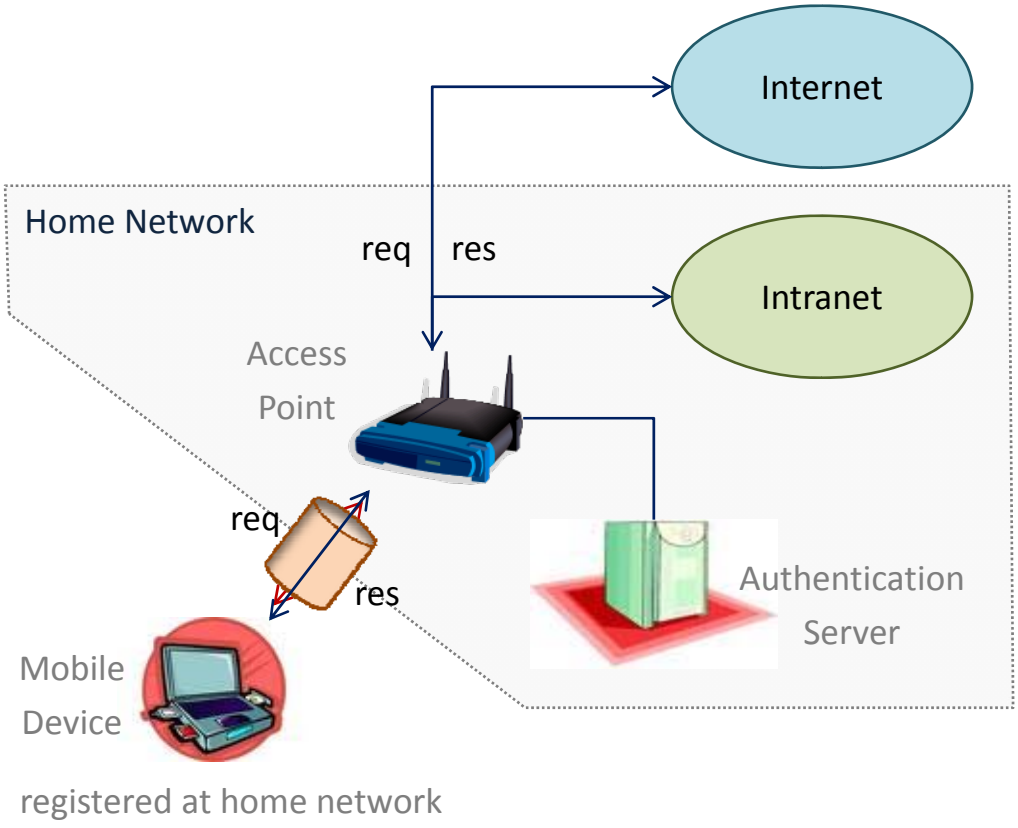
CASED

TECHNISCHE UNIVERSITÄT DARMSTADT

Securing Remote Access *Inside* Wireless Mesh Networks

Mark Manulis
Cryptographic Protocols Group
TU Darmstadt & CASED
Germany

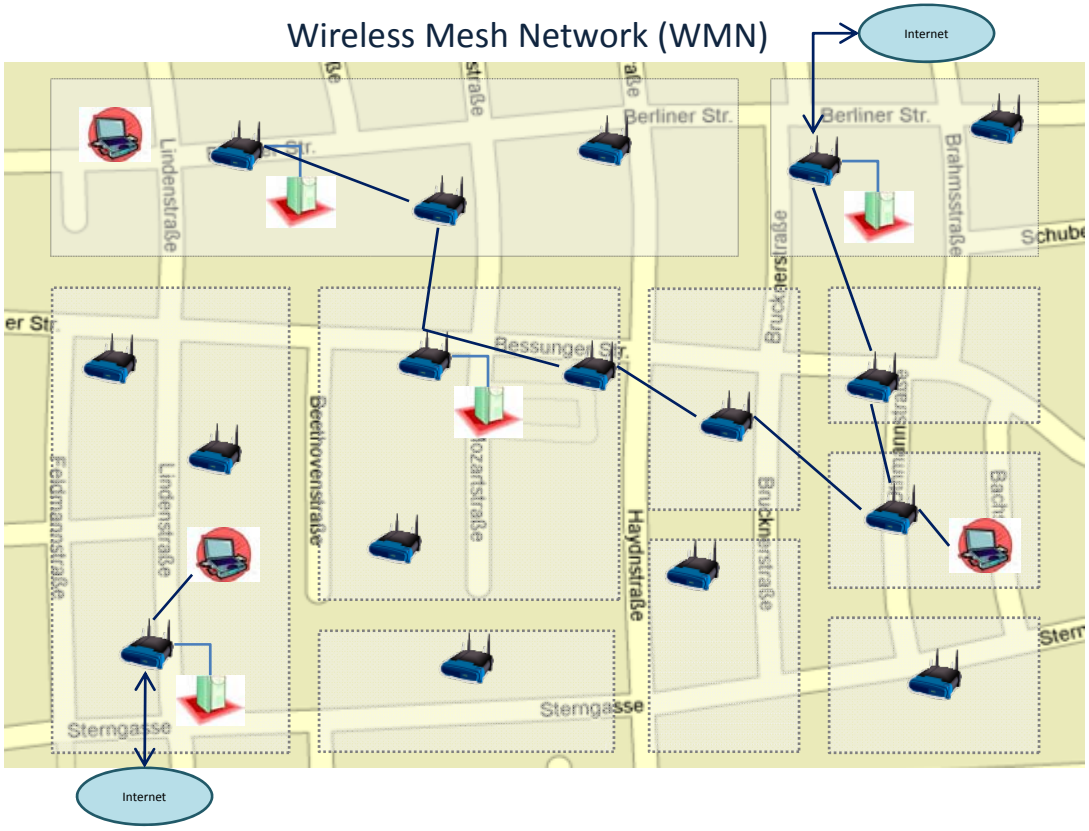
Wireless (Local-Area) Networks



Access in Wireless LANs

- IEEE 802.11i (WPA)
- IEEE 802.X (EAP + RADIUS)

Wireless Mesh Networks



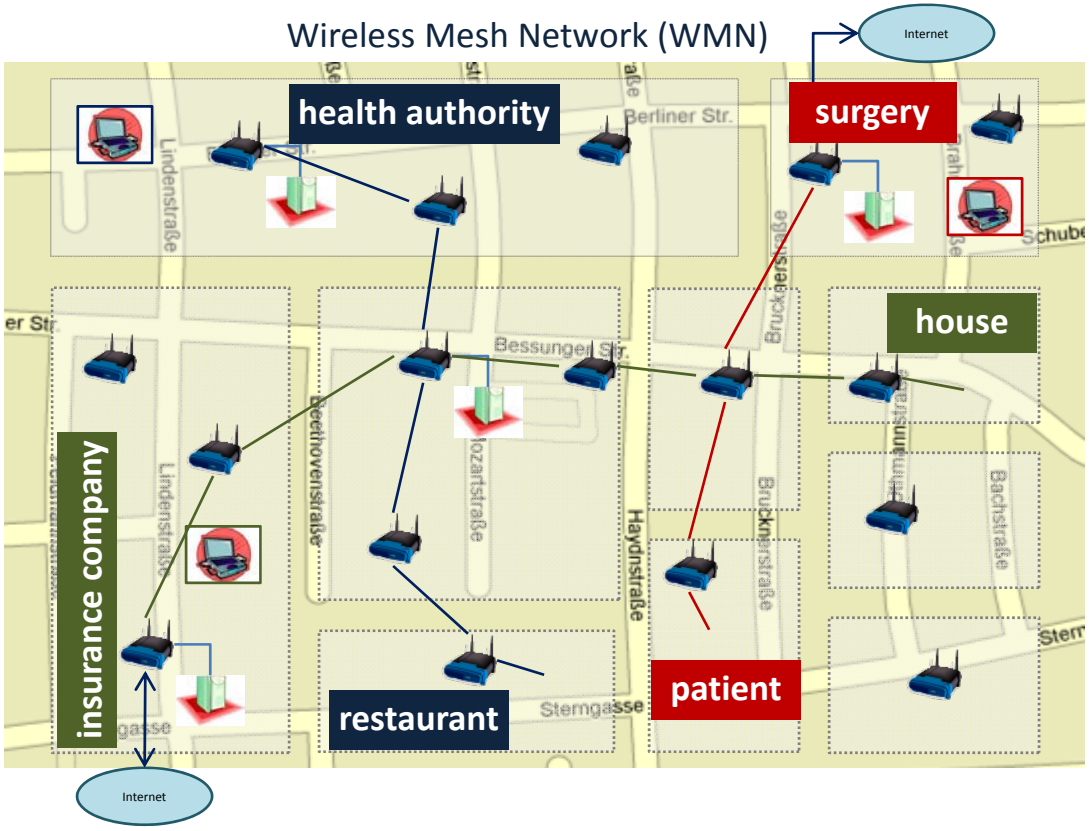
Access in Wireless LANs

- IEEE 802.11i (WPA)
- IEEE 802.x (EAP + RADIUS)

Wireless Mesh Networks

- composition of WLANs into one mesh
- dynamic routing (AODV, DSR, LQSR)
  IEEE 802.11s (upcoming standard)
- stable infrastructure
- powerful routers
- cooperation is inevitable
- useful in urban areas and communities

Application Scenarios



Urban Area WMNs

- private households
- places of public interest

Scenarios / Community Services

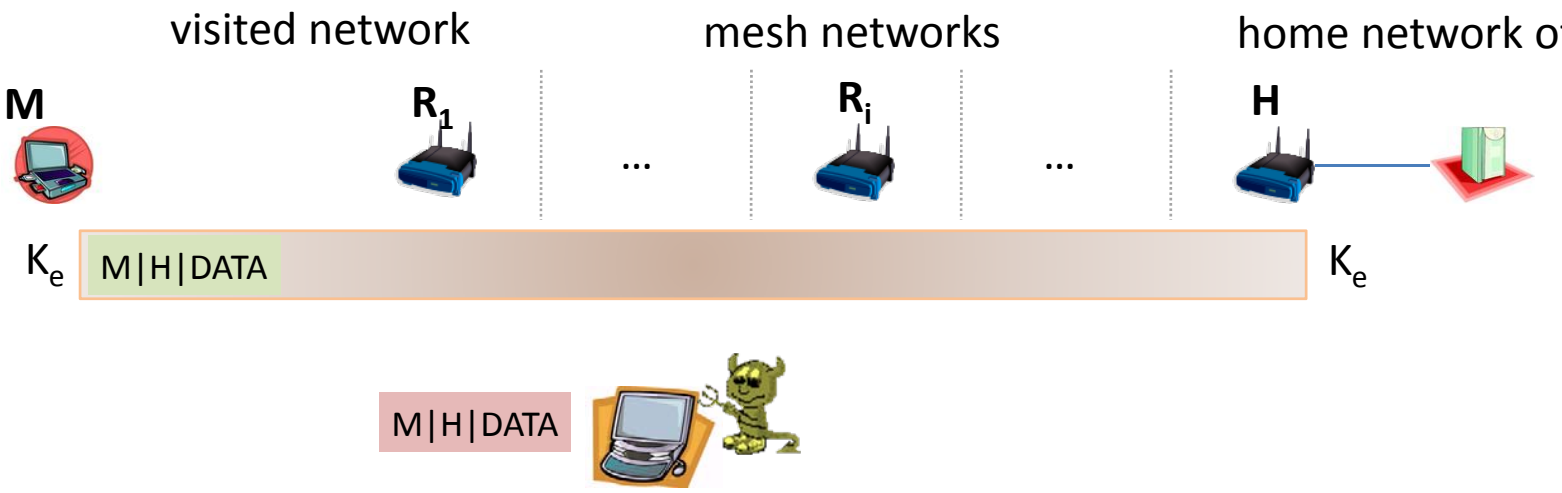
- doctors visiting patients
- health authority workers on patrol
- insurance salesmen visiting customers

…

Remote Access Control

- mobile devices ↔ home networks
- low mobility of users
- session-wise stable routes
- need for protection

Secure Remote Network Access



End-to-End Security

secure channel (authenticated and confidential) between M and R_n

typically realised via VPN tunnels (e.g. IKEv2 + IPsec)

visited and intermediate networks are treated as potential adversaries

Is this enough in WMNs?

wireless multi-hop channel allows injection of rogue packets

→ resource consumption attacks, negative impact on cooperation amongst R_i

The Concept of Path Security

Observations

end-to-end protection is transparent to the routing infrastructure

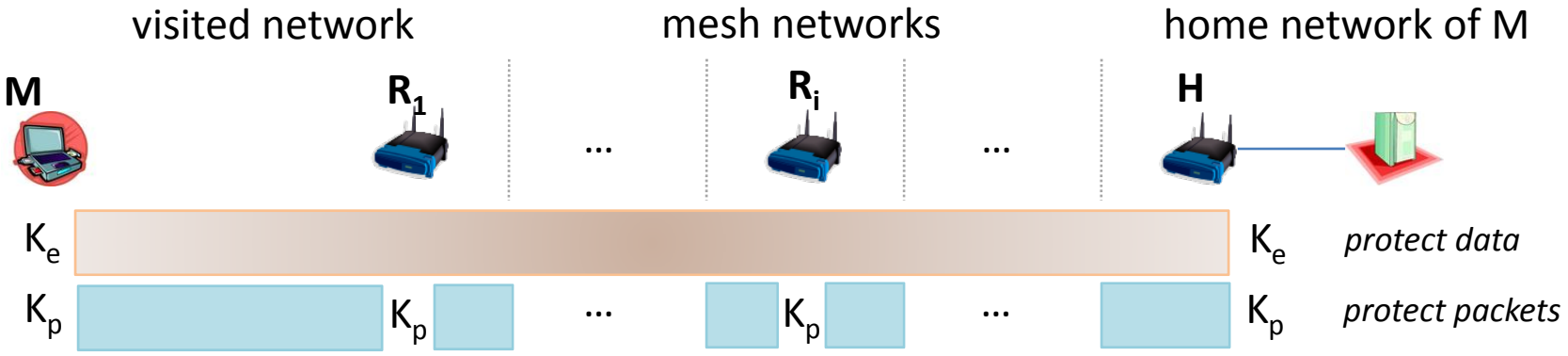
intermediate mesh routers cannot link packets to remote sessions

→ cannot distinguish packets originated by end points from rogue packets

→ some incentive mechanisms (e.g. reimbursement) would not work properly

New Concept: Path security

- binding between the session and the underlying path (feasible due to stable routes, low mobility)
- protection of packets along the path between M and H (using additional *path key* K_p)
- authentication between the end points and intermediate mesh routers



SERENA Protocol (Basic Version)

One protocol – Two Main Goals

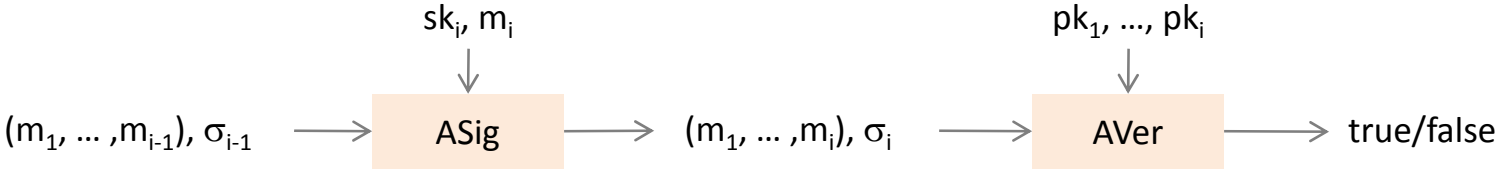
- end-to-end secure communication over wirelesss multi-hop channel
- security along the established wireless multi-hop path (i.e. path security)

Idea

compute path key as a by-product of a two-party key establishment protocol between M and H

Building blocks

- pseudo-random function PRF for the derivation of keys
- asymmetric encryption scheme (E, D) for the transport of the path key
- message authentication code MAC for authentication between H and M
- digital signature scheme (Sig, Ver) for authentication of H towards R_i
- sequential aggregate signature (ASig, AVer) for authentication of $\{R_i\}_i$ towards H



Initialization in SERENA

Initialization of the home network H

H holds a signature key pair (sk_i, vk_i)

Registration of M within H

- M and H share high-entropy symmetric keys (k_M, α_M)
- k_M will be used as a PRF key
- α_M will be used as a MAC key

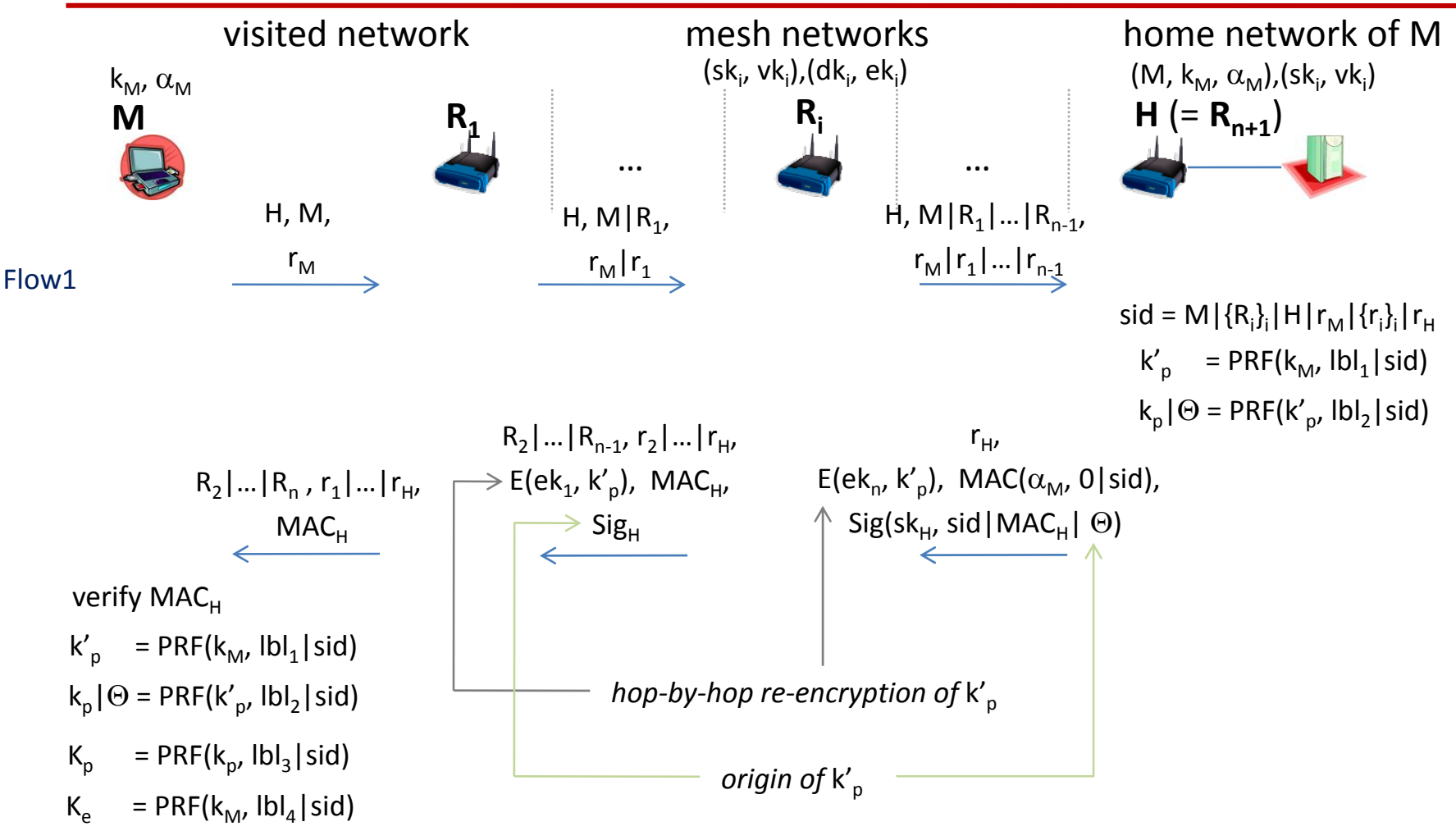
Initialization of mesh networks R_i

R_i holds own aggregate signature key pair (sk_i, vk_i) and own encryption key pair (dk_i, ek_i)

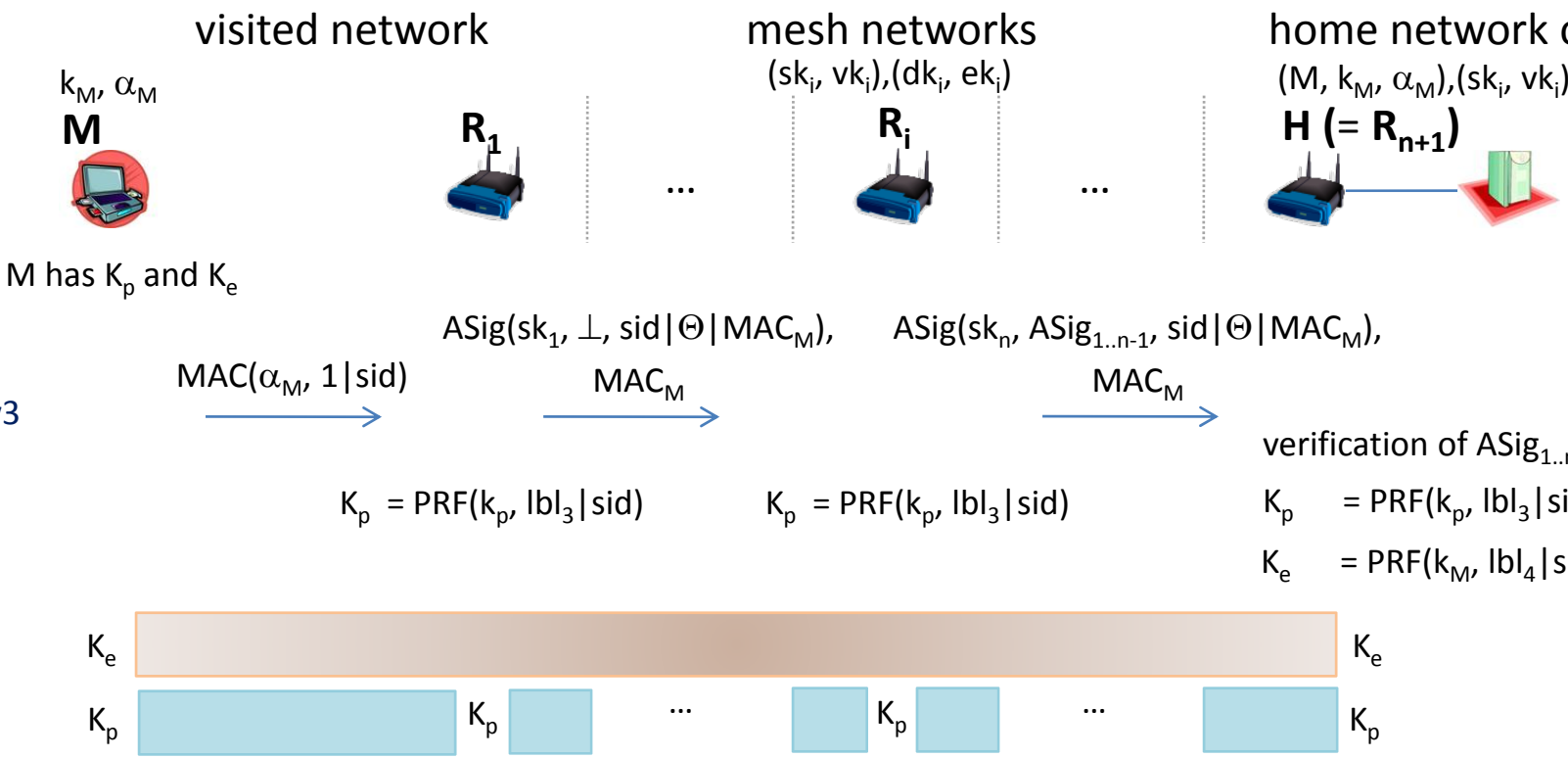
Practical remarks

- H is part of the same mesh
- „aggregate signatures imply signatures“ → H needs only one aggregate signature key pair
- k_M and α_M can be derived from one shared secret using PRF (possibly with expansion)
- public keys vk_i and ek_i are assumed to be known within the mesh

Execution of SERENA (Flows 1 and 2)

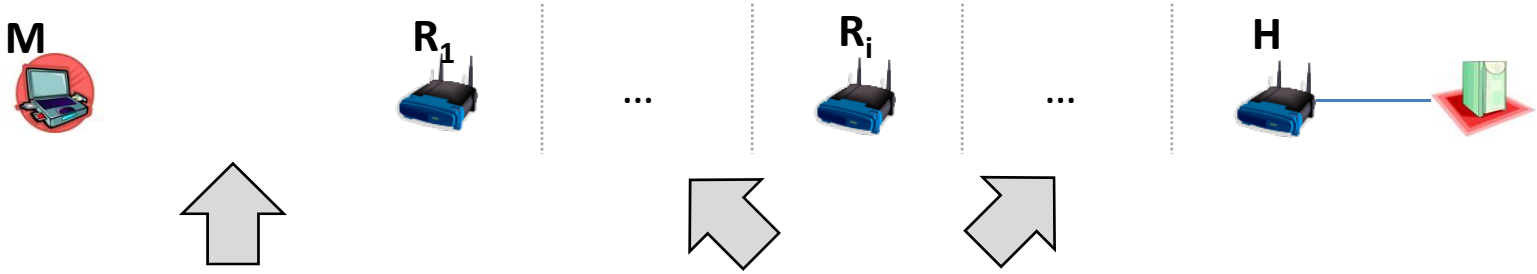


Execution of SERENA (Flow 3)



M obtains access to H over the wireless multi-hop path R_1 , …, R_n

Realization Ideas based on Standards



Execution of SERENA

1. R_1 works as access point and mesh router
2. M connects to R_1 at data link layer
3. M and R_1 start SERENA as new EAP method within IEEE 802.1X
4. Encapsulation of EAP messages along the path using some carrying protocol, e.g. PANA (RFC 5191)
5. H works as router and authentication server

Secure Remote Connection

end-to-end security	IPsec (AH/ESP) in the *tunnel mode* with K_e
path security	IPsec (AH/ESP) in the *transport mode* with K_p

In comparison to VPNs (IKEv2 + IPsec) we can have SERENA + IPsec

Extensions and Conclusion

Forward secrecy

- not considered in the basic version
- can be achieved for K_e using Diffie-Hellman method
- can be achieved for K_p using Generalized Diffie-Hellman method (Bresson et al. CCS'01)

Anonymity of M

- M can send $E(ek_H, M)$ instead of M since H would have an encryption key pair as well
- suitable encryption achieves unlinkability as well

Accounting between H and R_i

- in basic version R_i obtains $Sig(sk_H, sid|*)$
- signed message can be extended with a time-stamp

Security analysis

- extension of two-party Bellare-Rogaway'93 model to WMNs
- definitions of security for K_e and K_p and mutual authentication $M \leftrightarrow H$ and $H \leftrightarrow R_i$
- security proofs