OnboardICNg: a Secure Protocol for On-boarding IoT Devices in ICN

Alberto Compagno, Sapienza University of Rome/Cisco
Mauro Conti, University of Padova
Ralph Droms, Cisco

(to appear in ACM ICN '16)

OnboardICNg

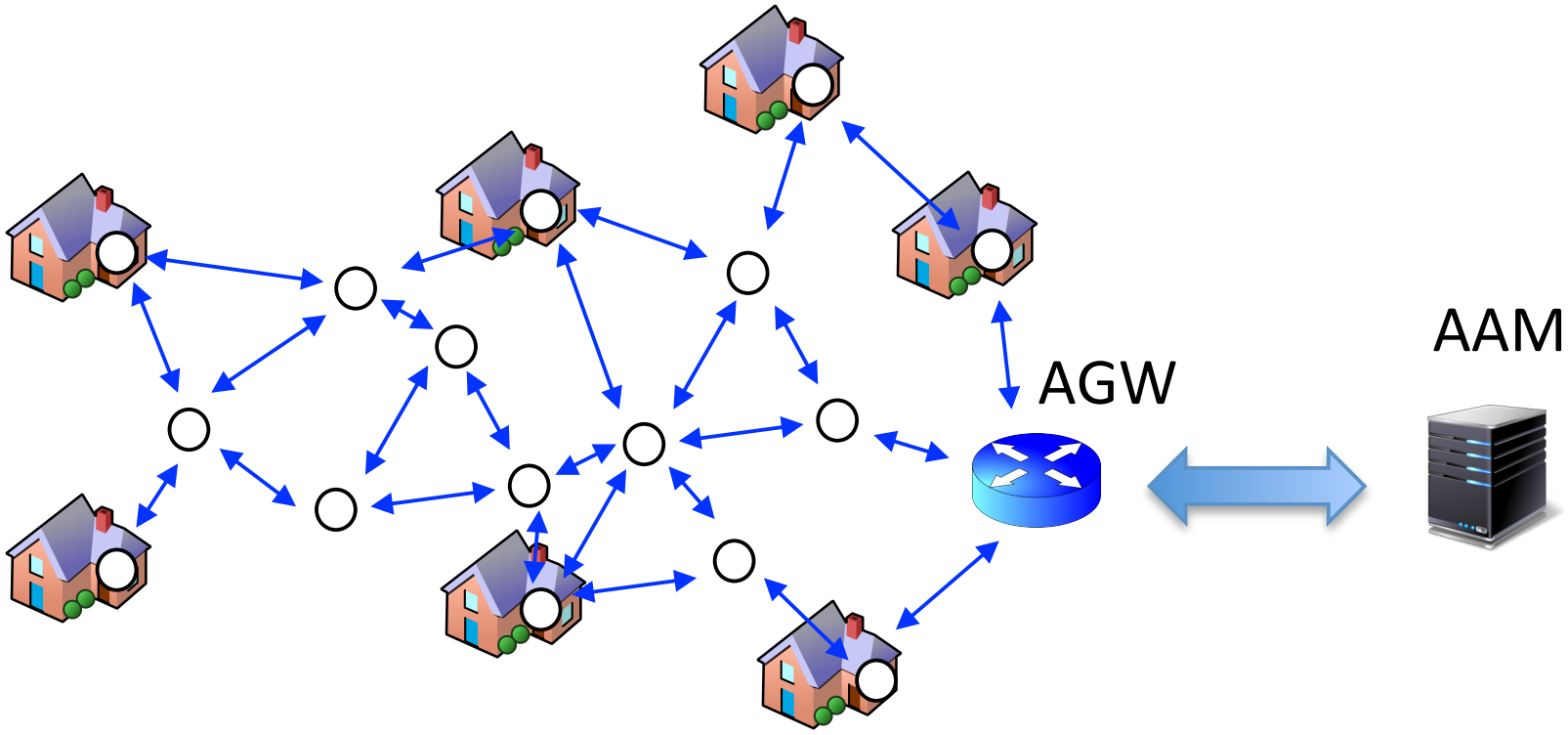
A secure protocol for on-boarding constrained devices into a wireless mesh network

Analog to EAP-PANA onboarding in ZigBee-IP

Roadmap:

- Protocol description
- Security properties
- Resource usage comparison to ZigBee-IP EAP/PA

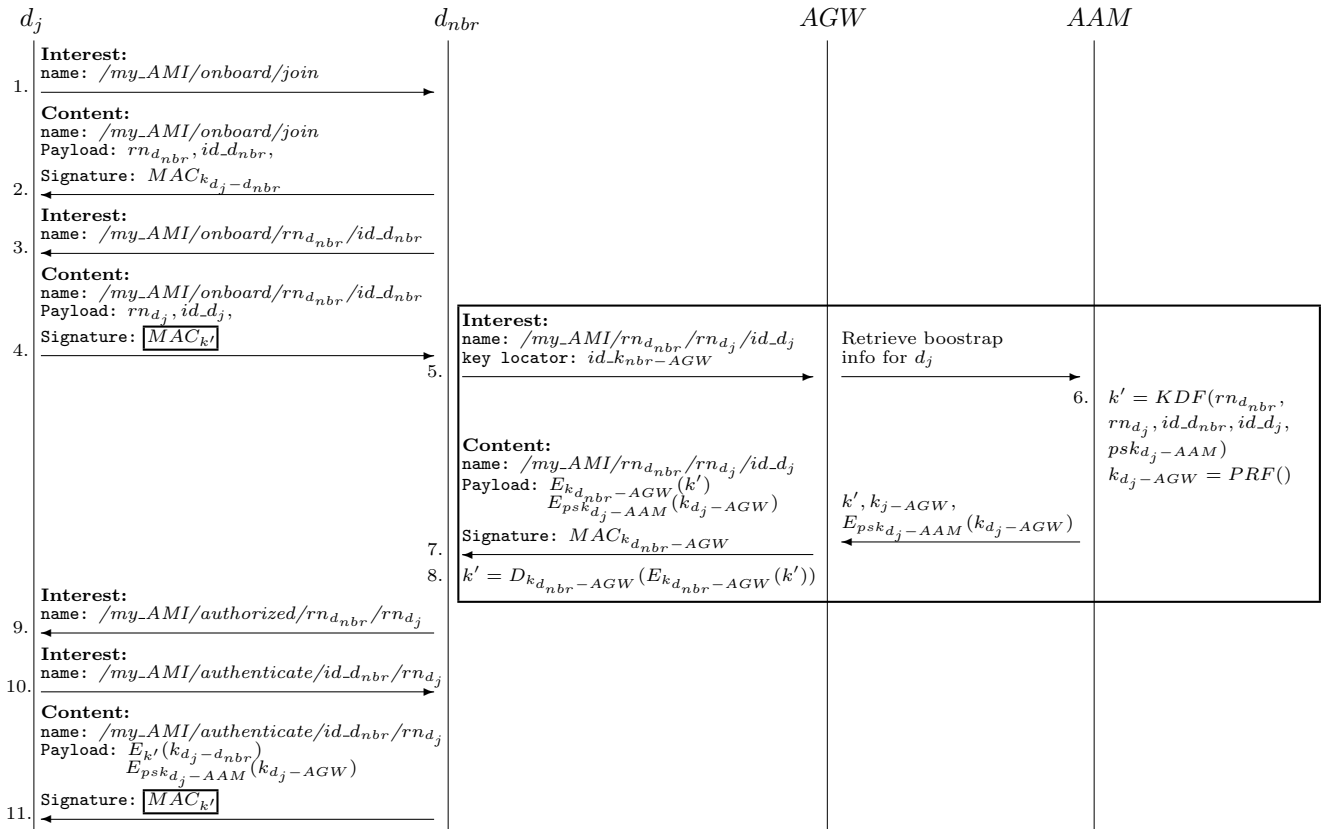
System Model



Design Requirements

- **Mutual Authentication:** The trusted network and the joining device d_j are able to mutually authenticate
- **Fresh Authorization:** The protocol guarantees that the authorization to join the network is fresh and unique, generated specifically for the current protocol session.
- **Minimal network traffic:** The protocol minimizes the interaction with the AAM in order to preserve the overall network's and devices' resources.
- **Bootstrap the initial key material:** The protocol must distribute the necessary cryptographic material to later allow a secure key management and communications.

Protocol Message Flow



Security Discussion

- Fraudulently join a trusted network

  Outsider: to mislead d_{nbr}, md_j needs to obtain a valid k'; however, (a) md_j cannot have a PSK to derive k', (b) k' cannot be eavesdropped

  Insider: (a) cd_{nbr} collaborates with md_j; however, the authorization phase for md_j at the *AAM* fails, or (b) cd_{nbr} clones itself to attach elsewhere, which can be detected by duplicate authorization at *AAM*

- Impersonate a trusted network

  Outsider: To force d_j to authenticate the malicious device md_{nbr} as a trusted device, the outsider must either retrieve a valid k' or break the AKEP2 scheme

  Insider: cd_{nbr} needs the PSK belonging to d_j to spoof the packet in step 11

- Obtain the distributed symmetric keys

  Outsider: PSK for d_j is never transmitted across the network; to extract k', attacker needs PSK for d_{nbr}, which is encrypted with PSK for d_j

  Insider: PSK for d_j is never transmitted across the network; to extract k', cd_{nbr} needs PSK for PSK for d_{nbr}, which has been securely established during d_{nbr}'s onboarding phase

Evaluation against EAP-PSK/PANA

Metric	OnboardICNg		EAP-PSK/PANA	
	d_j	d_{nbr}	d_j	d_{nbr}
Communication (bytes transmitted)	549 bytes	318 bytes	1380 bytes	2481 bytes
Computation (milliseconds)	60.73 ms	53.87 ms	72.65 ms	0.00 ms
Energy (microjoules)	5993 µjoules	7082 µjoules	10905 µjoules	20695 µjoules
Memory (bytes)	332 bytes	159 bytes	224 bytes	0 bytes

Conclusion

- OnboardICNg provides secure authentication and authorization to join a wireless mesh network using ICN
- Resilient to outsider and insider attacks
- Securely bootstraps cryptographic material for subsequent secure communication
- Resource utilization compares favorably with EAP-PSK/PANA