Cynthia Kuo, Mark Luk, Rohit Negi, Adrian Perrig

Message-in-a-Bottle (MiB):
Key Deployment for Sensor Networks

Problem

Key deployment for sensor networks should be wireless and secure

- Sensor nodes may be deployed in extreme environmental conditions, such as
  - On major highways or bridges
  - Under water
- Nodes may only support wireless interfaces
  - To protect nodes
  - To reduce manufacturing costs
- Secure sensor network operation depends on secure initial deployment of cryptographic keys

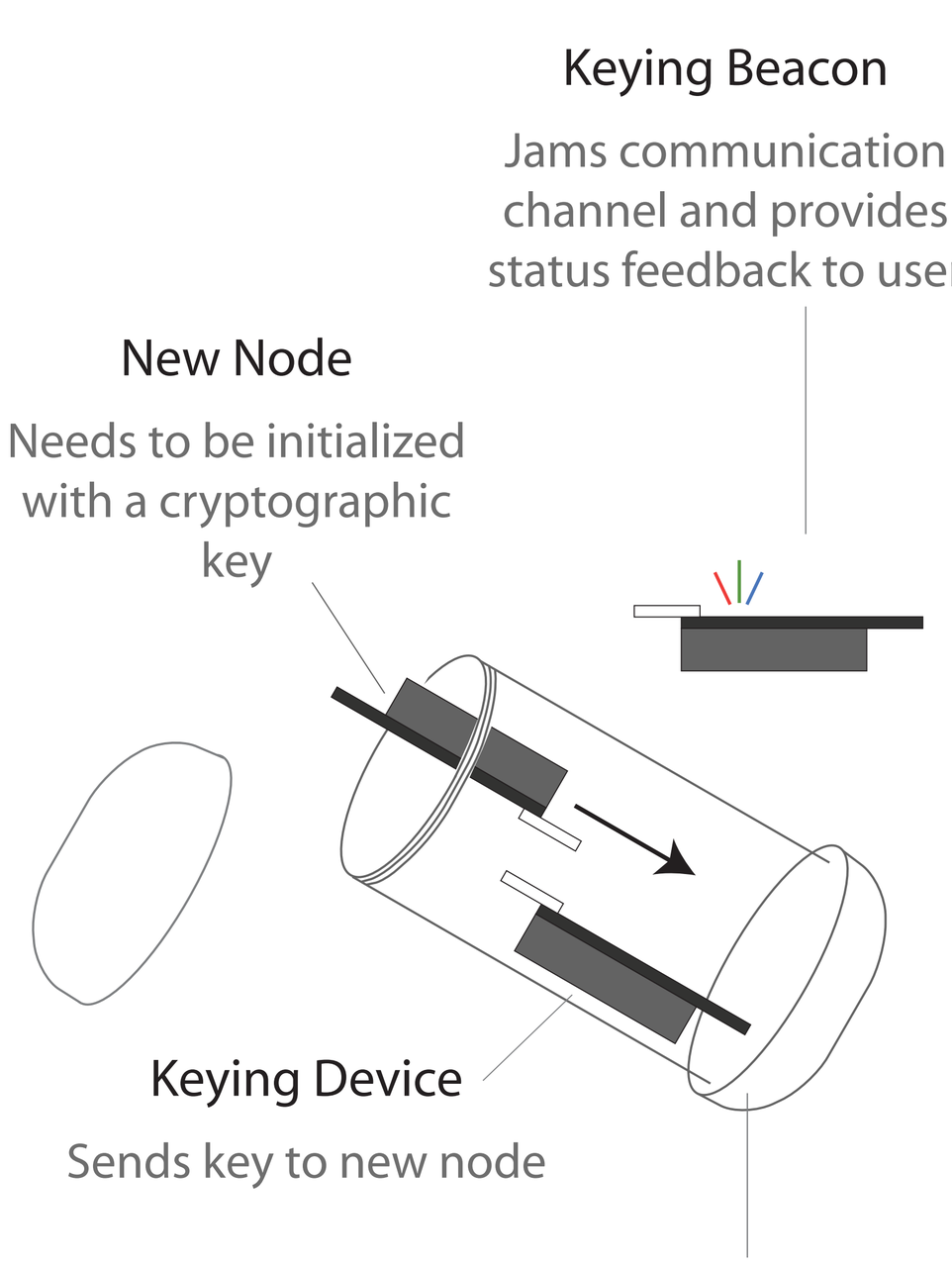
Requirements

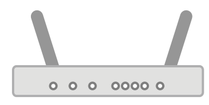
Secure
- Key secrecy
- Key authenticity
- Forward secrecy
- Transparent: Users know which devices are communicating
- Robust to user error

Easy
- Wireless: No specialized hardware for setup on individual nodes

Cost Effective
- No public key cryptography

How MiB Works

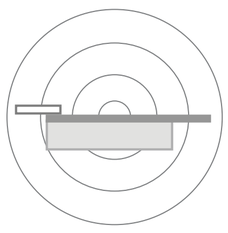




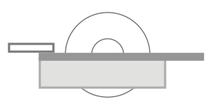
A base station (not shown) assigns keys to a **keying device** and a **keying beacon**.

The **keying device** and the **keying beacon** exchange heartbeat messages.

A user places a **new node** and the **keying device** in a **Faraday cage**. The user closes the **Faraday cage**.



The **keying device** and the **keying beacon** can no longer hear each other. The **keying beacon** jams at full power. Its LED turns blue.



If the **keying device** cannot hear jamming signals, it sends a key to the **new node**.

The **keying beacon** blinks its blue LED after enough time has elapsed (e.g., 5 seconds).

The user opens the **Faraday cage**. If key deployment succeeded, the **keying beacon**'s LED will be green. Otherwise, it will be red.

NATIONAL SCIENCE FOUNDATION

Carnegie Mellon