Securing Wireless LANs: Part 1

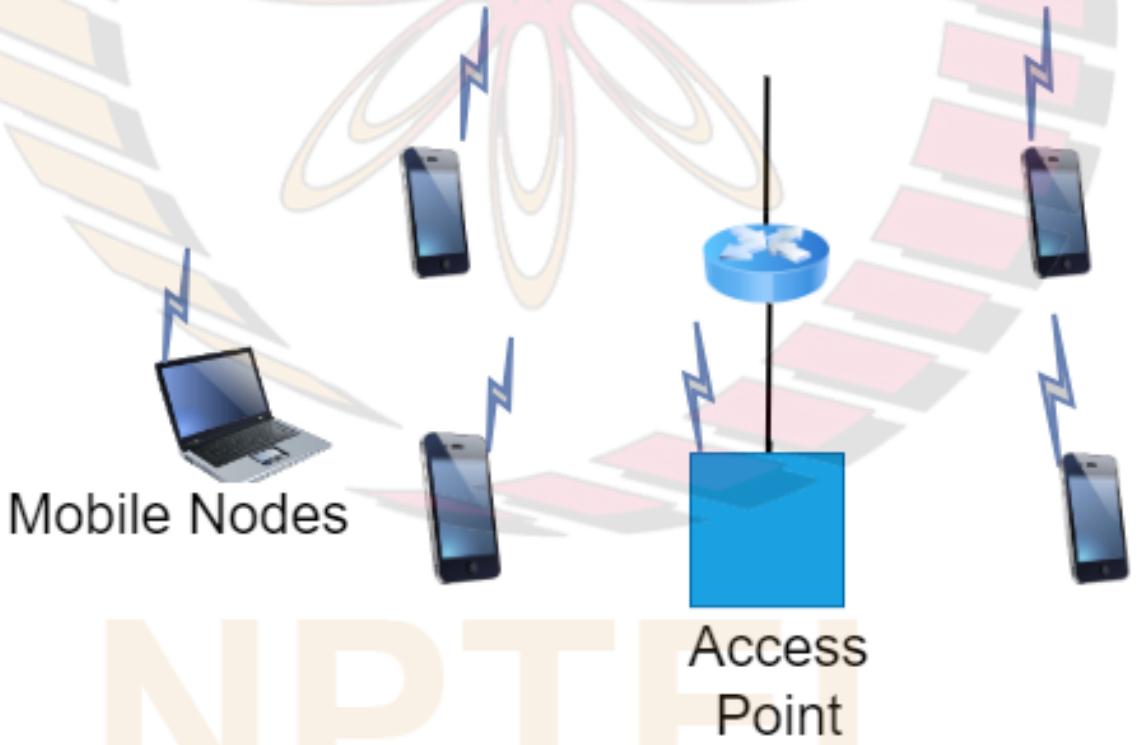
Gaurav S. Kasbekar
Dept. of Electrical Engineering
IIT Bombay

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

Wi-Fi (802.11)

- Mobile nodes and Access Point communicate over wireless channel (shared medium)



Wi-Fi (802.11) (contd.)

- Wi-Fi operates in Industrial, Scientific and Medical (ISM) bands (around 2.4 GHz, 5 GHz)
  - Originally meant for purposes other than telecom (e.g., microwave ovens)
  - Later *unlicensed* use by wireless devices (e.g., Wi-Fi, Bluetooth) allowed
- Binary exponential backoff based medium access control protocol used
- When destination receives an error-free packet, it sends an ACK to source
  - if source does not receive ACK, it retransmits packet

Security in 802.11

- Security important in 802.11 since:
  - wireless medium used; radio waves carrying transmissions can propagate beyond building containing Access Point and mobile devices; transmitted signal can be intercepted using packet sniffer placed near network
  - intruder can also transmit packets masquerading as Access Point or a legitimate mobile device
- In the original 802.11 standard (adopted in late 1990s), a set of security mechanisms known collectively as **Wired Equivalent Privacy (WEP)** were included
  - later several security flaws were found in WEP
- In 2004, **802.11i**, a more secure standard for 802.11 security was adopted; in 2009, another security related amendment, **802.11w**, was introduced
- Next: we discuss WEP, some of the flaws in it, 802.11i, and 802.11w

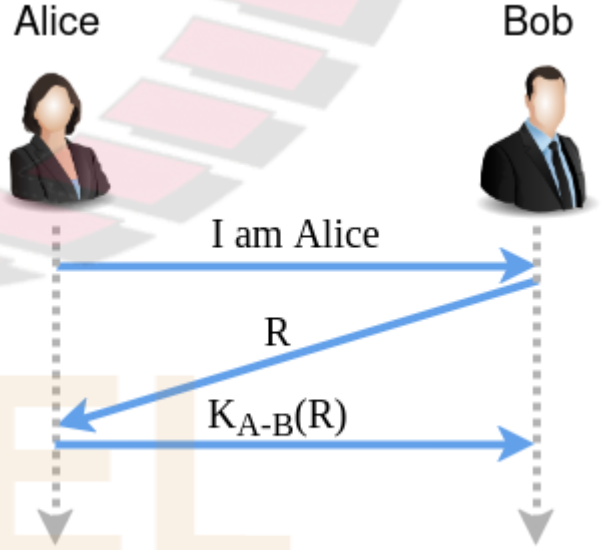
WEP

- Designed to provide authentication and data encryption between a mobile device (host) and AP
- Assumes that a symmetric shared key exists between host and AP
  - ❑No key management algorithm provided by WEP
  - ❑Assumed that host and AP have somehow agreed on symmetric key (*e.g.*, user may manually input key provided by system administrator)

WEP's Authentication Protocol

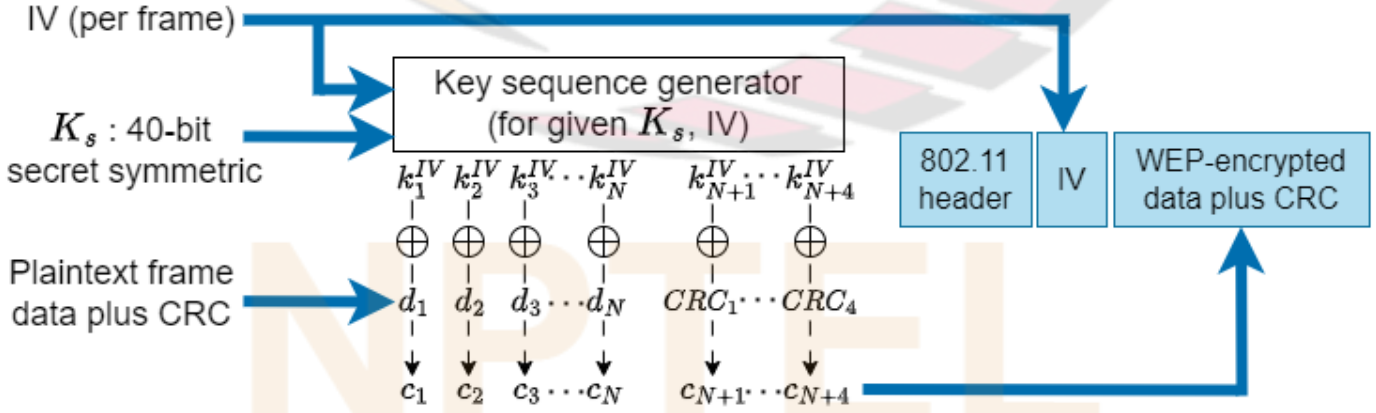
- Same as the authentication protocol **ap4.0** that we studied earlier

1) A host requests authentication by an AP
2) The AP responds with a 128 byte nonce value
3) The host encrypts the nonce using the symmetric key that it shares with the AP and sends it to AP
4) The AP decrypts and verifies the encrypted nonce sent by host



WEP's Data Encryption Protocol

- A 40-bit symmetric shared key, K_S, assumed to be known by both host and AP
- A 24 –bit *Initialization Vector* (IV) appended to K_S to get a 64-bit key that is used to encrypt a single frame
  - ❑ IV changes from frame to frame (*e.g.*, selected randomly)
- Suppose plaintext data is N bytes in length; 4-byte CRC computed for it
- The 64-bit key used to generate a stream of key values (1 byte each), k_1^{IV}, k_2^{IV}, k_3^{IV},… using RC4 stream cipher (details omitted)
- Ciphertext obtained by XORing (plaintext data+CRC) with the key value stream
- IV included in plaintext form in header of WEP-encrypted frame



Reasons for Using IV

- Recall: a 24 −bit *Initialization Vector* (IV) appended to K_S to get a 64-bit key that is used to encrypt a single frame
  - ❑ IV changes from frame to frame (*e.g.*, selected randomly)
- Reasons for using IV:
  1) To ensure that two identical plaintext messages do not produce the same ciphertext
  2) For every frame, the RC4 algorithm is initialized with the key value prior to the start of the key stream generation; if the key value were same for every frame, the RC4 algorithm would be initialized to same state every time
     - So key stream produced would be same for every frame
     - This would be a serious weakness since if attacker found out the key stream (e.g., by guessing the plaintext in a frame), he/ she would be able to decipher every frame by XORing the frame with the key stream