11TH INTERNATIONAL CONFERENCE
ON CRITICAL INFORMATION
INFRASTRUCTURES
SECURITY

10-12 October 2016
UIC HQ Paris

CRITIS
2016

Reliable Key Distribution in Smart Micro-Grids

Heinrich Strauss[a], Anne VDM Kayem[a]
and Stephen D Wolthusen[b]
Presented by **Anesu Marufu**[a]

[a] *Department of Computer Science, University of Cape Town*
[b] *NISLab, Faculty of Computer Science and Media Technology, NTNU-Gjøvik*

Outline

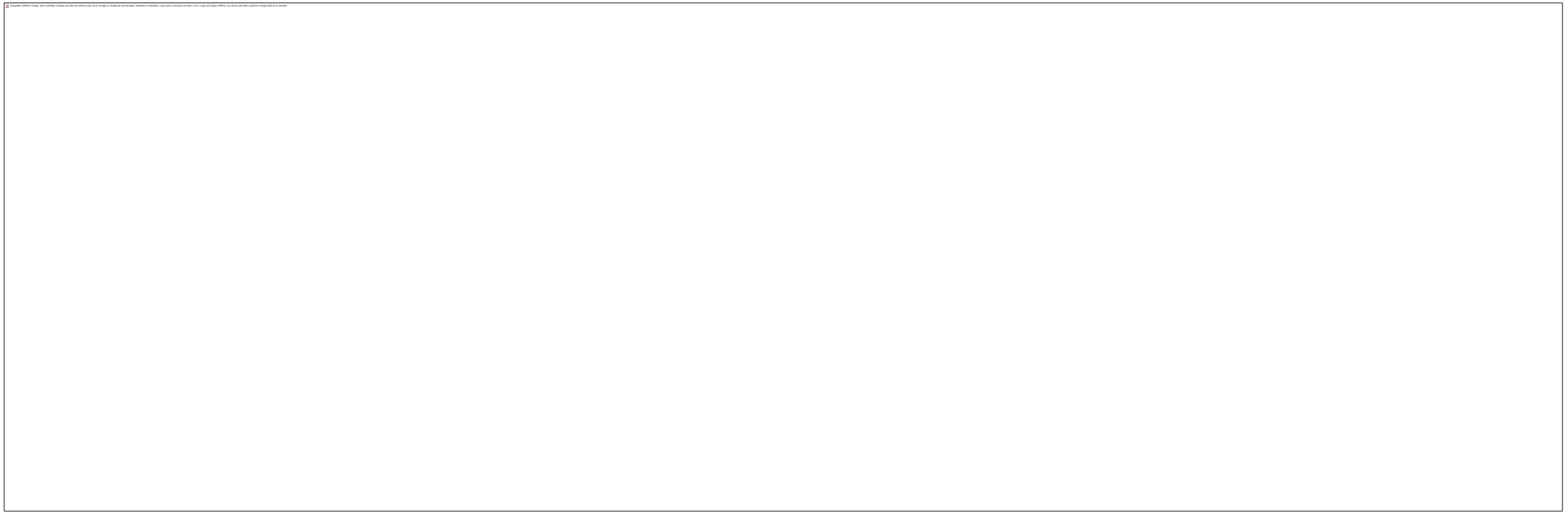
- Introduction
- Summary of Related Work
- Network Architecture
- Key Distribution Problem
- Correctness / Analysis Sketch
- Summary of Presentation
- References

Introduction

- Smart-Grids allow bi-directional information flow in a power network
- Micro-Grids enable use of self-generated power in isolated networks
- Smart Micro-grids combine the abovementioned concepts
  - Enable remote/mobile communities to manage a scarce resource

- How do we ensure attributable usage reports in a distributed, resource-constrained network?

Network – Physical Configuration



Problem

- User Trust in the network must exist for continued participation
  - If spurious reports are accepted as valid, this may be compromised
- Sensor Nodes are constrained
  - Power-resources are battery-backed (therefore limited)
  - Asymmetric cryptographic signatures are too expensive
- Network is not reliable
  - Based on Wireless links within and between locations
  - For constrained radio protocols, message sizes are small

Summary of Related Work

- Use Eschenauer-Gligor [1] algorithms
  - Probabilistic in the derivation of a shared-key
  - Expensive re-keying in the event of disclosure
- Symmetric Encryption
  - Pros: less intensive for constrained nodes
  - Cons: signing is still comparatively expensive
- Pre-Distribution and Delayed Authentication [2,3]
  - Nodes authenticate neighbours on critical path through the network

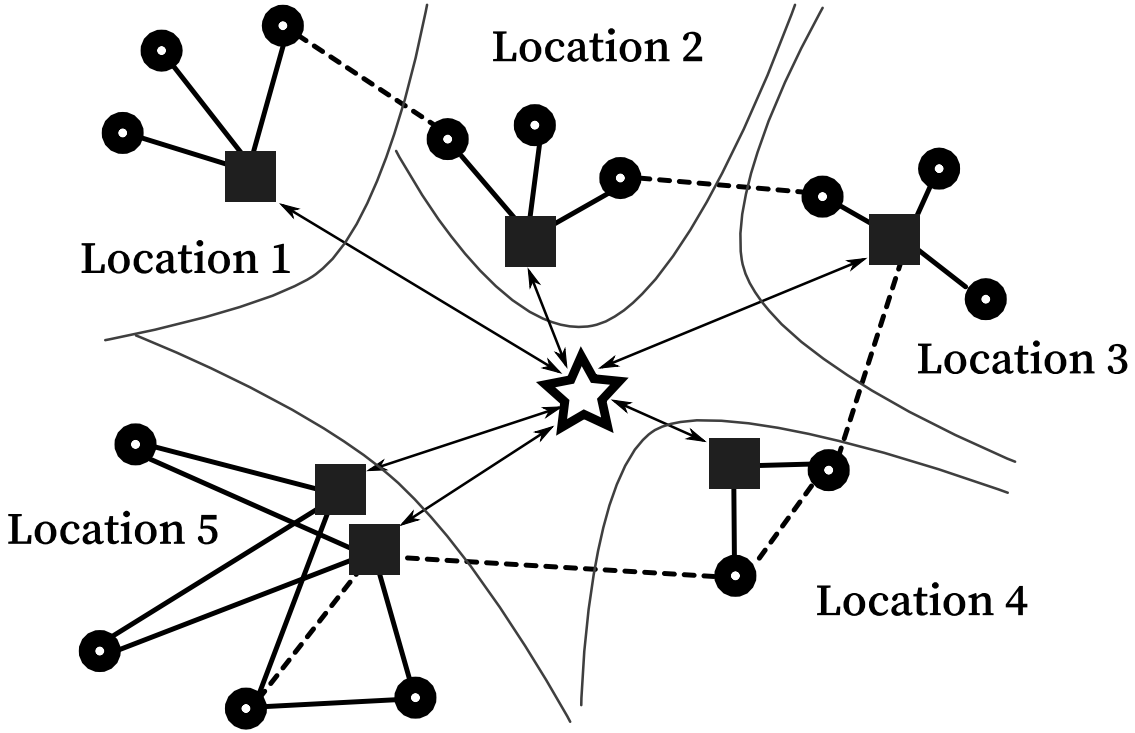
Requirements

- Unified neighbourhood-wide management network
  - For consolidation of aggregated usage reports
  - Security between devices ensured by Public-Key Cryptography (PKC)
- Per-location network for usage report collection
  - Usage report communication does not routinely extend beyond local network
  - Reports can be cached at sensor nodes in the event of short network outages
- Higher-powered Manager nodes in each location
  - Normally, a smart-device capable of asymmetric cryptographic operations [4]
  - Acts as gateway for nodes in each location

Key Distribution

- Key Pre-distribution
  - Central Global Pool of keys and key-tags
  - Partitioned into equal-sized location pools
  - Generated Centrally; distributed at node-addition time
- Key Revocation
  - Handled locally (per node)
- Key Validity
  - Keys are valid in a specific location only (determined by location pool)
  - Unless locally revoked, keys are considered valid
  - Manager nodes maintain a list of revoked keys per location

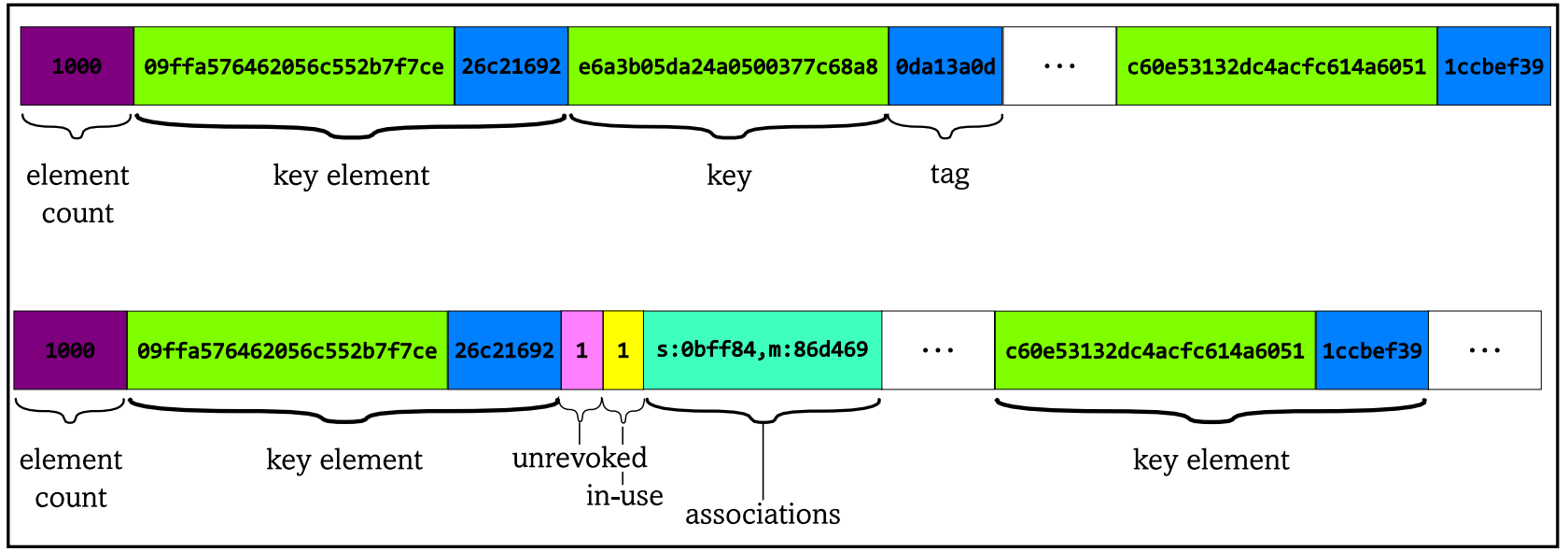
Network – Logical Configuration



- Utility Management Network
- Manager
- Sensor
- Neighbourhood Network
- shared key exists between nodes
- no shared key exists between nodes

Key Ring representation

- Representation dependent on location in network
  - At key-distribution, no metadata exists
  - On sensor/leaf nodes, usage data is included on key-ring



Correctness Analysis

- Network segmented into two classes: asymmetric and probabilistic symmetric
- Manager devices participate in both networks
  - PKI ensures security on the asymmetric network
  - Probabilistic EG-scheme ensures low probability of compromise in other network
- Barring node-compromise, keys are never disclosed in the clear over the transport medium
- If a node is known to be compromised, revocation can be initiated by the manager
  - List of compromised keys is distributed through the location
  - Damage restricted to single location (because of partitioning of key-pool)

Complexity Analysis

- The Key Distribution Center (KDC)
  - draws k random keys from a location pool ($O(k)$)
  - compares each key-tag to the list of key-tags issued to the n nodes in the location ($O(k\ n)$),
- This results in an algorithmic complexity of $O(n \times k^2) \approx O(n^3)$.
- Rekeying a k-key ring using a message size of μ, (key+tag)-length of ℓ
  - number of messages would be $n = \frac{k(\ell)}{\mu} + C$
- Online re-keying messages are very distinguishable from usage reporting traffic patterns

Conclusions – Summary and Future Work

- We can improve computational complexity by trading off heavy asymmetric encryption for symmetric encrypted between sensors and managers
- Managers act as gateways to node relaying messages to the central network
- Key Management Functions are maintained
  - Key Generation/Distribution
  - Key Revocation
  - Key Validity Checks

Selected References

- L. Eschenauer and V. D. Gligor: *A key-management scheme for distributed sensor networks*
  - Proceedings of the 9th ACM Conference on Computer and Communications Security, ser. CCS '02. New York, NY, USA: ACM, 2002, pp. 41–47.
- W. Du et al.: *A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments*
  - Journal of Network and Computer Applications, vol. 49, pp. 15–50, 2015.
- D. Liu and P. Ning: *Multilevel µTESLA: Broadcast authentication for distributed sensor networks*
  - ACM Transactions on Embedded Computing Systems (TECS) 3(4), 800-836 (2004)
- W. T. Kilenthong and P. Odton: *Access to ICT in rural and urban Thailand*
  - *Telecommunications Policy* 38.11 (2014), pp. 1146–1159.