Cryptographic Challenges for Smart Grid Home Area Networks Secure Networking

Apurva Mohan
Honeywell ACS Labs

November 7th, 2011
Gaithersburg, MD

Honeywell

Outline

- Introduction
- Overview of security challenges in HANs
- Communications security
- Key management
- Public key infrastructure
- Device hardware security
- Summary

Honeywell

Outline

- Introduction
- Overview of security challenges in HANs
- Communications security
- Key management
- Public key infrastructure
- Device hardware security
- Summary

Honeywell

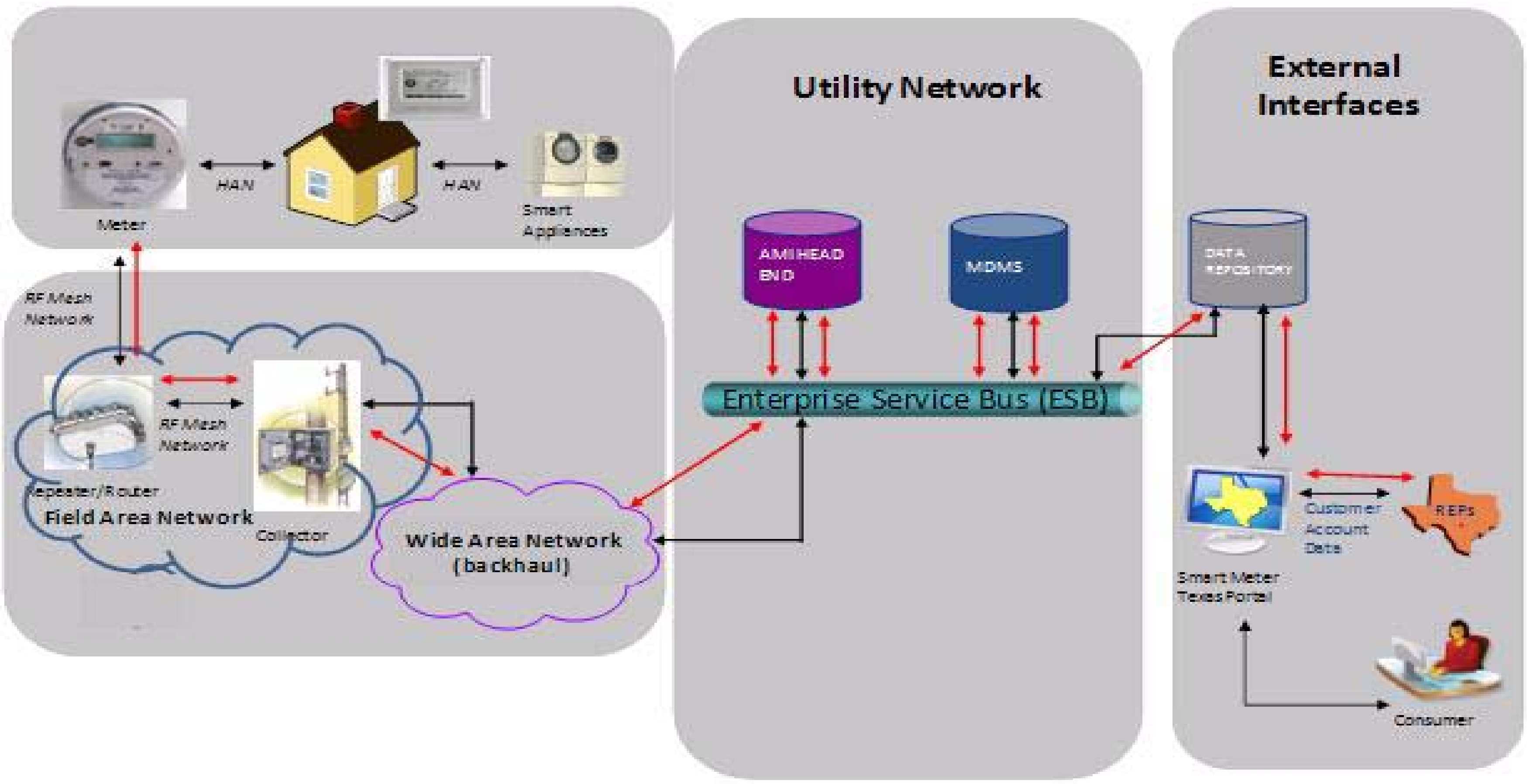
Smart Energy Profile

- ZIGBEE* Smart Energy Profile (SEP) is a specification for ZIGBEE energy HANs.
- Obj. – avoid grid disruption, protect HAN integrity and privacy
- Several security analyses have found security vulnerabilities.
- Honeywell's internal security analysis and mitigations white paper.
- NESCOR white paper addressing the issues.

* ZIGBEE is a registered trademark of the Zigbee Alliance.

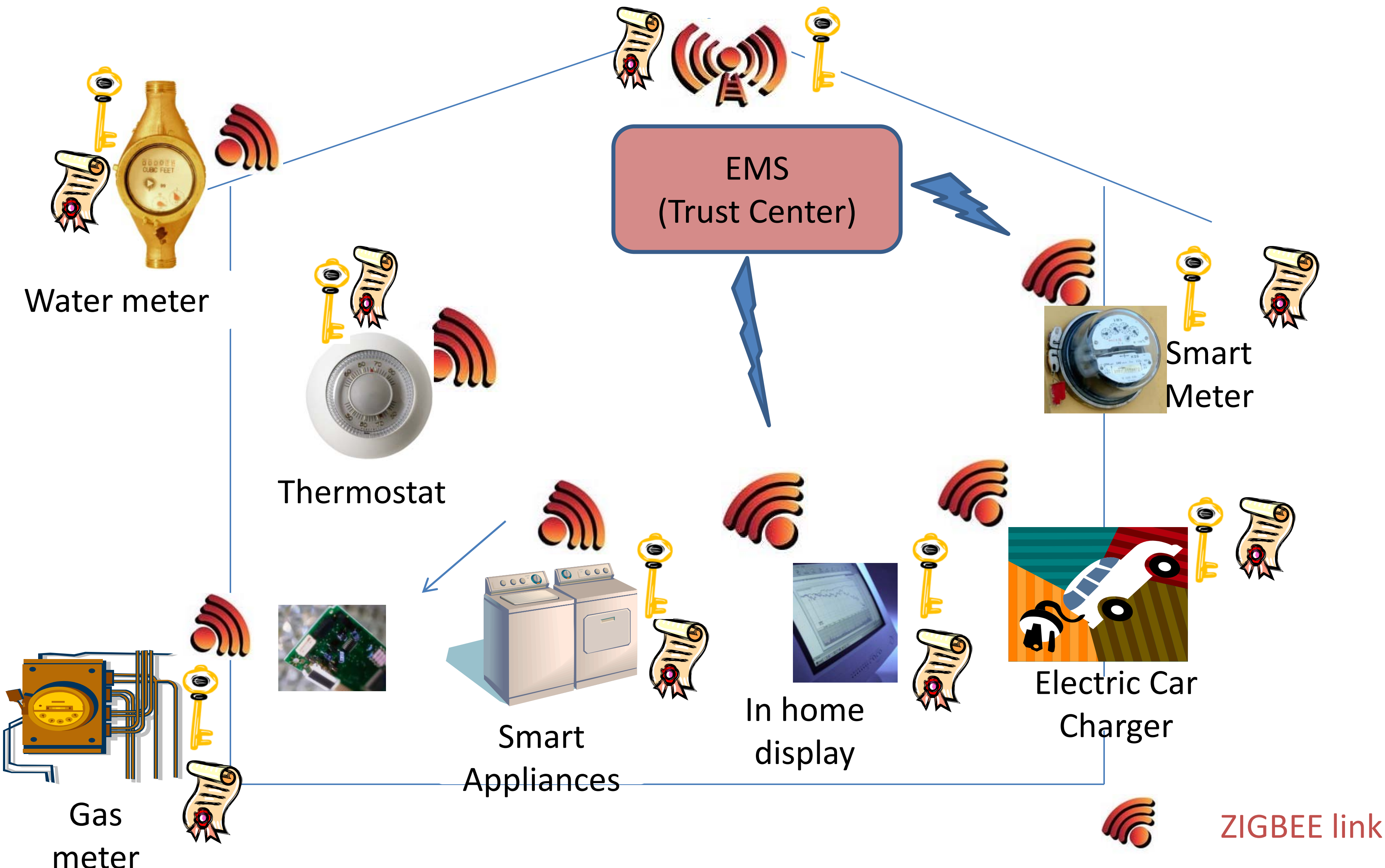
Honeywell

Architecture from TX-PUC



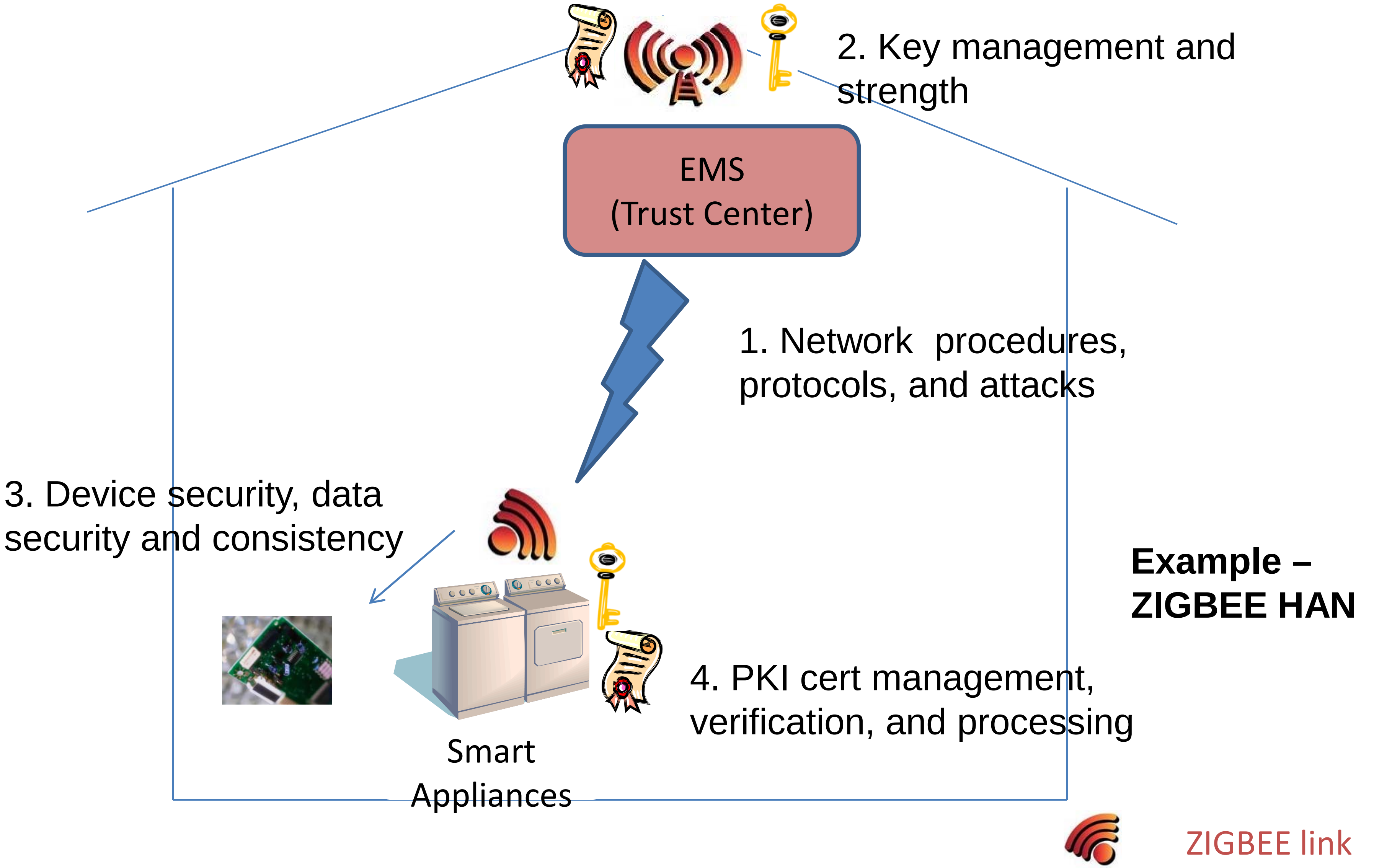
Ref. [1]

SEP Security Challenges Overview



Honeywell

Overview of security challenges



What’s the difference

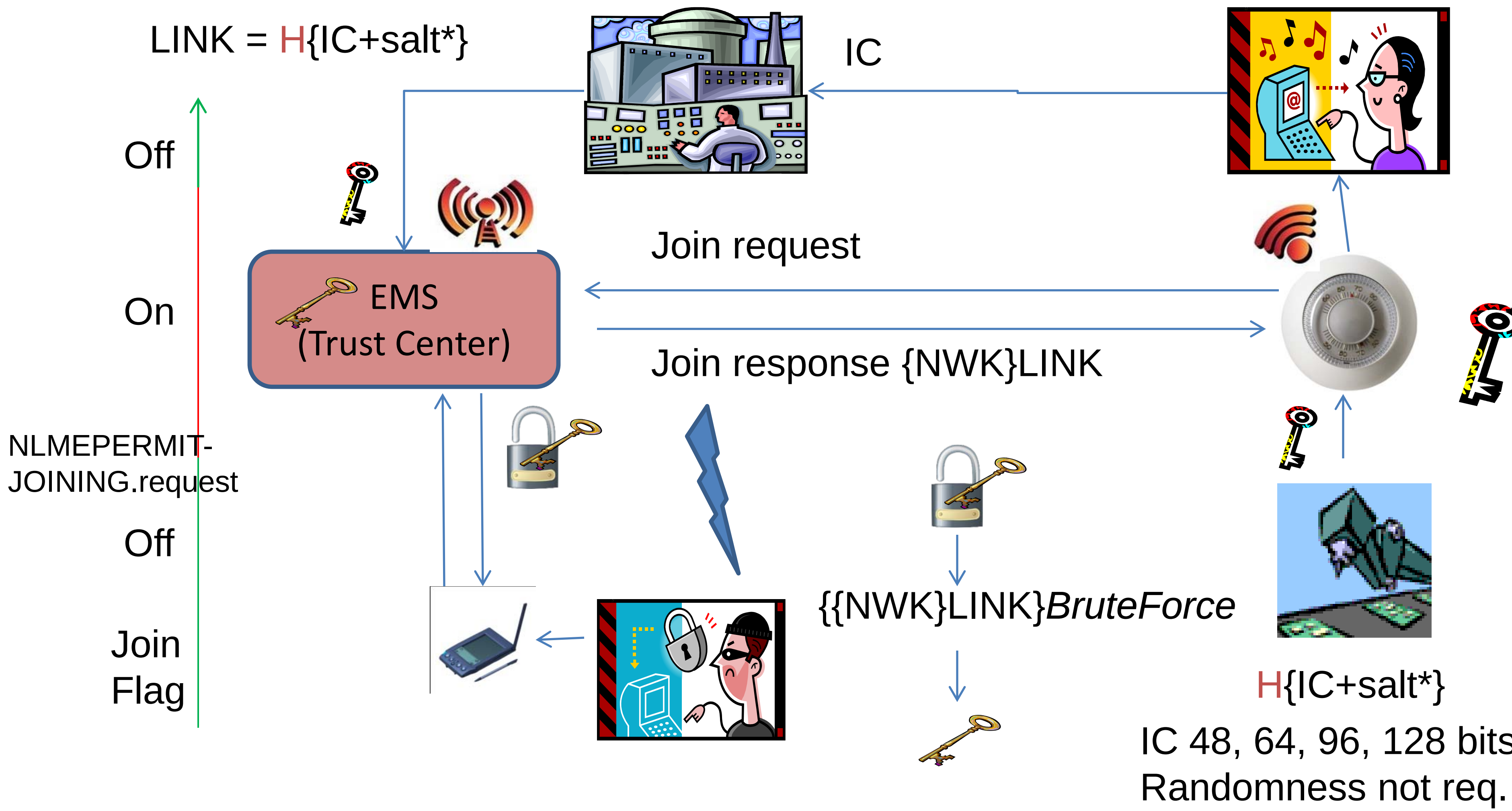
- Low end devices typically 8/16 bit, 16KB ROM, 512 RAM, low data rate (20 – 250 kbps).
- High computation, high resource crypto is unsuitable.
- Specific implementations for embedded control systems are needed.
- Compromises may reduce security – Using non approved algorithms, HASH truncation, minimal use of asymmetric crypto.

Honeywell

Outline

- Introduction
- Overview of security challenges in HANs
- Communications security
- Key management
- Public key infrastructure
- Device hardware security
- Summary

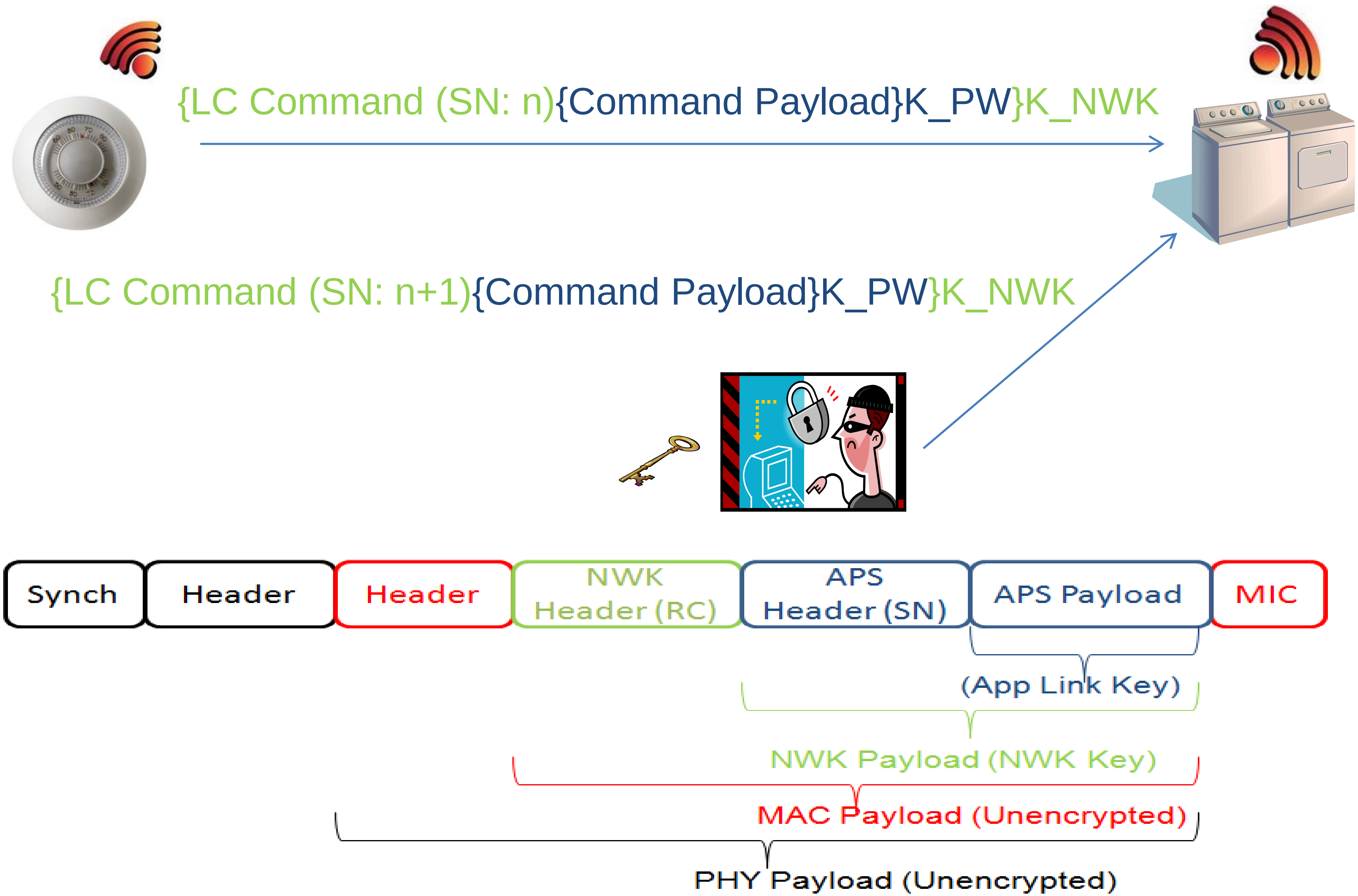
Join attack



* Well known salt
H – AES MMO Hash Algo

Honeywell

Masquerading/replay attacks



K_PW = Pairwise link key

Honeywell

Cryptographic requirements

- AES MMO hash Algorithm in ECMQV key est. protocol provides 80 bit security, not NIST approved but hardware suitable. Challenge – NIST approved 112 bit security algo which is hardware suitable.

- NIST examines underlying cryptographic primitives, not cert implementation (ECQV certificate or ECPVS signature scheme). Lightweight implementation of strong crypto primitives is required e.g. [2].

Cryptographic requirements

- CCM* on 128 bit block size and MMO has 128 bit output. Typically the messages are 4-12 bytes, the signature and encrypted blocks are large compared to message size.

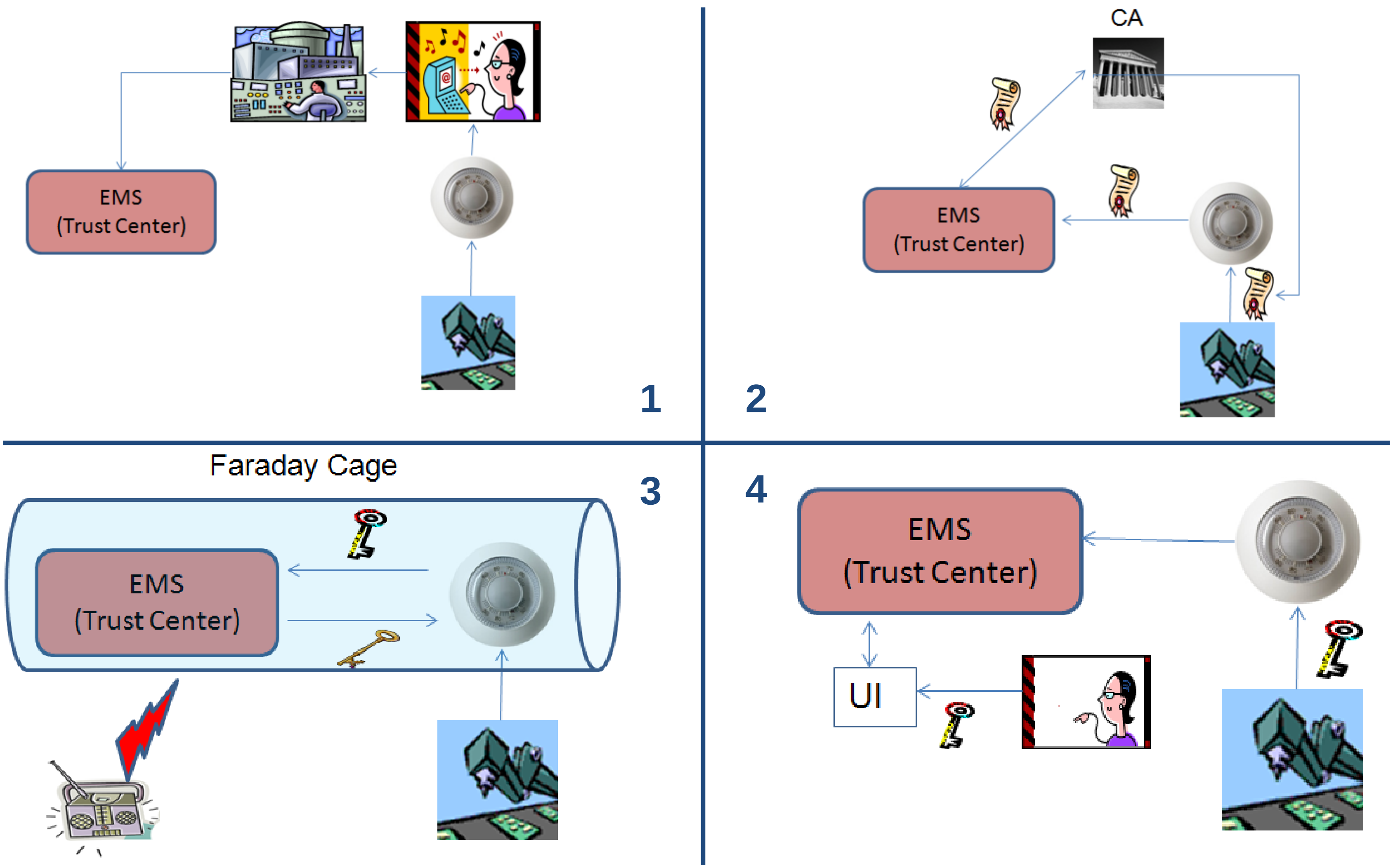
- Certificate revocation status requires CRL or online access. (example) Downloading CRL on a 512 RAM device is not practical. Online access is through TC. Optimization of PKI for embedded devices is required (like AES [2]).

Honeywell

Outline

- Introduction
- Overview of security challenges in HANs
- Communications security
- Key management
- Public key infrastructure
- Device hardware security
- Summary

Initial Key distribution



Honeywell

Network key update

- Backward security is straightforward.
- Forward security - Unicast (n Tx * 1 message) vs. Broadcast (1 Tx * n messages).
- Optimizing forward security – only when malicious or suspected malicious devices leave.
- Periodic update is also desired for security.
- Phased update – new key generation, key marked stale, key update, key switch.

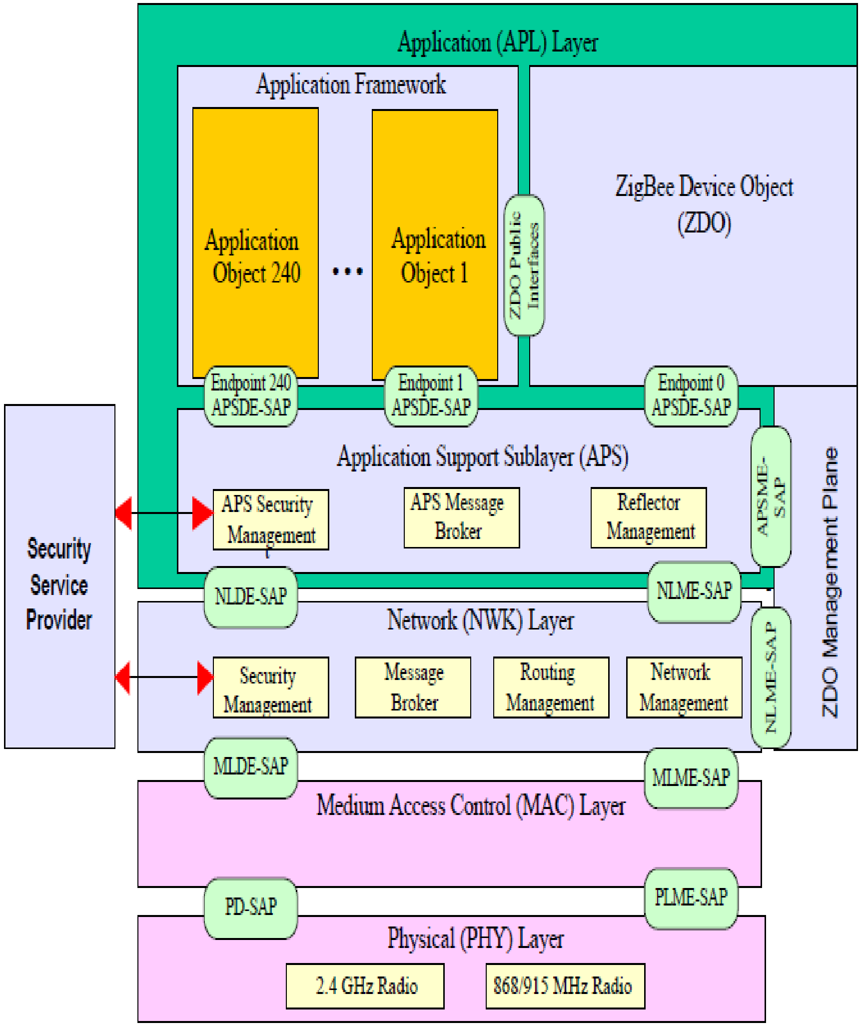
Honeywell

Key Domain Overlap

- Two primary types of keys – Link key and Network key.

- Link key usage – Application packet security, application level trust brokering, Initial network access, network re-join.

- Network key usage – Network access, network re-join, application packet security (some clusters), network management.



Ref [3]

Key Domain Overlap

Ideally - Strict key domain separation.
- Derived keys.
- Keys do not change domain.

Note: SEP does not provide any of these completely.

Outline

- Introduction
- Overview of security challenges in HANs
- Communications security
- Key management
- Public key infrastructure
- Device hardware security
- Summary

Honeywell

Attack 1 – IV Issues/ Access Control

Address	Security suite	Key	Last IV	Replay Ctr

- Collision in the key field causes the nonce to be reused, exposing confidential information.
- ACL state is not persistent across power resets.
- Low power mode should preserve nonce states.

- Access control issues for serial/USB ports.
- No ACL for sensitive data on the device.

Attack 2 – Physical Extraction of Security Data

- Unprotected data memory and flash memory.
- Entire device firmware can be copied including all cryptographic keys, certificates, ACL state, application details. (e.g. Travis Goodspeed [4])
- Adversary can launch *Side channel timing attack* on Pseudo-Random Number Generator (PRNG) to recreate the LFSR taps and then generate any future random cryptographic keys from it.
- *Other side channel attacks* – power consumption, TEMPEST.

Honeywell

Trust Center Security

- Strong data protection
  - Trust center data and flash memory.
  - ACL for on device sensitive data.
  - Strong authentication for device data access.
  - Self-erase functionality upon unauthorized access.
- Strong cyber attack resistance
  - Timeout for device engagements (e.g. registration).
  - Device blacklist and device status list (Insiders as well as outsiders).
  - No Inter-PAN communication.
  - Periodic/event based key updates, strong key generation/sharing/distribution
- Strong physical attack resistance
  - Physical seals/locks, tamper evidence.
  - USB/serial port may be disabled (if desired).

Honeywell

Top Research Challenges

- Developing suitable implementations of cryptographic primitives for embedded environments.
- Developing novel Key management techniques.
- Providing network security in the presence of weak hardware protection.

Honeywell

Summary

- Introduction to the ZIGBEE SEP 1.x.
- Security requirements and challenges in SEP 1.x were presented.
- Discussed some possible mitigations and what more is needed in terms of research in this area.
- With appropriate mitigations, SEP 1.x is suitable for use in HANs.

Questions

Honeywell

1. NESCOR , “Smart Energy Profile (SEP) 1.x Summary and Analysis”.
2. Didle et al., “Optimizing AES for Embedded Devices and Wireless Sensor Networks”.
3. ZigBee Specification version 1.1, The ZigBee alliance.
4. Travis Goodspeed, BlackHat conference 2011 presentation.