Securing Wireless LANs: Part 6

Gaurav S. Kasbekar

Dept. of Electrical Engineering

IIT Bombay

References

- J. Kurose, K. Ross, “*Computer Networking: A Top Down Approach*”, Sixth Edition, Pearson Education, 2013
- J. Edney, W.A. Arbaugh, “*Real 802.11 Security: Wi-Fi Protected Access and 802.11i*”, Pearson Education, 2004.
- B.L. Menezes, R. Kumar, “*Cryptography, Network Security, and Cyber Laws*”, CengageLearning India Pvt.Ltd., 2018

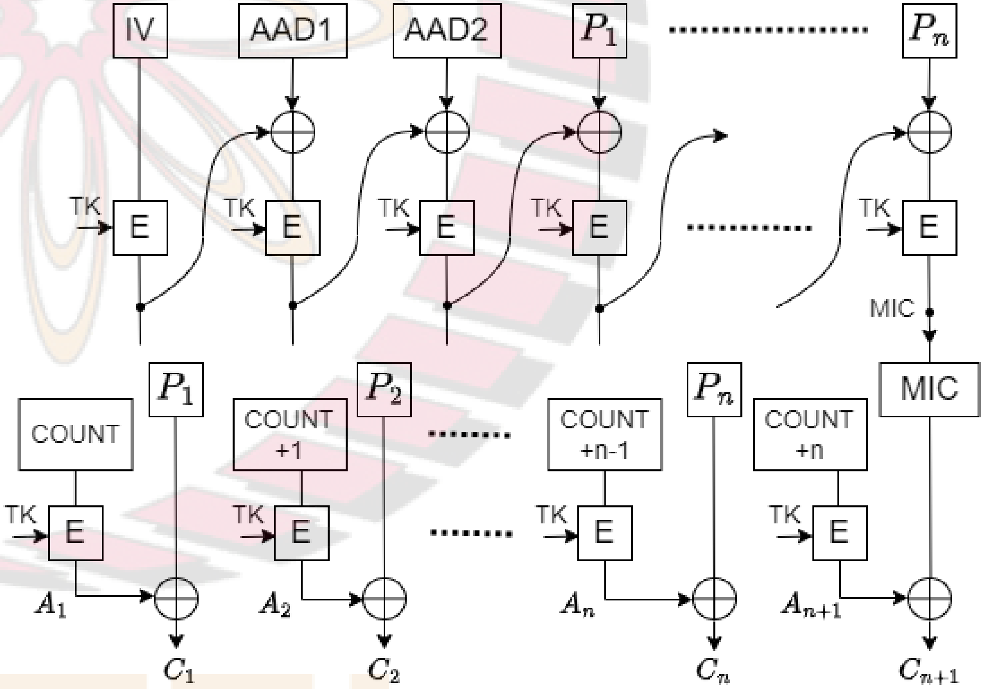
Counter Mode with CBC-MAC Protocol (CCMP)

CCMP

- Uses AES for both encryption and message integrity
- Unlike TKIP, same key (the 128-bit temporal key (TK)) is used for encryption and MIC computation
- Recall: a fresh encryption key computed for each frame in WEP and TKIP
- In contrast, same encryption key used for each frame in CCMP
- Reason:
    - ❑CCMP uses AES, which is a block cipher, in contrast to WEP and TKIP, which use RC4, a stream cipher
- A 48-bit packet number (PN) is initialized to 0 when a session is started between a sender and receiver
    - ❑increments by 1 for each packet sent
    - ❑analogous to the frame sequence counter used in TKIP

Message Integrity in CCMP

- MIC is computed for each packet using AES in Cipher Block Chaining (CBC) mode with block size 128 bits as shown in fig.
  - ❑ Output of the last block is 128 bits in length; its lower 64 bits are discarded to get a 64-bit MIC
- MIC computed over frame data ($P_1, \ldots, P_n$ in fig.) and some fields in MAC header (e.g., source and destination MAC addresses)
- Key for performing encryption in each stage is TK
- IV for MIC computation is a nonce, which includes the 48-bit PN



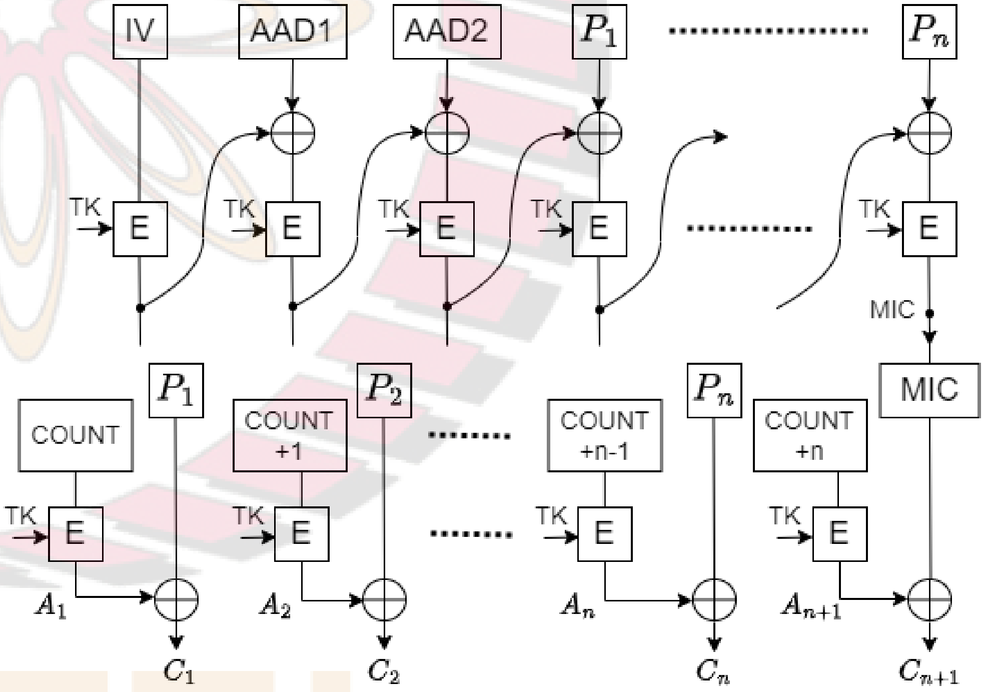
IV = Initialization Vector (includes 48-bit Packet Number)

AAD1, AAD2 = Additional Authentication Data (includes certain immutable fields of the MAC header)

COUNT is a function of the Packet Number

Message Integrity in CCMP (contd.)

- Above method for computing MIC is called *Cipher Block Chaining Message Authentication Code (CBC-MAC)*
- Note that MIC generated using this method is a function of all the bits of the message over which it is computed
  - if one or more bits of message change, then very likely that MIC changes
- CBC-MAC is a MIC generation technique that has been used for many years and has been standardized internationally. For its security analysis, see:
  - M. Bellare, J. Kilian, P. Rogaway, “The Security of the Cipher Block Chaining Message Authentication code”, *Journal of Computer and System Sciences*, 61(3), pp. 362-399, 2000.



IV = Initialization Vector (includes 48-bit Packet Number)

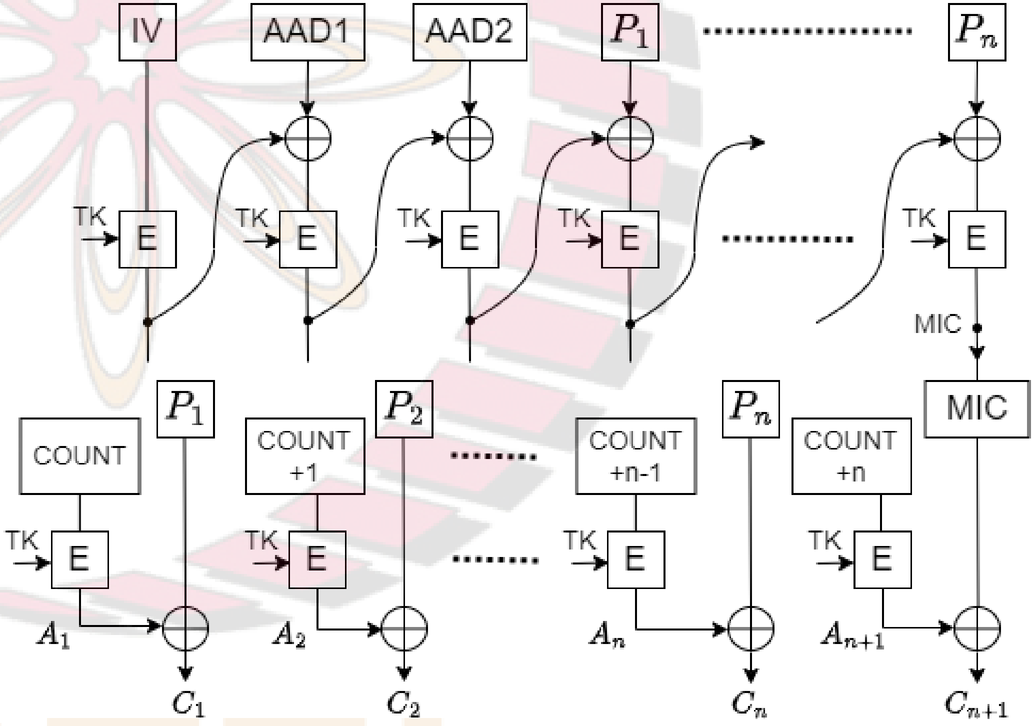
AAD1, AAD2 = Additional Authentication Data (includes certain immutable fields of the MAC header)

COUNT is a function of the Packet Number

Encryption in CCMP

- Frame data and MIC are concatenated and then encrypted using AES in counter mode as shown in fig.

- In fig., COUNT is a function of the PN
- Key for performing encryption of each block is TK
- Receiver performs decryption followed by MIC verification



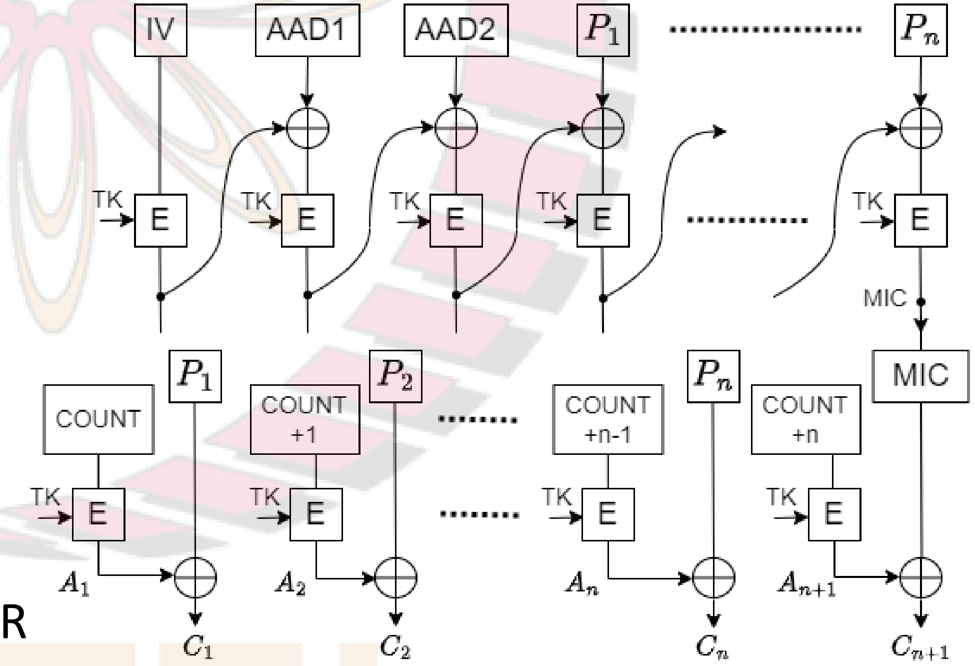
IV = Initialization Vector (includes 48-bit Packet Number)

AAD1, AAD2 = Additional Authentication Data (includes certain immutable fields of the MAC header)

COUNT is a function of the Packet Number

Use of Same Key for MIC Generation and Encryption in CCMP

- Recall: same key (TK) is used for encryption and MIC generation
- As discussed earlier, it is in general not good practice to use same key for two separate cryptographic functions
    - ❑ this rule broken here
- However, although same key used, it is in each case used in conjunction with an IV
- Construction of the IV is different for the counter mode and CBC-MAC portions
- Using this fact, this protocol has been shown to be secure by cryptographers:
    - ❑ J. Jonsson, “On the Security of CTR + CBC-MAC”, In *SAC – Ninth Annual Workshop on Selected Areas of Cryptography*, 2002.



IV = Initialization Vector (includes 48-bit Packet Number)

AAD1, AAD2 = Additional Authentication Data (includes certain immutable fields of the MAC header)

COUNT is a function of the Packet Number

Replay Attack Prevention in CCMP

- Recall:
  - ❑ a 48-bit packet number (PN) is initialized to 0 when a session is started between a sender and receiver
  - ❑ increments by 1 for each packet sent
- The PN is included in header field in a CCMP frame
- Sender and receiver keep track of the PN of the last frame sent/ received
- Upon receipt of a frame, receiver compares the value of PN in frame to the PN of last frame received
  - ❑ If former is less than latter, then received frame is discarded
- Hence, if old frame replayed by intruder, then it is discarded
- Suppose an intruder creates a new frame with a higher PN than PN of last frame sent by legitimate sender, and sends it to receiver
- Will receiver accept it?
  - ❑ No, since IV used for MIC computation includes the PN
  - ❑ So MIC verification at receiver will fail
- Thus, CCMP defends against replay attacks