ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 3, pp: (233-242), Month: July-September 2014, Available at: www.researchpublish.com

A COMPARATIVE ANALYSIS OF SAFETY MEASURES ATTACK IN WI-FI, WI-MAX AND BLUETOOTH

[1]Ms. A. Sivasankari, [2]Mrs. S. Sudarvizhi, [3]D. Mohana priya

[1, 2, 3] Department of Computer Science, D.K.M College for Women, Vellore, TamilNadu, India

Abstract: **The main objective is to discuss the security features and weakness of IEEE 802.15, IEEE802.11 and IEEE802.16 i.e. Wireless PAN, Wireless LAN and Wireless WAN networks. Bluetooth, Wi-Fi and Wi-Max are the three most widely used wireless networking technologies. These networks are exposed to many types of risks and have various flaws in their respective protocol structure. Bluetooth belongs to a category of Short-range Wireless technologies, Wireless LAN or Wi-Fi is the LAN network we use in our home, offices or buildings etc to provide user the network availability whereas WI-MAX is used on a bigger scale MAN i.e. providing the network coverage on a metro scale through cellular networks to compensate the wired broadband services. In this Paper, study of these popular wireless communication standards in current scenario, evaluating their security features in terms of various metrics. This dissertation focuses on the various types of attacks on these networks and the counter measures to overcome them.**

Keywords: **Bluetooth, WiFi, WiMAX, wireless network security, Lan Network, WLAN, WWAN, Brandband communication.**

I. INTRODUCTION

Most wireless networks are based on the IEEE 802.11 standards. A basic wireless network consists of multiple stations communicating with radios that broadcast in either the 2.4GHz or 5GHz band, though this varies according to the locale and is also changing to enable communication in the 2.3GHz and 4.9GHz ranges. services, or increased the cost of the same through an artificial scarcity. In addition to these delays, the demand for spectrum has grown significantly

802.11 networks are organized in two ways. In infrastructure mode, one station acts as a master with all the other stations associating to it, the network is known as a BSS, and the master station is termed an access point (AP). In a BSS, all communication passes through the AP; even when one station wants to communicate with another wireless station, messages must go through the AP. In the second form of network, there is no master and stations communicate directly. This form of network is termed an IBSS and is commonly known as an ad-hoc network.

802.11 networks were first deployed in the 2.4GHz band using protocols defined by the IEEE 802.11 and 802.11b standard. These specifications include the operating frequencies and the MAC layer characteristics, including framing and transmission rates, as communication can occur at various rates. Later, the 802.11a standard defined operation in the 5GHz band, including different signaling mechanisms and higher transmission rates. Still later, the 802.11g standard defined the use of 802.11a signaling and transmission mechanisms in the 2.4GHz band in such a way as to be backwards compatible with 802.11b networks.

Separate from the underlying transmission techniques, 802.11 networks have a variety of security mechanisms. The original 802.11 specifications defined a simple security protocol called WEP. This protocol uses a fixed pre-shared key and the RC4 cryptographic cipher to encode data transmitted on a network. Stations must all agree on the fixed key in order to communicate. This scheme was shown to be easily broken and is now rarely used except to discourage transient users from joining networks. Current security practice is given by the IEEE802.11 specification that defines new cryptographic ciphers and an additional protocol to authenticate stations to an access point and exchange keys for data.

A. Background of the Research

Wireless networks communication existed since the 20th century with the radio wave experimental discoveries made by Gaulielmo Marconi and Nikola Tesla. As an attempt to produce and detect radio waves over a long distance, their experiments set a platform for further wireless communication until today. The development of the wireless networking technology gave invaluable benefits to individuals, schools, businesses, research institutions, rural communities and government organizations. Wireless network communication has given freedom to mobile users to remain connected to their resources and services, without being worried about their location. As it continues to improve, it can now be used to transmit data, voice and video to a large number of devices ranging from the traditional desktop computers to hand-held devices such as cell phones.

As much as the wireless networking has given fashion of freedom to mobile users, its wide spread popularity and adoption was instead due to the low cost for deployment, flexibility and was easy and cheap install as compared to the wired networks. Wireless networks differ from the traditional wired networks in the way they handle the lower layers (physical layer and data link layer) of the Open Standard Interconnect (OSI). The wired network uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) media access control for data transmission (RFC 1208) where as the wireless networks uses the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) in order to improve its performance during communication. In the CSMA/CA transmission technique a device waits for the carrier (channel) to be free before transmitting thereby avoiding packet loss and re- transmission.

B. Problem Statement and Goals

Wireless networks have become an important tool in transmission of data, voice and video. Due to their benefits, it has been widely adopted by many organizations, businesses, individuals and research institutes. Also, today's need for cost-effective and extended coverage and broadband appeals for their convergence. Despite the popularity of wireless networks, there are a number of problems which were noted and needed to be addressed such as low availability, unreliability and weak security. Security being the major motivation of the research, a more depth knowledge and understanding of how security issues and concerns in wireless networks is needed. Wireless networks security issues and concerns are different in complexity from those of the traditional wired networks. The mode through which the wireless networks transmit wireless signals made it more difficult to protect, thereby making the network vulnerable to attacks. A wireless network, since its inception, has faced a major limitation in containing and protecting its wireless signals from being intercepted as it is transmitted over the air waves. Therefore, protecting information during wireless communication became of paramount importance. For a network to be considered secure, it must achieve three security aspects: confidentiality, integrity and authenticity (CIA). Since confidentiality, integrity and authenticity, beside Denial of Service (DoS) attack, are major aspects of security, there is a need to understand how they are addressed in a converged IEEE 802.x wireless network.

C. Methodology

The research thesis investigated the security issues on a converged IEEE 802.x wireless network. The investigation emanated from the problem statement above and included an analysis of the inherent security protocols and mechanisms thereby making some recommendation to implement a secure and robust security framework.

A detailed and critical literature research survey on the overview and comparison of the WiFi and WiMAX wireless was presented as background knowledge and understanding into converged wireless network. Each of these two networks was then analyzed in terms of both strength and weakness in their security implementations.

The exposure of the weakness in the implementation methods and security policy formulation was conducted using risk analysis. Risk analysis process was done to present and outline the probable risk which might be launched on a network thereby determining the risk damage and level upon network compromise intentionally and unintentionally.

The resultant risk matrix level table for WiFi and WiMAX from risk analysis then formed the basis for recommending risk mitigation implementation for a secure and robust network. At the same time, the risk matrix level table provides information for managing and maintaining the implemented infrastructure. From the selected security implementation infrastructure, performance test on the selected application was conducted to evaluate the impact of the security implemented methods proposed for the converged wireless network.

II. THIRD GENERATION MOBILE TECHNOLOGIES

3G stands for "third generation of mobile phone standards and technologies". It was developed under the IMT-2000 program (IMT, International Mobile Telecommunication) by the International Telecommunication Union (ITU). 3G has three standards, WCDMA (Wideband Code Division Multiple Access), CDMA2000 and TD-SCDMA (Time Division – Synchronized Code Division Multiple Access). Also, 3G's network is a wide area cellular telephone network. It can provide internet access and video telephone. Compared to 2G, the 3G has higher bandwidth and faster speed. With this advantage, 3G can provide varieties of service. 3G supports both fixed and mobile environment and is also backward compatible with 2G.

When doing vocal transmission, 3G can use Circuit Switch Mode for voice and video phone; for internet access/data transmission, 3G uses Packet Switch Mode. In this mode, users pay for how much they used, for example 0.099 cents per packet. Multimedia Message Service (MMS) is an important application of 3G. Although MMS has been applied to General Packet Radio Service (GPRS) as the 2.5G major application, with 3G's advantages, wireless communication companies can provide more choices (video, audio, pictures and text) with MMS.

A. WCDMA

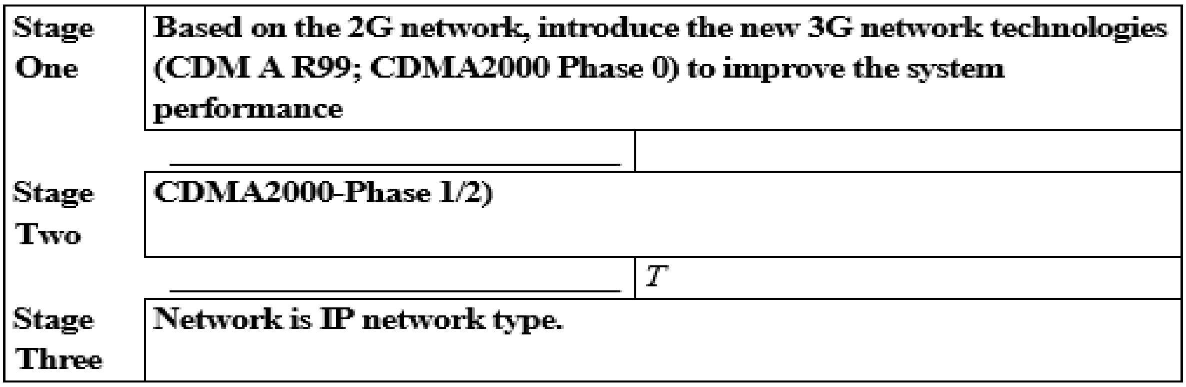
WCDMA was developed by an organization called 3GPP (3rd Generation Partnership Project, December 1998) and also a part of IMT-2000 program. The WCDMA is based on GSM (Global System for Mobile Communications/Pan- European digital cellular land mobile telecommunication system) and GPRS. GSM is based on Circuit Switch Mode and GPRS is based on Packet Switch Mode. In Europe, WCDMA is called Universal Mobile Telecommunications System (UMTS).

B. CDMA2000

CDMA2000 is the trade mark of TIA-USA (Telecommunication Industry Association) and which developed by 3GPP2. There were several versions of CDMA, CDMA2000 1X, CDMA2000 1X EV-DO. The evolution direction was the same with WCDMA, All IP network. Therefore, in CDMA-LMSD, the separation of control and payload was introduced.

C. TD-SCDMA

This standard was individually developed by China and co-work with 3GPP. Future development is still ongoing. Wireless technologies such as WiMAX, NFC and ZigBee are rapidly being adopted, along with existing wireless standards such as Bluetooth, Wi-Fi, GSM and other cellular technologies.



Stage One	Based on the 2G network, introduce the new 3G network technologies (CDM A R99; CDMA2000 Phase 0) to improve the system performance	
Stage Two	CDMA2000-Phase 1/2)	
		T
Stage Three	Network is IP network type.	

Fig-1 The Evolution of 3G

The popularization of 3G has several factors, such as the user's habits, market positioning, applications, and infrastructures. 3G has two opponents which are Wi-Fi and WiMax. They could be partners or enemies and it all depends on applications and market positioning. These wireless standards have their own advantages. 3G has bigger coverage and support mobility, but has lower data rate, and Wi-Fi has higher data rate, but smaller coverage and does not support mobility. On the other hand, WiMax has the biggest coverage, highest data rate and also support mobility.

D. Limitation

As the Internet goes into the wireless stage, internet access seems become more and more convenient. Wired Internet access, such as ADSL, can provide at least 100 Mbps data rate, and Wi-Fi, with the g standard, can achieve 54 Mbps, and it depends on the air-interface conditions however, if Wi-Fi wants to share the ADSL market, it still has a long way to go. Wi-Fi is strict to the operation environment and sensitive to channel fading, so reliability is a big issue. Since Wi-Fi is designed for small area not BWA, such as home or office, VoIP (Voice over IP), video service and a large file download are heavy duty for it. If a business building wants to install a wireless network for the whole building, every floor may need an individual AP (access point) or even more than one, depending on the location structure.

E. Wireless security and architecture

Wireless security is in many occasions comparable with the security of its wired equivalent. But still the mobility and increasing amount of wireless devices and networks bring new threats and make many of the old ones even bigger.

This chapter's focus is on the differences and similarities of wireless and wired security, the new threats brought by mobility, the security of networks and devices and effects of security, or lack of it. Also the ways of handling the threats will be discussed.

1. Security threats

The same basic security threats are confronted in fixed and wireless networks, but the wireless and mobility brings a new aspect for all of them. Due to the high and ever increasing number of wireless and mobile devices the affects can be exponential to those of the fixed ones. The basic types and threats are:

Multi-modal radios are capable of operating across multiple bands and technologies. The tri-band and world mobile phone are examples of multi-modal radios. Allotments and technical standards on a regional or global basis is not as critical.

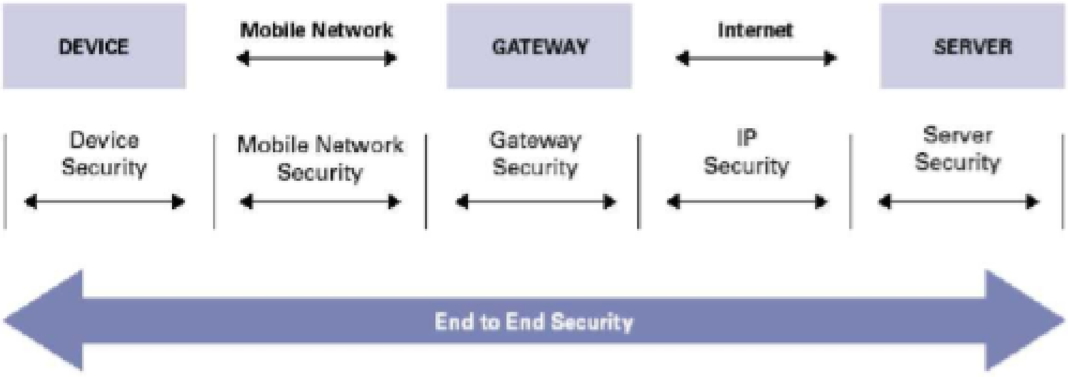


Fig-2 End-To-End Security Model

Keeping data private is a big issue for any wireless network. In the days of voice-only communications, the greatest worry was that an eavesdropper could listen to a private conversation, but mobile commerce makes security even more critical - if people are going to entrust their bank account to technology, it has to be secure. Security is an important enabler for the development, adoption and the usage of the mobile and wireless technologies and services. Business, as well as consumer, applications will not be able to realize their fullest potential unless a sufficient level of trust is established in the underlying security of mobile networks.

III. SYSTEM ANALYSIS

A. Wlan Radio Interface

For 802.11b systems both Frequency Hopping Spread Spectrum(FHSS) and Direct Sequence Spread Spectrum (DSSS)technologies are defined in the IEEE standard. However almost all of the 802.11b products don’t supply FHSS and therefore the following is restricted to DSSS.

Table-1 Characteristics Of Ieee 802.11

Bit Rate	Spreading	Modulation	Symbol Rate
11 Mbit/s	CCK	DQPSK	1.375 MSps
5.5 Mbit/s	CCK	DQPSK	1.375 MSps
2 Mbit/s	Barker	DQPSK	1.0 MSps
1 Mbit/s	Barker	DBPSK	1.0 MSps

Typical transfer rates for user data are 5 Mbit/s. For difficult propagation conditions (i.e. larger range, interference, ...), the system uses link adaptation to lower transfer rates. The next table gives an overview about the different data rates on the physical layer of 802.11b systems and the corresponding maximum range for open environments (i.e., outdoor or large halls) and for ―closed environments (i.e. indoor)

B. Bluetooth Architecture

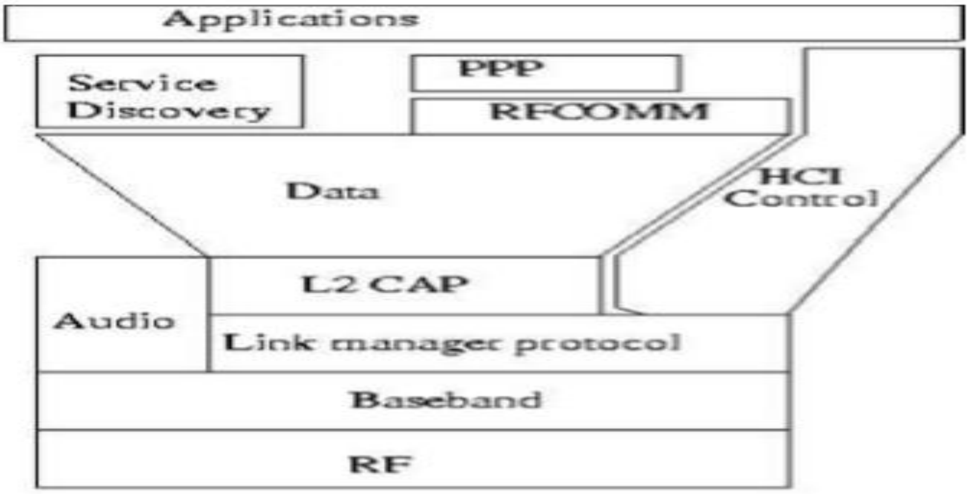


Fig-3 Bluetooth Architecture

C. Wimax Architecture

The IEEE 802.16e-2005 standard provides the air interface for WiMAX but does not define the full end-to-end WiMAX network. The WiMAX Forum's Network Working Group (NWG) is responsible for developing the end-to-end network requirements, architecture, and protocols for WiMAX, using IEEE 802.16e-2005 as the air interface.

The WiMAX NWG has developed a network reference model to serve as an architecture framework for WiMAX deployments and to ensure interoperability among various WiMAX equipment and operators.

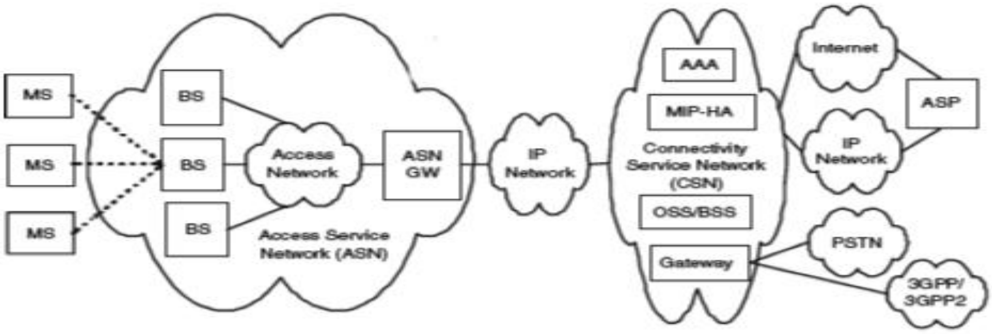


Fig-4 WiMax Architecture

The WiMAX architecture framework allows for the flexible decomposition and/or combination of functional entities when building the physical entities. For example, the ASN may be decomposed into base station transceivers (BST), base station controllers (BSC), and an ASNGW analogous to the GSM model of BTS, BSC, and Serving GPRS Support Node (SGSN)

D. Wifi Architecture

Wi-Fi mode eliminates the need for a network router or access point in a wireless home network. With ad hoc wireless, you can network computers together as needed without needing to be in reach of one central location. Most people use ad hoc Wi-Fi only in temporary situations to avoid potential security issues.Optional Components - Networking an ad hoc layout for Internet access, printers, or game consoles and other entertainment devices is not required for the rest of the home network to function. Simply omit any of these components shown that do not exist in your layout.

IV. RECONNAISSANCE ATTACKS

A. Packet Sniffers

As its name implies, a packet sniffer is a very good device used by the administrators for detecting any kind of fault in the network. As it is a good device for administrators for monitoring or analyzing a network, so is it a good device for attackers for capturing packets sent across networks.

B. Man-In-The Middle Attack

A man-in-the-middle attack necessitates that the hacker possess access to network packets that come via a network. A man-in-the-middle attack could be implemented using network packet sniffers and routing and transport protocols.

C. Denial of Sevice Attacks

A denial of service (DoS) attack damages or corrupts a computer system or denies all forms of access to the networks, systems or services even within the hacker's community. Denial of Service (DoS) attacks is regarded as less important and considered a bad form because they require little effort to execute. Although DoS implementation is easy and can cause little potential significant damage the attacks deserve special attention from security administrators.

D. IP Spoofing

This is a technique used to acquire unauthorized access to computers. In this kind of technique, the intruder sends illegitimate messages to a computer with an IP address which shows that the message is coming from a reliable and trusted host. Engaging in IP spoofing, hackers firstly use a variety of techniques to look for an IP address of a trusted host, then they modify their packet headers to appear as though the packets are coming from that trusted host.

E. Worm, Virus and Trojan horse Attacks

Some threat are categorized according to minor or primary vulnerabilities for the end-user, which could be handled by a layman by just explaining what he/she has to do. These attacks could be solved by the use of antivirus software or by restoring the affected machine to factory settings.

F. Mitigations of Network Threats and Attacks

Due to the unfortunate case of numerous threats and attacks that have befallen the networking industry, it becomes imperative to find ways of mitigating each of the attacks. As a result of fault from physical installation, planning of physical security to limit damage or theft of equipment during the process of installing hardware is very important. Few of the many ways that this action could be monitored or controlled is by making sure that no unauthorized access from the doors, ceiling, raised floor, windows, ducts or vents, monitoring and control closet entry with electronic logs, use of security cameras, and if possible.

The following are the tools that can be used to control packet sniffer attacks

1. **Authentication** For defense against packet sniffers, the use of strong authentication should be the first mitigation option. Strong authentication is a technique of authenticating users that cannot be circumvented easily. One Time Passwords (OTPs) are a clear example of strong authentication. An one-time password is a security mechanism that makes use of a mobile device in generating password each time an application requests for it.

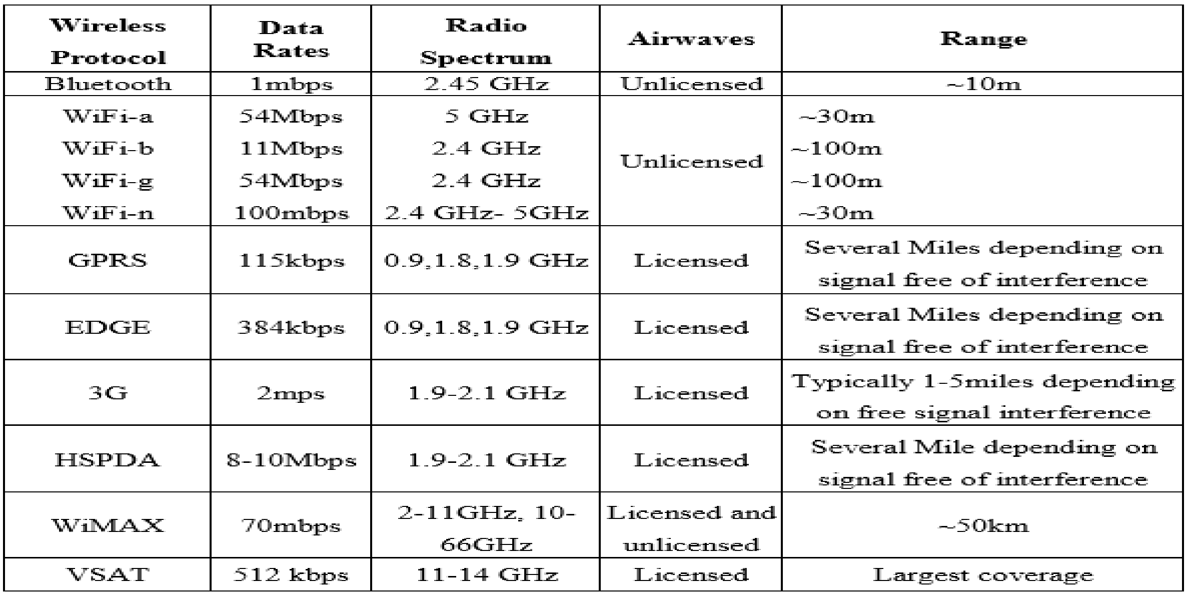
2. **Switched infrastructure** This technique counters the use of packet sniffers in a network environment. For instance, if an organization deploys a layer-2 switched Ethernet, access by intruders can only be gained to the traffic flow of the connected port. Obviously a switched infrastructure does not totally eradicate the threat of packet sniffers, but their effectiveness is reduced considerably.

3. **Anti-sniffer tools** Certainly, there would always be a solution for every threat, anti-sniffer is a software and hardware, designed for detection of the use of sniffers on a network, and can be implemented on networks.

4. **Cryptography** A communication channel is cryptographically secure when the only data a packet sniffer detects is a cipher text (a random string of bits) and not the original message. Cisco deploys network-level cryptography based on)

V. COMPARISON RESULT

Table-2 Wireless Technologies Comparison



Wireless Protocol	Data Rates	Radio Spectrum	Airwaves	Range
Bluetooth	1mbps	2.45 GHz	Unlicensed	~10m
WiFi-a	54Mbps	5 GHz	Unlicensed	~30m
WiFi-b	11Mbps	2.4 GHz		~100m
WiFi-g	54Mbps	2.4 GHz		~100m
WiFi-n	100mbps	2.4 GHz- 5GHz		~30m
GPRS	115kbps	0.9,1.8,1.9 GHz	Licensed	Several Miles depending on signal free of interference
EDGE	384kbps	0.9,1.8,1.9 GHz	Licensed	Several Miles depending on signal free of interference
3G	2mps	1.9-2.1 GHz	Licensed	Typically 1-5miles depending on free signal interference
HSPDA	8-10Mbps	1.9-2.1 GHz	Licensed	Several Mile depending on signal free of interference
WiMAX	70mbps	2-11GHz, 10-66GHz	Licensed and unlicensed	~50km
VSAT	512 kbps	11-14 GHz	Licensed	Largest coverage

MPDUs carries MAC message. Whereas the Transport connection transmits the MSDUs passed by layers above the MAC layer.The final important layer in terms of security is the Privacy Layer. It is a layer where authentication, encryption and key establishment are addressed. The CS and the CPS are responsible for ensuring a robust connection. There many protocols that are used in the PS to ensure seamless network. The AES-CCM is used to encrypt data, EAP protocol for data authentication while key establishment and management PKM-EAP authorization. In a simple illustration, the Management connection ID identifies the packet while the management. ATM sublayer for handling ATM networks and service whilst Packet Convergence sublayer used for packet data service such as the Ethernet, Internet Protocol and VLAN. The PS uses the PHY SAPs to exchange the MPDUs with the Physical Layer.There are different wireless technologies which are available today on the market.

All the technologies mentioned in the diagram are wireless technologies with similarities and differences. Since the table above provides an overview of these wireless technologies, there is need a to engage in a comparative discussion about their suitability in achieving wireless convergence in providing services to mobile users and wireless Internet connectivity.

A. WIFI VS. 3G/UMTS

Looking at these two wireless technologies, both facilitate mobility. They enable mobile devices to be moved around a particular coverage and remain connected without worry reinstalling cable infrastructure. WiFi mobility is referred to as local mobility since it is an Ethernet Network extension with a higher data rate (bandwidth) for a particular entity whereas the 3G offer narrower bandwidth while covering a large area. In the bid to counter the low data rates offered by 3G, the telecommunication industry introduced the HSDPA. The HSDPA significantly offers much better speeds up to 10mbps with lower packet delay. Mobile technologies are still constrained by limited coverage as signals fade and service diminishes as one moves away from the city (urban area centers).

B. WIMAX VS. 3G/UMTS

Though the mobile technologies provide ability for users to use it as an access technology, its data rates speeds are not able to compete with WiMAX. Theoretically, the mobile technologies have data speeds from 115kbps for GPRS, 384 Kbps up to 2Mbps for UMTS and 14.4Mbps for HSPDA while WiMAX offers high data speeds of up to 70Mbps for coverage of 50km. The HSPDA can provide a much faster theoretical maximum data rate of 14.4Mbps within a kilometer making it only suitable for short distance access technology.

C. WiMAX vs. VSAT

The VSAT as a satellite technology can be used to as a backbone to provide reliable, high bandwidth for Internet connectivity to countries and regions. The major disadvantage for using VSAT technology in providing long distance Internet connectivity is in the cost of installing and maintaining the service. Though the VSAT satellite communication is expensive it offers secure and cost-effective connection through the uses of VPN/IPSec as its security mechanisms.

D. WiFi vs. WiMAX

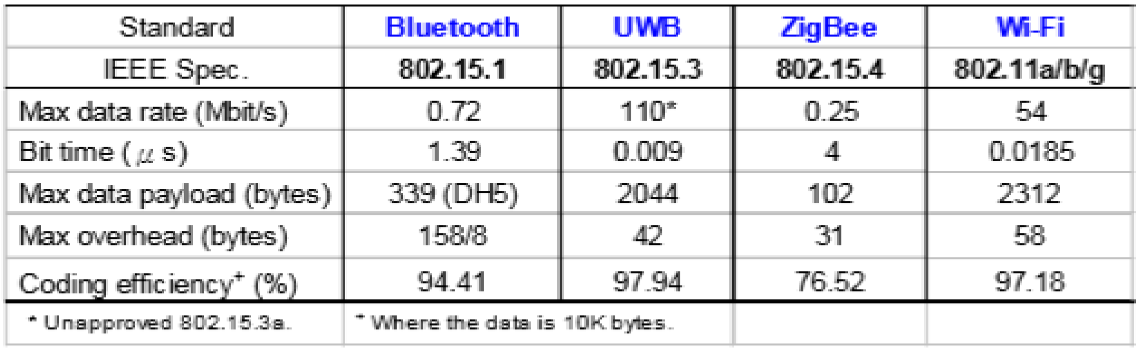
These two wireless technologies have common components in their operations with a major difference in the communication range. There is a need for many WiFi access point in order to cover the same distance covered by one WiMAX base station. Hence it is costly to deploy WiFi for longer distances. WiFi is an access technology suitable for indoor use due to its short ranges as an extension to LAN technology while WiMAX was designed for long distance, backhauling and optimized for MAN. As much as the WiFi has an advantage of providing end user access capabilities, it can only support a limited number of users (not more than 12 per base station) whereas the WiMAX base station can support an average of about five hundred users. WiMAX base station has a scheduling algorithm (First-In First-Out) which allocates a variable channel for each subscriber station to minimize the congestion and degrading throughput other than the random queue assignment based on MAC address in WiFi whereas.

VI. EVALUATION RESULT

A. Performance Analysis

In this subsection, the SCP from the CRtx to the CRrx will be analyzed first. Then the SCP within multiple consecutive time slots will be further investigated. Also, the coexistence of multiple CR links with primary links will be considered.

Table-3 Typical System Parameters Of The Wireless Protocols



Standard	Bluetooth	UWB	ZigBee	Wi-Fi
IEEE Spec.	802.15.1	802.15.3	802.15.4	802.11a/b/g
Max data rate (Mbit/s)	0.72	110*	0.25	54
Bit time (μ s)	1.39	0.009	4	0.0185
Max data payload (bytes)	339 (DH5)	2044	102	2312
Max overhead (bytes)	158/8	42	31	58
Coding efficiency^{+} (%)	94.41	97.94	76.52	97.18
* Unapproved 802.15.3a.	$^{+}$ Where the data is 10K bytes.			

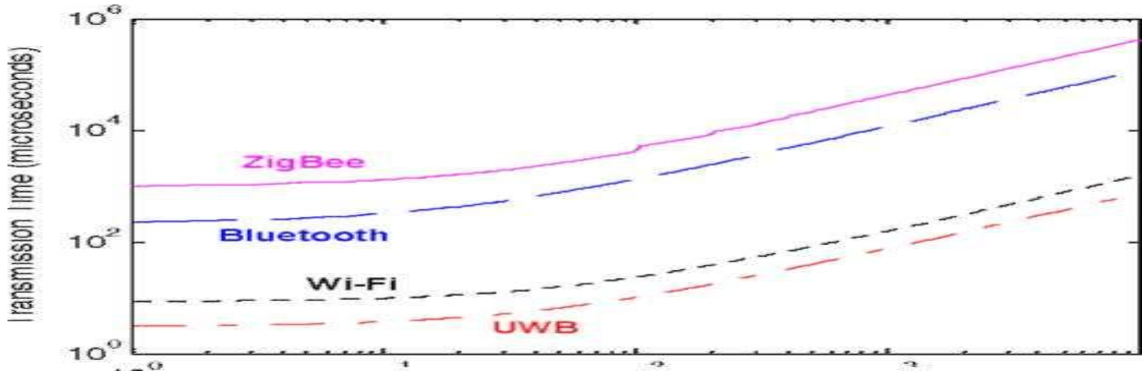


Fig-5 Comparison of the transmission time versus the data size.

For a wireless sensor network in factory automation systems, since most data size of industrial monitoring and control are generally small, (e.g. the temperature data in an environmental monitoring may required less than 4 bytes only), Bluetooth and ZigBee protocols may be a good selection (from a data coding efficiency point of view) in spite of their slow data rate.

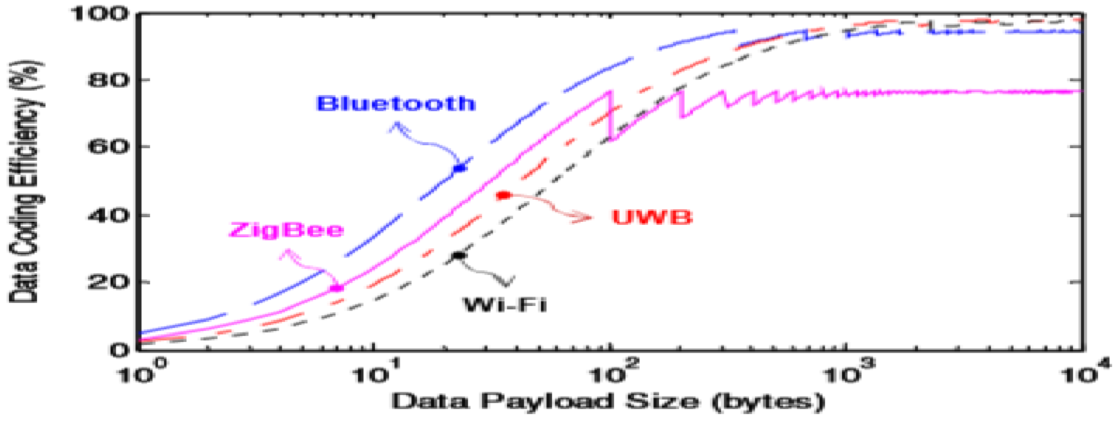
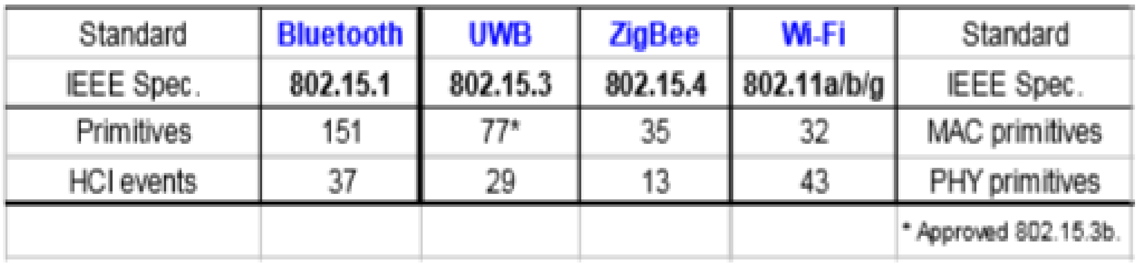


Fig-6 Comparison of the data coding efficiency versus the data size.

In this section, an evaluation of the Bluetooth, UWB, ZigBee, and Wi-Fi on different aspects is provided. It is important to notice that several slight differences exist in the available sources. For example, in the IEEE 802.15.4 standard, the action range is about 10m, while it is 70-300m in the released documents from ZigBee Alliance. Thus, this paper intends to provide information only, since other factors, such as receiver sensitivity and interference, play a major role in affecting the performance in realistic implementations.

Table-4 Number Of Primitives And Events For Each Protocol



Standard	Bluetooth	UWB	ZigBee	Wi-Fi	Standard
IEEE Spec.	802.15.1	802.15.3	802.15.4	802.11a/b/g	IEEE Spec.
Primitives	151	77*	35	32	MAC primitives
HCI events	37	29	13	43	PHY primitives
					* Approved 802.15.3b.

On the other hand, ZigBee is the simplest one with only 48 primitives defined in 802.15.4. This total number of primitives is only about one fourth the number of primitives and events defined in Bluetooth. As compared with the Bluetooth, UWB, and Wi-Fi, the simplicity makes ZigBee very suitable for sensor networking applications due to their limited memory and computational capacities.

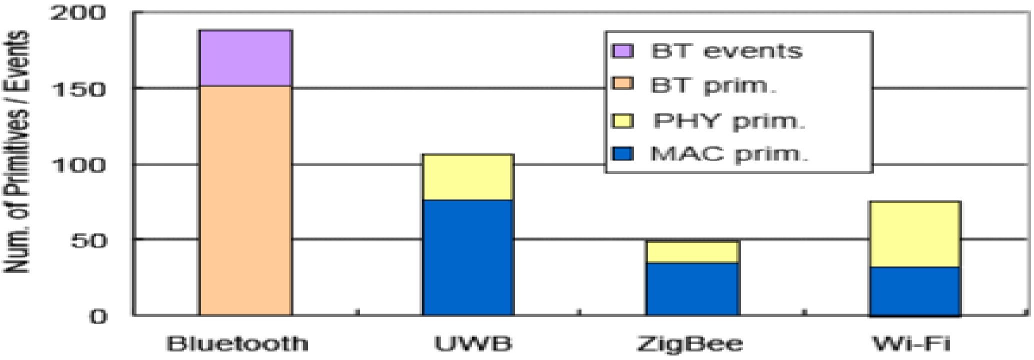


Fig-7 Comparison of the complexity for each protocol.

REFERENCES

[1] Gomes, Lee, "Many Wireless Networks Open to Attack," The Wall Street Journal Online, 27 April 2001

[2] Lemos, Robert, "Wireless Networks Wide Open to Hackers," CNET News.com, 12 July 2001

[3] Verton, Dan, "Flaws in Wireless Security Detailed," Computerworld, 16 July 2001

[4] The Bluetooth Blues‖, available at http://www.information-ge.com/article/2001/may/the_bluetooth_blues

[5] "Phone pirates in seek and steal mission", Cambridge Evening News, available at: http://www.cambridge-news.co.uk/news/region_wide/2005 /08/17/

[6] Garcia, Andrew, "WEP Remains Vulnerable," eWEEK, 26 March 2001

[7] TLA Specification for Ranging and Authentication Process of IEEE Std 802.16-2004,‖ http://list.cs.northwestern.edu/802.16/.

[8] A cost-based framework for analysis of denial of service in networks,‖ Journal of Computer Security, vol. 9, no. 1-2, 2002.

[9] Clincy, V.; Sitaram, A.; Odaibo, D.; Sogarwal, G,; "A Real-Time Study of 802.11b and 802.11g", Systems and Networks Communication, 2006. ICSNC '06. International Conference on, page(s): 69 - 69, Oct. 2006 . Intel Corporation http://www.intel.com/

[10] Vassis, D.; Kormentzas, G.; Rouskas, A.; Maglogiannis, I.; "The IEEE 802.11g standard for high data rate WLANs", Network, IEEE, Volume 19, Issue 3, June 2005.