Analysis and Issues of Wireless Protocols Standard Suits in WPAN

DR. P. RAJAMOHAN

Senior Lecturer, School of Information Technology, SEGi University,
Taman Sains Selangor, Kota Damansara, PJU 5, 47810 PJ, Selangor Darul Ehsan, Malaysia.
parthasarathy_rajamohan@yahoo.com & rajamohanp@segi.edu.my
www.segi.edu.my

***Abstract* - Wireless communications have become common place and wireless networks applications are found in a wide variety of industries and organizations. Wireless networks and devices are found in all circles of life today. Wireless networks will enable companies of all sizes to interconnect their offices without the high cost charged by telephone carriers for their landline connections. In this paper, focus all the types of wireless personal area networks technologies and architectures with security issues plus protocols standards, evaluating their main features and behaviors in terms of various metrics, including the transmission time, data coding efficiency, complexity, and power consumption. The major goal of this paper to contribute the research in the area of wireless personal area network protocols standards and comparison.**

Keywords* - *WPAN- Wireless Personal Area network, LR WPAN- Low Rate Wireless Personal Area Network, HR WPAN- High Rate Wireless Personal Area Network. IEEE - Institute of Electrical and Electronics Engineers.

I. INTRODUCTION

Wireless technology releases us from wires. A user can have a notebook computer, PDA, Pocket PC, Tablet PC, or just a cell phone and stay online anywhere a wireless signal is available. The basic theory behind wireless technology is that signals can be carried by electromagnetic waves that are then transmitted to a signal receiver. But to make two wireless devices understand each other, we need protocols for communication. It is easier to understand that the wireless technologies by categorizing them into three layers, as shown below. The three layers are device, physical, and application and service (protocol).

In the device layer (mobile devices) are gadgets ranging from the smallest cell phone to PDAs and notebook computers. These devices use wireless technologies to communicate with each other. The physical layer contains different physical encoding mechanisms for wireless communications. Bluetooth, 802.11x, CDMA, GSM, 3G and 4G are different standards that define different methods to physically encode the data for transmission across the airwaves. The application and service layer, also referred to as ISO layers 2 to 7 contains the protocols that enable wireless devices to process data in an end-to-end manner. Protocols like Wireless Application Protocol (WAP), Voice over IP (VoIP), and i-mode reside in this layer.

TABLE 1 : Different Layers of Wireless Technologies

Layer	Technologies
Application and service	Wireless applications: WAP, i-mode, messaging, Voice over Wireless network, VoIP, location-based services
Physical	Wireless standards: 802.11a, 802.11b, 802.11g, AX.25, 3G, CDPD, CDMA, GSM, GPRS, radio, microwave, laser, Bluetooth, 802.15, 802.16, IrDA.
Device	Mobile devices: PDAs, notebooks, cellular phones, pagers, handheld PCs, wearable computers.

Many security problems can be traced back to the end user in wired networks. Wireless networks are no exception, and it is typically the IT department's responsibility to protect the end user. The enterprise wireless network need the following technologies.

- Understand the capability of current products
- Understand your networking needs
- Understand the potential risk you are facing
- Find a solution tailored to your environment

The five major categories of wireless technologies distinguished by the distances, area of coverage, speed of transmission and applications platforms environment factors and others. The categories of wireless networks are WPAN- Wireless Personal Area Network, WLAN- Wireless Local Area Network, WMAN- Wireless Metropolitan Area Network, WiMAX- Worldwide Interoperability for Microwave Access and WWAN- Wireless Wide Area Network . All the above wireless networks technologies as I discussed in the following sections with analysis and performance of wireless personal area network standards of IEEE protocols suits, architectures, technologies and other security issues[1].

WPAN - Wireless Personal Area Network

Group of technologies that are designed for short-range communications. Eliminates the need for wires or cables to interconnect multiple devices. As the name "Wireless Personal Area Network" suggests, such a network is small in the range of about 10 meters (30 feet). Infrared Data

Association (IrDA) and Bluetooth and Zigbee are the main WPAN wireless technologies; they exist in the physical layer. The devices that take advantage of a WPAN include PDAs, printers, cameras, cell phones, and access points, etc.. WPAN devices use very little power, Short range helps maintain security and privacy. WPAN technology distinguished mainly two types such as Low rate WPAN and High Rate WPAN[1].

LR WPAN - Low rate WPAN (IrDA, Bluetooth and ZigBee)

The support of IrDA (Wireless Infrared Data Association) enables a user to transfer data between a computer and another IrDA-enabled device for data synchronization, file transfer, or device control. The speed for IrDA is up to 4 Mbps and the distance is usually less than 30 feet in an unobstructed line of sight.

Bluetooth (IEEE 802.15.1) uses radio waves to transmit data and therefore doesn't have the line-of-sight restrictions of IrDA. Bluetooth also supports higher data transmission rates 11 Mbps and uses the 2.4 GHz ISM bandwidth.

ZigBee (IEEE 802.15.4) connectivity of simple fixed and mobile devices with minimum power consumption and distance between 33 feet (10m) - 150 feet (50m) and the transmission rates 20 - 250 Kbps. ZigBee specification based on low-level performance requirements and sensors, control systems and devices designed to remain quiescent for long periods of time. ZigBee Transmissions designed for short range and some devices can route packets to other devices.[1].

Applications for Low Rate WPAN technology include:

- Synchronizing PDAs
- Cellular & Smartphones
- Home control systems (smarthome),
- Cordless telephones, Portable device data exchange
- Industrial control systems
- Location - smart tags used to locate people at home or at the office & Security systems,
- Interactive toys & Inventory tracking

HR WPAN - High Rate WPAN (WiMedia & UWB)

HR WPAN require high throughput, transceiver should be low-power, cost should be low, require quality-of-service (QOS) capabilities, connections should be simple and automatic, and devices should be able to connect to multiple other devices with security features should be included. WiMedia (IEEE 802.15.3 & IEEE 802.15.5) technology supports high data rates and defined two different architectures based on multimedia audio/visual applications and data transfer applications. UWB (IEEE 802.15.3a) technology to supports higher data rates and For multimedia and imaging applications.[1].

Applications for Low Rate WPAN technology include:

- Potential application:
  Connecting digital cameras to printers and
- kiosks:
  Connecting laptops to multimedia projectors and sound systems

II. WPAN PROTOCOLS ARCHITECTURES AND TECHNOLOGY

2. 1 WPAN - Wireless Personal Area Networks

2.1.1 Infrared

Most common infrared connection today based on the IrDA specifications . IrDA specifications define both physical devices and network protocols. IrDA devices' characteristics are provide walk-up connectivity, provide a point-to-point method of data transfer between only two devices at a time and cover a broad range of computing and communicating devices inexpensively implemented. There are currently four published versions of the IrDA specifications.

2.1.1.1 IrDA Version

SIR - Serial Infrared - Speed 9,600-115200 bps, FIR - Fast Infrared - 4 Mbps, VFIR - Very Fast Infrared - 16 mbps and UFIR - Ultra fast Infrared - 100 Mbps. IrDA PHY layer has two parts as Light emitting diodes (LEDs) send signals and Photodiodes receive signals[1].

Infrared WPANs (IrDA) - Serial Infrared (Version 1.0)

Like standard serial port on a PC. UART (Universal Asynchronous Receiver/Transmitter) microchip controls a computer's serial interface. Its clock speed 16 times faster than the data rate and transmitting a 0 using 7-3-6 through UART clock (i.e), Waits 7 clock cycles , Send an infrared pulse for 3 clock cycles and Send nothing for 6 clock cycles.[1]

Infrared WPANs (IrDA) - Fast Infrared (Version 1.1)

Extends data rate to 4 Mbps speed with communication sequence as transmit using SIR first then shift to FIR speed. FIR has 4-pulse position modulation (4-PPM) techniques. The information is conveyed by the position of a pulse within a time slot. The position of operation two bits (or dibits) are transmitted for each pulse.[1]

2.1.1.2 IrDA Protocols Stack

- IrDA Physical Layer Protocol (IrPHY) - Controls hardware that sends and receives IR pulses.
- IrDA Link Access Protocol (IrLAP) - Encapsulating frames and describing devices connection establishment and close.

- IrDA Link Management Protocol (IrLMP) - Detects presence of devices offering a service and checks the data flow.
- IrDA Transport Protocols (TinyTP) - Handles device channeling, performs error corrections and packets division.
- Optional extensions - IrWWW, IrTran-P (Infrared Transfer Picture), Infrared printing (IrLPT) and Other extensions: IrFM, IrSimple, and IrOBEX [1]

2.1.2 Bluetooth over IEEE 802.15.1

Bluetooth Special Interest Group (SIG) a small-form-factor with low-cost wireless radio communications. The partial adaptation of 802.15.1 specification standard approved in March 2, 2002 supporting fully compatible with Bluetooth version 1.1. Bluetooth, also known as the IEEE 802.15.1 standard is based on a wireless radio system designed for short-range and cheap devices to replace cables for computer peripherals, such as mice, keyboards, joysticks, and printers. This range of applications is known as wireless personal area network (WPAN). Two connectivity topologies are defined in Bluetooth: Piconet and Scatternet. A piconet is a WPAN formed by a Bluetooth device serving as a master in the piconet and one or more Bluetooth devices serving as slaves. A frequency-hopping channel based on the address of the master defines each piconet. All devices participating in communications in a given piconet are synchronized using the clock of the master. Slaves communicate only with their master in a point-to-point fashion under the control of the master. The master's transmissions may be either point-to-point or point-tomultipoint. Also, besides in an active mode, a slave device can be in the parked or standby modes so as to reduce power consumptions. A scatternet is a collection of operational Bluetooth piconets overlapping in time and space. Two piconets can be connected to form a scatternet. A Bluetooth device may participate in several piconets at the same time, thus allowing for the possibility that information could flow beyond the coverage area of the single piconet. A device in a scatternet could be a slave in several piconets, but master in only one of them. Bluetooth communication requires two preliminary things: first we have to know the devices in the neighborhood and second there must be a pre established circuit. Communication is also based on a master–slave principle. A group of equipments forms a cell called piconet. A piconet comprises a master and seven slaves at the maximum. Several piconets can overlap and form a "scatternet". In a piconet the communication is based on the master to harmonize the frequencies and channels. We know the neighbors through the discovery phase while in a scatternet there is a need to route data between masters and relay nodes.

Two slave devices cannot talk directly to each other except during the discovery phase. Channel allocation and communication establishment are under the responsibility of the master. Although there was a limitation in earlier versions of Bluetooth on the number of simultaneous channels in a piconet, it is removed from the current version as the cell capacity has increased significantly. The standard supports also broadcast by simply removing the destination from the messages. The master is responsible of polling nodes and also allocating/blocking new connection andwidth. It is responsible for setting the piconet synchronization clock and as we will see decides for the frequency hopping sequence (FHS). A slave can be part of several piconets. One major interesting feature of Bluetooth is that it is not dependent on the IP. This courageous design decision eases the deployment of devices that do not need to worry about upper layer problems such as address allocation, default router, netmask, etc. Auto configuration is hence much easier[1]-[3],[9].

2.1.2.1 Bluetooth Protocol Stack

In Bluetooth we identify several protocols: i. Lower layer protocols: Baseband, LMP, L2CAP, service discovery ii. protocol (SDP), iii. Interfacing protocols: RFCOMM iv. Applicative control specifications[2]: TCS Binary, AT Commands. Bluetooth RF layer - It defines and controls and how radio transmissions function (radio signals) initiated. Radio module - A single radio transceiver hardware required with speed of 1 Mbps (version 1.1) and 2 - 3 Mbps (version 2.0). with three types power class techniques. Power class 1 cover the distance of 330 feet (100 meters) with 100mW power level, Power class 2 cover the distance of 33 feet (10 meters) with 2.5mW power level and Power class 3 cover the distance of 3 inches (10 centimeters) with 1mW power level.

2.1.3 ZigBee over IEEE 802.15.4

Connectivity of simple fixed and mobile devices with 20 - 250 Kbps with minimum power consumption and the distance coverage 33 feet (10m) - 150 feet (50m). The ZigBee Alliance (formed in 2002). The ZigBee specification are based on low-level performance requirements, sensors and control systems, devices designed to remain quiescent for long periods of time. The transmissions designed for short range some devices can route packets to other devices. The basic classes of devices as Full-function, PAN coordinator and Reduced-function[1]-[3].

ZigBee is the architecture developed on top of the IEEE 802.15.4 reference stack model and takes full advantage of its powerful physical radio layer. IEEE 802.15.4 and ZigBee Alliance continue to work closely to ensure an integrated and complete solution for the market especially for sensor networking-based applications. ZigBee provides services such as security, discovery, profiling and so on for the two layers specified by the IEEE group. The different topologies that can range from a centralized star or a cluster-tree-based architecture to a complete mesh network. In the last case there is a need to have an additional routing protocol. A possible architecture for mesh network. Mesh networking enables to increase range, reliability (self-healing) and

formation of ad hoc networks where redundant paths are provided. The data rates and features i. Data rates from 20 to 250 Kbps, ii. Different topologies such as conventional star and mesh operation, iii. Addressing based on short 16 bits or normal MAC (64bits) addresses, iv. Support of simple access and slotted allocation with guarantees and v. Support of acknowledged data transfer, and an optional beacon structure.

2.1.3.4 ZigBee Protocol Stack

Based on OSI model and only layers that are relevant to support 27 channels across different frequency bands using DSSS technology with carrier is modulated with a sequence of 15 chips. ZigBee 802.15.4 frequency bands and data rates as in both PHY layer 868 and 915 MHz bands the frequency range from 868 to 868.6 MHz, chip rate 300 kchips/sec, BPSK modulation with bit rate 20 kbps and frequency range from 902 to 928 MHz, chip rate 600 kchips/sec, BPSK modulation with bit rate 40 kbps. In PHY layer 2450 bands frequency range from 2400 to 2483.5 MHz, chip rate 2000 kchips/sec, O-QPSK modulation with bit rate 250 kbps. For 2,450 MHz band, 16 different 32-bit chip sequences Offset Quadrature PSK (O-QPSK) that uses 2 carrier waves that are exactly 90 degrees out of phase.[1]-[4], [9]

IEEE 802.15.4 PHY frame format

802.15.4 MAC layer handles all access from upper layers to physical radio channel supporting CSMA/CA based access method. The superframe - mechanism for piconet transmission time management guaranteed time slots (GTS) with reserved periods for critical devices to transmit priority data between two beacons. Beacons - signal the beginning of a superframe contain type and number of time slots and time synchronization frame for the network. Beacon frames don't require device-to-device communications, procedures embedded in the hardware and designed to auto-associate with and join network. The Beacon frames device discovery for query others to self-identify and service discovery for identifies other's capabilities. [3]-[7]

ZigBee Network Topologies

Tree and mesh network - Alternate paths may be available for packets Cluster tree network - Alternate paths are available. If another full-function device is within its radio range Star Network - controlled by PAN coordinator[1].

ZigBee Power management

Routing requires lots of processing overhead. The Devices very small, low-speed, power-efficient for cluster tree. Interconnection will incur overhead. Standard favours battery-powered devices and maintains certain parameter values in case of a power failure.[1],[[10]

2.1.4 WiMedia and UWB over IEEE 802.15.3

UWB has recently attracted much attention as an indoor short-range high-speed wireless communication. One of the most exciting characteristics of UWB is that its bandwidth is over 110 Mbps (up to 480 Mbps) which can satisfy most of the multimedia applications such as audio and video delivery in home networking and it can also act as a wireless cable replacement of high speed serial bus such as USB 2.0 and IEEE 1394. Following the United States and the Federal Communications Commission (FCC) frequency allocation for UWB in February 2002, the Electronic Communications Committee (ECC TG3) is progressing in the elaboration of a regulation for the UWB technology in Europe. From an implementation point of view, several solutions have been developed in order to use the UWB technology in compliance with the FCC's regulatory requirements. [11]-[13]

Among the existing PHY solutions, in IEEE 802.15 Task Group 3a (TG3a), multiband orthogonal frequency-division multiplexing (MB-OFDM), a carrier-based system dividing UWB bandwidth to sub-bands, and direct-sequence UWB (DS-UWB), an impulse-based system that multiplies an input bit with the spreading code and transmits the data by modulating the element of the symbol with a short pulse have been proposed by the WiMedia Alliance and the UWB Forum, respectively. The TG3a was established in January 2003 to define an alternative PHY layer of 802.15.3. However, after three years of a jammed process in IEEE 802.15.3a, supporters of both proposals, MB-OFDM and DS-UWB, supported the shutdown of the IEEE 802.15.3a task group without conclusion in January 2006. On the other hand, IEEE 802.15.3b, the amendment to the 802.15.3 MAC sublayer has been approved and released in March 2006[1],[12]

2.1.4.1 WiMedia

IEEE 802.15.3 standard supports 11, 22, 33 - 55 Mbps (2.4 GHz ISM) defines the MAC and PHY layers. The WiMedia Alliance formed to support the development of any necessary higher-layer protocols and software specifications for 802.15.3 and defined 2 different architectures for multimedia audio / visual applications and data transfer applications. In lower layers MAC and PHY with implemented in hardware.[12]

2.1.4.1.1 WiMedia Protocol Stack

802.15.3 PHY layer converts data bits into a modulated RF signal and supports 2 different channel plans i.e coexistence channel plan and high-density channel plan. The Channels limited to 15 MHz and specifies 5 data rates from 11, 22, 33, 44 and 55 Mbps. The Trellis code modulation (TCM) encodes the digital signal and single bit errors detection and correction and also called forward error correction (FEC). [13]-[14]

Modulation enhancements as passive scanning with dynamic channel selection and ability to request channel quality information. Link quality and received signal strength indication over transmit power control. An 802.11 coexistence channel plan with lower transmit power and neighbor piconet capability.

802.15.3 MAC layer functionality

Connection time (association) is faster. Devices associated with the piconet can use a short, one-octet device ID. Devices can obtain information about the capabilities of other devices. Peer-to-peer (ad hoc) networking with data transport with QoS added with security in efficient data transfer using superframes.[13]

IEEE 802.15.3 Superframe Structure

A beacon consists of an optional contention access period (CAP) and the channel time allocation period (CTAP). Communication in an 802.15.3 piconet structure as Beacon frame sent by the PNC includes a variable indicating the end of the CAP. Devices can send asynchronous data in the CAP.

Devices can request channel time on a regular basis as requested channel time is called isochronous time. Devices can also request channel time for asynchronous communications in the CTAP. Communications use a time division multiple access (TDMA) scheme.

Power Management

802.15.3 devices can turn off completely for long periods of time without losing their association with the piconet. 802.15.3 power-saving methods as Device synchronized power save (DSPS) mode, Piconet synchronized power save (PSPS) mode and Asynchronous power save (APS) mode. The Wake superframe designated by the PNCand devices that are in power save mode wake up and listen for frames addressed to them. The additional power-saving methods are PNC can set a maximum transmit power level and Devices request a reduction or an increase in their own transmit power.[1],[14]

2.1.4.2 UWB

Allows new transmission techniques based on UWB to coexist with other RF systems with minimal or no interference. UWB characteristics are it transmits low-power, short-range signals, transmits using extremely short low-power pulses lasting only about 1 nanosecond, transmits over a band that is at least 500 MHz wide and UWB can send data at speeds of up to 2 Gbps.[1],[11]

2.1.4.2.1 UWB Protocols Stack

UWB PHY layer perform the digital signals need to be spread over a wide band using techniques such as FHSS or DSSS. UWB uses short analog pulses for signaling. It does not rely on traditional modulation methods and this technique is called impulse modulation. Most common Biphase modulation technique used by UWB and Uses a half-cycle positive analog pulse to represent a 1. Direct-sequence UWB (DS-UWB) work when transmitting pulses that are a nanosecond long and Signal spreads over a very wide frequency band in the UWB case, the signal spreads over a band that is at least 500 MHz wide. Orthogonal frequency division multiplexing (OFDM)used commonly referred to as MB-OFDM.

Frequency band is divided into five groups containing a total of 14 frequency bands and Each frequency band is 528 MHz wide with further divided into 128 frequency channels. The channels are orthogonal and they do not interfere with each another. The data bits are sent simultaneously (in parallel) proposed enhancement to 802.15.3 uses UWB technology to support higher data rates for multimedia and imaging applications. The Protocol Adaptation Layer (PAL) enables wireless FireWire at 400 Mbps based on an 802.15.3a/WiMedia platform with wireless USB (WUSB) version 2 based on the WiMedia specifications and transmits at 480 Mbps at a distance of up to 2 meters.

Ultra Wide Band is a digital transmission technology will soon support very high-speed transmissions UWB transmissions it bandwidth of at least 500 MHz. UWB transmits using very short pulses challenges for WPANs include speed, security, cost, industry support, interference, and protocol limitations. WPAN devices that are designed to be small and consume very little power have limited processing capabilities and storage.[1],[11],[15]

III. WPAN PROTOCOLS SECURITY ISSUES AND SOLUTIONS

Security in Infrared WPANs

Limited to LOS characteristic . IrDA specification makes no provision for encrypting data or protecting the connection. Users may encrypt a file before exchanging it. IrDA devices support open access methodology so that anyone can transmit files without first notifying the device's owner. Open access can be a major security concern. IrDA interface supports direct line of sight, it at first glance would appear to be the more secure of platforms. In fact, both IrDA and Bluetooth are well-attuned to the security requirements of users. IrDA relies on security protocols and authentication / encryption routines at a higher level of the protocol stack.[1]

3.1 Security in Bluetooth

Bluetooth provides security at LMP layer using authentication. Authentication is based on identifying the device itself. Authentication scheme is a challenge-response strategy in security mechanism. Encryption is the process of encoding communications and ensures that the transmissions cannot be easily intercepted and decoded.The Bluetooth security model includes a security dedicated entity called Security Manager Before the establishment of a connection, the security manager decides which security policy to apply. This decision is based on the used service type and the distant device with which the ommunication will take place. Security information needed by the security manager is stored in two databases: the database of the physical devices and another for services.[1]-[2]

Security levels

Bluetooth defines various security levels for peripherals and services. Each peripheral obtains a status when it connects, for the first time, to another peripheral. In the Generic Access Profiles (GAP), three modes are defined:

i. Level 1: None. No security function is activated, all Bluetooth devices may be freely connected.

ii. Level 2: application-level security/service level. This mode guarantees a security after connection establishment. This mode supports various controls according to applications and associated functions act at application level.

iii. Level 3: link-level security. It is the most secure mode: It inherits from mode 2 functionalities by adding a preliminary control at the time of connection attempt.

Encryption modes

Encryption Mode 1 — Nothing is encrypted

Encryption Mode 2 — Traffic from the master to one slave is encrypted but traffic from the master to multiple slaves is not encrypted.

Encryption Mode 3 — All traffic is encrypted

Main Procedures

The initialization phase represents an important phase. It includes four tasks which are:

i. Generation of the initialization key
ii. Authentication and generation of the authentication key
iii. Exchange of link key
iv. Generation of encryption key Communications between various Bluetooth entities use a link key. [1]-[2]

This key of 128 bits is generated in a different way according to the communication type:

i. At initialization step
ii. During the starting of a communication between two peripherals
iii. During a communication initiated by only one device (initialization key),
iv. During a communication between a master and several slaves. [1]-[2]

Authentication

Bluetooth uses a challenge/response mechanism with shared symmetric keys. The authentication begins by emitting a request to another peripheral by exchanging BD ADDR and link key. Upon authentication, encryption is used to communicate. Without knowledge of PIN code, a peripheral cannot be recorded if the phase of authentication is activated. In order to facilitate the procedure, the PIN code can be stored inside the unit Bluetooth uses a challenge/response exchange for authentication in which the knowledge of the requestor of the secret link key KAB is controlled through a protocol applying symmetric keys. A temporary link key is used at the time of the first contact, thereafter the semi-permanent key shared by the two units A and B is used. The iterative per-block symmetric encryption algorithm $E1$ is used.

Unit A sends a random number, noted AU RANDA, with a code of authentication noted$E1$ for the unit B. The unit B calculates SRES and returns the result to unit A calculates SRES and will authenticate the unit B if SRES = SRES_. SRES is calculated by using algorithm SAFER + based on the $E1$ function which takes as input parameters (AU RANDA, address BD ADDR of the peripheral, current link key). At each authentication a new random number AU RANDA is generated.[1]-[3]

3.2 Security in ZigBee

ZigBee is designed as a global hardware and software standard for wireless networking devices. Its main features are: highly reliable, low cost, low power, low data rates and highly secure. Three security levels are specified: none, ACLs and symmetric. key employing AES 128-bit encryption. The concept of “trust centre” is used. We can use link and network keys. Two operations are supported: authentication and encryption. Security can be customized for applications and keys can be hardwired into applications.

Symmetric keys for authentication and encryption in addition: Frame integrity uses a message integrity code (MIC). Access control is based on access control list (ACL) - Sequential freshness & Security service used by the receiving device. Ensures that the same frames will not be transmitted more than once. Security modes: Unsecured mode, ACL mode & Secured mode.[3]-[5].

Different types of keys are defined: master key, link key and network key.

i. The master key, designed for long-term security between two devices, can be set up over-the-air or by using out-of-band mechanisms (eavesdropping should be prevented during this setup phase). It is sent by the trust centre. It can also be a factory-installed option.

ii. The link key is provided for security between two devices. It is derived from the master key. It can also be factory-installed option.

iii. The network key serves to provide security across the network and protects against outsiders attacks. It can lso be factory-installed option. Link and network keys can be updated periodically. These keys need to be set up with and between new devices that join the network. If keys are set up over-the-air only, the last link is vulnerable to a one time eavesdrop attack. After a device joins it needs to store multiple keys.[3]-[7]

Authentication

Authentication provides assurance about the originator of the message. It prevents an attacker from modifying a hacked device to impersonate another device. Authentication is possible at network level or device level. Network-level authentication is achieved by using a common network key. This prevents outsider attacks while adding very little in memory cost. Device level authentication is achieved by using unique link keys between pairs of devices: This prevents insider and outsider attacks but has higher memory cost.

Encryption

Prevents an eavesdropper from listening to messages. ZigBee uses 128-bit AES encryption. Encryption protection is possible at network level or device level. Network-level encryption is achieved by using a common network key. This prevents outsider attacks while adding very little in memory cost. Devicelevel encryption is achieved by using unique link keys between pairs of devices. This prevents insider and outsider attacks but has higher memory cost. Encryption can be turned off without impacting freshness, integrity or authentication. Some applications may not need encryption protection.[7]-[10]

3.3 Security in WiMedia and UWB

Security for IEEE 802.15.3 HR WPANs mainly based on the Advanced Encryption Standard (AES). Defines how any two devices can establish a secure communications session. To protect both the information and the integrity of communications at the MAC and PHY layers 802.15.3 also supports message integrity verification at the MAC layer. It prevents a man-in-the-middle attack. The WiMedia UWB radio has been chosen by the Bluetooth Special Interest Group (BT-SIG, as an alternate MAC/PHY (AMP) for high-speed Bluetooth. Members of the WiMedia Alliance have been active in implementing the Bluetooth PAL and have taken prototypes to various BT plugfest. The adoption of the corresponding test specification by the BT-SIG has paved the way for formal interoperability testing to begin, with a view to inclusion in the forthcoming Seattle release. The arrival of chipsets to support UWB over Bluetooth is imminent, and we expect to see consumer implementations of the technology in the first half of 2009. [1],[11]-[15]

WiMedia members are free to implement proprietary A/V multimedia PALs on the WiMedia Common Radio Platform. One application that has seen early adoption of the technology is streaming multimedia where UWB offers an optimum combination of speed (such as for handling the bandwidth of HD video), range and low power[11]-[15].

IV. COMPARISON OF WPAN PROTOCOLS

Table 2 shown the comparison of summarizes the main differences among the WPAN protocols such as LR WPAN and HR WPAN. Each protocol is based on an IEEE standard.In general, the Bluetooth, ZigBee and UWB are intended for WPAN communication while Wi-Fi is oriented to WLAN (about 100m). However, ZigBee can also reach 100m in some applications. FCC power spectral density emission limit for UWB emitters operating in the UWB band is -41.3 dBm/Mhz. This is the same limit that applies to unintentional emitters in the UWB band, the so called Part 15 limit. The nominal transmission power is 0 dBm for both Bluetooth and ZigBee, and 20 dBm for Wi-Fi.[1],[6],[8]

TABLE 2 : Comparison of WPAN Protocols

WPAN 802.15	LR WPAN	LR WPAN	HR WPAN
Standard	**Bluetooth**	**ZigBee**	**WiMedia / UWB**
IEEE Spec.	802.15.1	802.15.4	802.15.3 & 802.15.3a
Frequency Band	2.4 GHz	868/915 MHz; 2.4 GHz	3.1-10.6 GHz
Max Signal Rate	1 Mb/s	250 Kb/s	110 Mb/s
Nominal Range	10 m	10 - 100 m	10 m
Nominal TX Power	0 - 10 dBm	(-25) - 0 dBm	-41.3 dBm/MHz
Number of RF Channels	79	1/10; 16	(1-15)
Channel Bandwidth	1 MHz	0.3/0.6 MHz; 2 MHz	500 MHz - 7.5 GHz
Modulation Type	GFSK	BPSK (+ ASK), O-QPSK	BPSK, QPSK
Spreading	FHSS	DSSS	DS-UWB, MB-OFDM
Coexistence	Adaptive	Dynamic	Adaptive

Mechanism	Freq. Hopping	Freq. Selection	Freq.Hopping
Basic Cell	Piconet	Star	Piconet
Extension of the Basic Cell	Scatternet	Cluster Tree, Mesh	Peer-to-peer
Max Number of Cell Nodes	8	> 65000	8
Encryption	E0 Stream Cipher	AES block cipher (CTR, Counter Mode)	AES block Cipher (CTR, Counter Mode)
Authentication	Shared Secret	CBC-MAC (ext. of CCM)	CBC-MAC (CCM)
Data protection	16-bit CRC	16-bit CRC	32-bit CRC

* Unapproved draft.
• Acronyms: ASK (amplitude shift keying), GFSK (Gaussian frequency SK), BPSK/QPSK (binary/quardrature phase SK), O-QPSK (offset-QPSK), OFDM(orthogonal frequency division multiplexing), COFDM (coded OFDM), MB-OFDM (multiband OFDM), M-QAM (M-ary quadrature amplitude modulation), CCK (complementary code keying), FHSS/DSSS (frequency hopping/direct sequence spread spectrum), BSS/ESS (basic/extended service set), AES (advanced encryption standard), WEP (wired equivalent privacy), WPA (Wi-Fi protected access), CBC-MAC (cipher block chaining message authentication code), CCM (CTR with CBC-MAC), CRC (cyclic redundancy check).

V. CONCLUSION

In this paper, focus all the types of wireless personal area networks technologies and architectures with security issues plus protocols standards and evaluating their main features and behaviors in terms of various metrics, including the transmission time, data coding efficiency, complexity, and power consumption. The major goal of this paper contribute to research in the area of wireless standards applicable in to wireless personal area network. The comparison of all wireless personal area networks protocols standards and suits for entire short distances communications.

VI. REFERENCES

[1] Olenewa, J.& Ciampa, M. (2007), "Guide to Wireless Communications," 2nd edn, Course Technology. Chapters - WPAN.

[2] E. Ferro and F. Potorti, "Bluetooth and Wi-Fi wireless protocols: A survey and a comparison," IEEE Wireless Commun., vol. 12, no. 1, pp. 12-16, Feb. 2005.

[3] J. S. Lee, "Performance evaluation of IEEE 802.15.4 for low-rate wireless personal area networks", IEEE Trans. Consumer Electron., vol. 52, no. 3, pp. 742-749, Aug. 2006.

[4] Roanoke, "ZigBee collocated on an industrial floor," in Proc. IEEE Int. Conf. Ind.Electron. (IECON'03), VA, Nov. 2003, pp. 2381-2386.

[5] J. S. Lee and Y. C. Huang, "ITRI ZBnode: A ZigBee/IEEE 802.15.4 platform for wireless sensor networks," in Proc. IEEE Int. Conf. Systems, Man & Cybernetics, Taipei, Taiwan, Oct. 2006, pp. 1462-1467

[6] Jin-Shyan Lee, Yu-Wei Su, and Chung-Chou Shen, "A Comparative Study of Wireless Protocols:Bluetooth, UWB, ZigBee, and Wi-Fi," The 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON), Nov. 5-8, 2007, Taipei, Taiwan,

[7] Baker, N. "ZigBee and Bluetooth: Strengths and weaknesses for industrial applications," IEE Computing & Control Engineering, vol. 16, no. 2, pp 20-25, April/May 2005.

[8] K. Shuaib, M. Boulmalf, F. Sallabi, and A. Lakas, "Co-existence of Zigbee and WLAN: A performance study," in Proc. IEEE/IFIP Int. Conf. Wireless & Optical Communications Networks, Bangalore, India, April 2006.

[9] Dr.Hari Ramakrishna, K.Ravi, "A Study on Multi Wireless Technologies – Architecturesand Security Mechanisms,"IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011

[10] A. Sikora and V. F. Groza, "Coexistence of IEEE802.15.4 with other systems in the 2.4 GHz-ISM-Band," in Proc. IEEE Instrumentation & Measurement Technology Conference, Ottawa, May 2005, pp.1786-1791.

[11] D. Porcino and W. Hirt, "Ultra-wideband radio technology: Potential and challenges ahead,"IEEE Commun. Mag., vol. 41, no. 7, pp. 66-74, July 2003.

[12] WiMedia Alliance, "Multiband OFDM Physical Layer Specification," WiMedia Release Spec. 1.5, August 2009.

[13] WiMedia Alliance, "Multiband OFDM Physical Layer Specification", WiMedia Release Spec. 1.5, August 2009.Jd. P. Pavón, S. N. Shankar, V. Gaddam, K. Challapali, and C. T. Chou, "The MBOA-WiMedia specification for ultra wideband distributed networks," IEEE Communications Magazine, vol. 44, no. 6, pp. 128–134.

[14] J. W. Kim, K. Hur, J. O. Kim, D. S. Eom, and Y. Lee, "A disturbed resource reservation structure for mobility and qos support in wimedia networks," IEEE Transactions on Consumer Electronics, vol. 56, no. 2, pp. 547–553, 2010

[15] W. Wang, C. K. Seo, and S. J. Yoo, "Power aware multi-hop packet relay MAC protocol in UWB based WPANs in Mobile Ad-hoc and Sensor Networks," vol. 3794 of Lecture Notes in Computer Science, pp. 580–592, 2005.

AUTHORS PROFILE

DR. P. RAJAMOHAN received his Bachelor of Science Degree in Physics later he obtained his Post Graduate Diploma in Computer Applications (PGDCA), Master Degree in Computer Applications (MCA) and PhD in Computer Science. His primary research interest in Virtual Private Network Implementation for Efficient Data Communication and wireless Networks Communications. He is the member of the Institution of Engineers (India), member of Associate in Cisco Certified Networks, member of the International Association of Engineers (IAENG) and member of the Computer Science Teachers Association, USA (CSTA). Dr. P. Rajamohan, over all his 20 years experiences in both academic and IT industry. He is currently working as a Senior Lecturer in School of Information Technology, SEGi University, Malaysia.