

Towards Addressing Common Security Issues in Smart Grid Specifications

**Apurva Mohan
Himanshu Khurana
Honeywell ACS Labs**

**ISRCS 2012
August 15th, 2012**

Honeywell

Contents

- **Introduction**
 - Motivation
 - Background

- Guidelines for Addressing Security in Smart Grid Specifications
 - Clear enumeration of objectives
 - Derive and state security requirements
 - Relate security mechanisms to objectives
 - Provide details of security mechanisms
 - Document residual risk

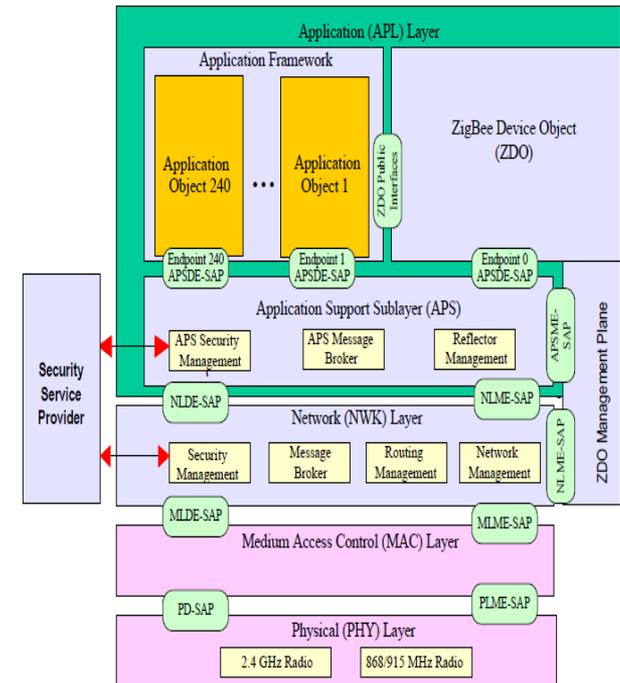
- Discussion and conclusion

Motivation

- Smart grid standards are often derived from other standards.
- Deployment lifetime is typically 20+ years.
- Security is included in ad-hoc and retrospective fashion.
- Security for cyber-physical systems is complex.
- Smart grid increased target of cyber attacks.

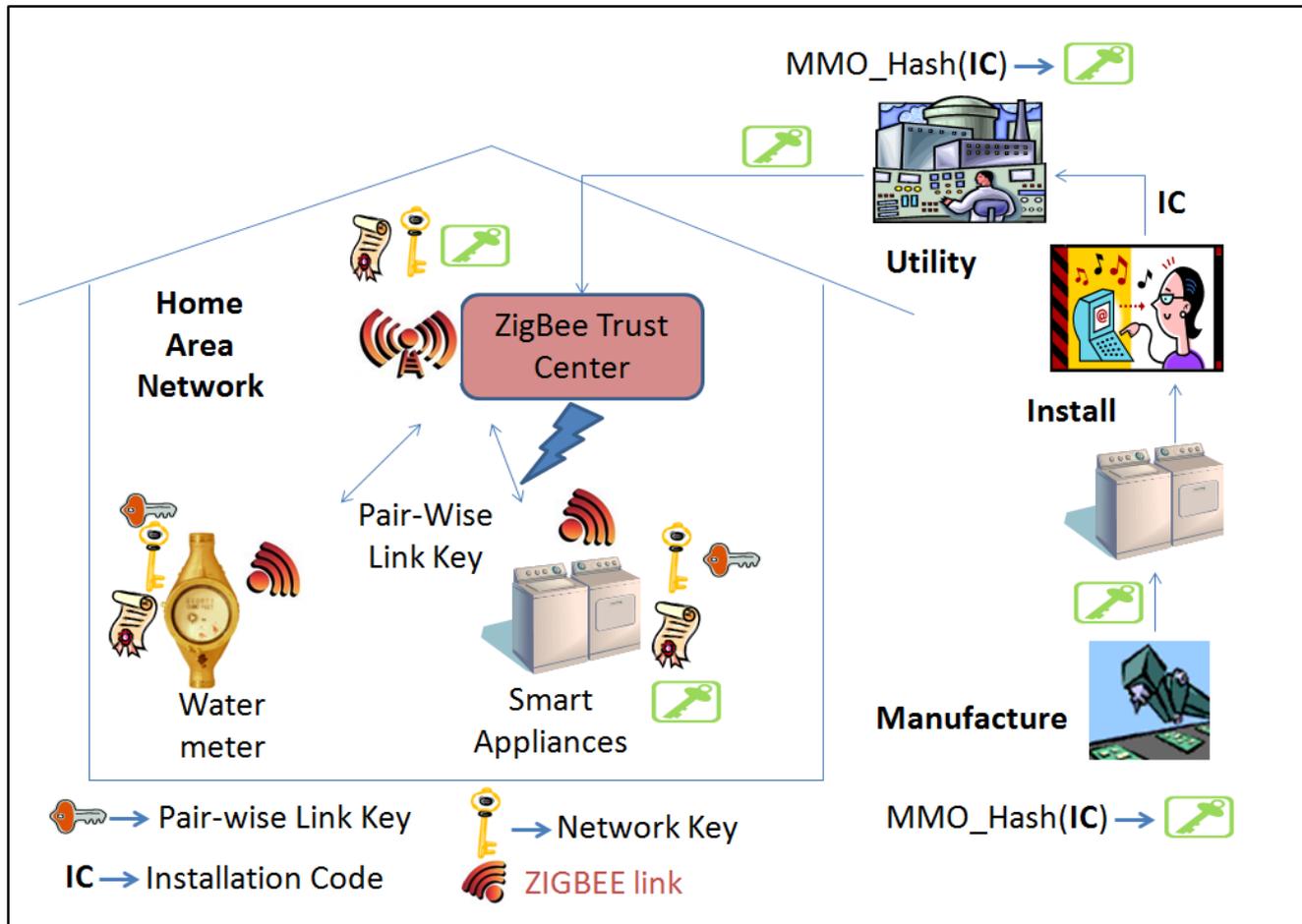
Background – ZigBee Smart Energy Profile 1.x

- SEP HAN
 - Trust center, routers, end devices.
- Network Communication and Security
 - Trust center manages authentication, key generation and management, network coordination.
 - Secure communication supported by group keys and pair wise keys.
 - ECC standard.
 - MMO hash for temp link keys and HMAC for permanent keys.
 - Shared secret based authentication.
 - CBKE mode.
 - Secure application level clusters.



Reference: ZigBee Specification v1.1

ZigBee Home Area Network (HAN)



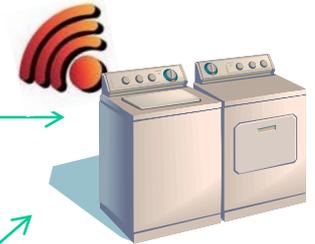
Contents

- Introduction
 - Motivation
 - Background
- Guidelines for Addressing Security in Smart Grid Specifications
 - Clear enumeration of objectives
 - Derive and state security requirements
 - Relate security mechanisms to objectives
 - Provide details of security mechanisms
 - Document residual risk
- Discussion and conclusion

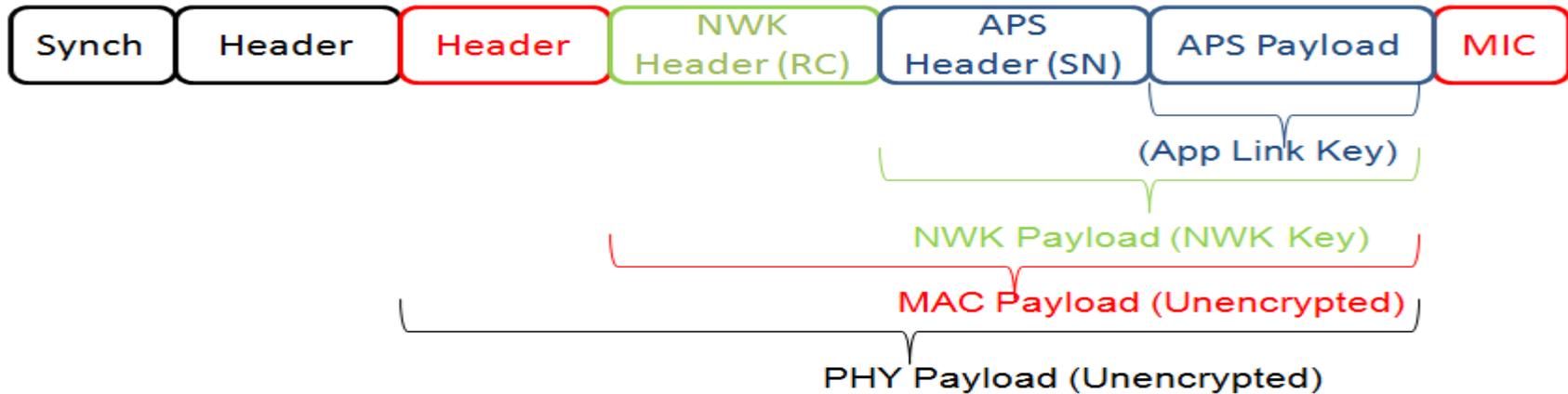
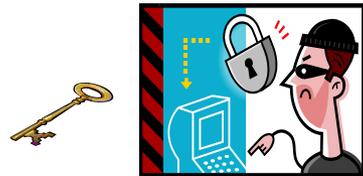
Replay Attacks by Insiders



{LC Command (SN: n){Command Payload}K_PW}K_NWK



{LC Command (SN: n+1){Command Payload}K_PW}K_NWK



K_PW = Pair-wise link key

Clear Enumeration of Security Objectives - Current

- Security Objectives are not stated explicitly in SEP 1.x.

Clear Enumeration of Security Objectives - Proposed

- Clearly state the security objectives of the technology.
- Derive from high level conceptual objectives like CIA, Non-repudiation, Privacy.
- If objectives are application or deployment scenario specific, that should be made explicit.

Integrity is an important objective in HANs because integrity of sensitive information like network and link keys should be verified before use. Moreover, sensitive command and application message need to be verified to prevent an adversary maliciously modifying them.

Derive and State Security Requirements - Current

- Security Requirements are not stated explicitly in SEP 1.x.

Derive and State Security Requirements - Proposed

- Derive security requirements from security objectives and impose them.
 - i) Using relevant standards, guidelines, and best practices.
 - ii) Developing use and abuse cases considering the application scenario and deployment environment(s).
- Create a mechanism to trace them throughout the specification development.

All cryptographic keys and load control commands should be encrypted before being shared on the network and only the intended recipients should possess the decryption keys.

Relate Security Mechanisms to Objectives - Current

- Security objectives are not stated explicitly.
- Security procedures and mechanisms are defined in the specification.
- There is a loose connection among the mechanisms but there are gaps too.

Relate Security Mechanisms to Objectives - Proposed

- Create security mechanisms.
- Relate them to security objectives.
 - All the stated requirements are completely met.
 - No included security mechanisms either violate or are outside the scope of the stated objectives.

The application level load control commands should be encrypted with the trust center link key. Replay protection should be provided for this command by using a monotonically increasing sequence number.

Provide Details of Security Mechanisms - Current

- Details of security mechanisms and procedures exist but have issues
 - Lack of consistency e.g. key update procedures.
 - Incorrect details e.g. join flag on, re-join procedure.
- References to the details are not provided consistently.

Provide Details of Security Mechanisms - Proposed

- Sometimes flexibility is favored – understand/state the tradeoff.
- If multiple mechanisms like encryption algorithms, key lengths, or hash algorithms are specified, state the security tradeoffs.
- Provide proper reference to security mechanisms and encourage community developed solutions/implementations.

a) The application level load control command payload should be encrypted using the trust center link key. The header is encrypted using the network key. The encryption algorithm used in both these operations is AES-CCM with 128 bit symmetric Key.*

b) The message payload should include a monotonically increasing serial number to guarantee message freshness.

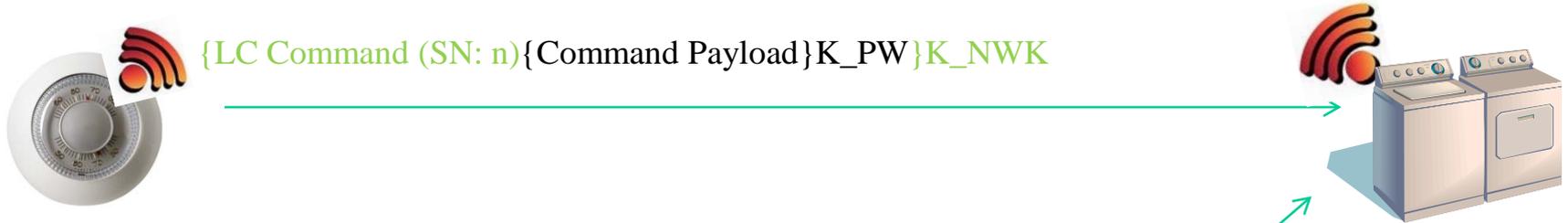
Document Residual Risk - Current

- The residual risk in the standard is not addressed.

Document Residual Risk - Proposed

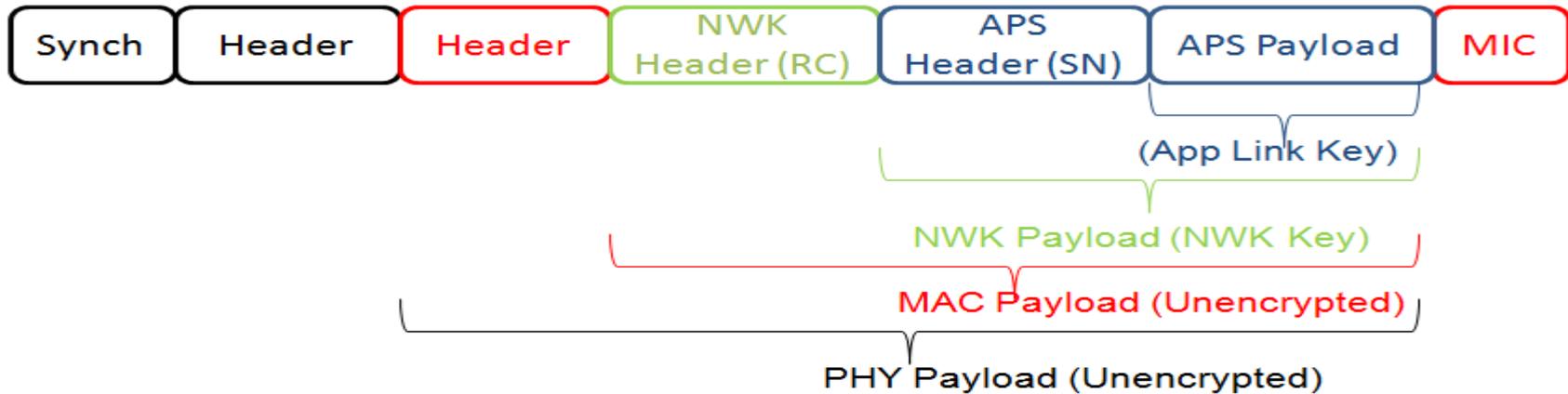
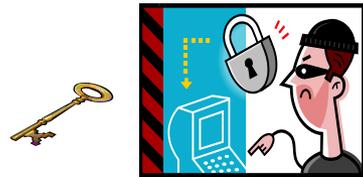
- The residual risk in the technology specification should be understood and clearly documented.

Replay Attacks by Insiders



{LC Command (SN: n){Command Payload}K_PW}K_NWK

{LC Command (SN: n+1){Command Payload}K_PW}K_NWK



K_PW = Pairwise link key

Contents

- Introduction
 - Motivation
 - Background
- Guidelines for Addressing Security in Smart Grid Specifications
 - Clear enumeration of objectives
 - Derive and state security requirements
 - Relate security mechanisms to objectives
 - Provide details of security mechanisms
 - Document residual risk
- Discussion and conclusion

Discussion and Conclusion

Clear Enumeration of Security Objectives

Derive and State Security Requirements

Relate Security Mechanisms to Objectives

Provide Details of Security Mechanisms

Document Residual Risk

Thank You !

For Questions or Comments, contact:

Apurva.Mohan@Honeywell.com