A Study on Multi Wireless Technologies – Architectures and Security Mechanisms

Dr.Hari Ramakrishna
Professor, Department of CSE,
Chaitanya Bharathi Institute of technology
Gandipet -500 075, Hyderabad,

K.Ravi
Asst. Professor, Dept. of Informatics
Alluri Institute of Management Sciences

ABSTRACT
Years are going and the Wireless Communication medium is changing its structure is also changing. In this paper, we focus four types of wireless communication technologies. This paper describes the architectures of these four technologies with there security issues.
All these four models have there different structures and have different mechanisms to handle the data communication between the stations. In this paper we also defined the IEEE 802.1X standards for the four different models and there mechanisms.

Keywords: Wi-Fi, Bluetooth, ZigBee, WiMAX, Networks, IEEE 802.1X, Security, Architecture

1. INTRODUCTION

Today wireless is becoming the leader in communication choices among users. It is not anymore a backup solution for nomadic travelers but really a new mood naturally used everywhere even when the wired communications are possible. Many technologies evolve then continuously, changing the telecommunication world. In this paper we consider four wireless technologies with there architectures and security aspects. The four wireless technologies are:

1) Wi-Fi
2) Bluetooth
3) ZigBee
4) WiMAX

In this paper we can see the IEE 802.1X standard wireless communication models for these wireless technologies. There are many models but we can few of them. We can also see the advantages over the previous technologies in different aspects. Final this paper cover the security issues in these technologies

2. IEEE 802.11 ARCHITECTURE FOR Wi-Fi

The IEEE 802.11 standard defines three modes for Wi-Fi wireless Technology

1) Infrastructure Mode
2) Ad hoc Mode
3) Mesh Mode

2.1 INFRASTRUCTURE MODE
Within the infrastructure mode, the wireless network consists of at least an access point (AP) connected to the fixed network infrastructure and a set of wireless client stations. This configuration is based on a cellular architecture where the system is subdivided into cells. Each cell in the IEEE 802.11.

The stations within a base stations (BSS) execute the same MAC protocol and compete for access to the same shared wireless medium. We can refer to it in the following sections as a cell. Although a WLAN may be formed by a single cell, the maximum distance between stations is limited by many factors like RF output power and the propagation conditions of the indoor/outdoor environments. To provide for an extended coverage area, multiple BSSs are used where the APs are connected through a backbone called a distribution system (DS).

The whole interconnected WLAN including at least two different BSSs (with respect to their APs) and the DS, is seen as a single logical IEEE 802 network to the logical link control (LLC) level and is called an Extended Service Set (ESS). The majority of WLANs should be able to reach the fixed LAN services (file servers, printers and Internet access). The DS is responsible of transporting the packets between various cells within the ESS area. Data transfers occur between stations within a BSS and the DS via an AP. DS handles address mapping and networking functions.

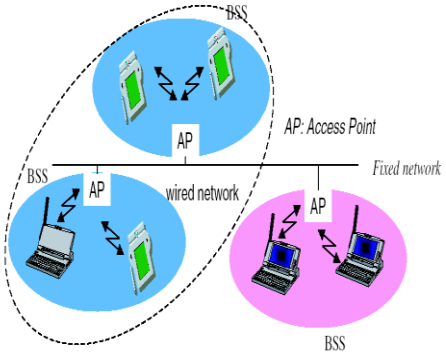

Figure 1: Infrastructure mode in IEEE 802.11 for Wi-Fi

2.2 AD HOC MODE:
The ad hoc mode (Figure 2.6) simply represents a group of IEEE 802.11 wireless stations that communicate directly between them without having a connection with an AP or a connection to

a fixed network through the DS. This configuration is sometimes referred as a peer-to-peer configuration. Each station can establish a communication with any other station in the cell which is called an independent cell Independent Basic Service Set (IBSS). These networks have been studied at the beginning of the 1970s and were named packet radio networks (PRNET).

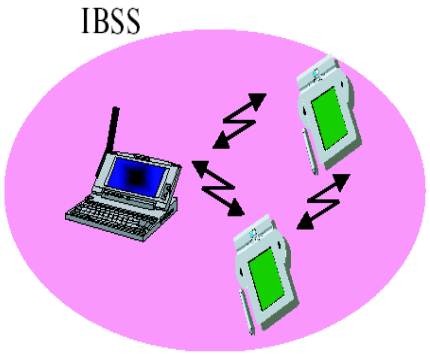

Figure 2: Ad hoc mode

This mode allows to create quickly and simply a wireless network where there is not fixed infrastructure or where such an infrastructure is not necessary for the required services (hotel room, conference centers or airport), or finally when the access to the fixed network is prohibited or difficult.

2.3 **MESH MODE**

The third type defines a hybrid configuration combining infrastructure and ad hoc modes

2.4 **Wi-Fi SERVICES**

The IEEE 802.11 standard Wi-Fi technology architecture supports a series of basic services that are:

i. Association/disassociation / resuscitation

ii. Delivery of the MAC/MSDU frames

iii. Authentication/deauthentication

iv. Diffusion and broadcast

v. Beacon and probing

vi. Privacy/confidentiality

3. IEEE 802.15.1 ARCHITECTURE FOR BLUETOOTH

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" (see Figure 3.3). 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.

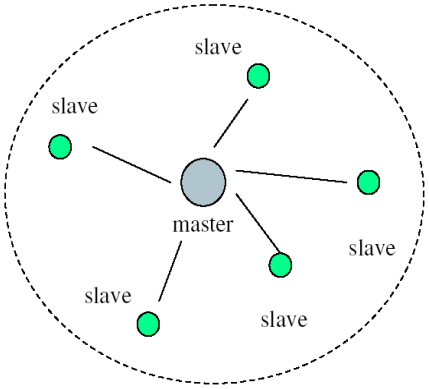

Figure 3: IEEE 802.15.1 Bluetooth Master/Slave Architecture

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.

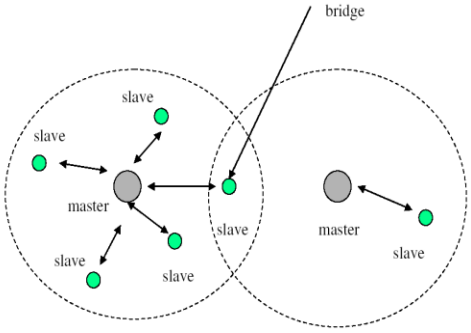

Figure 4: Bluetooth Scatternet

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. 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: TCS Binary, AT Commands

4. IEEE 802.15.4 ARCHITECTURE FOR ZIGBEE

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.

As shown in Figure 5 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.

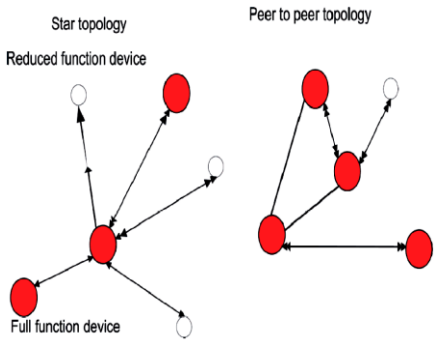

Figure 5: Basic possible topologies and node categories in IEEE 802.15.4

A possible architecture for mesh network is shown in Figure 6: Mesh networking enables to increase range, reliability (self-healing) and formation of ad hoc networks where redundant paths are provided.

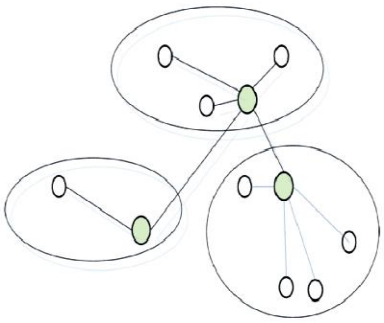

Figure 6: Mesh Network of ZigBee

4.1 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 (64 bits) addresses

iv. Support of simple access and slotted allocation with guarantees

v. Support of acknowledged data transfer, and an optional beacon structure

5. IEEE802.16 STANDARDS AND WIMAX

The IEEE 802.16 group has started to produce recommendations for a relatively long period. The evolution of the wireless physical layers is seen in the different versions, the same way it can be noticed in IEEE 802.11 standard. That is why we can see a first physical layer implementing plesiochronous digital hierarchy (PDH) like data rates with a line of sight restrictive condition.

Few years later, with the familiarization to OFDM, a new version has come up with "line of sight" restriction removed but with lower throughput.We did not see any IEEE 802.16 equipment in the first editions of the standard, not because the lack of products, but because of the unclear legislation in that area together with the wide deployment of fixed asymmetric digital subscriber line (ADSL) wired lines.

5.1 BACKHAUL SOLUTIONS

The first use case is based on fixed IEEE 802.16 equipment. Independent of the used version, we can employ the technology in a fixed infrastructure as shown in Figure 7:

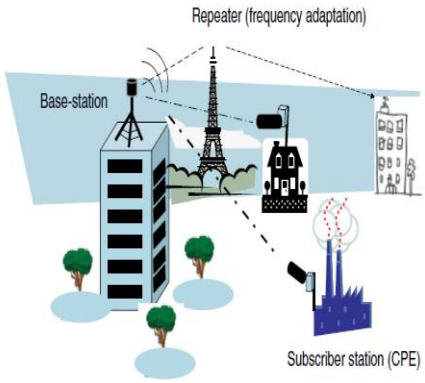

Figure 7: IEEE 802.16 first deployment scenario

In this scenario, the two possible cases are the deployment of point to point connections that can span tens of kilometers. The second scenario is the deployment of local loop alternatives to ADSL where the receiver is located inside each house or inside customer premises as shown in Figure 8. The latter may use omni or angular antennae.

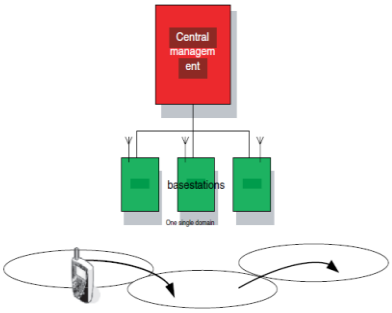

Figure 8: IEEE 802.16 second deployment scenario

5.2 MOBILE SOLUTIONS

The second use case of the standard is based on a different version and provides a mobility scheme for cellular like data transmission. In that case IEEE 802.16 provides the physical and MAC layer only to support the handover. It is different from the 3G family of standards that provide a complete architecture which includes management of the subscribers and the whole network, while IEEE 802.16 stops at layer 2. This also means that handover is done between contiguous base stations and is not provided for interdomain operation.

The standard is targeted to rural areas in the beginning of development especially when local loops are not available. It is in that case financially much more efficient and effective. Normally, the base stations reside in a central point accessible to the Internet and the outside world by satellite links or any other means. They connect to remote transceivers called customer premises equipments (CPEs).

The CPEs are for the time being located on top of the roofs and there should be a second technology that concentrates traffic from the whole building to that CPE. In a later view we would find the CPEs deployed in the residences themselves and hence we would not need anything else to interconnect the final customer to the IEEE 802.16 infrastructure. The usage of this technology is also regulated, since power has to be in the range of few watts and frequency is generally located in the 3.5 GHz band.

5.3 LAYERED ARCHITECTUE FOR WiMAX

IEEE 802.16 is again part of the IEEE 802 group and hence should conform to the bridging (or any layer-2 rules) concepts. The addressing is based on MAC addresses and the base station is seen as a bridge. Nothing prevents it to be a router, but it should implement all layer-2 functionalities also. Addressing, as it is going to be explained, is used as an identification for nodes, but the use of circuits with a circuit identifier replaces this address as long as the node is recognized by the network.

The layers are divided into a MAC and a physical layer. In the MAC layer several sublayers are defined. The first is called the service-specific and is the adaptation of IEEE 802.16 to the available packet types: ATM, Ethernet and IP. Of course, in practice it is only IP that is generalized in the available products.

The MAC sublayer is based on a connection-oriented principle. It is very close to the ATM transport protocol. The connection is using a context that describes the mapping between the incoming flows and the underlying Quality of Service (QoS). As we will see later, a station registers itself to the base station, negotiates the physical layer characteristics and then can communicate in directionally.

A service flow defines the negotiated QoS for all matching packets to service-specific sublayer. The QoS can be changed dynamically and it supports extremely well data bursts. Everything is negotiated for uplink and downlink separately.

6. SECURITY IN WI-FI SYSTEMS

Security in wireless networks gained an increasingly important interest since the publications of scientific articles which clearly describe the insufficiencies of the used mechanisms; particularly those concerning the IEEE 802.11/Wi-Fi systems. Confidentiality and authentication must be taken into account since most wireless architectures are connected to a fixed infrastructure.

6.1 BASIC MECHANISM

The IEEE 802.11 standard defines basic mechanisms to enhance security. These mechanisms are:

i. Access control

ii. Authentication of stations which are connected to the network

iii. Confidentiality and integrity of data thanks to the WEP protocol.

These mechanisms are limited to make secure exchanges between two stations.

6.2 ACCESS CONTROL

Access control is performed mainly using two techniques based on the use of SSIDs and/or access control lists (ACLs).

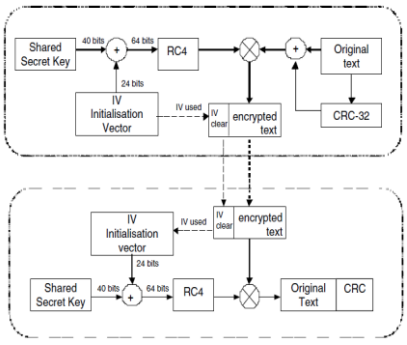

Figure 10: Data encryption/decryption using WEP

The message to be encrypted (called plaintext) undergoes a transformation using a function parameterized by a key. The result of the encryption algorithm is called cipher text and can then be transmitted. An intruder can then listen to or completely copy the cipher text. However, this intruder is supposed not to have the key of deciphering, what makes impossible the recovery of information sent in clear.

6.5 DECRYPTION.

The decryption algorithm, illustrated in Figure 11, includes the following steps:

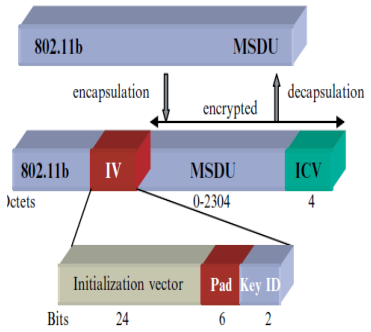

Figure 11: Encrypted packet format

i. Generation of the decryption key from the IV of the received message and the identifier of the decryption key.

ii. Decryption of the received message with the key to obtain the initial message.

iii. Check of the integrity of the decrypted message by using ICV algorithm..

6.6 AUTHENTICATION MODELS

IEEE 802.11 standard proposes two authentication systems:

1) The Open System Authentication (OSA) It is the first technique suggested by default. There is no explicit authentication; a station can join any access point and listen to data in clear within a cell

2) The shared key authentication (SKA)

6.7 KEY MANAGEMENT

No mechanism of distribution of keys is mentioned in the standard. Consequently, the equipment suppliers implement specific solutions in their products. Unfortunately, in the majority of the cases, it is not possible to verify the consistency of the implemented procedures; in spite of that security faults are always detected. WEP keys can be used in two manners:

1) The first method provides a window with four keys (taking into account the reservation of 2 bits for their description in Key ID of the Stations and access points can decrypt frames using one of these four keys.

2) The second method is called key mapping table. In this method, each MAC address can have a separate key. This table at least contains ten entries and the maximum size is directly related to the chipset. Assign a separated key to each user permits to better protect the frames.

7. SECURITY ARCHITECTURE FOR BLUETOOTH

The security model, illustrated by Figure 12, includes a security dedicated entity called Security Manager

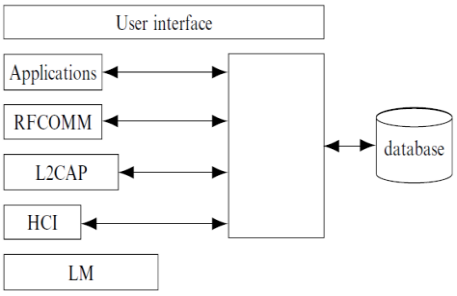

Figure 12: Bluetooth security model

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 communication 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.

7.1 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. Mode 1: none. No security function is activated, all Bluetooth devices may be freely connected.

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

iii. Mode 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.

Bluetooth offers three security levels:

1) Authorized and authenticated
2) Authenticated
3) Free access

7.2 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. 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

A total diagram describing the various phases is given by Figure 13. We assumed that only two peripherals A and B wish to communicate. The following steps occur:

I. A and B switch on
II. A and B communicate in order to establish a shared secret key for next communications
III. A and B use the non-volatile stored key to exchange data

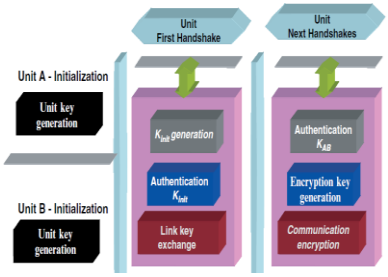

Figure 13: Bluetooth Security Mechanism

7.3 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 keyK_{AB} 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 *E*1 is used.

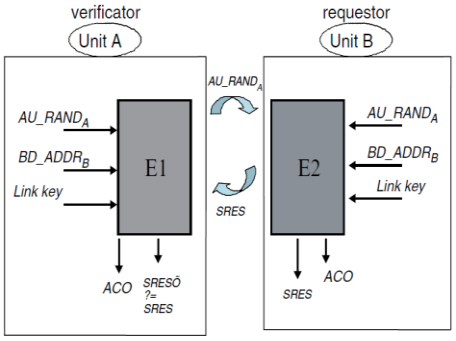

Figure 14: Authentication procedure

Unit A sends a random number, noted AU RANDA, with a code of authentication noted*E*1 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 *E*1 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.

8. ZIGBEE SECURITY

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.

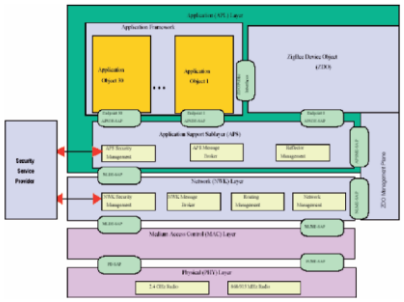

Figure 15: ZigBee security architecture

8.1 ZIGBEE SECURITY ARCHITECTURE

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 also 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.

8.2 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.

8.3 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. Device-level 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.

9. WiMAX AND IEEE 802.16 SECURITY

The security is considered as a sublayer and implements privacy, authentication and confidentiality for the wireless network. Like IEEE 802.11 it is restricted to the link so it concerns connections between the base station and stations.

Since IEEE 802.16 is probably not used in a private context but for an operator willing to earn benefits from this service, the security system is normally robust against theft of service such as bandwidth, connections and so on. The base station is also protected against management attacks. Since the system is strongly centralized a certificate-based security is very suitable and easy to deploy.

9.1 SECURITY SERVICE

The security service is hence divided into two parts: the authentication/key derivation and the encryption

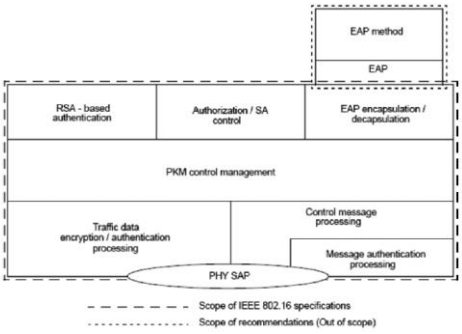

Figure 16: Security services

Like IPsec, IEEE 802.16 defines the security association (SA) that the base station and stations hold to support the application of security. They define *Primary, Static* and *Dynamic* SAs. Stations must have a primary SA at initialization. The static SA is only concerning base stations. Dynamic SAs are created and removed at the speed connections are created and removed. Static and dynamic SAs can be shared by several stations if the connection is a group communication.

In the SA we will find the negotiated cryptographic suite, its identifier called an SAID. The primary SAID is to manage the main connections with the base station and its SAID is equal to the primary CID. This SA is also responsible for storing keying material with its lifetime so that whenever an expiry happens a reeling happens between the station and its base. The defined suites in the IEEE 802.16 2004 define encryption, authentication and method for encryption, they were as follow:

i. No encryption and no authentication, 3DES 128

ii. CBC 56-bit DES, no authentication and 3DES

iii. No encryption, no authentication and RSA 1024

iv. CBC 56-bit DES, no authentication and RSA 1024

v. CCM AES, no authentication and AES 128

9.2 SECURITY ENHANCEMENT FOR MOBILE COMMUNICATIONS

The new features are mainly related to three things:

i. EAP integration in the authentication phase

ii. A version two PKM algorithm

iii. Group key derivation

iv. Another integrity check method called Cipher-based MAC

v. Mention of pre-authentication but no proposals yet

As for the pre-authentication, it simply means that a node should derive the AK before it moves to another base station. How this is done and when is not really explained and is left for any eventual next version of the standard. We use the PKMv2. It uses a slightly different key hierarchy that defines what keys are necessary and how they are generated. It is different due to the presence of two authentication systems, one based on RSA and the other on EAP.

The first keys are used to protect management message integrity and transport the traffic encryption keys (TEK). The TEK are derived through the first keys plus as usual some exchanged parameters in the initialization. They rename the RSA-generated keys as the pre-primary AK (pre-PAK), and the ones generated through EAP-based authentication as the mobile station keys MSK where MSK is a shared "master key" derived by two peers.

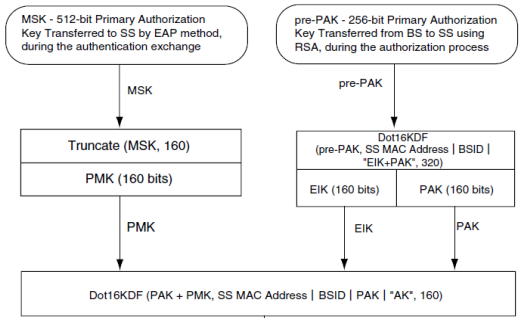

Figure 17: PKMv2 used in mobile 802.16

The mobile station keys MSK where MSK is a shared "master key" derived by two peers.
The general procedure to extract AK from those is as follows:

10. SUMMARY

For Wi-Fi technology, an important list of security faults was detected because mainly of the weaknesses of protocol WEP and the absence of mechanism of key distribution. However, some attacks are still possible like dictionary and DoS attacks.

Security procedures in Bluetooth are more elaborate than in Wi-Fi, but there are always weaknesses. Authorization system must be reinforced. This is possible without changing the protocol stack but by modifying the security manager and the initialization procedure. Other improvements are possible.

ZigBee provides pretty good security mechanisms for low rate and short range wireless systems. These mechanisms are settled in combination between layer 2 and high layers. Revocation is not supported but next versions of the standard will probably include it.

WiMAX security applies a classical approach based on using certificates. Also the use of EAP makes WiMAX security similar to the one adopted in Wi-Fi networks. Beyond the information and sensitizing of users, it is essential to configure its network in a protected way. This step includes configuration of link and transport layers but also periodic audit and permanent monitoring of its network.

11. REFERENCES

[1] L.M.S.C of the IEEE Computer Society, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band", *IEEE Standard 802.11b*, 1999 editions, 1999

[2] *Specification of the Bluetooth System*, volumes 1 and 2, version 1.0B December 1999.

[3] *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Enhancements for Quality of Service (QoS)*, IEEE 802.11e/D4.0, 2003.

[4] Geier J., *Wireless LANs*, Wiley, New York, 2000.

[5] Geier J., *Wireless LANs: Implementing High Performance IEEE 802.11 Networks*, 2nd edition, SAMS, 2002.

[6] Haarsten J.C., "The Bluetooth Radio System", *IEEE Personal Communications Magazine*, volume 7, pp.28–36, February 2000.