

---

---

# Indoor WLAN Design

*Part IX: 802.11i*

**Kjell Jørgen Hole**  
UiB

Last updated 10.02.09  
Mail: [Kjell.Hole@ii.uib.no](mailto:Kjell.Hole@ii.uib.no)  
URL: [www.kjhole.com](http://www.kjhole.com)

## Outline

---

[KJhole.com](http://KJhole.com)

- Is WPA (or TKIP) good enough?
- Introduction to the AES block cipher
- The AES-CCM protocol used in 802.11i
- **Security recommendations**
- Introduction to WiMax
- WiMax versus Wi-Fi and 3G

## WPA

---

- WPA is better than WEP
- Unfortunately, all is not well with WPA:
  - weak integrity check (Michael)
  - weaknesses in the key mixing
- There is a need for a better security standard, not based on WEP
- 802.11i, or WPA2, is one answer to this need
  - 802.11i is based on the Advanced Encryption Standard (AES)

9.3

## AES—Advanced Encryption Standard

---

**AES** Block cipher for the protection of sensitive, unclassified information. Standardized by NIST (National Institute of Standards and Technology) in May of 2002, see FIPS 197

- divides a message into 128-bit blocks of data
- encrypts and decrypts the 128-bit blocks
- key size can be set to 128, 192, or 256 bits
- Different *modes of operation* convert between plaintext messages and 128-bit encrypted blocks

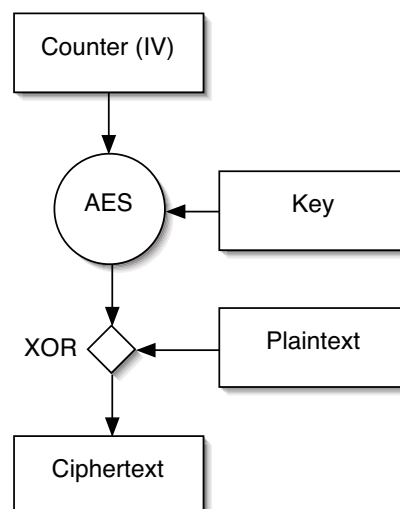
9.4

## Counter Mode

- The **counter mode** does not use the AES block cipher directly to encrypt a data block
- Instead, a 128-bit Initialization Vector (IV), denoted the **counter**, is first encrypted and then XORed with the data block
- The IV is changed for each new 128-bit block. It is initialized from a nonce and incremented by 1 for each new message
  - note that two identical blocks of data result in different encrypted blocks because the data blocks are XORed with different encrypted IV values

9.5

## Illustration of Counter Mode



9.6

- AES is used as a *stream cipher*
- Decryption is the same as encryption because XORing the same value twice return the original value
  - only necessary to implement AES encryption
- Encryption of multiple blocks can be done in parallel with a bank of AES encryption devices because the counter values are known at the start
- It is not necessary to pad the last (short) block with zeroes

9.7

## Counter Mode + CBC MAC = CCM

---

- The *Counter Mode with CBC MAC\** (**CCM**) protocol, also denoted CCM mode, defines a set of rules that uses the AES block cipher to enable both message
  - encryption
  - authentication
- CCM is described by Doug Whiting, Russ Housley, and Niels Ferguson in RFC 3610
- The CCM mode is approved by NIST as a general mode for use with AES

\*Cipher Block Chaining Message Authentication Code

9.8

## Message Authentication with CBC MAC

---

- In addition to the counter mode, CCM utilizes *Chiper Block Chaining* (**CBC**) for message authentication
- CBC produces a MIC (Message Integrity Code)
  - also called a Message Authentication Code (MAC), resulting in the name CBC MAC
- CBC MAC is a well known technique that has been used for many years

9.9

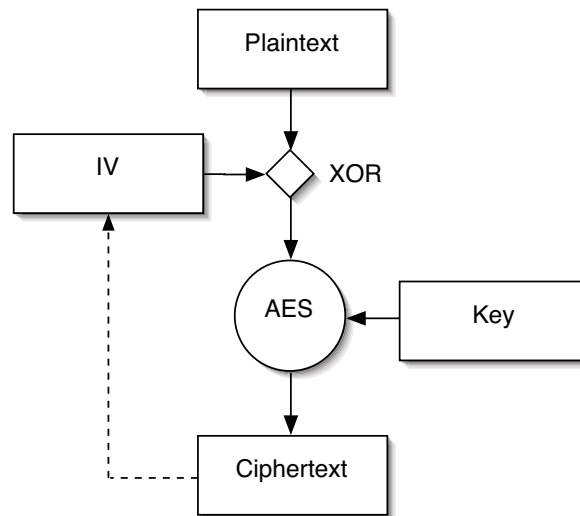
## CBC-MAC Procedure

---

[KJhole.com](http://KJhole.com)

1. Take the first block in the message, XOR it with an IV, and encrypt the result using AES
  2. XOR the encrypted block with the second block in the message and encrypt the result
  3. XOR the result with the third block in the message and encrypt that...and so on
- This CBC-MAC procedure generates a single 128-bit block that combines all the data in the message

9.10



9.11

## CBC-MAC Properties

- The CBC MAC cannot be parallelized
- Requires that the message is an exact number of blocks
  - the CCM protocol provides a solution based on padding

9.12

1. Specification of an IV so successive messages are separated cryptographically
2. Linking together the encryption and the message authentication under a single key
  - note that one should not use the same key for two separate cryptographic functions
  - in this case, the key is used in conjunction with two different IVs, leading to two separate keys

9.13

3. Extension of the authentication to cover data that is not to be encrypted
  - the header of an 802.11 frame is not encrypted, but it is authenticated by CBC-MAC

9.14

## Key Hierarchy Revisited (1)

---

- For unicast communication, a master key, the *Pairwise Master Key* (**PMK**), is generated by the EAP framework and the authentication server
  - MS must store one PMK
  - BS must store one PMK for each associated MS (!)
  - all PMKs are 256 bits long
- 802.1X is used to transmit nonces to the BS and MS. *Encryption* keys, referred to as **temporal keys**, are then generated from the PMK and the nonces

9.15

## Key Hierarchy Revisited (2)

---

[KJhole.com](http://KJhole.com)

- Two sets of temporal keys are generated, *session keys* (or pairwise keys) and *group keys* (or groupwise keys)
- Group keys are shared amongst all the MSs connected to the same BS and are used for multi-cast traffic
- Session keys are unique to each association between an individual MS and the BS
- All temporal keys are 128 bits long

9.16

## Comparisons

KJhole.com

Description	WEP	WPA	WPA2
<i>Cipher</i>	RC4	RC4	AES
<i>Key Size</i>	40 bits	128 bits encryption 64 bits MIC	128 bits
<i>IV length</i>	24-bit	48-bit	48-bit
<i>Packet Key</i>	Concatenated	Mixing Function	Not needed
<i>Data Integrity</i>	CRC-32	Michael	CCM
<i>Header Integrity</i>	None	Michael	CCM
<i>Replay Attack</i>	None	IV Seq.	IV Seq.
<i>Key Management</i>	None	EAP-based	EAP-based
<i>Authentication</i>	N/A	802.1X, EAP	802.1X, EAP

9.17

## Security Recommendations (1)

KJhole.com

- Do not use WEP!
- Only use *WPA Personal* for small, low-risk networks
  - home networks with very few users
- Only use *WPA Enterprise* for small, low-risk office networks
  - plan to upgrade to WPA2

9.18

## **Security Recommendations (2)**

KJhole.com

- Use WPA2 for medium-risk commercial networks
  - utilize EAP-TLS if PKI is available
  - use PEAP or TTLS if there is no PKI
  - avoid authentication with LEAP
- External WPA2 review by Ron Rivest, David Wagner, Phil Rogaway, and others

9.19

## **Security Recommendations (3)**

KJhole.com

- Do not use wireless 802.11 technologies for high-risk networks
  - the real strength of 802.11i is not known
  - cryptographers and security experts must evaluate 802.11i for several more years before it is possible to determine the level of security
  - even if 802.11i is highly secure, the client OS is likely to have a relatively low degree of security, leading to a significant risk of malicious software taking (partial) control of the client

9.20

- Possible to use higher-layer security protocols (IPsec, SSL, SSH) without any protection on the data link layer
- Note that an attacker controlling e.g. an VPN client can use the encrypted tunnel to access the protected network
  - use firewall and antivirus software on client

9.21

**WiMax**

9.22

- **WiMax** (Worldwide Interoperability for Microwave Access) is the brand name for wireless products conforming to the IEEE 802.16-2004 standard
- WiMax specifies communication between *fixed* stations in the 10 to 66 GHz range and the 2 to 11 GHz range
- An amendment 802.16-2005 (formerly called 802.16e) introduces multiple antenna communication and supports *mobile* systems with speed up to 120 km/h

9.23

- WiMax utilizes Orthogonal Frequency Division Multiplexing (OFDM) signaling with 256 subcarriers
- The 10 to 66 GHz frequency range requires Line-of-Sight (LoS) signal propagation between a BS and a Subscriber Station (SS)
- LoS propagation of the signal is not required in the 2 to 11 GHz range

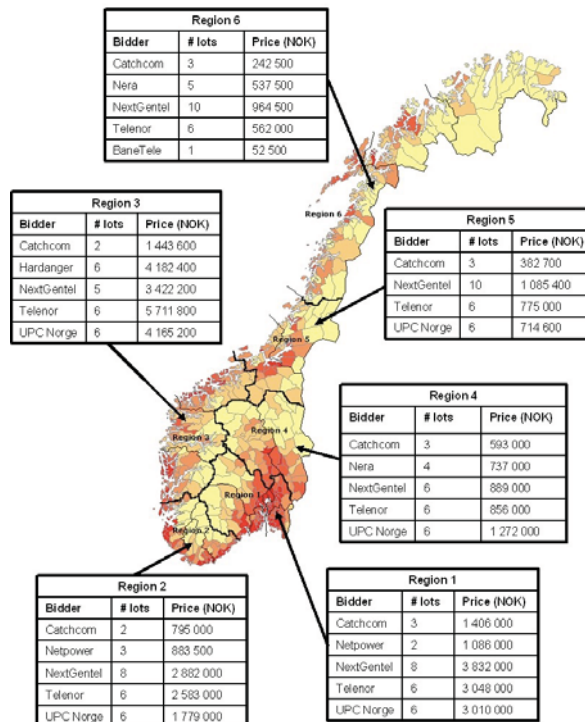
9.24

# WiMax Frequencies (2)

- Unlike other wireless standards, WiMax allows for communication over multiple broad frequency ranges
- Makes it possible to transmit over the frequencies with the least interference
- **Remark.** The lower frequencies are of most commercial interest

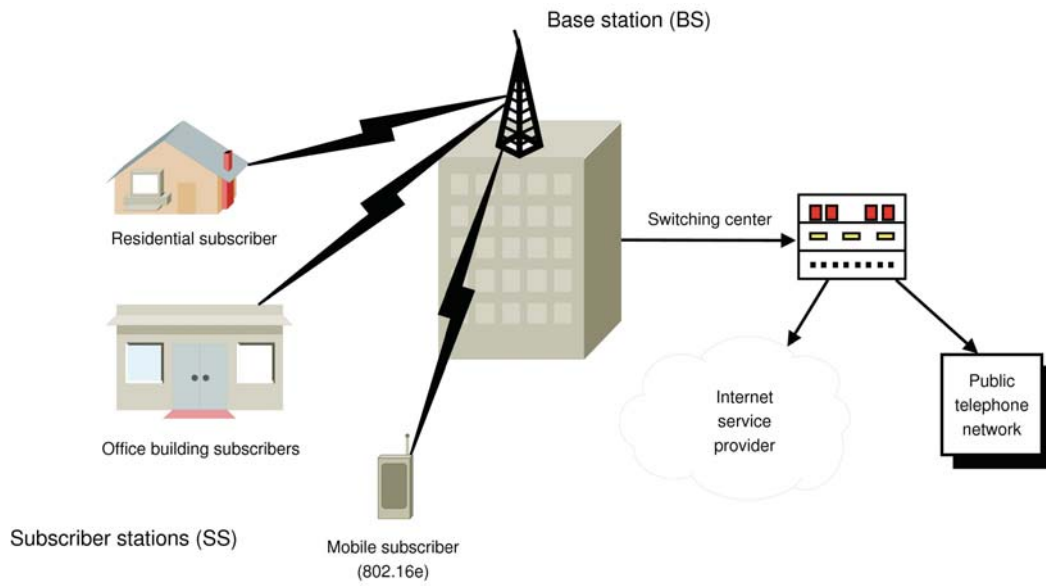
9.25

Results of the Norwegian 3.5GHz auction



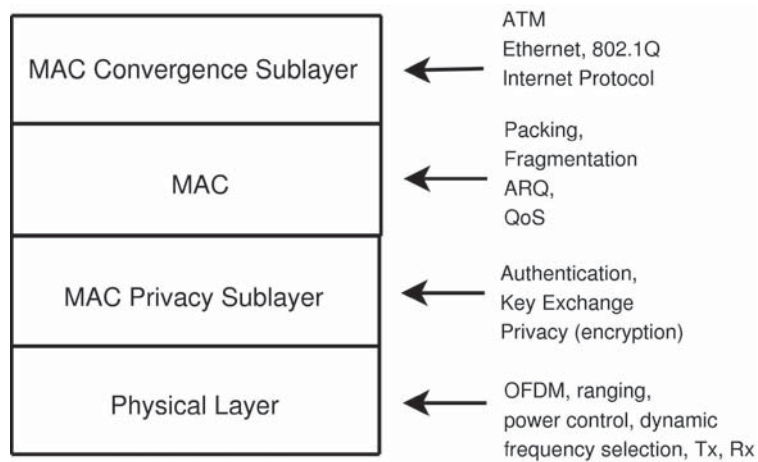
9.26

# Typical WiMax Scenario



9.27

# Protocol Layers



9.28

## MAC Privacy Sublayer

---

KJhole.com

- The Media Access Control (MAC) privacy sublayer consists of two protocols:
  - *Encapsulation protocol* supports authentication and encryption between SS and BS
  - *Key management protocol* distributes keying material from BS to SS

9.29

## MAC Layer (1)

---

KJhole.com

- MAC layer supports multiple high-speed physical layers
  - room for new physical layers in the future
- MAC protocol is connection oriented
- MAC scheduling allocates time slots to stations to maintain a large network throughput

9.30

## MAC Layer (2)

KJhole.com

- MAC supports Quality of Service (QoS) by balancing the needs of the stations
- *Management* connections handle broadcast data, initial ranging, bandwidth requests, and general management messaging
- For each SS, a secondary management connection carries IP management packets

9.31

## Service Range and Data Rates

KJhole.com

- Service range of up to 50 km, but a range of 5 to 8 km more likely in practice
- Practical maximum data rates for 802.16-2004 are between 500kbit/s and 2 Mbit/s for each user (?)
  - early equipment need outdoor antennas
- A WiMax BS may serve as many as 500 customers

9.32

## WiMax vs. Wi-Fi (1)

---

KJhole.com

- While 802.16-2004 is a Wireless Metropolitan Area Network (WMAN) Wi-Fi (802.11a,b,g,h,n) is a short-range indoor network
- WiMax is a wireless alternative to cable and Digital Subscriber Line (DSL) technologies
- **Remark.** To NextGenTel, WiMax is an alternative to the wired (“last mile”) access offered by the telephone company Telenor

9.33

## WiMax vs. Wi-Fi (2)

---

KJhole.com

- Wi-Fi MSs and BSs typically have *omnidirectional* antennas
- WiMax devices and BSs have (multiple) *directional* antennas
- WiMax supports a *fixed* point-to-multipoint network allowing hundreds of users to connect to the Internet via a centrally placed BS
- Wi-Fi supports *mobile* indoor clients

9.34

## WiMax vs. Wi-Fi (3)

---

KJhole.com

- The Wi-Fi MAC protocol uses Carrier Sense Multiple access with Collision avoidance (CSMA/CA) to control access to the communication medium
- WiMax has a MAC protocol that reserves time slots after an initial contention the first time a station wants to access
- Because Wi-Fi utilizes a contention-based MAC protocol, the efficiency goes down as the number of users increases
- The WiMax MAC is able to schedule a large number of users and maintain QoS

9.35

## Uses for WiMax (1)

---

KJhole.com

- 802.16-2004 can serve as a high-speed backbone, connecting 802.11a,b,g,h,n hotspots with each other and other parts of the Internet
- WiMax may serve as a backbone network both in metropolitan and rural areas
- WiMax may be ideal for a wireless ISP (WISP)

9.36

## Uses for WiMax (2)

---

KJhole.com

- In a home scenario, a WiMax transceiver (on an outside wall) will be connected to a Wi-Fi router
  - all PCs in the home connect wirelessly to this Wi-Fi router

9.37

## WiMax vs. 3G (1)

---

KJhole.com

- 802.16-2005 supports mobility and is a competing standard to 3G mobile networks
- It is very expensive and time-consuming for providers to put up radio towers for new cells in a cellular network
- While 3G providers have networks in place, WiMax providers have to build new networks
- Since the service area of a tower decreases with increasing transmit frequency, WiMax providers may have to put up more towers than 3G providers

9.38

- Some 3G providers may install WiMax in existing radio towers to provide better service
- 3G providers have a huge advantage over new WiMax providers in terms of costs
- The mobile WiMax version is not likely to survive in the long run. There may be a smaller market for fixed WiMax links.