

CANA Security Architecture

BROADWAY Project IST-2001-32686

S. Vassilaras, D. Vogiatzis, T. Dimitriou, G. Yovanof

Athens Information Technology (AIT)

e-mail: [svas](mailto:svas@ait.edu.gr), [dvog](mailto:dvog@ait.edu.gr), [tdim](mailto:tdim@ait.edu.gr), gyov@ait.edu.gr

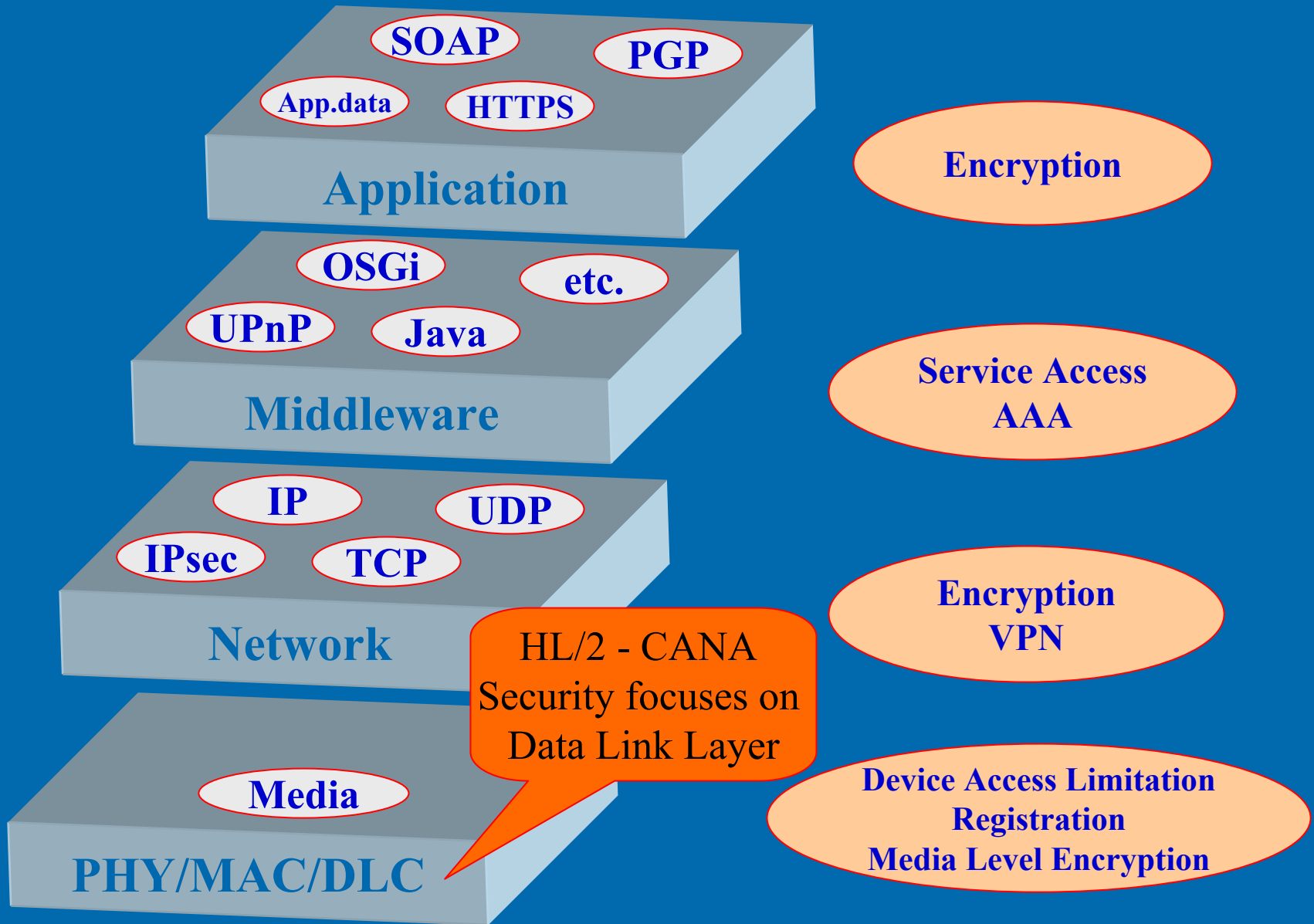


Outline

- Link Layer Security in WLANs
- HIPERLAN/2 Security Architecture
- Centralized Ad-Hoc Network Architecture (CANA)
 - Neighborhood Discovery
- CANA Security Goals & Architecture
 - Key Distribution in the Cluster
 - Security Against Protocol Attacks
- Conclusions



End-to-end Security Solution





Need for Link-Layer Security

- Upper Layer security cannot protect
 - Meta-data : layer headers, control & management data
- Different links in the path of e2e communication
 - May have specific threat characteristics unaddressed by upper layer, e.g., may start/end before e2e comm. completes
 - Different layers of multihop routing can change threat model e.g., IP routing vs. LAN bridging
- Downsides
 - Bulk protection of data at lower layers carries more burden (power, cost)
 - Adds to overhead if higher layer security is present
 - Authentication still requires higher layers: harder reach at lower layers
- Link security has been added to all subscriber access technologies with shared topologies: 802.11i, 802.15 (Bluetooth, Zigbee & WiMedia), 802.16 WiMax (DOCSIS, BPI+)



HL/2 Security - Authentication

Aim: Mutual authentication between AP and MT's (optional) during the Association Phase

- Pre-shared symmetric key authentication (128 bits key)
- RSA-based authentication (512, 768 or 1024 bit keys)
- ✓ Long term keys
- ✓ Key generation, management, storage: outside scope of standard



Authentication Credentials

- Each device comes with a set of **public/private** keys used to build the trust relationship with other devices
 - Hardware/SW keys, e.g. **MAC ID, SIM card, or passwords**
- Upper layers define policies for obtaining the keys and participating in the network
 - e.g., PKI Infrastructure



HL/2 Security - Encryption

Aim: Confidentiality and integrity of transferred data (optional)

- Encrypt Data using DES or 3DES
 - Encryption is possible in AP-MT and MT-MT communication (Direct Mode)
- AP-MT **key exchange** using Diffie-Hellman (DH) protocol
- DM common keys generated and distributed by AP to MT's
 - AP can read all transmitted data (considered trusted)
- **Key Refresh** mechanism

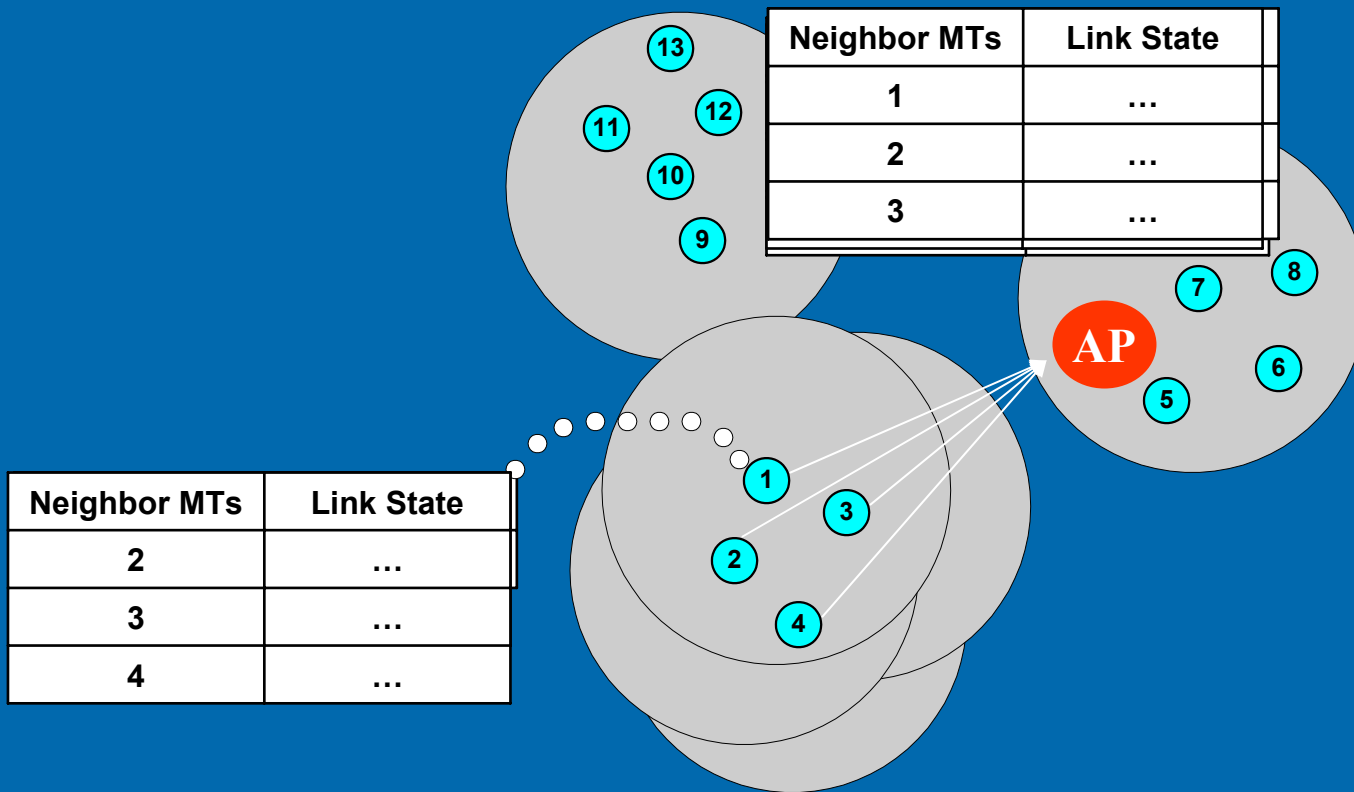


CANA Security Goals

- **Goal: Secure Operations at the MAC Layer**
 - Secure Association
 - Secure Neighborhood-Discovery
 - Secure Data Transmission
- **Built on-top of HL/2 Security Architecture**



Centralized Ad-Hoc Network Architecture (CANA) Neighborhood Discovery (ND)





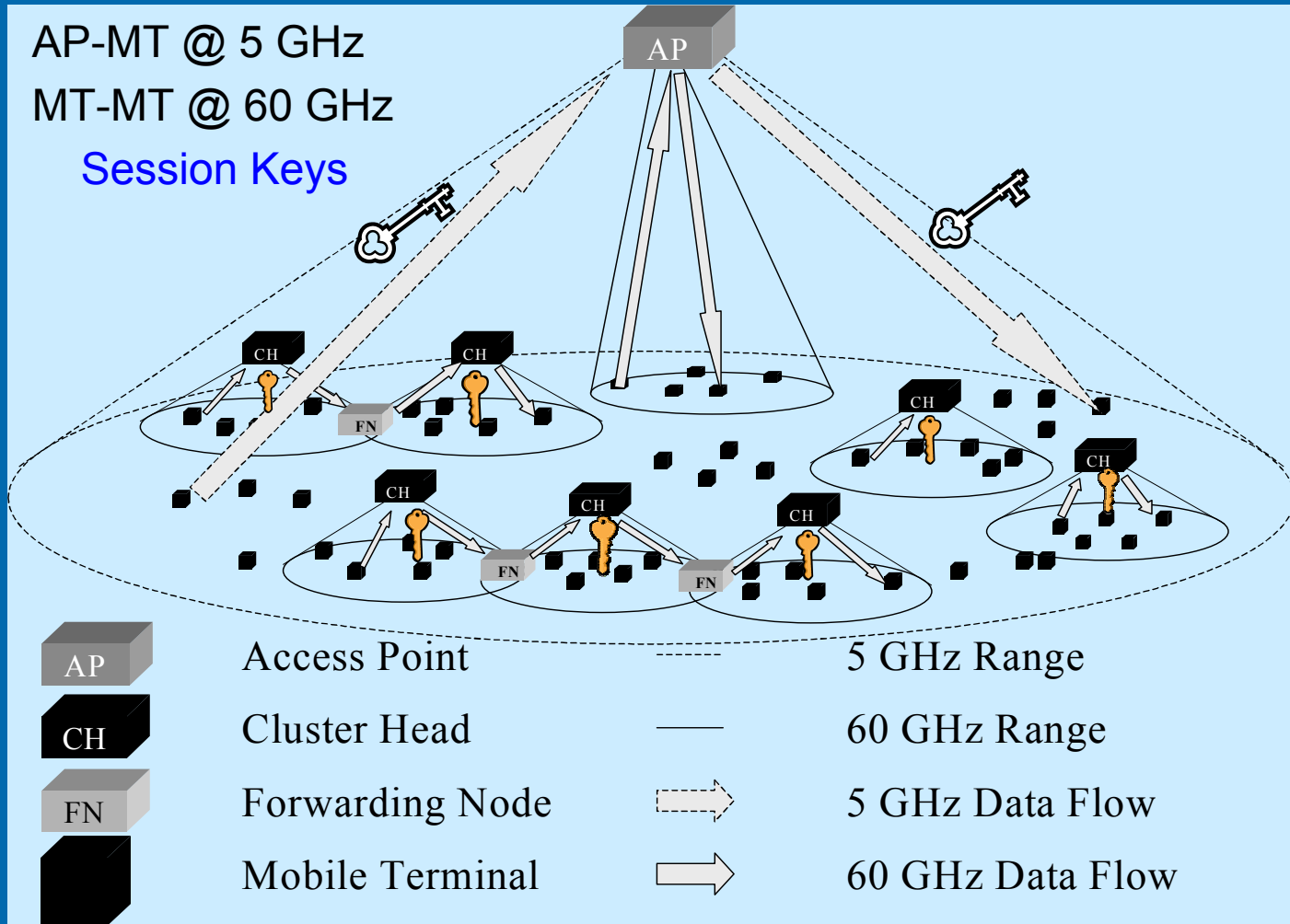
CANA System Architecture



AP-MT @ 5 GHz

MT-MT @ 60 GHz

Session Keys





Session Key Distribution

- Distribution of the 60 GHz mode **Session Keys** from the AP to the CH's and the MT's
 - At 5 GHz, at the end of the ND phase

	8	7	6	5	4	3	2	1
Octet 4	DLCC ID						Future use	
...	SESSION_KEY_PART							
Octet 51								

	8	7	6	5	4	3	2	1
Octet 4	DLCC ID						Future use	
...	MT_RESPONSE							
Octet 51								



CANA Specific Security Requirements

CANA differs from HL/2 from a security point of view in that:

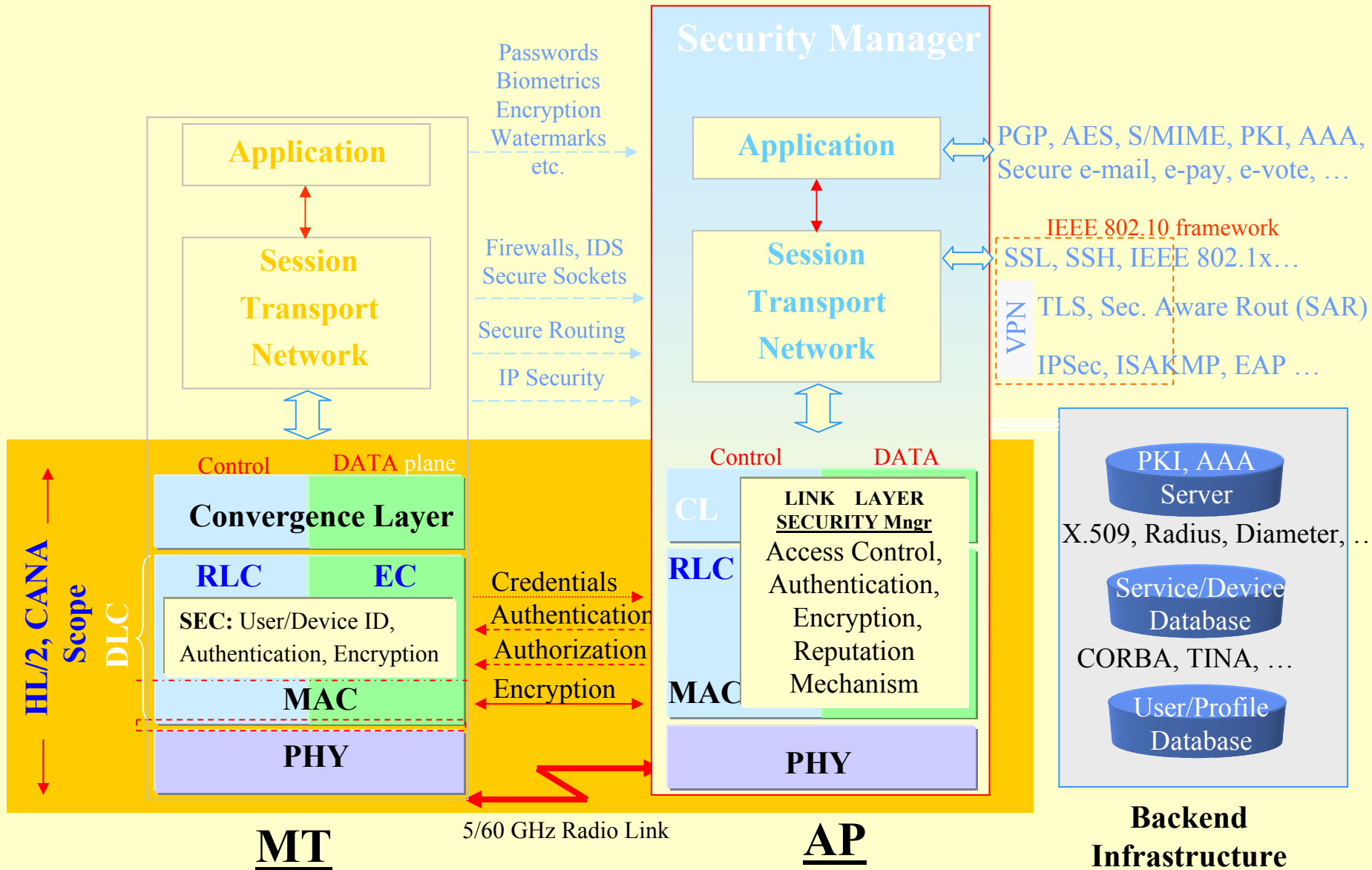
- AP cannot receive all transmissions in 60 GHz
- CH's and FN's are not necessarily trusted
- ND and Routing Protocol attacks
- AP (not CH) generates symmetric keys used by MT's in a cluster



Security Manager

- AP retains the role of **Security Manager**
- Also in charge of **Reputation Mechanism**
- Key component in the overall Security Architecture
- AP is considered to be a **trusted** device
- Assumption:
AP has access to a AAA Server

CANA Security Framework





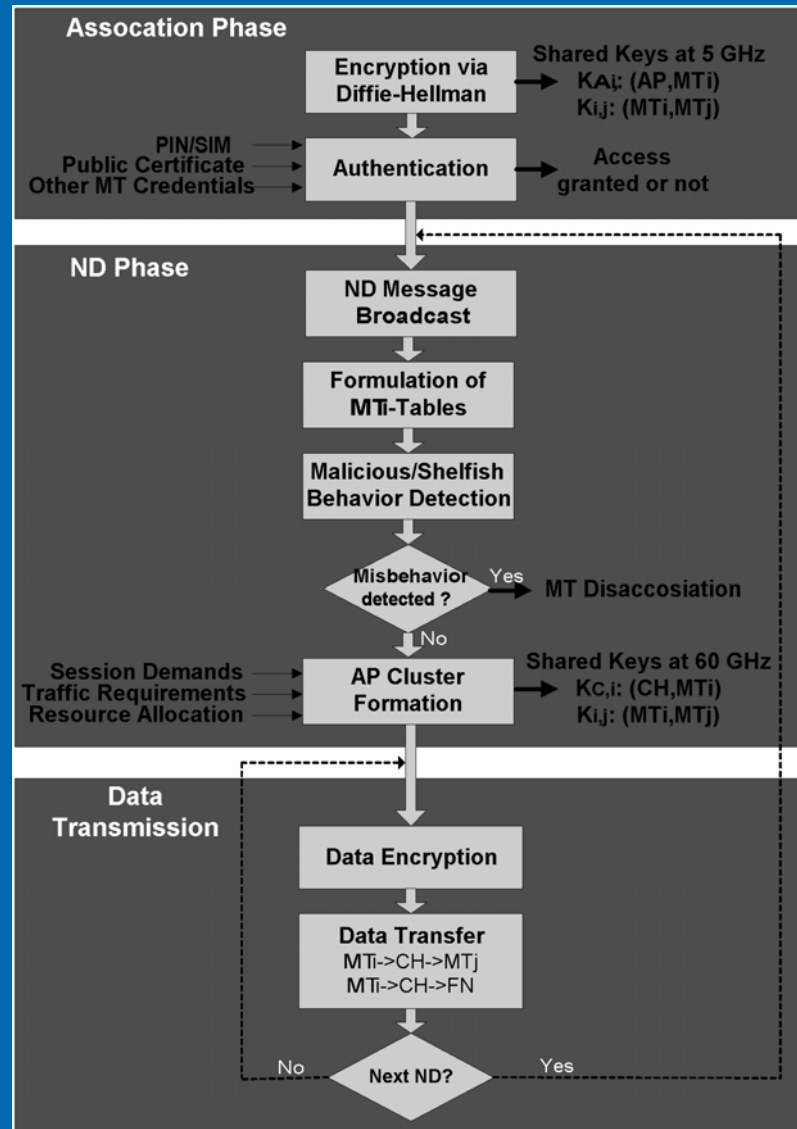
Security Phases

- Association: all MT's to AP
 - Authentication: shared key establishment between AP and each MT
- ND phase
 - Secure cluster formulation among authenticated MT's
 - Malicious – selfish misbehavior detection
 - Properly behaved MT's are granted authorization to participate in a cluster (CH-MT shared key distribution)
- Data Transmission
 - Possible encryption of data as required by upper layers



Security Mechanism of CANA

CANA
modifications
add-ons



Same as in
HL/2



Security Considerations for ND Phase

- An MT can be **Malicious** or **Selfish**, though authenticated
- A **Trust Metric** for each MT is maintained at the AP
- Security protocol should be able to detect and isolate these nodes

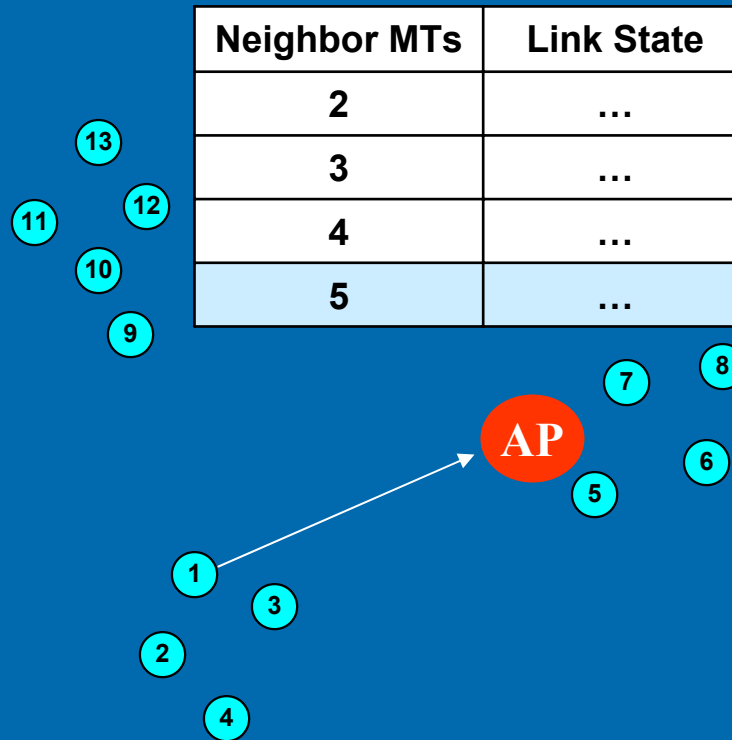


Types of Attack/non-cooperative Behavior

- Modifying MTi-table by *adding* or *removing* nodes
- **Refusing** to send “hello messages”
 - Impossible to detect non-cooperative behavior
 - Not worse than when detected and isolated
- **Replaying** “hello messages” - Wormhole attack
 - impossible in the ND phase of CANA
 - Each MT gets a specific time slot in which to send hello messages



ND Misbehavior – Row Addition



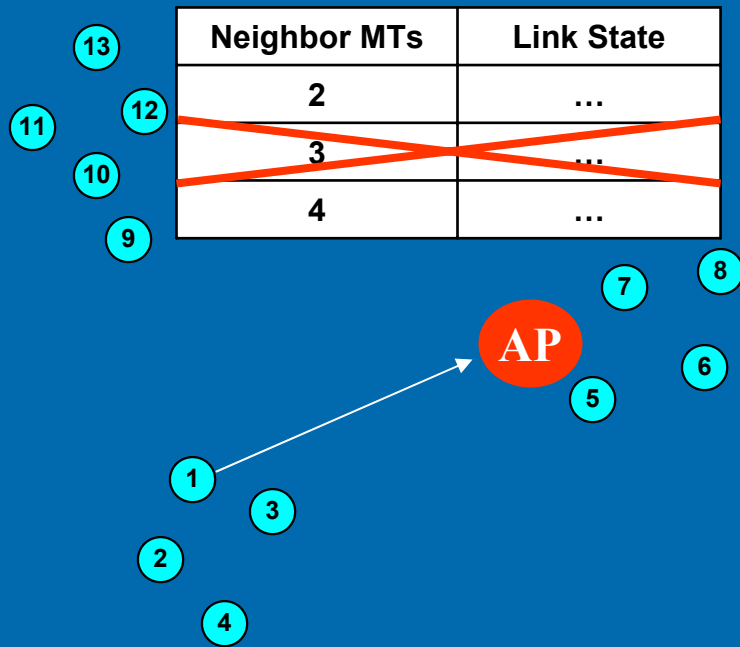


Addressing Security Issues in the ND Phase – Row Addition

- Each MT shares a **symmetric key** with the AP
- Each *Next ND phase* message contains a **random number (r.n.)**
- Each MT **encrypts** this r.n. with its key and includes the result in the hello messages
- The MT_i-tables are **modified** to include a column with these encrypted values and a column with the time-slot when hello message was received
- (1) This way, an addition of false rows to the MT_i-table will be detected by the AP



ND Misbehavior – Row Removal



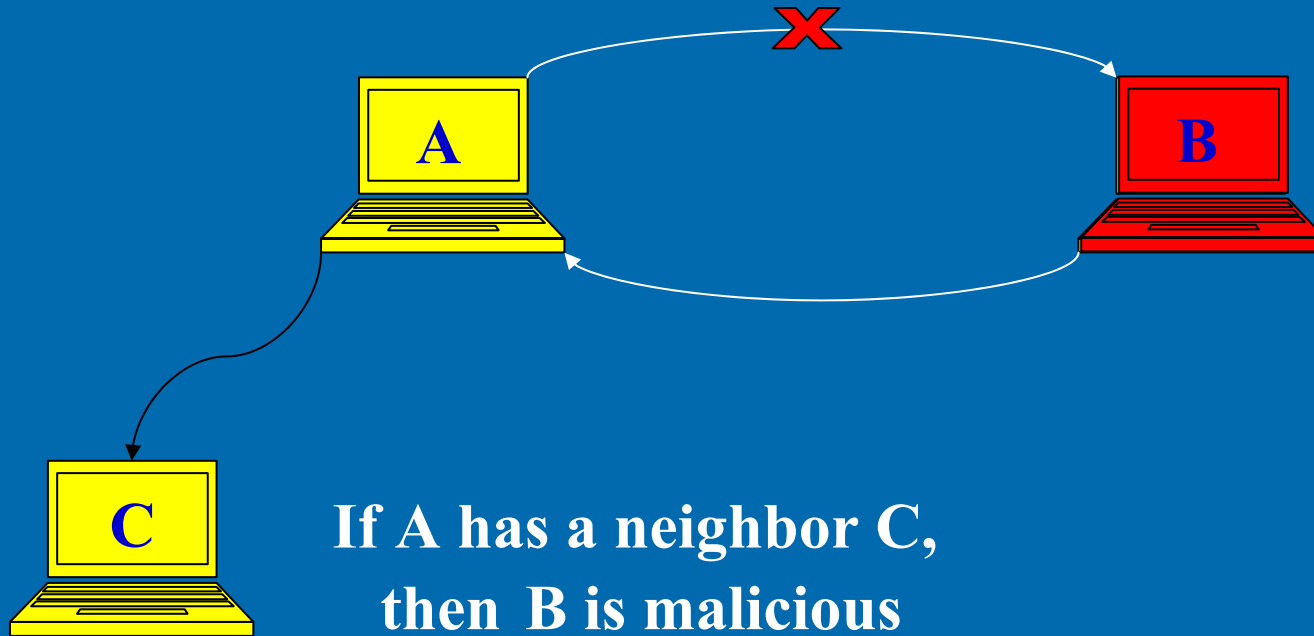


Addressing Security Issues in the ND Phase – Row Removal

- (2) The AP compares MTi-tables to detect **removal of rows** (nodes). Assumptions: symmetric channel, single malicious nodes
- Node A says he heard node B but B says he didn't hear A:
 - Either B is lying (i.e., has removed a row)
 - or, A didn't send hello messages
- Need for **Reputation Mechanism**. AP keeps *Trust Metric* for each MT

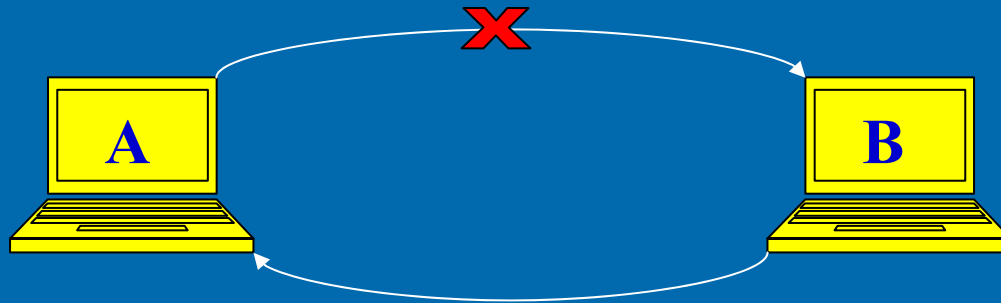


Reputation Mechanism illustration





Reputation Mechanism illustration



If A has no other neighbors,
then the AP doesn't know which node has misbehaved.

Reduce A's trust metric by **a**

If B is malicious it doesn't know in advance if A has other neighbors. Takes risk in accusing A: If A actually has other neighbors B will get caught and being punished (its trust metric will be reduced)!!!



DLC Security Considerations During Data Transmission

- A malicious/selfish CH or FN can **modify** the routing info of a packet or **refuse** to forward it to save resources.
 - The MT that sent this packet to the CH can listen to the channel to make sure that it got forwarded correctly.
 - With the FN this is not possible (two different channels!!!). Hard to address this issue.
 - Need reputation mechanism to inform the AP and other MT's that a node is misbehaving
- A malicious MT can send big amounts of data to clog the network (DoS attack).
 - Data from un-authorized nodes are discarded
 - Misbehavior by an authorized node can be detected at the AP during the establishment of the **session** links.



Conclusions

- CANA security architecture based on HL/2
- CANA raises additional security issues due to its Ad-hoc nature
- Security mechanisms to address ND phase and Data Transmission protocol attacks
 - **Reputation Mechanism** to detect and isolate selfish and malicious nodes
- Enhanced key generation and distribution scheme