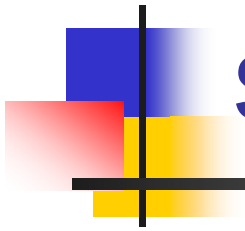
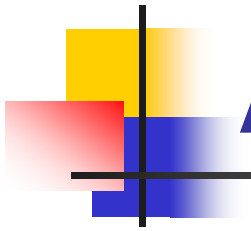


Wireless communications systems security

Alexey Fomin, SUAI

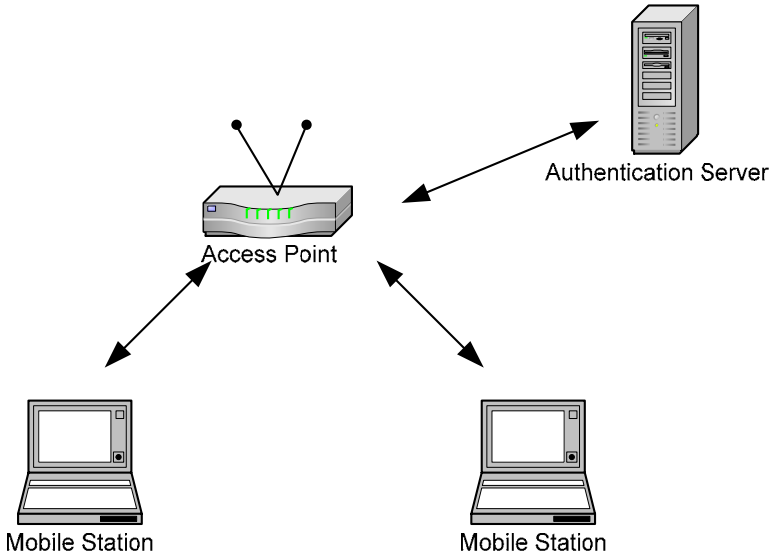
fomin@vu.spb.ru



Agenda

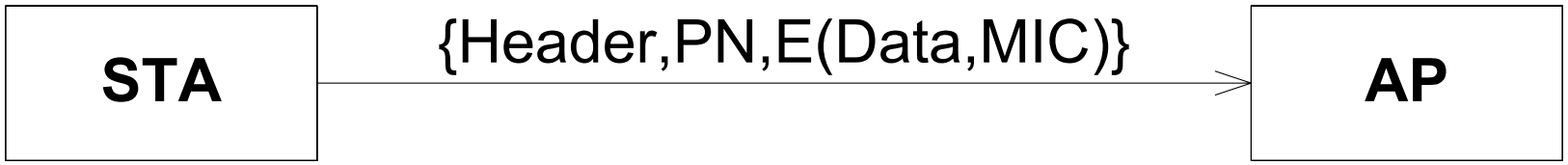
- Current security solutions in wireless systems (802.11)
- Open problems

Security Tasks



- Message authentication & privacy
- Node\Base Station mutual Authentication
- Key Management

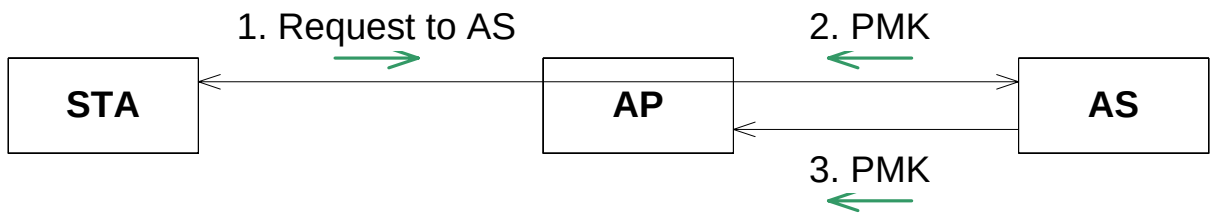
Message Protection



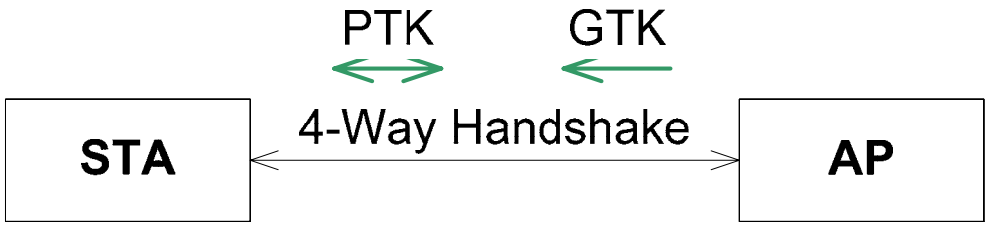
- Message Protection
  - Encryption (E(*)) (provides Privacy)
  - Packet Number (PN) (provides Freshness)
  - Message Integrity Code (MIC) (provides Authentication)
- Key hierarchy
  - PMK = pair-wise master key
    - PTK = pair-wise transient key (unicast traffic protection)
    - GTK = group temporal key (broadcast traffic protection)

Key Management

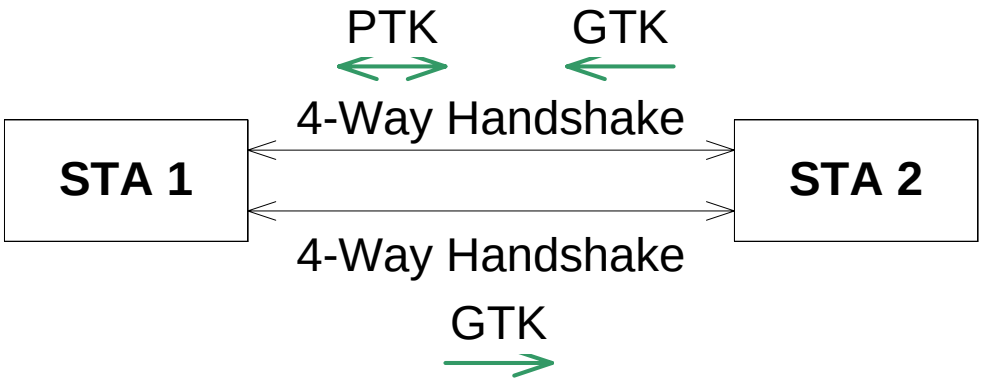
- PMK
  - Administrator provides STA and AP with PSK
    - Only STA and AP are involved
  - Administrator provides STA with key for AS (authentication server)
    - EAP-TLS, EAP-PSK,...
    - Obtaining PMK in a distributed way by using AS (802.1X)



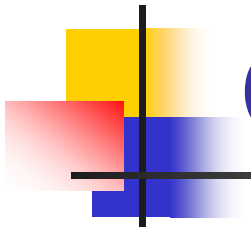
Obtaining PTK and GTK



BSS mode



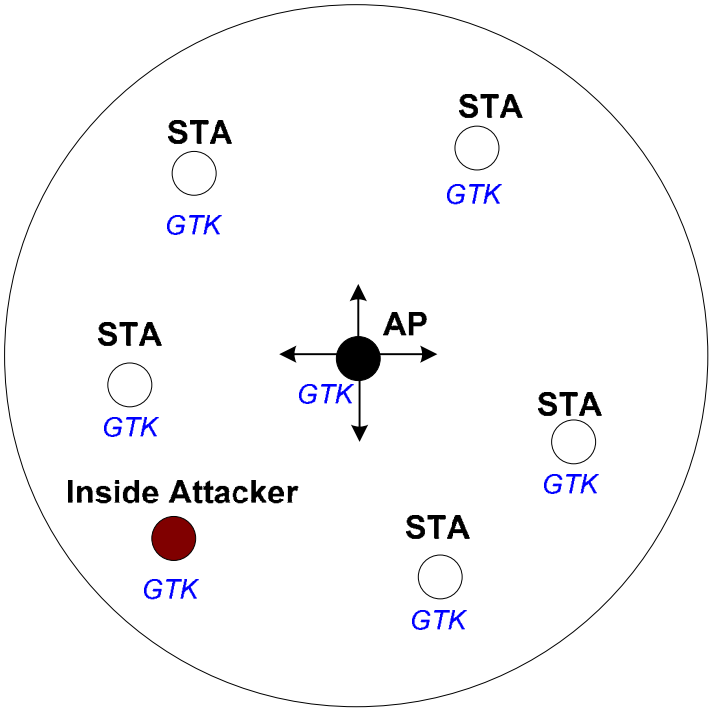
IBSS mode



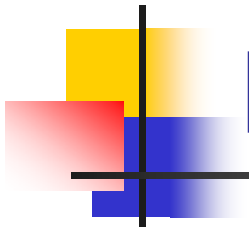
Open Problems

- Authentication of broadcast frames
- Authentication of management frames
- Key management in ad-hoc (IBSS) networks

Broadcast Frames Authentication



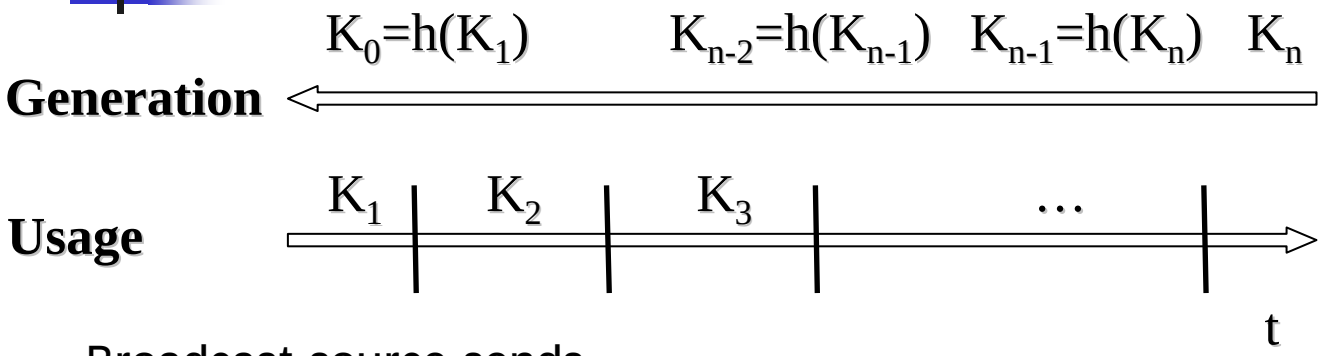
- AP distributes GTK to all STAs during association process
- Broadcast data frames are protected by using of GTK
  - Nodes can not identify real source of the broadcast frame
  - Any STA could send broadcast data frames acting as AP



Possible Solutions

- Public Key Signature
  - Computational overhead is too big
- MICs on pair-wise keys
  - Network overhead is too big
- One/multi time signature
  - Network overhead is too big
- TESLA
  - Delayed authentication

TESLA



- $K_{j-1}=H(K_j)$
- K_0 - verification key

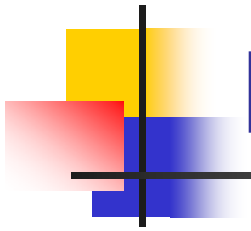
- Broadcast source sends

$$M \rightarrow M \,||\, j \,||\, K_{j-1} \,||\, \mathrm{MIC}(K_j,\ j \,||\, K_{j-1} \,||\, M)$$

  for all messages during period *j*

- Broadcast destinations
  - Cache all the frames received during period *j*
  - Verify that $K_{j-2}=H(K_{j-1})$
  - Use K_{j-1} to validate the MICs of all frames received during the previous period j–1

Disadvantages: Delayed authentication, Time synchronization

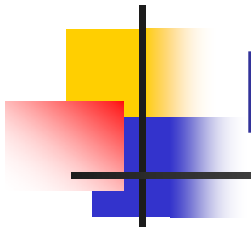


Management Frames

- Mgmt frames are more important for functioning of the network
- Stronger protection should be used
- Broadcast Protection Issues
  - Beacon Protection
  - Deauthentication/deassociation Protection

Beacon Protection

- Problem Statement
  - Beacon should be received by STA before authentication/association, i.e. before keys are available
- Possible solution
  - Accept several initial beacons without authentication
  - After authentication/association use TESLA

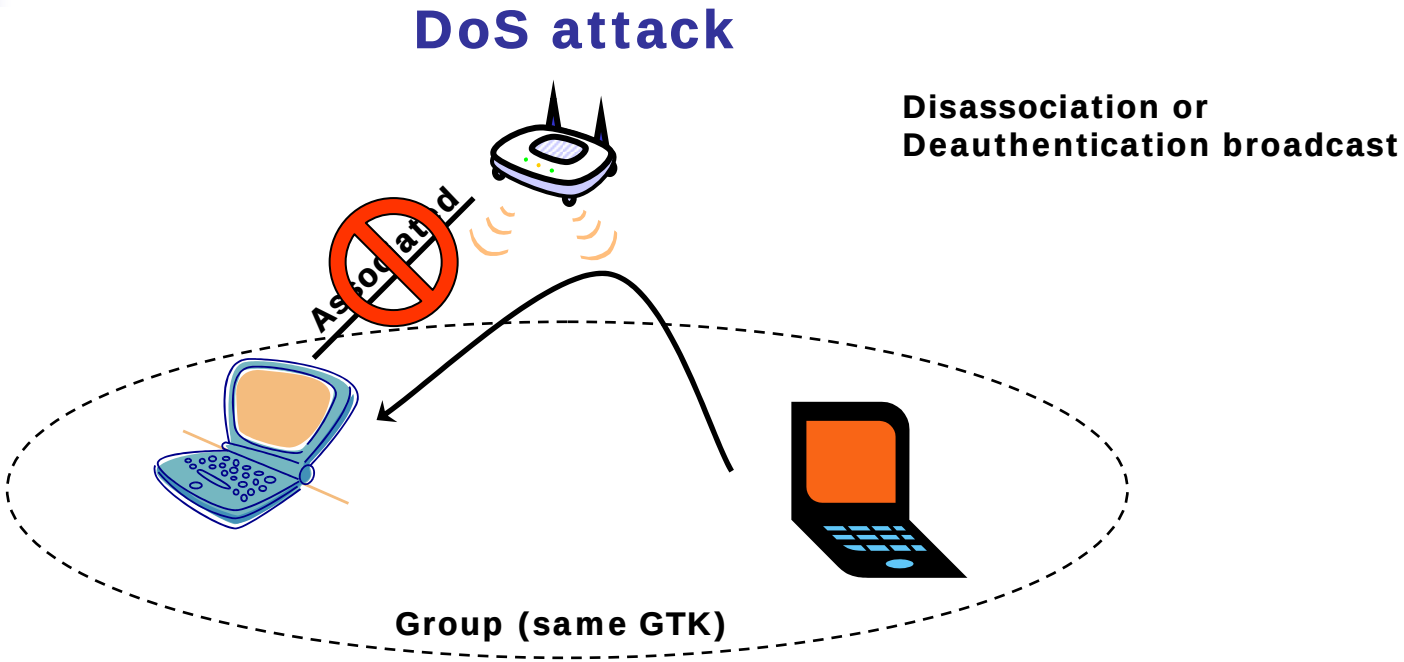


Beacon Protection

- Beacon is authenticated using TESLA
- TESLA requires time synchronization
- Time synchronization is provided in beacon

Chicken and Egg problem

Deauthentication Protection

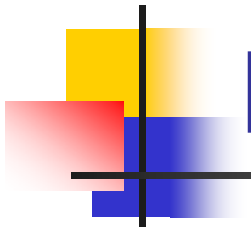


- Need to protect management frames that a Access Point uses to disassociate or deauthenticate.
- Otherwise attacker can forge such frames which results in a DoS attack.

Possible Solution

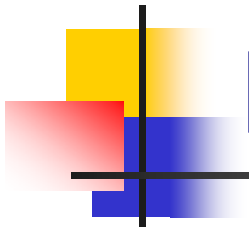
- AP distributes the commitment value CV = hash(CGTK) to STAs
- When AP sends broadcast Disassociation/Deauthenticate, it disclosures CGTK
- When an STA receives a protected broadcast, it accepts frame only if CV = hash(CGTK)

- This broadcast frame was successfully protected, because it is sent only once per session.
  - One-time signature



Public Key Infrastructure (PKI)

- Binding between PK and user
  - User certificate (CERT)
    CERT=<Name, Tstart, Tend, PK, CA Signature>
- Certificate management
  - Issuing, renewal, revocation
  - Done by trusted third party Certificate Authority (CA)

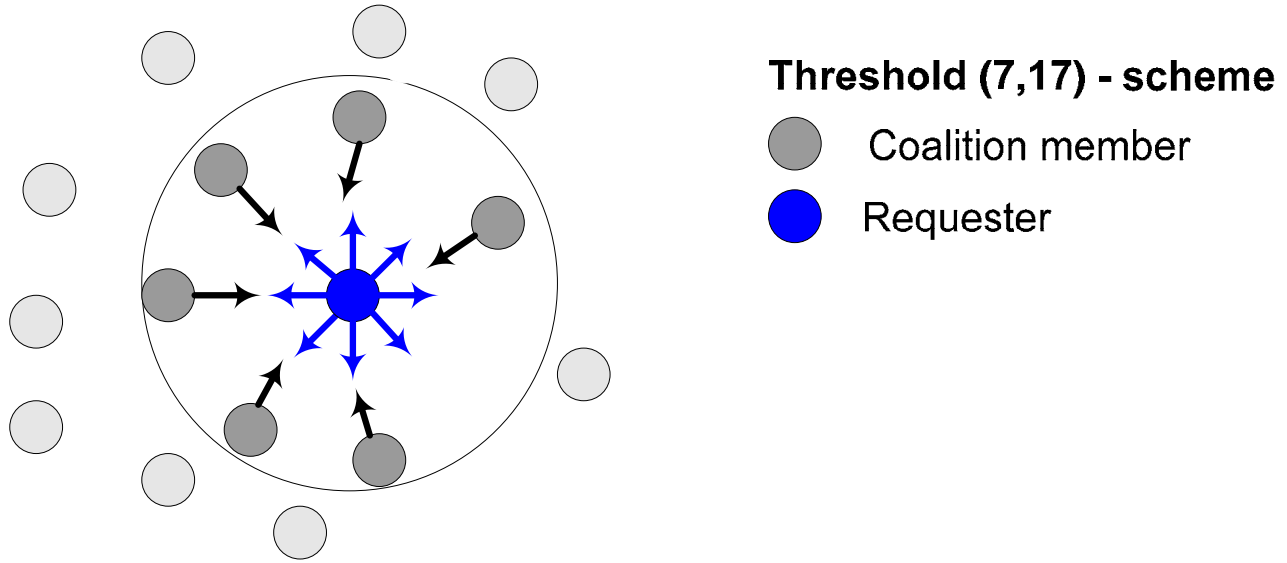


Key Management

- Centralized certification authority (CA), which provides STAs with certificates, exists in scenarios discussed previously
- There are scenarios (e.g. MANET), where such authority is not available (no fixed infrastructure)
  - To use certificate in self-organized networks we need to distribute the functionality of CA
    - Distribute signing procedure

Distributed Certification Authority

- Distributed signing procedure => distributed secret key
- Secret Sharing (t,n)-scheme
  - SK_{CA} is shared among all n nodes
  - $t<n$ nodes can make calculation with SK_{CA}
  - Less than t nodes can not



Thank You