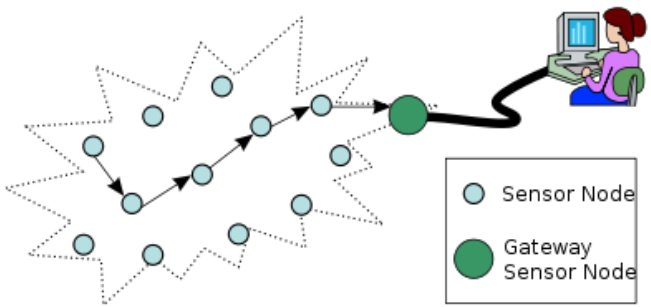
Improving key management in wireless sensor networks

Filip Jurnečka

DTEDI

November 6, 2012

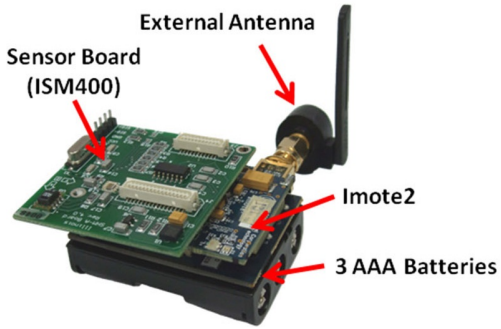
Wireless sensor network (WSN)



- A distributed (or hierarchical) multi-hop heterogenous network composed of a
  - large number of tiny low-end devices (motes, nodes...).
    - they are usually equipped with sensors and radio.
    - limited processing power, memory and energy.
  - one or a few powerful secured devices (base stations).
- The network is used to monitor some physical phenomena.
- Applied in various scenarios like battlefield management, monitoring wildfire, vibrations on an engine or pressure in car tires.

Wireless sensor network (WSN)

(a) TelosB mote

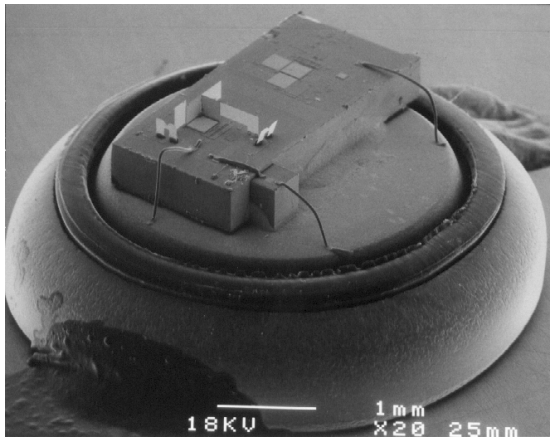


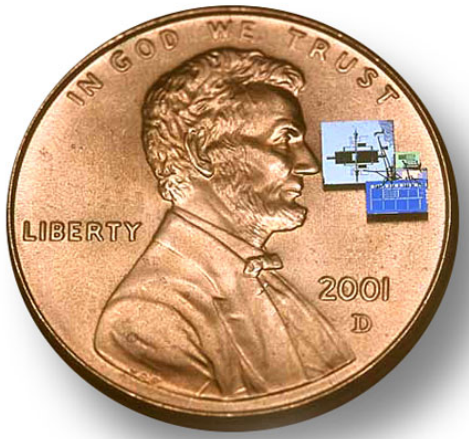
(b) Imote2 mote

- MICAz
  - 8-bit Atmel microcontroller ATmega128L operating at up to 16 MHz
  - 4kB RAM, 128kB program flash, 512kB Measurement Serial Flash
- TelosB
  - 16-bit Texas Instrument microcontroller MSP430 operating at 8 MHz
  - 10kB RAM, 48kB program flash, 1024kB Measurement Serial Flash
  - powered by two AA batteries
- Imote2
  - 32-bit processor Intel PXA271 operating at up to 416 MHz
  - 256kB SRAM, 32MB flash, 32MB SDRAM

Key management schemes' (KMS) properties

- Memory footprint
- Communication overhead
- Processing speed
- Network bootstrapping
- Network resilience
- Connectivity
  - Global connectivity
  - Local connectivity
  - Node connectivity
- Scalability
- Extensibility
- Energy





Existing taxonomies

Published taxonomies of key management schemes are based on:

- encryption key mechanism
  - Asymmetric cryptography
  - Symmetric cryptography
  - Other solutions
- characteristic
  - Self-enforcing schemes
  - Arbitrated schemes
  - Pre-distribution schemes
- characteristic, take 2
  - Key pool schemes
  - Mathematical schemes
  - Negotiation schemes
  - Public key schemes
- network structure
  - Centralized key schemes
  - Distributed key schemes
- probability of keying
  - Probabilistic key schemes
  - Deterministic key schemes

Existing solutions for key establishment

- Asymmetric cryptography
  - RSA
  - ECC
  - Identity-based key agreement scheme
- Symmetric cryptography
  - Master key based pre-distribution scheme
  - Base station participation scheme
  - Trusted third node based scheme
  - Pair-wise key pre-distribution scheme
  - Probabilistic key pre-distribution schemes
- Other solutions
  - Key infection scheme
  - Hybrid schemes

Many protocols lack reviews and thus might have previously unknown shortages.

Master key pre-distribution

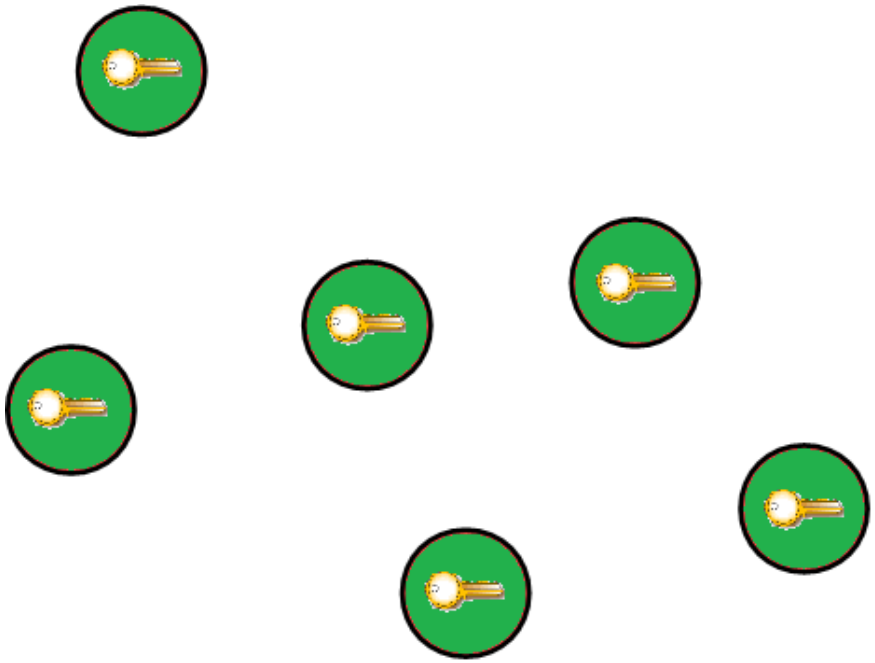


Figure : Same key shared by all nodes

- Perfect in terms of memory storage
- Completely fails with single node

Master key pre-distribution

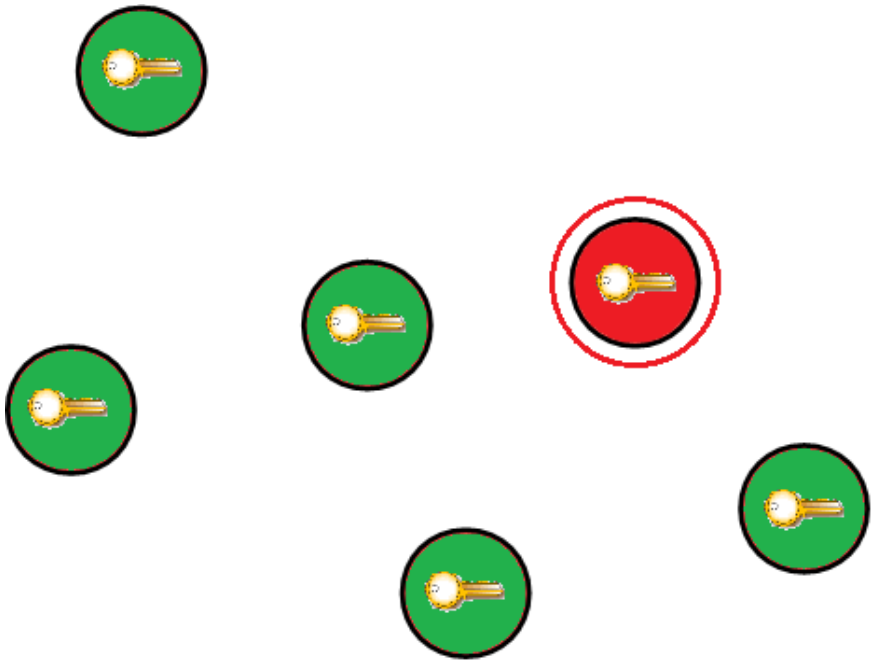


Figure : Capturing a single node implies capturing all keys

- Perfect in terms of memory storage
- Completely fails with single node

Master key pre-distribution

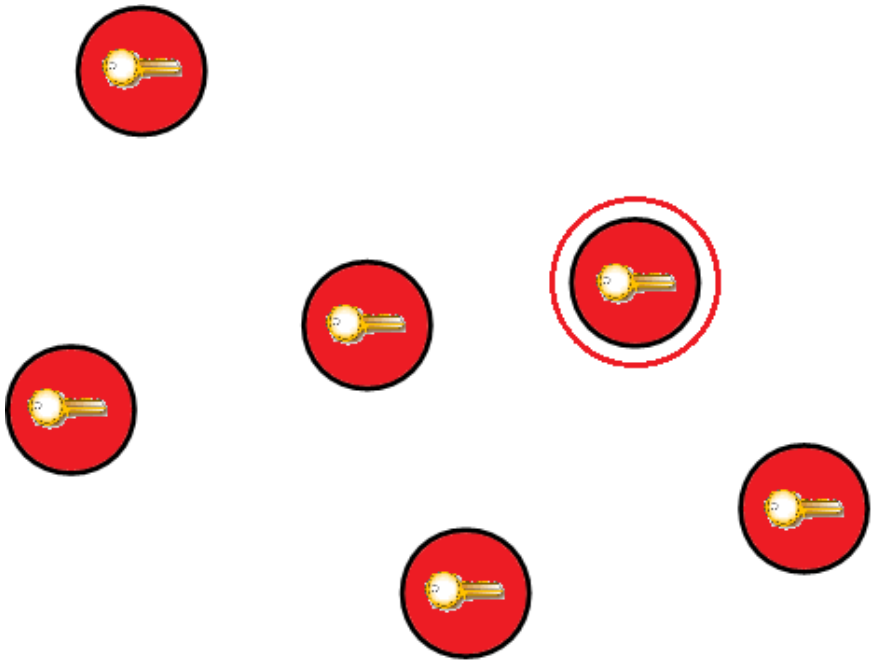


Figure : All communication is now exposed to the attacker

- Perfect in terms of memory storage
- Completely fails with single node

Eschenauer-Gligor (EG) probabilistic pre-distribution

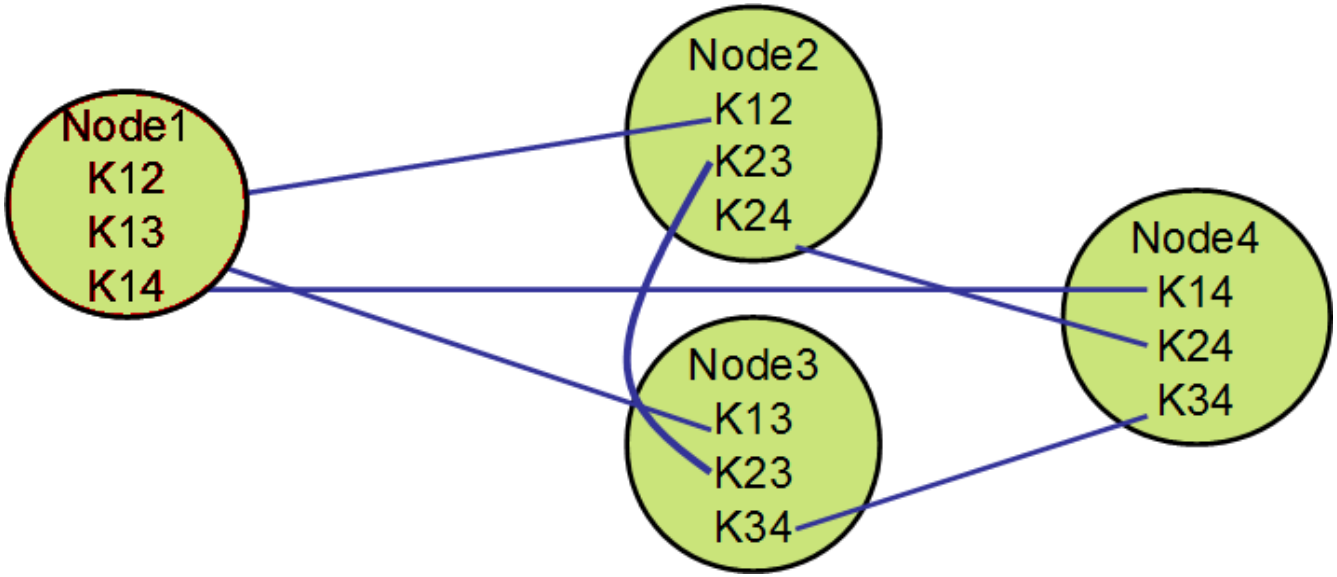


Figure : Each node loaded a random subset of keys

- Only links to captured node are compromised
- Not scalable in terms of memory storage
- Key from captured node can be used everywhere

Eschenauer-Gligor (EG) probabilistic pre-distribution

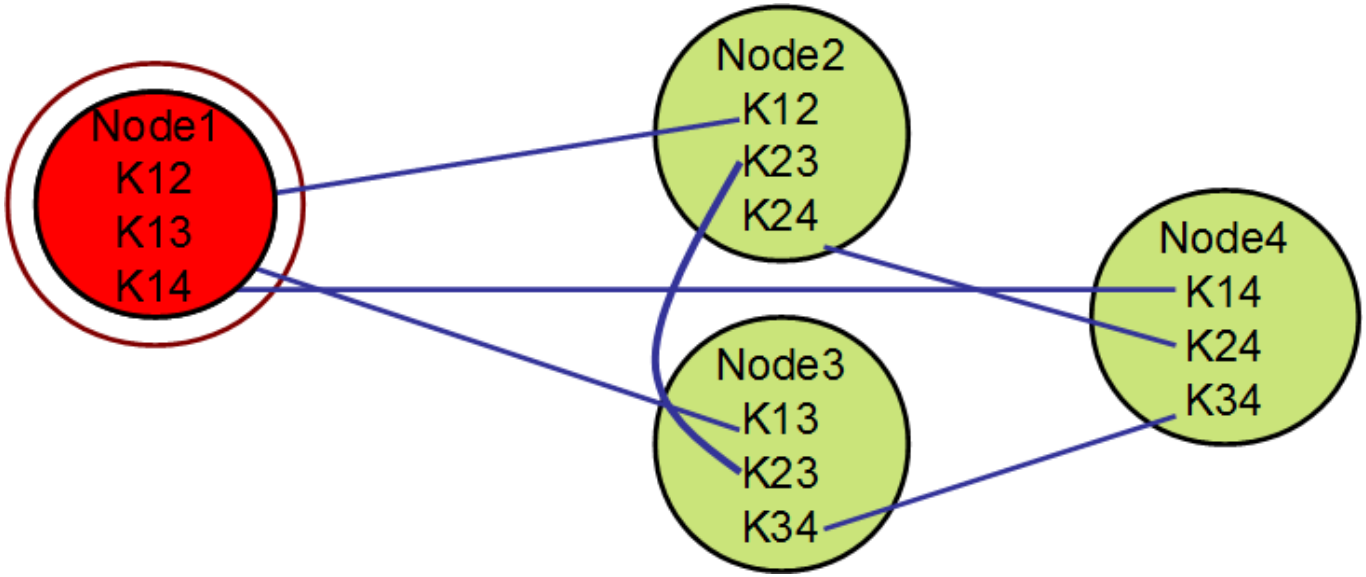


Figure : Capturing of single node reveals keys shared with neighbours

- Only links to captured node are compromised
- Not scalable in terms of memory storage
- Key from captured node can be used everywhere

Eschenauer-Gligor (EG) probabilistic pre-distribution

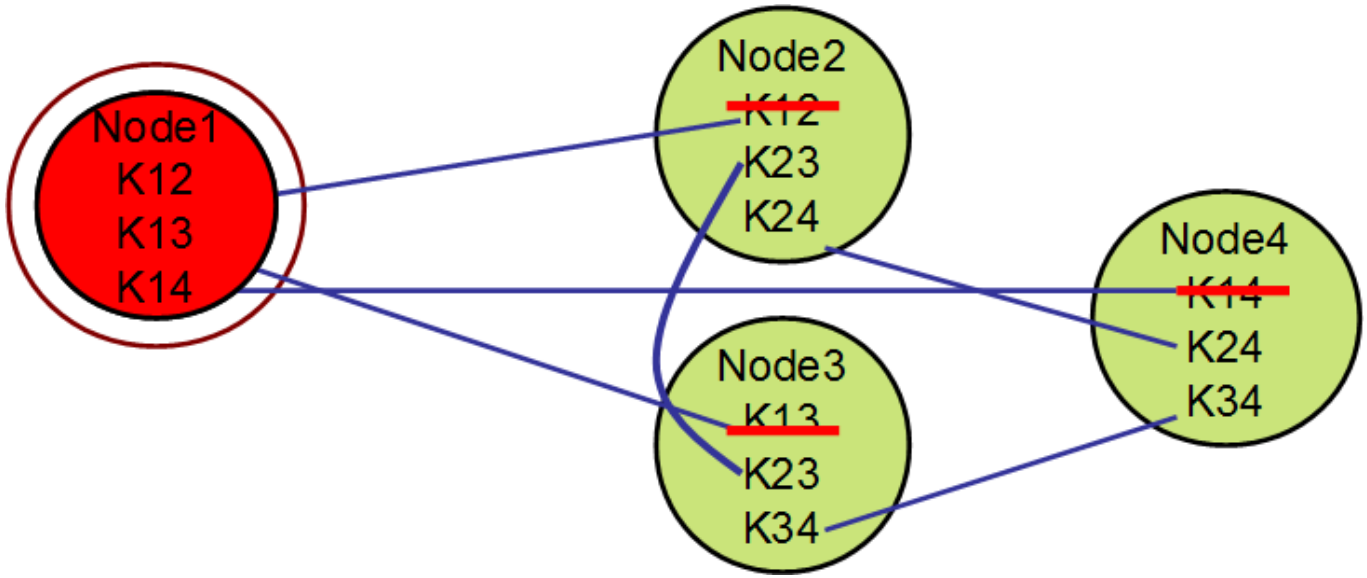


Figure : Capturing of single node reveals keys shared with neighbours

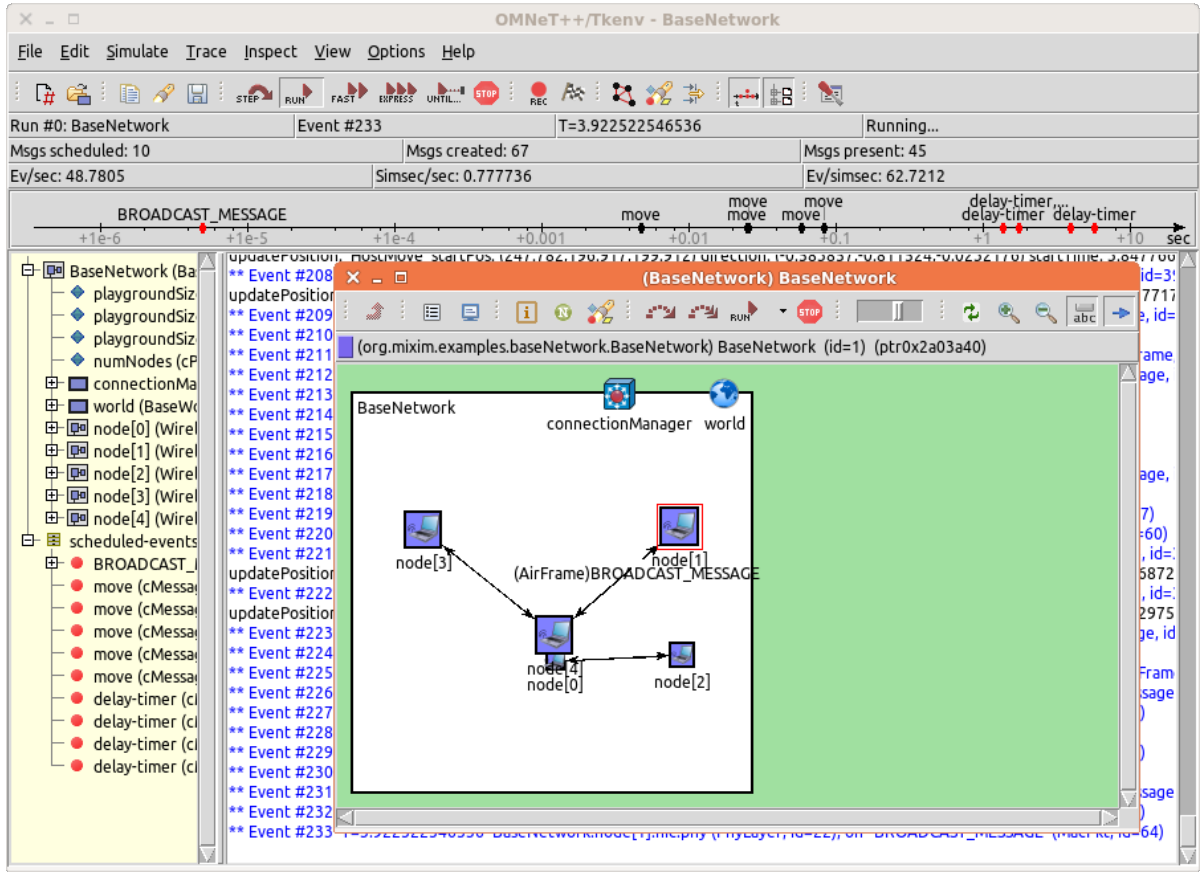
- Only links to captured node are compromised
- Not scalable in terms of memory storage
- Key from captured node can be used everywhere

Motivation for simulating WSNs

- Building a WSN testbed is very expensive.
- The network management is time consuming.
- Simulations are repeatable.
- Simulations allow for large scale evaluations.
- Correctness of the simulation depends on the **model**.

Mainstream WSN simulators

- NS-2
- TOSSIM
- OMNeT++
  - **MiXiM**
  - Castalia
- J-Sim
- Cooja
- WSNet
- ATEMU
- Avrora
- SensorSim
- and many others



Simulation model

- Topology
- Radio propagation
- Energy consumption
- Networking stack
- Security model support
- Attacker model support
- Memory requirements model
- Computational complexity model

Attacker model

The **real world** attacker model from key infection scheme.

- Attacker can be present in the deployment area prior to the deployment, but only able to monitor a small portion of the communication during the initialization phase.
- Attacker can perform passive attacks during the initialization phase such as eavesdropping only.
- After the initialization phase, the attacker can become global and execute any attack, including a node capture.

Based on parameter settings, we could identify general classes of attackers.

The proposal

- Construct a unifying taxonomy of WSNs key management schemes.
  - Analysis of existing taxonomies.
  - Include the parameters of KMSs to the taxonomy.
  - Unification done probably by multi-dimensional or hierarchical taxonomy.
- Add a security model support and implement a representational subset of KMSs to the MiXiM simulator and TinyOS.
  - Review protocols during implementation.
  - Measure memory requirements of the protocols' infrastructure together with the stored keying material.
- Optionally introduce new KMSs for WSN.
- Add the attacker model support to the MiXiM simulator thus allowing to evaluate proposals from security point of view.
  - Generalize the definition of an attacker to WSN and define classes of common attackers to evaluate security of proposals against.

Are there any questions?

Thank you!

Are there any questions?
Thank you!