

---

---

# WiFi Security

*Part V: 802.11i*

**Kjell Jørgen Hole**  
UiB

Last updated 28.09.11  
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 4G

## WPA

---

- WPA is better than WEP
- Unfortunately, all is not well with WPA:
  - weak integrity check (Michael)
  - weaknesses in the key mixing (not discussed)
- 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)

5.3

## 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

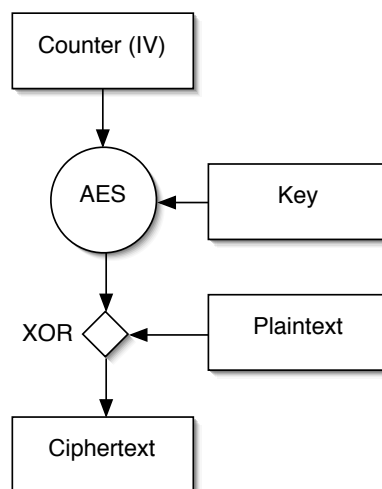
5.4

## 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

5.5

## Illustration of Counter Mode



5.6

## Counter Mode Properties

- 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

5.7

## 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
  - integrity
- 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

5.8

## Message Integrity with CBC MAC

---

- In addition to the counter mode, CCM utilizes *Chiper Block Chaining* (**CBC**) for message integrity
- 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

5.9

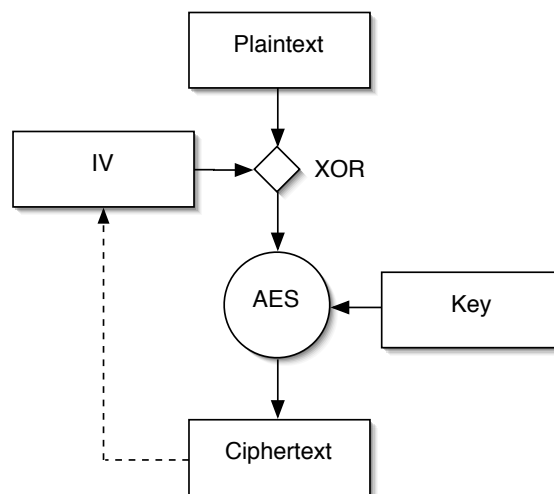
## CBC-MAC Procedure

---

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

5.10



5.11

## 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

5.12

1. Specification of an IV so successive messages are separated cryptographically
2. Linking together the encryption and the message integrity 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

5.13

3. Extension of the message integrity to cover data that is not to be encrypted
  - the header of an 802.11 frame is not encrypted, but its integrity is protected by CBC-MAC

5.14

## 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

5.15

## Key Hierarchy Revisited (2)

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

5.16

## 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

5.17

## Security Recommendations (1)

KJhole.com

- Do not use WEP!
- Only use *WPA Personal* (pre-shared key) for small, low-risk networks
  - home networks with very few users

5.18

## **Security Recommendations (2)**

---

KJhole.com

- Only use *WPA2 Personal* for small, low-risk office networks
- Use *WPA2 Enterprise* for medium-risk commercial networks
  - utilize *EAP-TLS* if *PKI* is available
  - use *PEAP* or *TTLS* if there is no *PKI*

5.19

## **Security Recommendations (3)**

---

KJhole.com

- Do not use wireless *802.11* technologies for high-risk networks
  - even if *802.11i* is highly secure, the client software is likely to have a relatively low degree of security, leading to a significant risk of malicious software taking (partial) control of the client

5.20

- 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

5.21

## WiMax

5.22

- **WiMax** (Worldwide Interoperability for Microwave Access) is the brand name for wireless products conforming to the IEEE 802.16 standards
- “Fixed WiMax” specifies communication between *fixed* stations in the 10 to 66 GHz range and the 2 to 11 GHz range
- “Mobile WiMax” utilizes multiple antenna communication below 6GHz to support *mobile* systems with speed up to 120 km/h

5.23

## WiMax Frequencies (1)

---

- 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

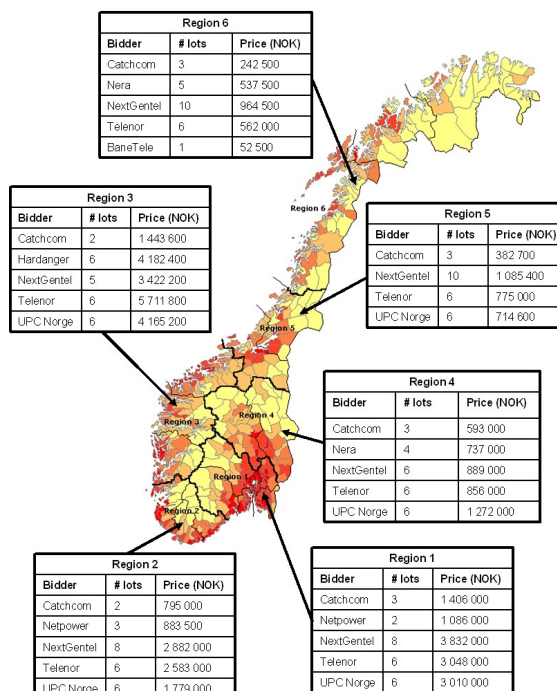
5.24

# 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

5.25

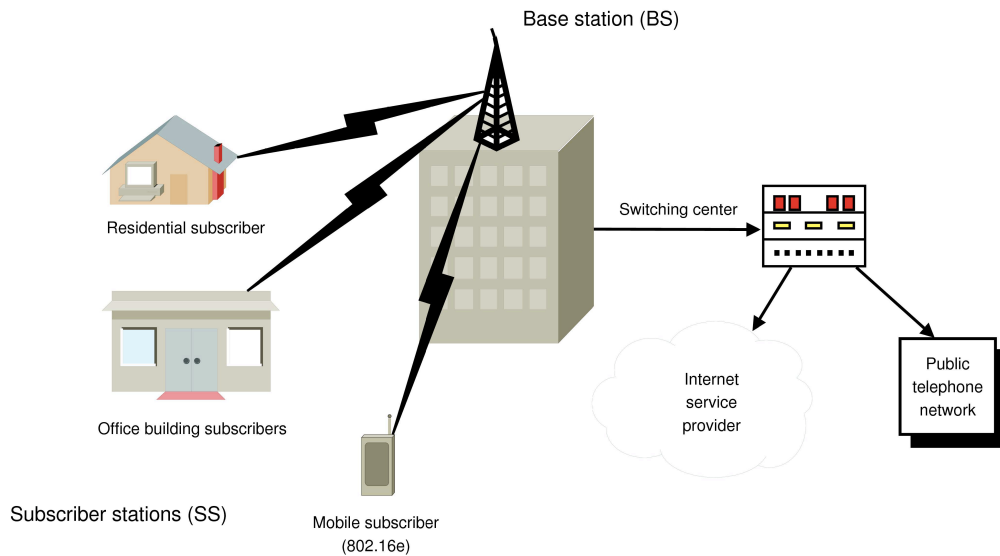
Results of the Norwegian 3.5GHz auction



5.26

## Typical WiMax Scenarios

KJhole.com



5.27

## Uses for WiMax (1)

KJhole.com

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

5.28

## Uses for WiMax (2)

---

KJhole.com

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

5.29

## 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

5.30

## MAC Physical Layer (1)

---

KJhole.com

- MAC physical 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

5.31

## MAC Physical 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

5.32

## **Service Range and Data Rates**

---

KJhole.com

- Service range of up to 50 km for fixed WiMax, and 5 to 10 km for mobile WiMax
- WiMax update (IEEE 802.16m) is expected to offer peak rates of at least 1 Gbit/s to fixed users and 100 Mbit/s to mobile users
- A WiMax BS may serve as many as 500 customers

5.33

## **WiMax vs. Wi-Fi (1)**

---

KJhole.com

- While fixed WiMax is mainly a Wireless Metropolitan Area Network (WMAN), Wi-Fi is a short-range indoor network
- Fixed WiMax is a wireless alternative to cable and Digital Subscriber Line (DSL) technologies

5.34

## WiMax vs. Wi-Fi (2)

---

KJhole.com

- Wi-Fi MSs and BSs typically have *omnidirectional* antennas
- Fixed 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

5.35

## WiMax vs. Wi-Fi (3)

---

KJhole.com

- 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

5.36

## **WiMax vs. 4G (1)**

---

KJhole.com

- WiMax supports mobility and is a competing standard to 4G mobile networks
- It is very expensive and time-consuming for providers to put up radio towers for new cells in a cellular network
- While 4G 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 4G providers

5.37

## **WiMax vs. 4G (2)**

---

KJhole.com

- Some 4G providers may install WiMax in existing radio towers to provide better service
- 4G providers have a huge advantage over new WiMax providers in terms of costs

5.38