

Modular Analysis of the 802.11i Protocols

Anupam Datta

Ante Derek

Changhua He

John C. Mitchell

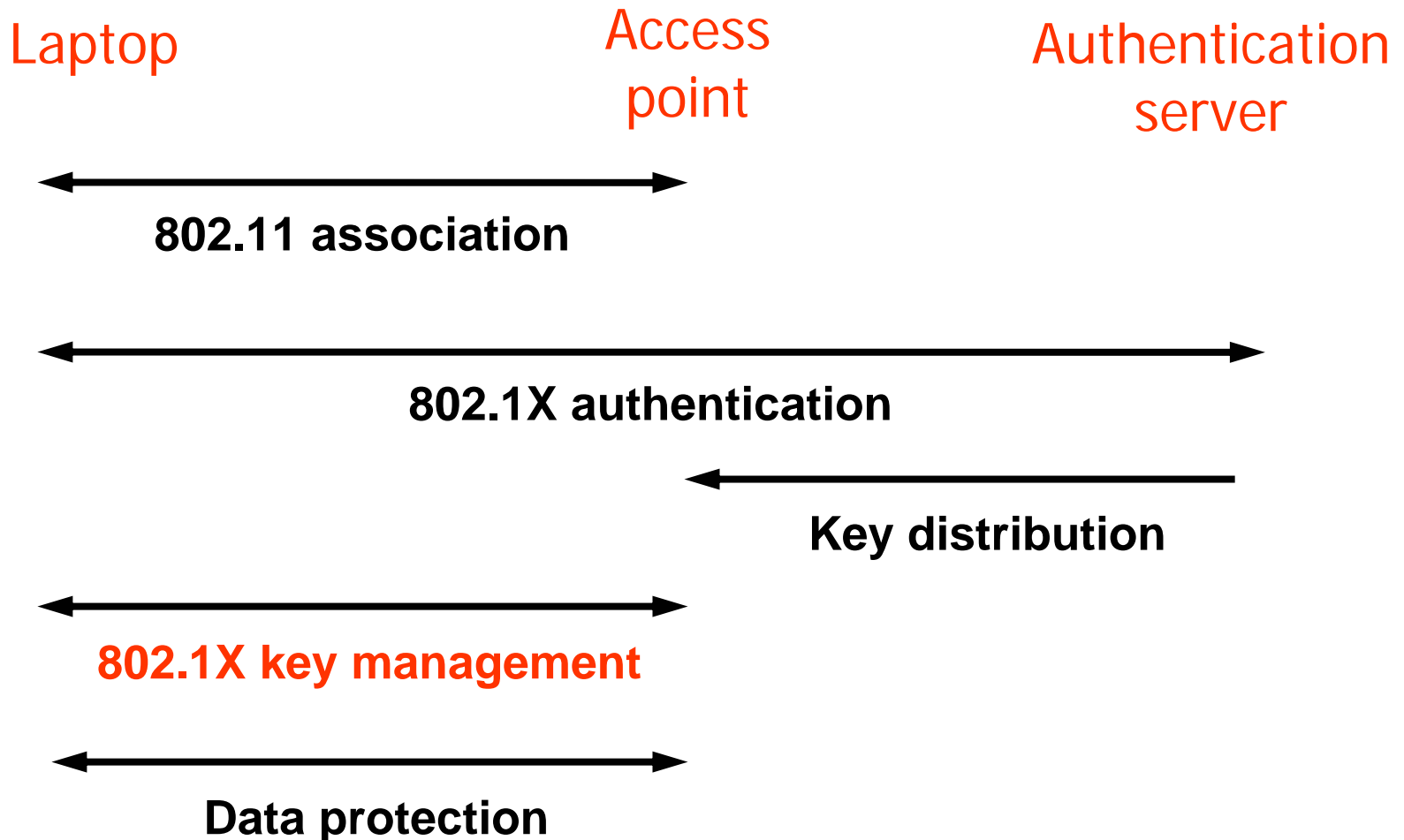
Stanford University

October 22, 2004

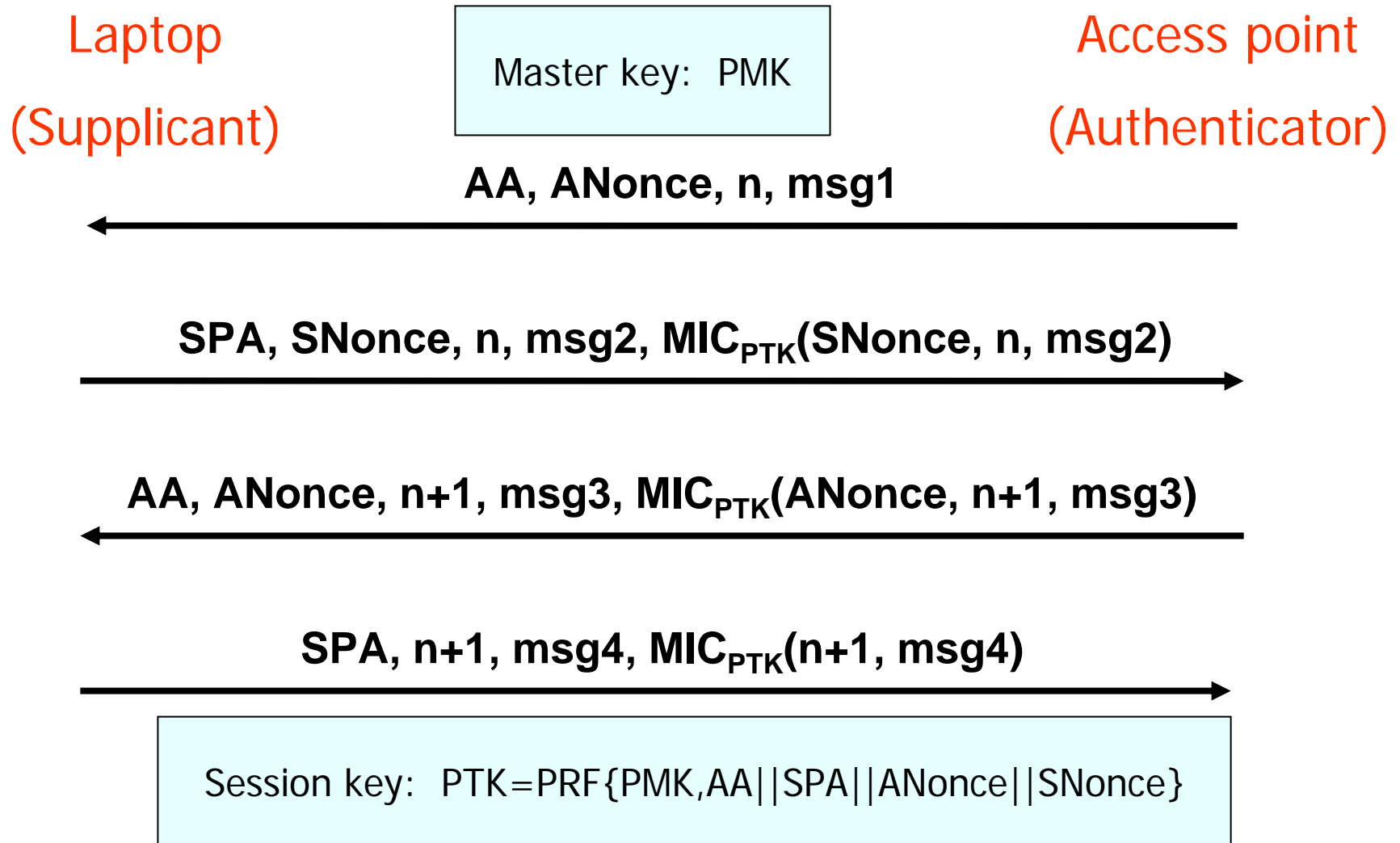
Wireless security

- Wired Equivalent Privacy (WEP)
 - create “privacy achieved by a wired network”
- IEEE 802.11i goals:
 - Authentication
 - Confidentiality
 - Data origin authentication
 - Replay detection

RSNA Sub-protocols



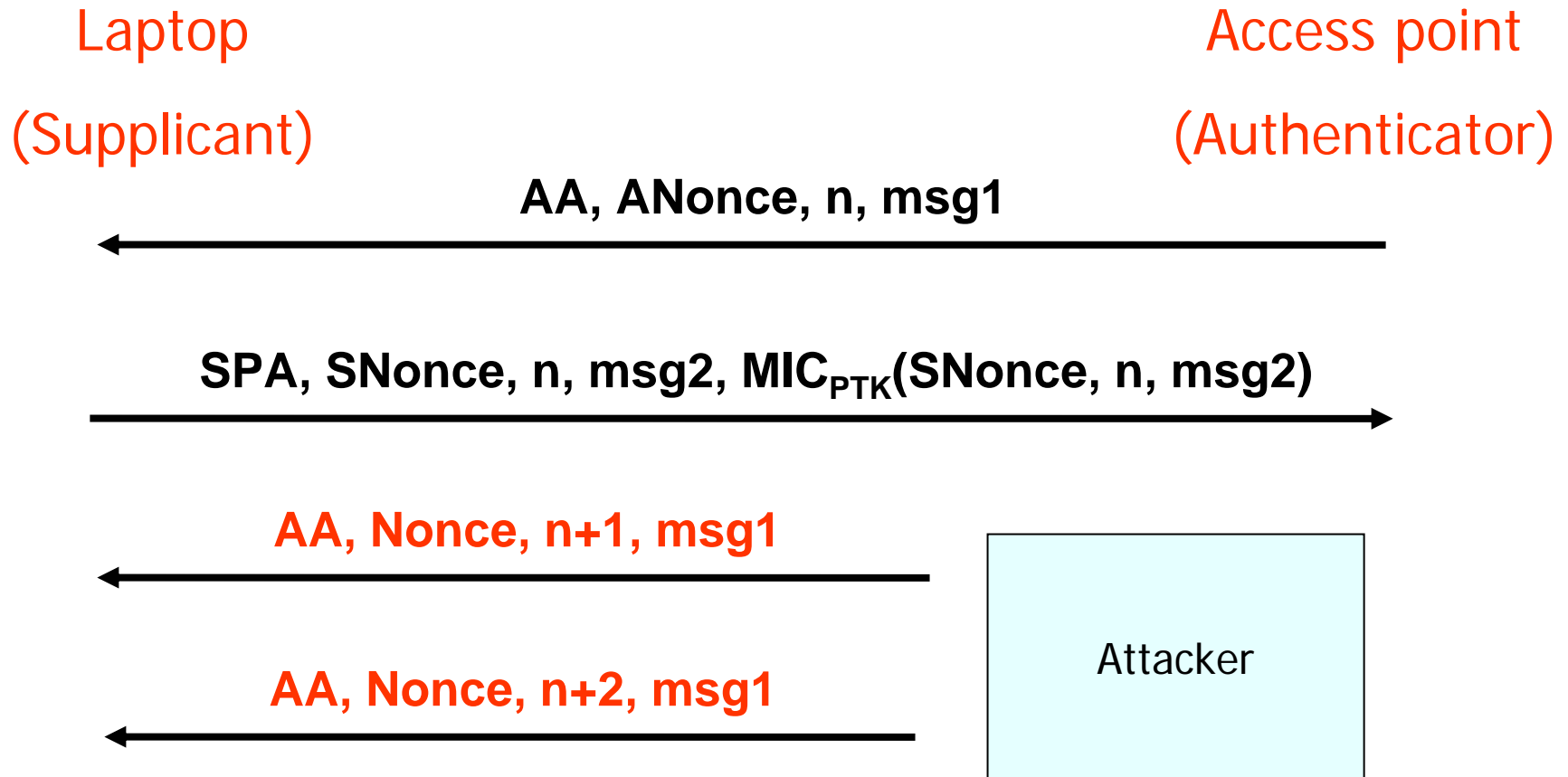
Idealized 4-Way Handshake



Idealized 4-Way Handshake

- Murphi analysis [He, Mitchell, WiSe04]
- DoS Attack
 - Multiple parallel instances are needed for supplicant due to packet loss
 - Standard: two instances
 - First message is not authenticated
 - Attacker can stop the protocol by forging initial messages

DoS attack

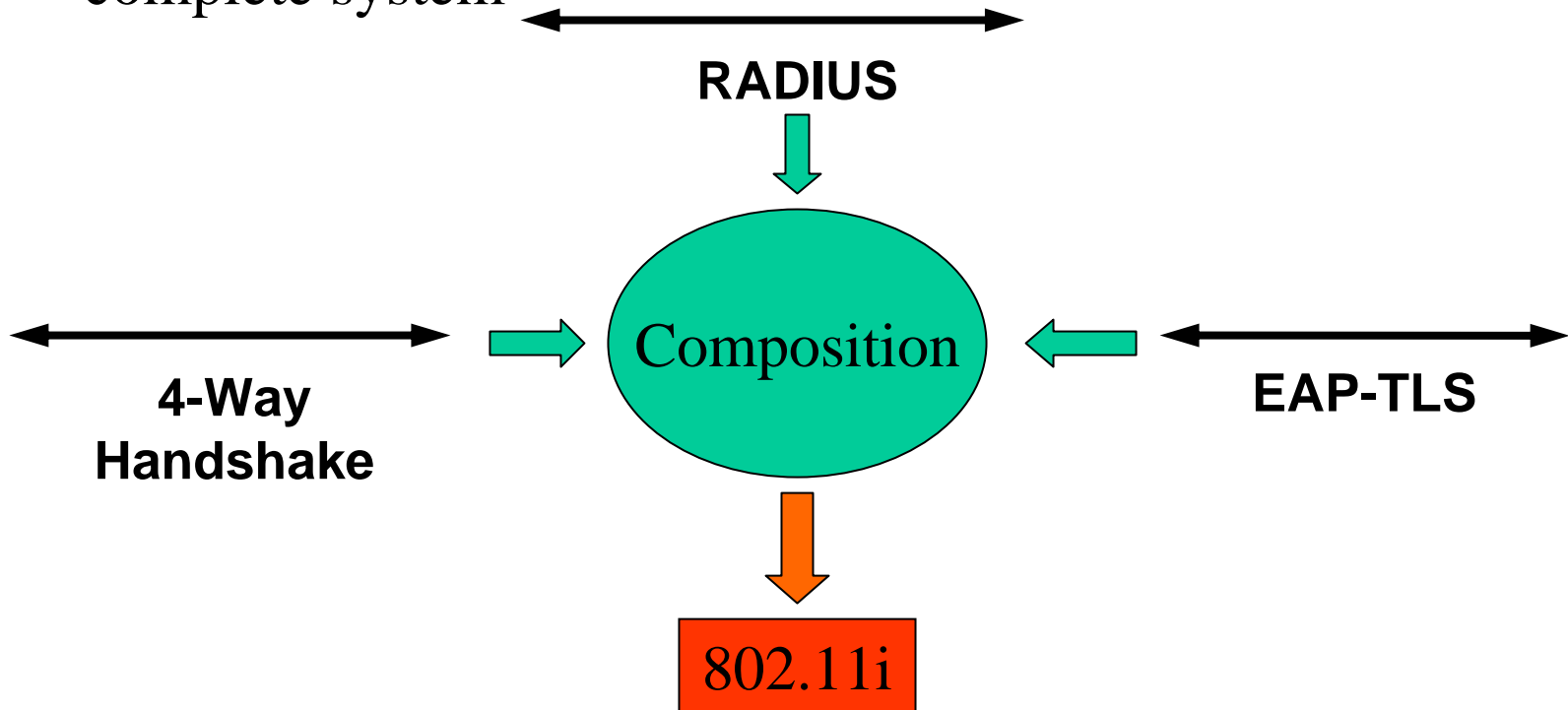


DoS attack - Fixes

- Random queue drop
 - Protocol remains vulnerable
- Authenticate first message
 - Requires changes in the message format
- Supplicant uses the same nonce until a handshake is completed
 - Eliminates the attack
 - No changes in the message format
 - Adopted by the the IEEE 802.11i working group

802.11i Analysis using PCL

- Analyze components of 802.11i using Protocol Composition Logic
- Use composition theorems to prove the properties of the complete system



Current Status and Future Work

- Current Status
 - Murphi analysis of the 4-Way Handshake
 - DoS attack found and fixes proposed
 - Redundant fields identified
- Work in progress
 - PCL analysis of TLS
 - PCL analysis of the 4-Way Handshake
 - Composition results