IT | SECURITY
RESEARCH GROUP

# Secure and Efficient Handover Protocols for WMNs

## 14th IEEE WoWMoM 2013, Madrid, Spain

André Egners
RWTH Aachen University (Germany)

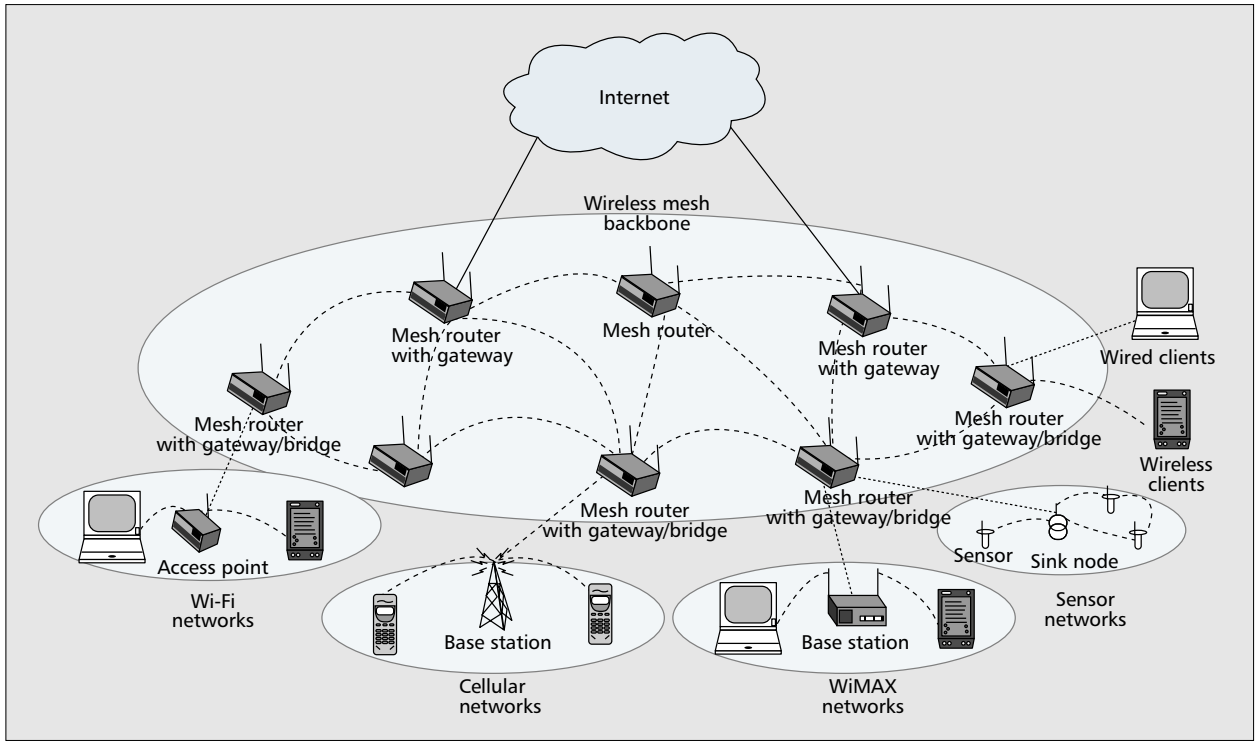
07.06.2013

IT | SEC

IT | SEC

# Motivation

## Enabling handover with infrastructure support in a secure fashion

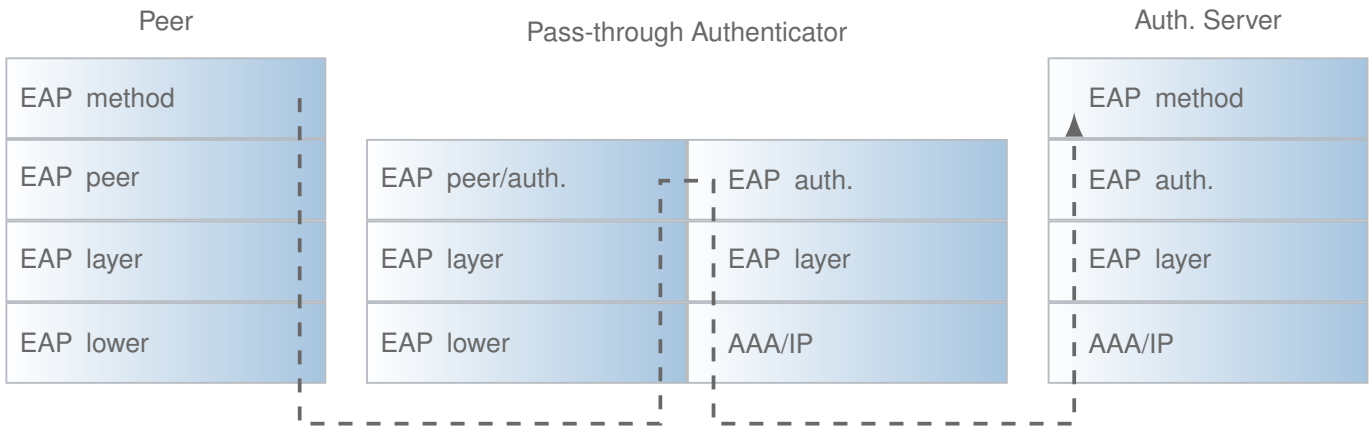



- WMNs are easy to deploy, to extend, and provide relatively high data rates
- Existing security architectures seldom address secure handover
- How can we leverage the infrastructure of these networks?

IT | SEC

# EAP

## Extensible Authentication Protocol

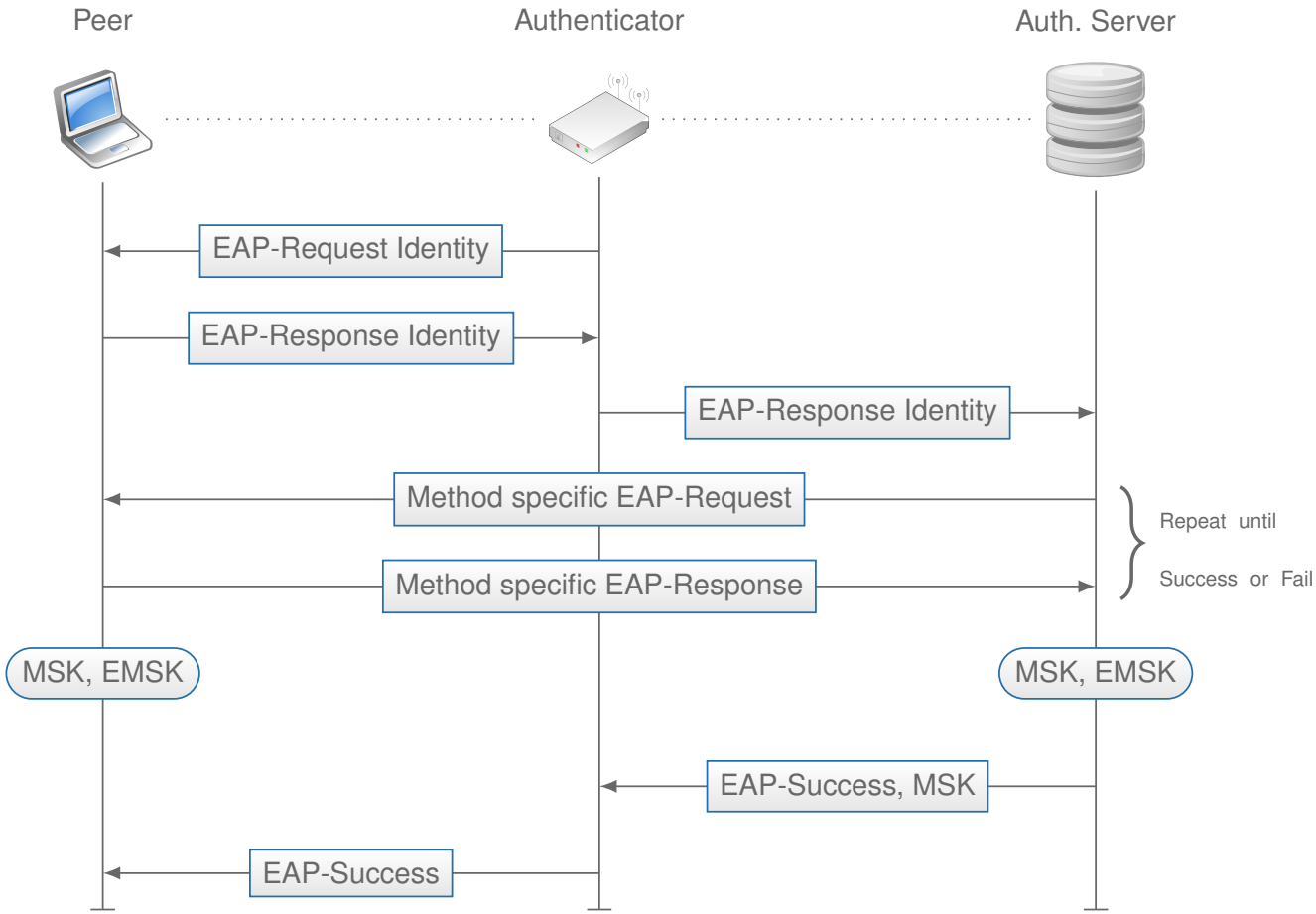



- Supports multiple authentication methods (EAP-TTLS, PEAP, AKA,...)
- Key generating EAP methods:
  - MSK (Master Session Key)
  - EMSK (Extended Master Session Key)

IT | SEC

# EAP

## EAP Operation

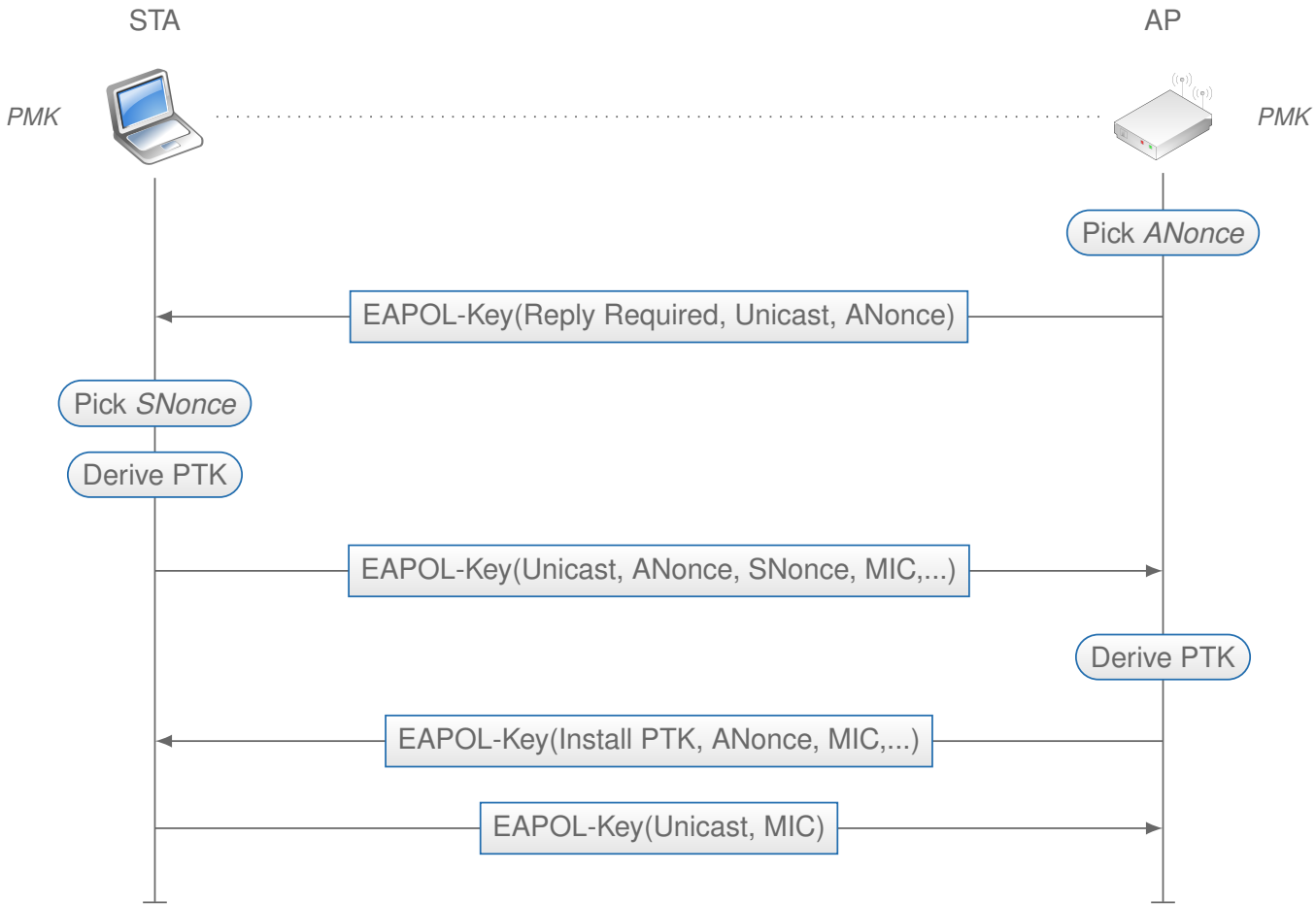



- MSK and EMSK are generated by EAP method
- PMK = first 256 bits of MSK
- 4-way handshake uses PMK to derive transient keys

IT | SEC

# IEEE 802.11i

## 4-way handshake

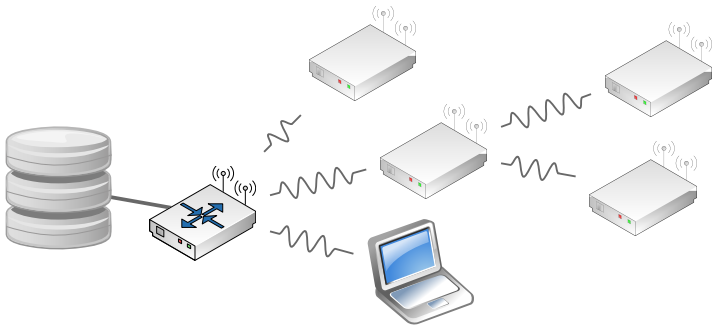


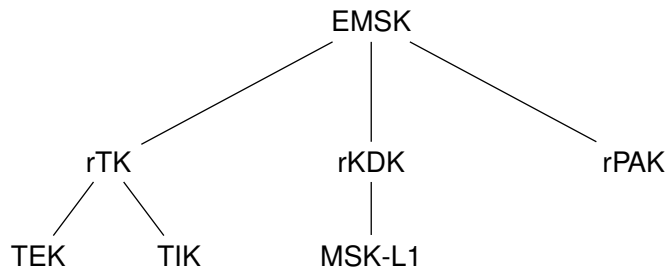

- Goal: Secure link layer communication
- EAPOL = EAP Transport Over LAN
- $\sim$ 4*ms*

IT | SEC

# FSASD

## Framework for Sequential Deployment of WMNs






- Allows simple and secure sequential deployment of WMNs
- Uses EAP-TTLS which provides secure EAP authentication over several hops
- EMSK spawns key hierarchy to derive keys for IPsec ESP
- Authentication traffic is secured by IPsec
- 3-party handshake protocol for sequential deployment (3PHSD)
  - MC $\leftrightarrow$ MG, MC $\leftrightarrow$ MC, MC $\leftrightarrow$ MR

IT | SEC

# Related Mechanisms

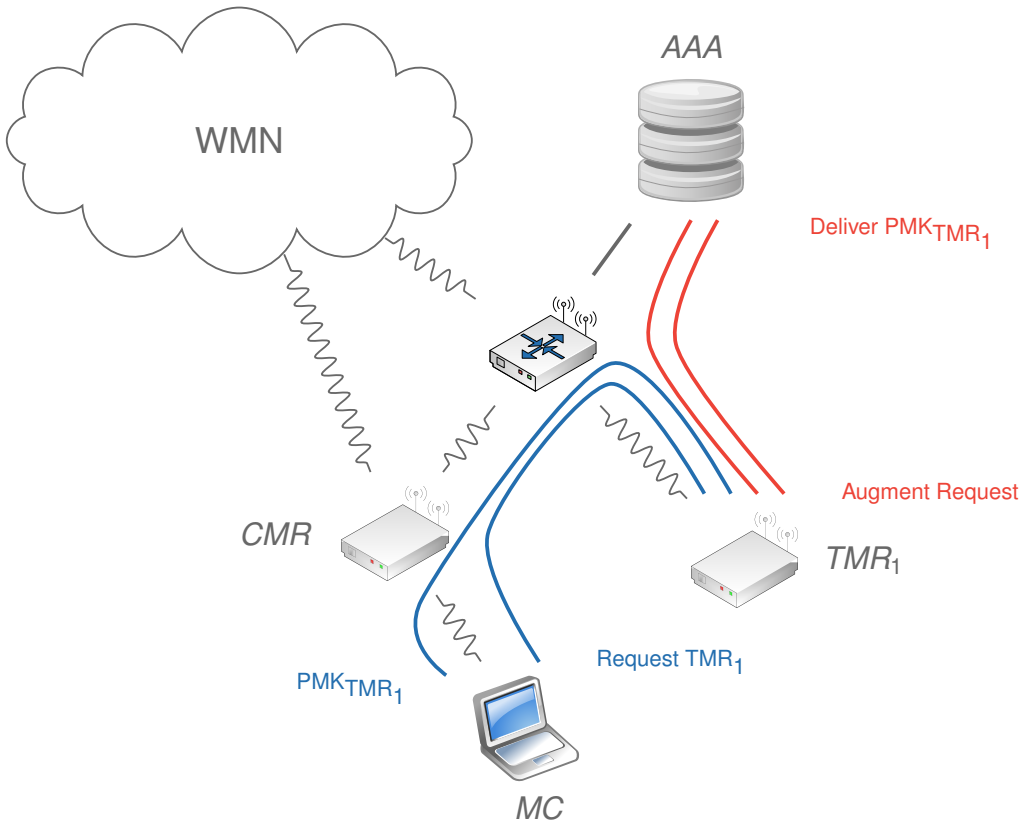
## ...and “standards” *not* for WMNs

- 802.11r - trusted APs, no secure key transport between APs
- ERP - insecure key transport AAA-NAS
- CAPWAP - new split of PHY/MAC, custom devices required

IT | SEC

# 3-Party-Handshake Protocol for Handover (3PHSH)

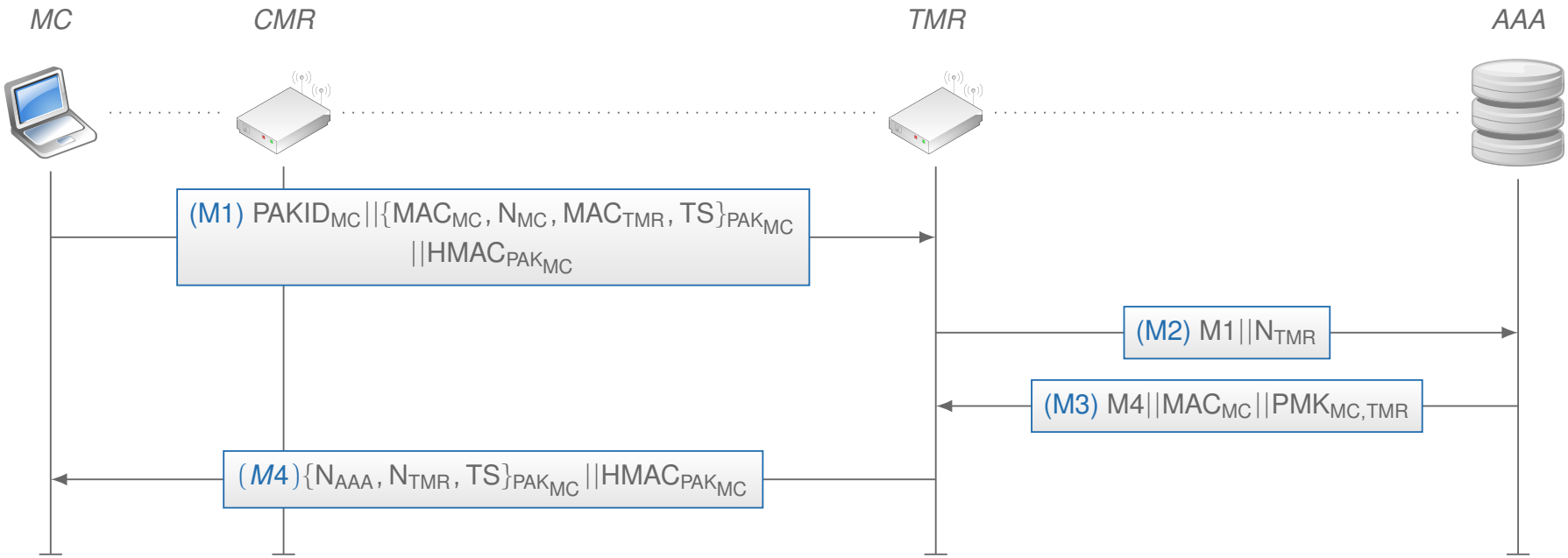
## Overview




- Extend 3PHSD to pro-actively request a fresh PMK for one TMR
- TMR and MC cache PMK
- Use cached PMK to avoid full EAP-TTLS re-authentication

# 3-Party-Handshake Protocol for Handover (3PHSH)

## Message Flow

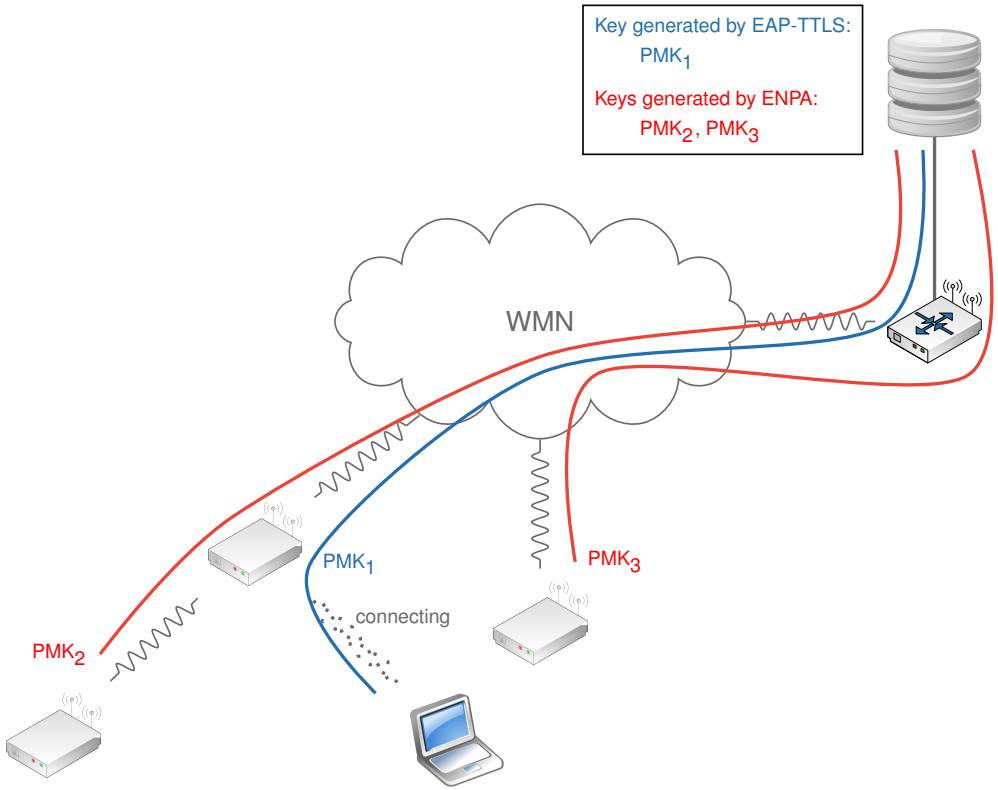



$$PMK_{MC,TMR} = KDF(rKDK_{MC,AAA}, \text{key\_label}||N_{TMR}||N_{AAA}||N_{MC}||MAC_{MC}||MAC_{TMR})$$

IT | SEC

# EAP-TTLS Neighborhood Pre-Authentication (ENPA)

## Overview

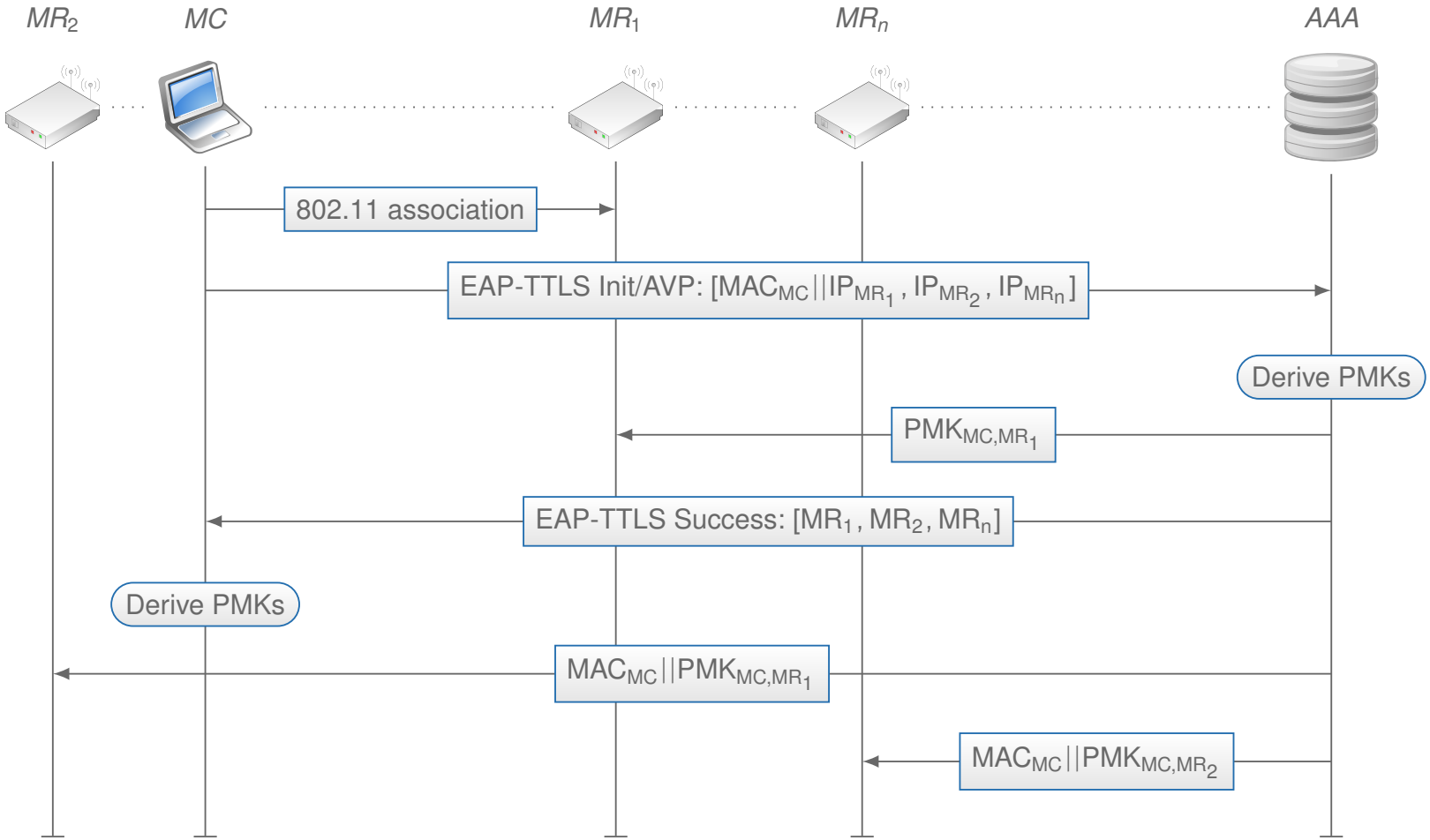



- Request fresh PMKs for the other MRs during initial association
- Embedded into EAP-TTLS authentication
- Also works with EAP methods supporting Diamter AVPs
- Use cached PMKs to avoid full EAP-TTLS re-authentication

IT | SEC

# EAP-TTLS Neighborhood Pre-Authentication (ENPA)

## Message Flow

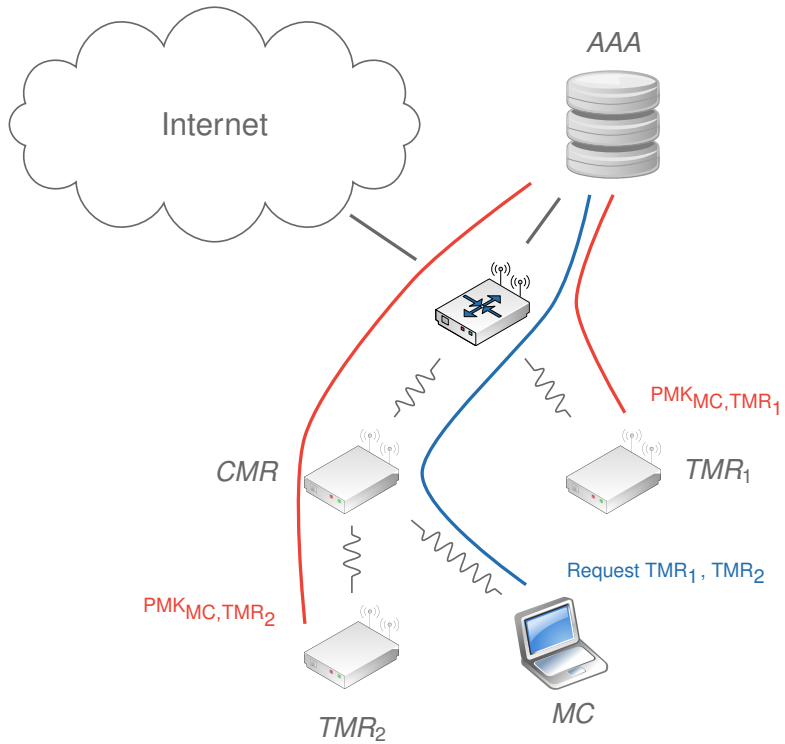



$$PMK_{MC,TMR_i} = KDF(rKDK_{MC,AAA}, \text{key\_label}||IP_{TMR_i}||\text{tls\_client\_random}||\text{tls\_server\_random})$$

IT | SEC

# Neighborhood Pre-Authentication (NPA)

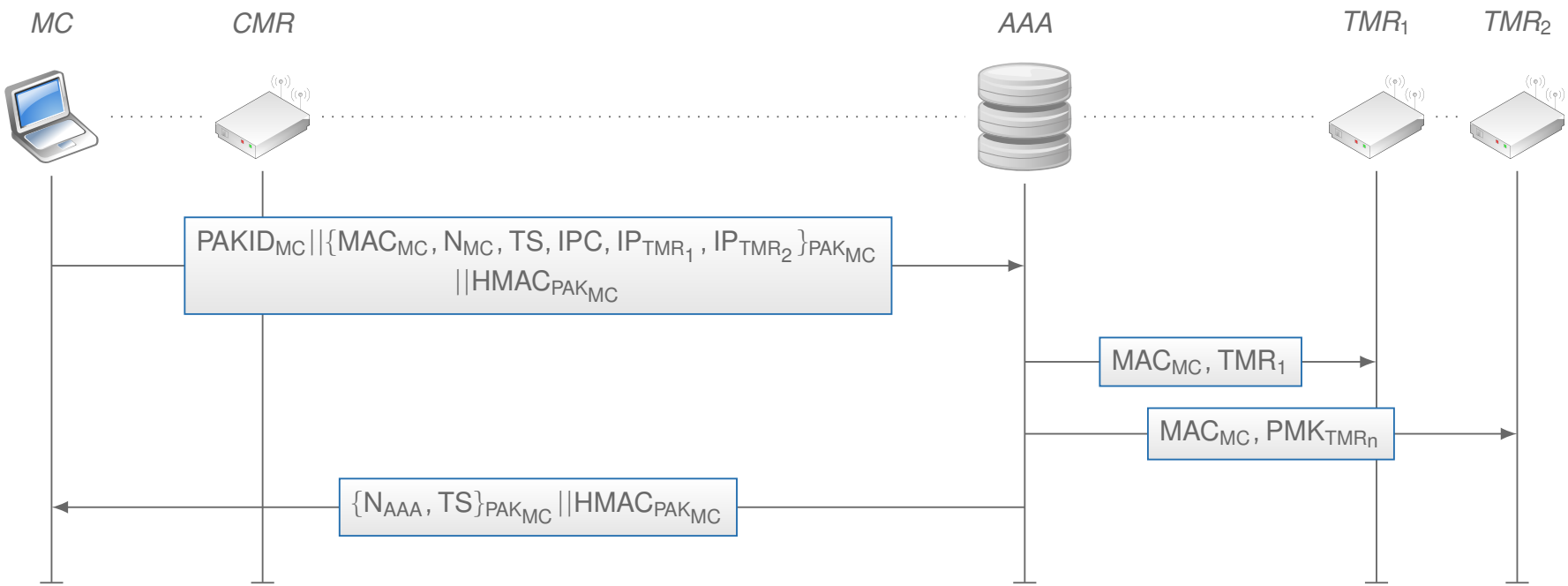
## Overview




- “Combine” 3PHSH and ENPA
- MC is connected to WMN
- Request PMKs for several TMRs in range at once
- Use cached PMK to avoid full EAP-TTLS re-authentication

# Neighborhood Pre-Authentication (NPA)

## Message Flow




$$\mathrm{PMK}_{\mathrm{MC,TMR}_i} = KDF(rKDK_{MC,AAA}, \mathrm{key\_label}||MAC_{MC}||N_{MC}||N_{AAA}||IP_{TMR_i}) \quad (1)$$

IT | SEC

# Security Analysis

## Overview

- Analysis is based on “Best Practice” RFC 4962 “Guidance for AAA Key Management”
- 11 requirements a protocol should satisfy
- ENPA is embedded in a AAA protocol
- 3PHSH and NPA can only be used after a successful authentication

IT | SEC

# Security Analysis

1. Cryptographic algorithm independent ✓
2. Strong, fresh session keys ✓
3. Limit key scope ✓
4. Replay Protection ✓
5. Authenticate all parties ✓
6. Peer and authenticator authorization ✓
7. Keying material confidentiality and integrity ✓
8. Confirm ciphersuite selection ( )
9. Uniquely named keys ✓
10. Prevent the domino effect ✓
11. Bind the key to its context ✓

# Performance Evaluation



See paper

# Conclusion

- No secure and practical approaches for WMNs exist
- Three protocols to pro-actively request PMKs
  - 3PHSH
  - ENPA
  - NPA
- MC determines candidate MRs itself (currently IP included in beacons)
- Exploited the security properties of FSASD
- Two protocols are faster than the EAP-TTLS re-authentication
  - 3PHSH (wireless hops 7): $\approx 25ms + 4ms$
  - NPA (max. distance 4, IP count 5): $\approx 10ms + 4ms$
- ENPA nearly same duration as EAP-TTLS: $300ms$
  - takes $5ms$ longer for adding 1 TMR
  - only 4-way-handshake needed to roam afterwards: $4ms$

IT | SEC

Q?

André Egners
Research Group IT Security
RWTH Aachen University
Germany
egners@umic.rwth-afachen.de
https://itsec.rwth-aachen.de