over 802.11g (2009)	2009	20-40	MIMO-OFDM
IEEE 802.11 ad	operate in the 60GHz millimeter wave spectrum; transmission rate of 802.11ad is 7Gbit/s	2012	2160	OFDM,SINGLE CARRIER,LOW-POWER SINGLE CARRIER
IEEE 802.11 ac	compared to 802.11n include wider channels (80 or 160 MHz versus 40 MHz) in the 5 GHz band	2013	40-80-160	MIMO-OFDM

Table 2 : Bluetooth versions and features

2. Security vulnerabilities in Wifi

An attack is an action that is carried out by an intruder in order to compromise information in an organization. Unlike wired networks, a WLAN uses radio frequency or infrared transmission technology for communication; thus, making them susceptible to attack. These attacks are aimed at breaking the confidentiality and integrity of information and network availability[18][19].

Attack type	Attack clasification	Purpose
Traffic Analysis	Confidentiality	The Attacker determines the overall network activity e,g Netstumbler
Eavesdropping	Confidentiality	gain access to the network traffic, reads message contents, cracks the encrypted messages
Man in the middle Attack	Confidentiality	read the private data from a session or modifies it
Evil twin AP	Confidentiality	an attacker sets up a phony access point in the network that pretends to be a legitimate one by advertising that WLAN's name i.e. extended SSID. E,g Karma
Session Hijacking	Integrity	an attacker takes an authorized and authenticated session away from the legitimate user of the network.
Replay Attack	Integrity	uses the legitimate authentication sessions to access the WLAN using authentication of captured session or sessions
802.11 frame injection attack	Integrity	intruders capture or send forged 802.11 frames
802.11 data/802.11X EAP/802.11 Radius Replay attack	Integrity	Captures data frames and inject those frames to gain access
802.11 data deletion	Integrity	The Attacker deletes the data in transit
Denial of Service attack	Availability	The attacker tries to prevent or prohibit the normal use of the network communication
RF jamming	Availability	The attacker jams the WLAN frequency with a strong radio signal which renders access- points useless
802.11 Beacon Flood	Availability	The Attacker floods th network with illegitimate packets
802.11 associate authentication flood	Availability	A type of DoS attack, an attacker sends thousands of authentication/association packets from MAC addresses in order to fill up the target AP's association table.
802.11 de-authentication & dis association	Availability	The attacker pretends to be a client or AP and sends unauthorized management frames
Fake SSID	Availability	The attacker floods the air with thousands of beacon frames with fake SSIDs and all the access points become busy processing the fake SSIDs
EAPOL flood	Availability	the attacker deluges the air with EAPOL beacon frames with 802.11x authentication requests to make the 802.1x RADIUS server busy.
AP theft	Availability	the attacker physically removes the access point from the public space making the network unavailable for the user

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 11, November-2016

Queensland DOS/virtual Carrier sense attack	Availability	an intruder exploits the clear channel assessment (CCA) by periodically claiming a large duration field in a forged transmission frame to make a channel appeared busy.
War Driving	Access Control	The attacker discovers wireless LANs by listening to the beacon or by sending a probe request. This attack provides the launch point for further attacks
Rogue Access point	Access Control	The attacker fools the legitimate client by changing its SSID to the same as that used by the target organization
MAC Address Spoofing	Access Control	The attacker gains access to privileged data and various resources by assuming the identity of a valid user in the network.
Unauthorised Access	Access Control	the attacker is not aiming at a particular user, but at gaining access to the whole network.
Dictionary and brute force attack	Authentication	A brute force attack involves trying all possible key's in order to decrypt the message; dictionary attacks only try the possibilities which are most likely to succeed
Shared key guessing	Authentication	The attacker attempts 802.11 shared key authentication with the cracked WEP keys or with the provided vendor default key
PSK cracking	Authentication	The cracker captures the WPA-PSK key handshake frame, & run a dictionary or a brute force attack to recover the WPA-PSK key.
Application Login theft	Authentication	The cracker captures user credentials e.g. e-mail address and passwords etc. from clear text application protocols.
VPN login Cracking	Authentication	The attacker runs brute force attacks on the VPN authentication protocol in order to gain the user credentials
Domain Login Cracking	Authentication	The cracker runs a brute force or dictionary attack on NetBIOS password hashes.
802.1X Identity theft	Authentication	The attacker captures 802.1X identity response packets.
802.1X LEAP Cracking	Authentication	The intruder captures 802.1X lightweight EAP beacon frames and then runs a dictionary attack in order to recover user credentials.
802.1X Password	Authentication	The attacker repeatedly attempts 802.1X authentication to guess the user's password by using a captured user's identity

Table 3: Bluetooth Attack classification with threat levels

III. A COMPARISON OF THE BLUETOOTH AND WIFI PROTOCOLS

In this section, we provide a comparison of services provided by Bluetooth and Wi-fi protocols in terms of capacity, range, network topology, security, QoS support, and power consumption[7][16][20].

Service	Bluetooth	Wifi
Frequency band	2.4 GHz	2.4 GHz, 5 Ghz
Nominal range	10m	100m
Typical output power	1–10 mW (1–10 dBm)	30–100 mW (15–20 dBm)
Maximum number of devices in the basic cell	8 active devices; 255 in park mode	Unlimited in ad hoc networks (IBSS); up to 2007 devices in infrastructured networks.
Basic cell	Piconet	BSS
Noise adaptation	Link layer	Physical layer
Multiplexing	FHSS	DSSS, CCK, OFDM
Extension of the basic cell	Scatternet	ESS
Channel access method	Centralized: polling	Distributed: CSMA/CA
Procedures used for the network setup	Inquiry, Page	Ad hoc networks: Scan, Authentication infrastructured: Scan, Authentication, Association
Authentication	Shared secret, pairing	Shared secret, challenge-response
Encryption	E0 stream cipher	RC4 stream cipher, RES
Typical current absorbed	1–35 mA	100–350 mA
Power save modes	Sniff, hold, park; standby	Doze

Table 3: Overview of Bluetooth and Wi-fi

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 11, November-2016

IV. CONCLUSION

This article gives a broad overview of the two most popular wireless standards, with a comparison in terms of capacity, network topology, security, QoS support, and power consumption. Some of these characteristics, such as data link types and performance, topologies, and medium access control, are stable and well defined by the standards. Others, such as power consumption, QoS, and security, are open challenges, where the technology is continuously improving, as far as both the standards and their implementations are concerned. Research areas include finding an efficient solution to the hidden terminal problem, supporting real-time transmissions in such a way that real-time traffic constraints map the user QoS requirements, developing efficient routing algorithms in mobile multihop environments, increasing data transfer security while maintaining ease of use, mitigating interference, and using new multiplexing techniques such as UWB and MIMO. Standardization is evolving quickly, with sev-eral complementary standards, among which Bluetooth and Wi-Fi dominate. Both have plenty of room for improvement, which is being explored by standardization committees. Other actors are the HomeRF and HiperLAN, which are not currently significant factors in the marketplace; others may appear in the next few years.

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] Bluetooth® 5 quadruples range, doubles speed, increases data broadcasting capacity by 800% , https://www.bluetooth.com/news/pressreleases/2016/06/16/-bluetooth5-quadruples-rangedoubles-speedincreases-data-broadcasting-capacity-by-800

[4] Chih-Yung Chang a, Kuei-Ping Shih a, Chung-Hsien Hsu b, Hung-Chang Chen, "A location-aware multicasting protocol for Bluetooth Location Networks", Information Sciences 177 (2007) 3161–3177

[5] Souron, E., Oussalah, M., & Alakhras, M. (2012). Bluetooth -model analysis and simulation using NS2. Proceedings of the 11th IEEE International Conference on Cybernetic Intelligent Systems 2012, CIS 2012, 178–183. https://doi.org/10.1109/CIS.2013.6782153

[6] Martínez-, R., Martínez-peláez, R., Rico-novella, F., Satizábal, C., & Jhon, J. (n.d.). Performance Analysis of Mobile Payment Protocols over the Bluetooth Wireless Network Protocols over the Bluetooth Wireless Network. Electronic Engineering, 1–11.

[7] Bluetooth SIG, Specification of the Bluetooth system – wireless connections made easy, Bluetooth Core Specification v1.1, 2001. Available from: http://www.bluetooth.org/spec.

[8] Raza, S., Misra, P., He, Z., & Voigt, T. (2015). Bluetooth Smart : An Enabling Technology for the Internet of Things, 155–162.

[9] Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. Proceedings of the IEEE, 104(9), 1727–1765. https://doi.org/10.1109/JPROC.2016.2558521

[10] John Paul Dunning, "Taming the blue beast: A Survey of Bluetooth-Based Threats. Security & Privacy", IEEE, 2010.

[11] Dennis Browning, Gary C. Kessler , "Bluetooth Hacking: A Case Study" 2012

[12] Bluebugging. (n.d.). trifinite.stuff Web site. Retrieved January 27, 2009, from http://trifinite.org/trifinite_stuff_bluebug.html

[13] Bluejacking. (2009, January 6). Wikipedia. Retrieved January 27, 20909, from http://en.wikipedia.org/wiki/Bluejacking

[14] Bluesmack. (n.d.). trifinite.stuff Web site. Retrieved January 27, 2009, from http://trifinite.org/trifinite_stuff_bluesmack.html

[15] Bluesnarfing. (n.d.). Bluejacking Tools: The Biggest Collection of Bluetooth Tools on the

[16] Internet Web site. Retrieved January 27, 2009, from http://www.bluejackingtools.com/bluesnarfing/

[17] Wi-fi specification, *"IEEE-SA Standards Board Operations Manual"*. *IEEE-SA. Retrieved 2015-09-13*.

[18] IEEE 802.11, https://en.wikipedia.org/wiki/IEEE_802.11#cite_ref-IEEE-SA_Standards_Board_Operations_Manual_1-0

[19] B. Forouzan, Data Communications & Networking. 4th edition. New York: McGraw-Hill, 2008

[20] Waliullah, M. D. G. (2014). Wireless LAN Security Threats & Vulnerabilities. (IJACSA) International Journal of Advanced Computer Science and Applications, 5(1), 176–183. https://doi.org/10.1017/CBO9781107415324.004

[21] Ferro, E., & Potortì, F. (2005). Bluetooth and Wi-Fi wireless protocols: A survey and a comparison. IEEE Wireless Communications, 12(1), 12–26. https://doi.org/10.1109/MWC.2005.1404569

[22] ABI Research, "GNSS Markets to Reach More Than 10 Billion Annual IC Shipments by 2021", https://www.abiresearch.com /press/abi-research-forecasts-wi-fi-bluetooth-802.15.4-nfc.