Security Analysis on Wireless LAN protocols

HORI Yoshiaki
hori@csce.kyushu-u.ac.jp

Kyushu University / ISIT

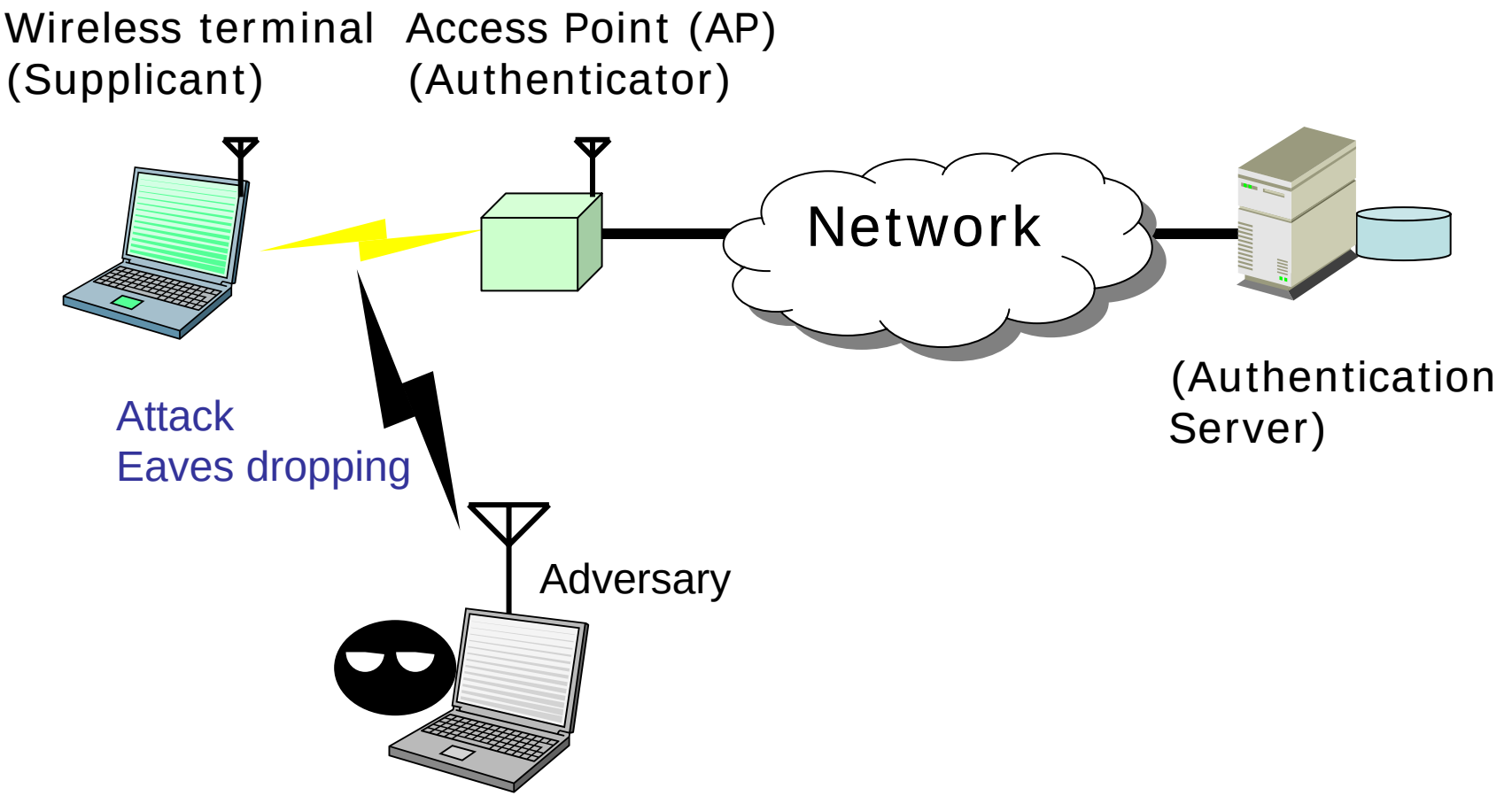
Contents

- Security analysis on IEEE 802.11i
  - Short summary of
    C. He and J. C. Mitchell, “Security Analysis and Improvements for IEEE 802.11i,” NDSS05, February 2005
- Security analysis on MIS protocol
  - Yet another wireless LAN protocol based on IEEE 802.11 physical layer

Wireless LAN and Security

- Wireless LAN (WLAN)
  - WLAN uses wireless media instead of wired media in order to provide connectivity for a terminal.
    - A wireless terminal is connected with Access Point (AP) by using of wireless media.
  - WLAN provides mobility, no wire
    → WLAN enables easily to build LAN
  - Currently WLAN become widely deployed.
- WLAN security
  - WLAN security has become a serious concern for many organizations.
  - Security requirements for a WLAN
    - Data condidentiality
    - Integrity
    - Mutual authentication
    - Availability

WLAN security model



Wireless Threats

(by C. He and J. C. Mitchell, Stanford Univ.)

- Wireless Threats
  - Threat 1: Passive Eavesdropping
  - Threat 2: Message Injection
  - Threat 3: Message Deletion and Interception
  - Threat 4: Masquerading and Malicious AP
  - Threat 5: Session Hijacking
  - Threat 6: Man-in-the-Middle
  - Threat 7: Denial of Service

  Threats 1, 2, and 3: attack all three type of frames in the Link Layer

  Threats 4, 5, and 6: defeat mutual authentication

  Threats 7: interferes with availabilit

IEEE 802.11i overview

- IEEE standard approved and published on June 2004
- Designed to provide enhanced security in the Media Access Control (MAC) layer for 802.11 wireless networks
  - 802.11i works well for data confidentiality, integrity, and mutual authentication.
- Defined Robust Security Network Association (RSNA) which provides
  - two data confidentiality protocols;
    - Temporary Key Integrity Protocol (TKIP)
    - Counter-mode/CBC-MAC Protocol (CCMP) with AES-128 (128bit Key and 128bit Block size)
  - Authentication and key management protocol
    - Extensible Authentication Protocol (EAP) scheme, e.g. EAP-TLS, provides mutual authentication.
    - 4-way handshake enables to share Pairwise Transient Key (PTK) derived from their Pairwise Master Key (PTK).
- Also supported pre-RSNA for compatibility with 802.11
  - Wired Equivalent Privacy (WEP)

Data confidentiality and Integrity

- CCMP appears to provide satisfactory data confidentiality, integrity, and replay protection for data packets against threats 1, 2 and 3.
- However, threats 1, 2 and 3 remain with management frames and control frames because these frames are neither encrypted nor authenticated by the link layer encryption algorithm.

Authentication and Key Management

- If the complete RSNA handshakes are performed, the authentication and key management process appear to be secure.
- However, since an adversary can interfere with early stages in RSNA handshakes, it may prevent completion of the RSNA.
- Some attacks for 802.11i
  - Security level rollback attack
    - Bogus beacon and bogus probe response from an authenticator (access point), and bogus association request.
  - Reflection attack on the 4-way handshake

Availability

- Known DoS Attacks
- Michael Algorithm Countermeasure (in TKIP)
  - Not affected with CCMP
- RSN IE (RSN Information Element) Poisoning
- 4-Way Handshake Blocking
- Failure Recovery

Known DoS Attacks

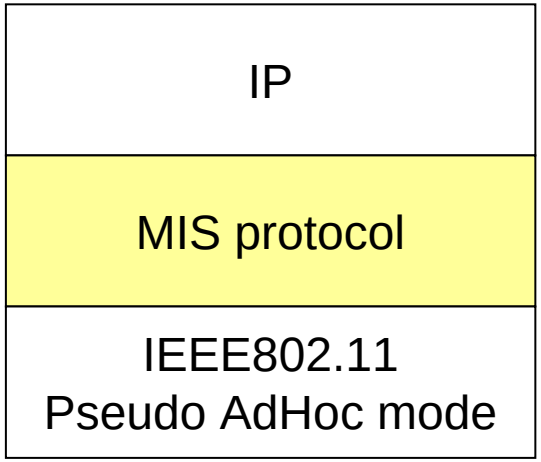
- An adversary can easily forge the management frames and the control frames to launch a DoS attack.
  - The most efficient attack is to forge and repeatedly send Deauthentication or Deassociation frames. These attacks persist even if 802.11i is used.
  - There are also several DoS attacks that exploit the unprotected EAP messages in 802.1X authentication. However, these vulnerabilities fortunately can be eliminated in 802.11i by simply ignoring these messages.
    - EAPOL (EAP over LAN)-Start, EAPOL-Success, EAPOL-Failure, EAPOL-Logoff

Summary: 802.11i security

- Satisfactory data confidentiality, integrity, and replay protection for data packets is provided by using of CCMP (AES).
- Mutual authentication is provided by EAP-TLS and 4-way handshake.
- In order to support above features and to keep upper compatibility with IEEE802.11 and IEEE 802.1X (pre-RSNA), we should consider availability.

MIS Protocol

- Between a terminal (MN: mobile node) and a base router (BR).
- MIS protocol provides security features:
  - Mutual authentication between MN and BR
  - Sharing session key between MN and BR
  - Packet authentication and Data encryption
- Advantages
  - Fast authentication and Data encryption



Protocol Layers

- MIS protocol can work as WLAN security protocol
  - MIS uses pseudo adhoc mode (IEEE 802.11 physical layer) of IEEE 802.11 network interface card.

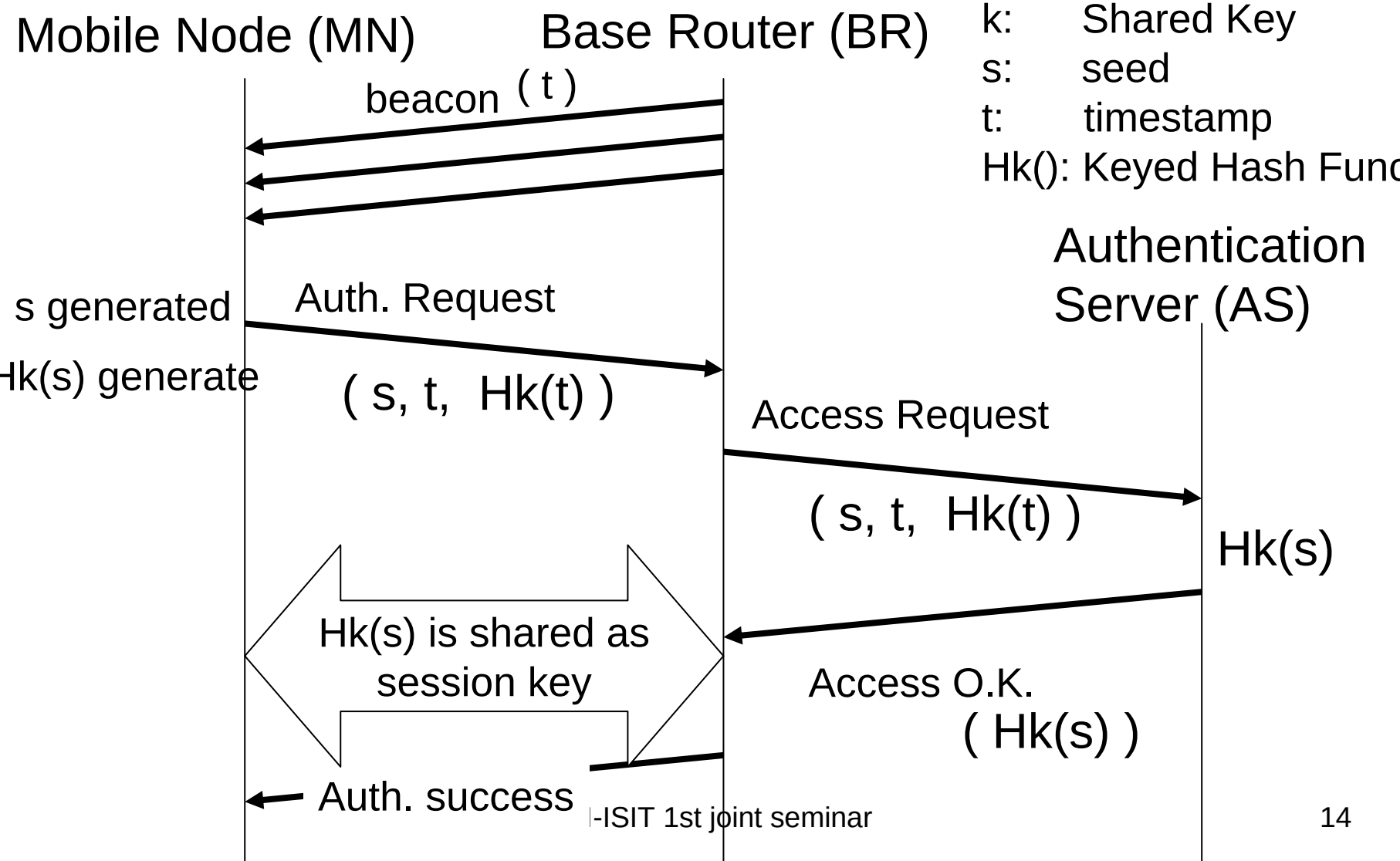
Design and Standardize

- Some ideas of MIS protocol were written in 2001
  - "Fast Authentication System for Secure Wireless Internet Services" (K. Fujikawa, H. Nakano, M. Ohta, M. Hirabaru, H. Mano, and K. Ikeda)
    IPSJ SIGDPS technical report, 2001-DPS-107, March 2002

- Protocol specifications were approved by Mobile Broadband Association (MBA) and published on their Web.
  http://www.mbassoc.org/

- Protocol Documents
  (but these are written in only Japanese)
  - MBA standard 0201, "MIS protocol specification ver. 1.02" (announced on April 2004)
  - MBA standard draft 0301, "MISAUTH protocol specification" (annouced on June 2004)

MIS protocol time chart



Objective

- Security analysis on MIS protocol on Wireless LAN.
- We attempt to evaluate MIS protocol security.
  - Confidentiality and Integrity
  - Authentication and Key Management
  - Availability

Confidentiality and Integrity

- MIS protocol provides data encryption and integrity by using of AES-CBC-128bit and HMAC-MD5.
  - It is appropriate with enough key length rather than WEP.
- MIS protocol also does not provide encryption and integrity check of control messages before sharing session key.
  - MIS control message:
    - Beacon message
    - Authentication Request message
    - Authentication Success message
    - Authentication Failture message
    - Session close message

Authentication

- MIS protocol carries out mutual authentication between Mobile Node (MN) and Base Router (BR).
- MIS protocol enables message authentication after sharing session key.
  - Authentication failure message also is used at renew of session key. The protocol specification said “authentication is not provided for authentication failure message.”

Availability

- MIS protocol has some weakness for DoS attack by using of forged control messages because of a lack of authentication.
  - Beacon message
  - Authentication failure message
    - Forged authentication failure message at the authentication process and the renew of session key.
  - Authentication request message

Countermeasure of MIS protocol

- Forged authentication failure message
  - Waiting timeout
- Forged authentication failture message at renew session key
  - New control message for renew session key is required.

Summary

- MIS protocol provides confidentiality, integrity, mutual authentication equivalent to IEEE 802.11i.
- MIS protocol also some weakness against DoS attack like IEEE 802.11i.
- We can measure against DoS attack by a little modification of MIS protocol because it is so simple.