Wireless Standards and Mesh Networks

Stephen Asherson, Pieter Kritzinger and Paolo Pileggi
Data Network Architectures Group,

Technical Report CS07-02-00
Computer Science Department University of Cape Town,
Private Bag, Rondebosch, 7700, South Africa
Email:{sasherso,psk,plgpao001@cs.uct.ac.za}

Abstract - *On March 13th 1980, the Computer Society of the Institute of Electronics and Electrical Engineering (IEEE) approved project 802. IEEE 802 is led by the LAN/MAN Standards Committee(LMSC). Until today, 22 Working Groups (WGs) mainly define standards for the lowest two layers of the ISO/OSI reference model in the 802. For wireless communication, 802.11 WG defines the Wireless Local Area Network (WLAN), 802.15 WG defines the Wireless Personal Area Network (WPAN), and 802.16 WG defines the Wireless Metropolitan Area Network (WMAN) standard.*

With Multiple Input/Multiple Output (MIMO), Ultrawideband (UWB) and sensitive Modulation and Coding Schemes (MCSs), the latest developments in the IEEE 802 standards enable data rates beyond 500Mbps for new applications of wireless communication. Similar to preceding wireless technologies, data rate slows down by increase in distance of the communication entities. However, demands for new applications emerge that need high data rates regardless of distance. To overcome the link speed limitation, dense deployment of wireless networks is needed[1].

Wireless Mesh Networks (WMNs) help to overcome current dependencies of wireless communication systems on wired backbones by enabling cost-effective and rapid deployment for a new generation of wireless services.

Keywords: Fixed ad-hoc mesh networks, 802 standards, WiFi, WiMax, wireless networks

I. Introduction

Wireless communication standards involve various versions of IEEE 802.11 [1], commercially known as *WiFi*; 802.15 or Personal Area Networks (PAN) and IEEE 802.16, commercially called *WiMax*. In this report we provide insight into those features of WiFi and WiMax that are important for a basic understanding of each of these and their inter-operability [5]. We do not consider PAN's.

II. IEEE 802.11

The 802.11 family currently includes six over-the-air modulation techniques that all use the same protocol. The most popular (and prolific) techniques are those defined by the b, a, and g amendments to the original standard; security was originally included and was later enhanced via the 802.11i amendment. 802.11n is another modulation technique that has recently been developed; the standard is still under development, although products designed based on draft versions of the standard are being sold.

Other standards in the family (c-f, h, j) are service enhancements and extensions or corrections to previous specifications. 802.11b was the first widely accepted wireless networking standard, followed, somewhat counter-intuitively, by 802.11a and then 802.11g.

All IEEE 802.11 versions use CSMA/CA as the multiple access technique and TDD for duplexing, and allow for 12 – 13 (see Sec. III) parallel frequency channels.

A. IEEE 802.11a

The 802.11a amendment to the original IEEE 802.11 standard was ratified in 1999. The 802.11a standard uses the same core protocol as the original standard, operates in 5GHz band, and uses a 52-subcarrier Orthogonal Frequency-Division Multiplexing (OFDM) with a maximum raw data rate of 54Mbps, which yields realistic net achievable throughput in the mid-20Mbps. The advantages of using OFDM include reduced multi-path effects in reception and increased spectral efficiency. The data rate is reduced to 48, 36, 24, 18, 12, 9 then 6Mbps if required. *802.11a has 12 non-overlapping channels, 8 dedicated to indoor and 4 to point to point. It is not inter-operable with 802.11b, except if using equipment that implements both standards*.

Since the 2.4GHz band is heavily used, using the 5GHz band gives 802.11a the advantage of less interference. However, this high carrier frequency also brings disadvantages. *It restricts the use of 802.11a to almost line of sight*, necessitating the use of more access points; it also means that 802.11a cannot penetrate as far as 802.11b since it is absorbed more readily, other things (such as power) being equal.

B. IEEE 802.11b

The 802.11b amendment to the original standard was ratified in 1999. IEEE 802.11b has a maximum raw data rate of 11Mbps and uses the same CSMA/CA media access method defined in the original standard. Due to the CSMA/CA protocol overhead, in practice the maximum 802.11b throughput

[1]Part of the text in this report was copied directly from Wikipedia[2] or the standard documents. The rest was gleaned from sources cited or condensed from general reading and own past knowledge.

that an application can achieve is about 5.9Mbps using TCP and 7.1Mbps using UDP.

Since 802.11b is a direct extension of the DSSS (Direct-Sequence Spread Spectrum)[2] modulation technique defined in the original standard, 802.11b products appeared on the market very quickly. Technically, the 802.11b standard uses Complementary Code Keying (CCK) as its modulation technique, which is a variation on CDMA and was first suggested by Golay in 1961[4]. It is not a simple technique to understand and not much can be found in the wireless communication literature. Chip sets and products were easily upgraded to support the 802.11b enhancements. The dramatic increase in throughput of 802.11b (compared to the original standard) along with substantial price reductions led to the rapid acceptance of 802.11b as the definitive wireless LAN technology.

IEEE 802.11b is usually used in a point-to-multi-point (PMP) configuration, wherein an *Access Point (AP)* communicates via an omni-directional antenna with one or more clients that are located in a coverage area around the access point. Typical indoor range is 30m at 11Mbps and 90m at 1Mbps. With high-gain external antennas, the protocol can also be used in fixed point-to-point (PTP) arrangements, typically at ranges up to 8Km although some report success at ranges up to 80-120Km where line of sight (LOS) can be established.

C. IEEE 802.11g

In June 2003, a third modulation standard was ratified: 802.11g. This flavour works in the 2.4GHz band (like 802.11b) but operates at a maximum raw data rate of 54Mbps, or about 24.7Mbps net throughput (like 802.11a). 802.11g hardware will work with 802.11b hardware. Details of making b and g work well together occupied much of the lingering technical process.

In older networks, however, the presence of an 802.11b participant significantly reduces the speed of an 802.11g network. The modulation scheme used in 802.11g is OFDM for the data rates of 6, 9, 12, 18, 24, 36, 48, and 54Mbps, and reverts to (like the 802.11b standard) CCK for 5.5 and 11Mbps and DBPSK/DQPSK+DSSS[3] for 1 and 2Mbps.

Even though 802.11g operates in the same frequency band as 802.11b, it can achieve higher data rates because of its similarities to 802.11a. The maximum range of 802.11g devices is slightly greater than that of 802.11b devices, but the range in which a client can achieve full (54Mbps) data rate speed is much shorter than that of 802.11b.

D. IEEE 802.11n

In January 2004 IEEE announced that it had formed a new 802.11 Task Group to develop a new amendment to the 802.11 standard for wireless local-area networks. The real data throughput is estimated to reach a theoretical 540Mbps (which may require an even higher raw data rate at the physical layer), and should be up to 50 times faster than 802.11b, and up to 10 times faster than 802.11a or 802.11g.

802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput through spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti[4] coding.

E. IEEE 802.11s

This is the unapproved IEEE 802.11 standard for Extended Service Set (ESS) Mesh Networking. It specifies an extension to the IEEE 802.11 MAC to solve the inter-operability problem by defining an architecture and protocol that support both broadcast/multicast and unicast delivery using "radio-aware metrics over self-configuring multi-hop topologies."

F. IEEE 802.11T

The IEEE 802.11T is also referred to as the Wireless Performance Prediction (WPP) – test methods and metrics recommendation. Given the complexity of the IEEE 802.11 family of protocols, a test specification is particularly important so that products specifications and performance can be ascertained. The capital T in the name shows this is a "recommended practice" and not a standard.

The goal of the 802.11T project is to provide a set of measurement methods, performance metrics, and test recommendations that enable manufacturers, independent test labs, service providers, and end users to measure the performance of IEEE 802.11 standard equipment and networks.

III. Channels in 802.11

Wi-Fi consists of unlicensed channels 1-13 from 2412MHz to 2484MHz in 5MHz steps. That is, 802.11b and 802.11g (as well as 802.11n when using the 2.4GHz band) divide the 2.4GHz spectrum into 13 overlapping, staggered channels whose center frequencies are 5MHz apart.

The 802.11b, and 802.11g standards do not specify the width of a channel; rather, they specify the center frequency of the channel and a spectral mask for that channel. The spectral mask for 802.11b requires that the signal be attenuated by at least 30dB from its peak energy at $\pm$11MHz from the center frequency, and attenuated by at least 50dB from its peak energy at $\pm$22MHz from the center frequency.

IV. Security aspects of 802.11x

IEEE enhanced 802.11 with certain security measures at the MAC layer to produce 802.11i. In particular, the 802.11i extension specifies two classes of security algorithms:

- Algorithms for establishing a Robust Security Network Association (RSNA).
- Pre-RSNA algorithms. These algorithms originated from the original IEEE 802.11 standard.

Pre-RSNA algorithms cover data confidentiality as well as authentication mechanisms. Apart from Open Systems Authentication, pre-RSNA algorithms are in fact deprecated and

[2]Refer to Sec. XI for a basic description of DSSS

[3]See Sec. XI for an explanation of DBPSK, QAM and DQPSK

[4]See Sec. XI for an explanation of Alamouti coding

Data rate(MBps)	Modulation	Coding rate	Ndbps	1472 byte transfer time (μs)
6	BPSK	1/2	24	2012
9	BPSK	3/4	36	1344
12	QPSK	1/2	48	1008
18	QPSK	3/4	72	672
24	16-QAM	1/2	96	504
36	16-QAM	3/4	144	336
48	64-QAM	2/3	192	252
54	64-QAM	3/4	216	224

TABLE I
IEEE 802.11A DATA RATES, MODULATION AND CODING TECHNIQUES

their use is discouraged and while they are comprehensive, we do not report on them here.

Owing to the fact that the security provided in the original IEEE 802.11 standard was inadequate and found to be flawed in many areas, the IEEE defined a security amendment known as IEEE 802.11i. IEEE 802.11i introduces what is known as Robust Security Network Association (RSNA) algorithms which provide security enhancements over the original 802.11 standard in the areas of station authentication, authorization, key management, and data confidentiality.

A. RSNA Station Authentication

IEEE 802.11 RSNA algorithms support two methods for stations to perform authentication:

1) 802.1X port based authentication using the Extensible Authentication Protocol (EAP) which uses the uncontrolled/controlled port model to authorize and control data flow between an authenticator/Access-Point (AP) and any supplicant(s).
2) and Pre-Shared Key (PSK) authentication.

When using 802.1X EAP authentication, authentication information is exchanged between an authenticator and a supplicant in a 802.11 data frame via the 802.1X uncontrolled port. The 802.1X controlled port is blocked and restricts general data flow between the two stations until an 802.1X authentication procedure completes successfully. The 802.1X EAP procedure also makes use of another party known as the authentication Server (AS), commonly implemented as a RADIUS server. IEEE 802.11 assumes a secure connection between AS and AP. The entire authentication process can be broken into several stages, briefly explained as follows:

A station/supplicant first determines the security policy of the AP. This is achieved by either monitoring beacon frames sent by the AP, or through active probing by the supplicant station. At this stage, the supplicant remains unauthenticated and disassociated from the AP. An initial authentication and association between the station and AP then takes place via a series of authentication and association requests and responses. This initial authentication is Open Systems authentication and is only kept for backward compatibility. The association between the station and AP is used to establish security parameters prior to further authentication. At this stage the station is weakly authenticated and associated, however the 802.1X controlled port remains blocked. This series of exchanges is indicated in figure 1.

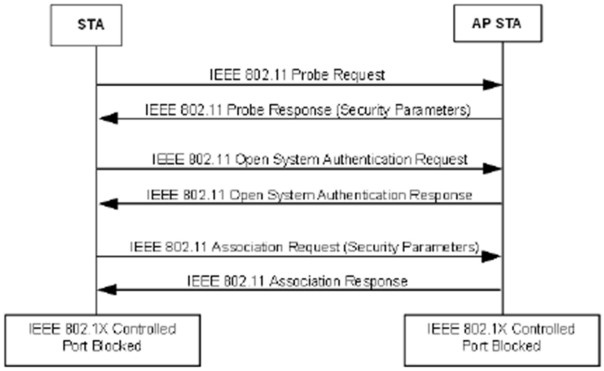

Fig. 1. Initial authentication and association stage of a 802.11 RSNA establishment

If 802.1X authentication is used, the EAP authentication process commences. This process is initiated either by the AP sending the supplicant station an EAP-Request message, or by the supplicant sending the AP an EAP over LAN (EAPOL) Start message. The supplicant and AS then perform mutual authentication using an EAP authentication protocol, most commonly using EAP Tunneled Transport Layer Security (EAP-TTLS), whilst the AP serves as a relay point. During this stage the supplicant and AS generate and establish a common Pairwise Master Key (PMK); in addition, the AS provides the AP with the required material allowing the AP to generate the same PMK. If static pre-shared keys are configured, these keys can serve as the PMK and the 802.1X EAP stage can be skipped. This stage is illustrated in figure 2.

The final stage of the RSNA establishment procedure consists of a 4-way handshake between the supplicant and AP. The supplicant and AP first confirm the existence of a common PMK. A fresh

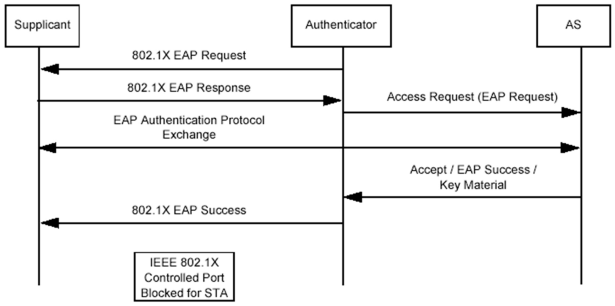

Fig. 2. 802.1X EAP Mutual authentication and PMK establishment

Pairwise Transient Key (PTK) is then established and cipher suite parameters selected for the following data session. This stage may also be used to distribute a Group Transient Key (GTK) to the supplicant. Upon successful completion of this stage, the AP and supplicant have established a security association between them and the 802.1X controlled port is unblocked to permit general data traffic. The 4-way handshake is illustrated in figure 3.

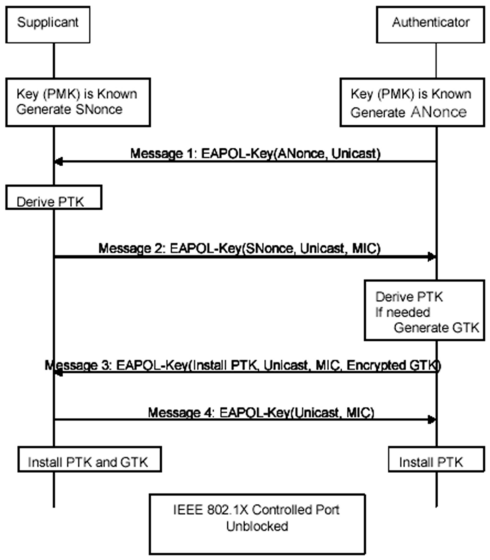

Fig. 3. 4-way Handshake between supplicant and authenticator

B. Data Confidentiality

The IEEE 802.11i amendment supports two algorithms for data privacy:

1) The Temporal Key Integrity Protocol (TKIP) offers many enhancements over the Wired Equivalent Privacy (WEP), the data confidentiality mechanism defined in 802.11. In summary, TKIP uses a 128-bit temporal key which when combined with the MAC address of the station and a 16-octet IV, is used for encryption. The temporal key is shared amongst clients and access points. Although TKIP also uses the RC4 stream cipher for encryption, one significant difference is that TKIP periodically refreshes temporal keys. TKIP uses a Message Integrity Code (MIC) known as *Michael* as an improvement over WEP's ICV in order to ensure the integrity of a message. TKIP is only a temporary solution to improve on the shortcomings of WEP.
2) Enterprise Access Server (AES) in Counter Mode CBC-MAC Protocol (CCMP) mode. This method offers the highest security in terms of encryption and integrity. A 128-bit AES key is used for encryption; the AES-CCMP algorithm also provides a MIC over the entire message for integrity purposes.

V. IEEE 802.16

WiMAX is defined as *Worldwide Interoperability for Microwave Access* by the WiMAX Forum, formed in April 2001 to promote conformance and inter-operability of the standard IEEE 802.16, also known as *WirelessMAN*.

The WiMAX IEEE 802.16 media access controller is significantly different from that of IEEE 802.11 WiFi MAC. In WiFi, the MAC uses contention resolution access. All subscriber stations going through a single Access Point (AP) are competing for the AP's attention on a random basis. This can cause distant nodes from the AP to be repeatedly interrupted by less sensitive, closer nodes, greatly reducing their throughput. This makes services, such as VoIP or IPTV which depend on a determined level of quality of service (QoS) difficult to maintain for large numbers of users.

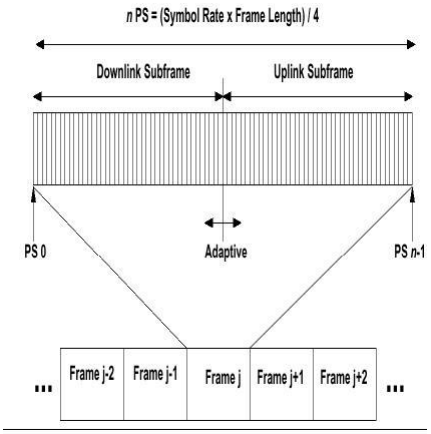

Fig. 4. General IEEE 802.16 TDD Frame (10–66 GHz)

In contrast, the 802.16 MAC, where Access Points are now called *Base Stations (BS)*, is a scheduling MAC where the *Subscriber Station (SS)* only has to compete once, for initial entry into the network. After that it is allocated a time slot by the BS as indicated in Figure 4. The time slot can expand and constrict, but it remains assigned to the SS meaning that other subscribers are not supposed to use it but rather take their turn in time. Unlike 802.11, this scheduling algorithm is stable under overload and over-subscription. It is also much more

bandwidth efficient. The scheduling algorithm also allows the base station to control QoS by balancing the assignments among the needs of the SSs[5].

Uplink scheduling is performed by the BS with the intent of providing each connected SS with the bandwidth requested for uplink transmissions as illustrated in Figure 5. By specifying a scheduling service type and its associated QoS parameters, the BS scheduler can anticipate the throughput and latency needs of the uplink traffic and provide polls and/or grants at the appropriate times.

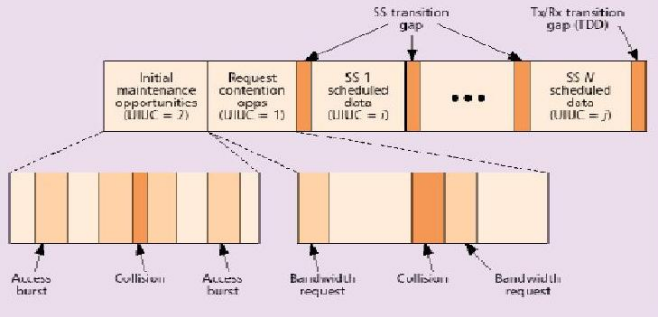

Fig. 5. IEEE 802.16 TDD Uplink frame structure

Downlink scheduling is performed by the BS as illustrated in Figure 6 and is much more versatile, and therefore more complex, than the uplink. The BS is the only transmitter operating in this direction and therefore operates in a PMP mode. All SSs capable of listening to that portion of the down-link sub-frame listens and if the DIUC is its own, it will copy the corresponding PDU. Since the BS is in full control, it can send data to an SS using a negotiated burst profile. The data are transmitted in order of decreasing robustness to allow SSs to receive their data before being presented with a burst profile that could cause them to lose synchronization with the down-link[3].

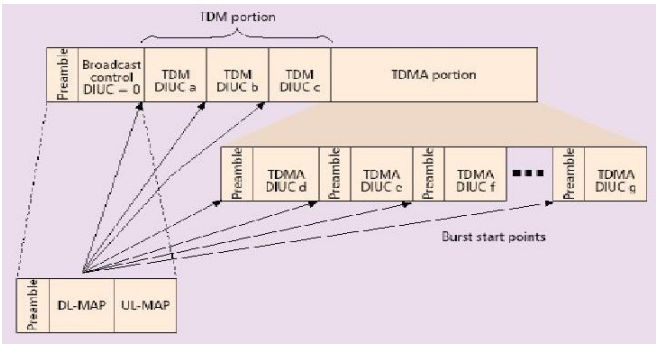

Fig. 6. IEEE 802.16 Downlink frame structure

A recent addition to the WiMAX standard is underway which will add full mesh networking capability by enabling WiMAX nodes to simultaneously operate in *subscriber station* and *base station* mode. This will blur that initial distinction and allow for widespread adoption of WiMAX based mesh networks and promises widespread WiMAX adoption. WiMAX/802.16's use of Orthogonal Frequency Division Multiple Access (OFDMA)which works by assigning a subset of sub-carriers to individual users allows wireless mesh networks to be much more robust and reliable.

The original WiMAX standard, IEEE 802.16, specifies WiMAX in the 10 to 66GHz range. IEEE 802.16a, updated in 2004 to 802.16-2004, added support for the 2 to 11GHz range, of which most parts are already unlicensed internationally and only very few still require domestic licenses. Most business interest will probably be in the 802.16-2004 standard, as opposed to licensed frequencies.

The WiMAX specification improves upon many of the limitations of the WiFi standard by providing increased bandwidth and stronger encryption. It also aims to provide connectivity between network endpoints without direct line of sight in some circumstances. The details of performance under non-line of sight (NLOS) circumstances are unclear as they have yet to be demonstrated. It is commonly considered that spectrum under 5-6GHz is needed to provide reasonable NLOS performance and cost effectiveness for PTMP (point to multi-point) deployments.

IEEE 802.16 can provide flexible QoS offerings, such as

- Constant Bit Rate (CBR).
- Real-time Variable Bit rate (rt-VBR).
- Non real-time VBR (nrt-VBR).
- BE, with granularity within classes.

VI. Various 802.16 standards

The following is a listing of the various, current versions of 802.16:

A. 802.16

The original standard, published in April 2002. This defines a MAC layer and several physical layer specifications. The MAC supports FDD and TDD, as well as real-time adaptive modulation and coding. The high frequencies limit the use to line-of-sight. The physical layer of the standard covers the spectrum from 10 to 66GHz, which includes the LMDS bands.

B. 802.16a

A completed amendment that extends the physical layer to the 2 to 11GHz spectrum range. The 802.16a standard also specifies three possible modulations: single carrier, 256 OFDM, and orthogonal frequency division multiple access (OFDMA). The lower frequencies make non-line of sight a possibility, which can also be helped by OFDM's ability to handle multi-path signals. Range can be up to 50 kilometers, with typical cell footprints in the 6 to 10 kilometer range. Total data rate can be up to 100Mbps in each 20MHz channel. This extension is the focus of the WiMAX Forum.

C. 802.16c

This standard specifies profiles, conformance standards, and test suites for 802.16 (10-66GHz) implementations. The profiles are completed, but the conformance tests are still in development.

[5]Scheduling has many open research questions

D. 802.16d

This standard specifies system profiles for 802.16a (2-11GHz) implementations with the working group still in progress.

E. 802.16e

A nascent effort to extend the 802.16a standard for portability or mobile clients. At the beginning of 2006 it was still very early in the process.

VII. Security in IEEE802.16

Security in IEEE 802.16 is provided by a security sub-layer that lies within the MAC layer just above the physical layer. The security sub-layer provides the following two main functions:

1) An encapsulation protocol that provides data packet encryption services for packet transmission over the network. The protocol defines the set of supported cryptographic suites and algorithms, and rules on how the algorithms must be applied to MPDU payloads.
2) Key Management Protocol (PKM) which defines the secure distribution, synchronization, and refreshing of keying material between an SS and BS. The PKM also enforces authentication and conditional authorization to network services.

Prior to explaining these 2 functions, the concept of a Security Association (SA) will be briefly introduced. The IEEE 802.16 MAC layer is connection orientated. There are two types of connections namely, management connections, and data connections. IEEE 802.16 uses the concept of an SA to define the security parameters associated with a particular connection. An SA is a set of security parameters that a BS shares with one or more of it's SSs to enable secure communication flows across the 802.16 network. An SA is identified by its Security Association Identity (SAID).

A. Key Management Protocol

An SS node begins authorization by sending an `Authorization Request` message to a chosen BS. Included in the request are the SS's credentials (X.509 Certificate), and the cryptographic algorithms that the requesting SS supports.

The BS verifies the credentials presented by the SS and determines common security suites and parameters. The BS responds with a `Authorization Response`. Included in the response is an Authorization Key (AK) encrypted with the SS's Public Key from the X.509 certificate and the identities (SAIDs) of the SAs that the SS is authorized to obtain keying information for. Using the AK, the BS and SS can generate a common Key Encryption Key (KEK) and two message authentication keys (HMACs), one for uplink and one for downlink directions.

In order for the data connections to be encrypted between the BS and SS, the BS and SS require common keying material for the security associations that are associated with those services/connections. An SS can request the keying material known as a Traffic Encryption Key (TEK) for a specific security association from the BS. To acquire the TEK for a specific SA, the SS must send a TEK key request containing the SAID of the desired SA. If the SS is authorized for the requested SA, the BS will generate a reply with the following information:

1) The encrypted TEK for the requested SA. Encryption of the TEK is performed using the KEK or the RSA public key of the requesting SS.
2) The sequence number of the AK being used due to periodic refreshing of the AK.
3) The IV that will be used by the encapsulation protocol for data encryption.

The message authentication keys in the request and reply are used to provide message integrity and proof of the KEK. The TEK request sequence is illustrated in figure 7.

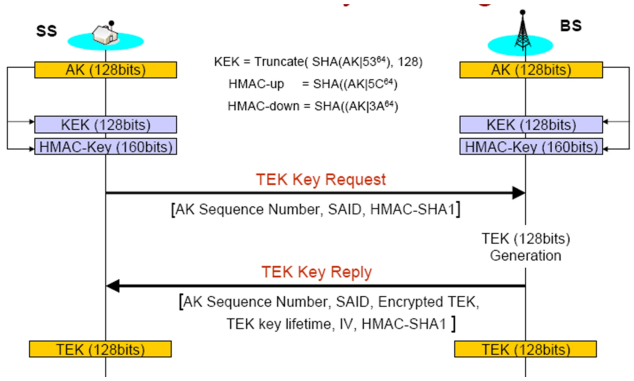

Fig. 7. A TEK key request and Reply between SS and BS

B. Data Confidentiality

IEEE 802.16 supports two different algorithms for data encryption:

1) DES in Cipher Block Chaining (CBC) Mode. A 56 bit DES key (TEK) is used. This method does not provide message integrity or replay protection.
2) AES in CCM (Counter with CBC-MAC) mode. A 128 bit AES key (TEK) is used. This method does provide a message integrity check, and provides replay protection using packet numbers.

VIII. Summary of 802.16

The following provides a summary of the most salient facts on 802.16:

1) On the uplink the SS is allotted a variable length TDMA slot.
2) On the downlink the SS is addressed in a Time Division Multiplex (TDM) stream.
3) Time-Division Duplex (TDD):
   - Uplink and downlink time-share the same Radio Frequency (RF) channel.
   - Uplink and downlink are not symmetric and vary dynamically.

4) Frequency-Division Duplex (FDD):
   - Downlink and uplink are on separate RF channels
   - Half-duplex SSs are supported.
   - Uplink and downlink are not symmetric and are statically assigned.
5) SSs do not transmit and receive simultaneously thus saving cost.

IX. Comparison

Table II summarizes the main features of the 802.11 and 802.16 standards mentioned above.

X. Commercial offerings in RSA

The following WiMax products are currently available in South Africa.

A. Alcatel–Lucent

Alcatel-Lucents vision sees the provision and enhancement of user-centric broadband-based communication and entertainment networks. Their network architectures deliver broadband services for *Triple Play* and *IPTV* and exploit the services offered by *IP Multimedia Subsystem* (IMS) by integrating these services into their network products.

Their *OmniAccess switch* product supports up to 512 Access Points (APs) on a single Wireless-LAN (WLAN) appliance. Security is based on the IEEE 802.11i standard specification and mobility is supported. Each WLAN AP supports IEEE 802.11 b/a/g user access and sub-5 millisecond handoff between APs.

Alcatel-Lucent products are being developed to cater for WiMAX Wireless-MAN (WMAN) technologies. Their WiMAX solution is based on IEEE 802.16 e-2005 . It allows for IP high-speed data and mobility. Unbound broadband data, Voice over IP (VoIP) and gaming/video services are possible. This product is available in the 2.3, 2.5 and 3.5GHz licensed frequency bands.

Another product is the Alcatel-Lucent Unlicensed Mobile Access (UMA). A specific version of this application, the Alcatel-Lucent 1430 Unified Home Subscriber Server (HSS), can support Authentication, Authorization and Accounting (AAA) for a WiMAX- or WiFi-deployed operator's architecture. Specifically, it can support the WiMAX authentication specific model, (Extensible Authentication Protocol) (EAP) Tunneled Transport Layer Security (TLS) Authentication Protocol (EAP-TTLS).

Alcatel-Lucent is focussed on the user-centric aspects of solutions that involve Fixed-to-Mobile Convergence (FMC), Public Switched Telephone Network (PSTN)-to-Next Generation Network (NGN), Wireless Broadband Access (WBA) solutions, and the exploitation of IMS-services.

B. iBurst

iBurst is a South African wireless broadband internet service provider (ISP). Their pure IP, end-to-end system is based on IntelliCell technology - developed by the US company ArrayComm - and consists of two components: The network operator-deployed base stations (BSs) (with a maximum base station capability of 20 Mbps) and the wireless modems that connect to the BSs. Ideally their system can support up to ten users (but is capable of coping with more) and mobile nodes moving no faster than 100km/h.

The iBurst system protocol is capable of supporting 16 Mbps per user, but offers an initial 1 Mbps downlink and 345Kbps uplink data rates per user to its clients. The upgrade of the iBurst system promises twice the current data rate capabilities, maintaining the 3:1 throughput asymmetry. The medium access methods are Time Division Duplexing (TDD), Time Division Multiple Access (TDMA) and Spacial Division Multiple Access (SDMA) with a channel spacing of 625KHz. A spectral efficiency of 4 bps/Hz/cell is obtained by multiplying the three time slots allocated per carrier by the 475Kbps allocated to each slot and then dividing this by the 625KHz carrier as well as the 0.5 reuse factor.

Other features of the air interface include Forward Error Correction (FEC) and Automatic Repeat Request (ARQ) for error-free linkage within the coverage area, dynamic resource allocation with bandwidth on demand, and full mobility (handover) support. The system also supports built-in air interface Quality of Service (QoS).

ArrayComm is developing the remaining iBurst air interface system elements through the IEEE 802.20 working group. This Working Group (WG) is more colloquially known as the Mobile Broadband Wireless Access (MBWA) WG. It has as goal similar to that of the IEEE 802.16 e (mobile WiMAX). The iBurst MBWA system was adopted as one of the two initial technical specifications of this WG on 19 January 2006.

XI. Definitions

DIRECT SEQUENCE SPREAD-SPECTRUM (DSSS): transmissions multiply the data being transmitted by a "noise" signal. This noise signal is, as is the case for CDMA, a pseudo-random sequence of 1 and -1 values, at a frequency much higher than that of the original signal, thereby spreading the energy of the original signal into a much wider band.

The resulting signal resembles white noise, like an audio recording of "static", except that this noise can be filtered out at the receiving end to recover the original data, by again multiplying the same pseudo-random sequence to the received signal (because 1 1 = 1, and -1 -1 = 1). This process, known as "de-spreading", mathematically constitutes a correlation of the transmitted PN sequence with the receiver's assumed sequence.

DIFFERENTIAL QUADRATURE PHASE SHIFT KEYING (DQPSK): Instead of using the bit patterns to set the phase of the wave, it can instead be used to change it by a specified amount. The demodulator then determines the changes in the phase of the received signal rather than the phase itself. Since this scheme depends on the difference between successive phases, it is termed *differential quadrature phase-shift keying*[4].

DIFFERENTIAL BINARY PHASE SHIFT KEYING (DBPSK): The same as DQPSK except that it uses two instead of four

Feature	802.11	802.11b	802.11a	802.11g	802.16	802.16a
Media Access Method	CSMA/CA				TDM downlink, TDMA uplink	
Duplexing mode	TDD				TDD, FDD and H-FDD	TDD, FDD and H-FDD
Assigned spectrum	2.4 GHz or infrared	2.4 GHz	5.8 GHz	2.4 GHz	10 – 66 GHz	2 - 11 GHz
Maximum throughput	2 Mbps	11 Mbps	54 Mbps			70 Mbps
Propagation distance	up to 180 metres				up to 50 kilometres	
Network architecture supported	PTMP				PTP, PTCM	PTMP, PTCM, mesh
Transport protocols supported	Ethernet				TCP, ATM	TCP, ATM
Modulation Technique	FHSS or DSSS	DSSS with CCK	OFDM	OFDM with CCK and DSSS	QUAM, PSK	OFDM
Adaptive modulation	No				Yes	
Support for full mobility	No					Upcoming
QoS support	Same policy for all connections to a single AP				UGS-, rtPS-, nrtPS-, BE service	

TABLE II
A COMPARATIVE TABLE OF CERTAIN IEEE STANDARDS AND AMENDMENTS FOR WGS 11 AND 16

points in the 360° circle.

QUADRATURE AMPLITUDE MODULATION (QAM): QAM conveys data by changing some aspect of a carrier signal, or the carrier wave, (usually a sinusoid) in response to a data signal. In the case of QAM, the amplitude of two waves, 90 degrees out-of-phase with each other (in quadrature) are changed (modulated or keyed) to represent the data signal.

SPACETIME BLOCK CODING OR ALAMOUTI CODING: This a technique used in wireless communications to transmit multiple copies of a data stream across a number of antennas and to exploit the various received versions of the data to improve the reliability of data-transfer. The fact that transmitted data must traverse a potentially difficult environment with scattering, reflection, refraction and so on as well as be corrupted by thermal noise in the receiver means that some of the received copies of the data will be "better" than others. This redundancy results in a higher chance of being able to use one or more of the received copies of the data to correctly decode the received signal. In fact, spacetime coding combines all the copies of the received signal in an optimal way to extract as much information from each of them as possible.

BASE STATION (BS):The radio receiver/transmitter that serves as the hub of a local wireless network, and which may also be the gateway between a wired network and the wireless network. In the IEEE802.16 standards AP's of the IEEE 802.11, are called stations.

ACCESS POINT (AP): A central communication point or node or server to which client wireless communication devices connect.

SUBSCRIBER STATION (SS): Client wireless devices devices connecting to a BS or Access Point (AP).

EXTENDED SERVICE SET (ESS): This definition is set forth in the IEEE 802.11-1999 standard. An ESS is a set of one or more interconnected BSs and integrated local area networks (LANs) that appear as a single BS to the logical link control layer at any station associated with one of those BSs. The set of interconnected BSs must have a common Network Name or SSID. They can work in the same channel, or work in different channels to boost aggregate throughput.

MULTIPLE INPUT MULTIPLE OUTPUT (MIMO): A system employing at least two transmit antennas and at least two receive antennas to improve the system capacity, coverage or throughput.

REFERENCES

[1] IEEE 802 standards.
[2] Wikipedia: The free encyclopedia.
[3] C.ECKLUND. IEEE Standard 802.16: A technical overview of the WirelessMAN Air Interface for broadband wireles access. *IEEE Communications Magazine* (June 2002).
[4] HAMMONS, A., AND GAMAL, H. The theory of space-time codes for PSK modulation. *IEEE Trans. Information Theory 46*, 2 (March 2000).
[5] HIERTZ, G., AND MAX, S. E. A. Wireless mesh networks in the IEEE LMSC. In *Proceedings of Global Mobile Congress 2006* (Beijing, China, Oct 2006), p. 6.