Ultra-Lightweight Key Predistribution in Wireless Sensor Networks for Monitoring Linear Infrastructure

Keith M. Martin Maura B. Paterson

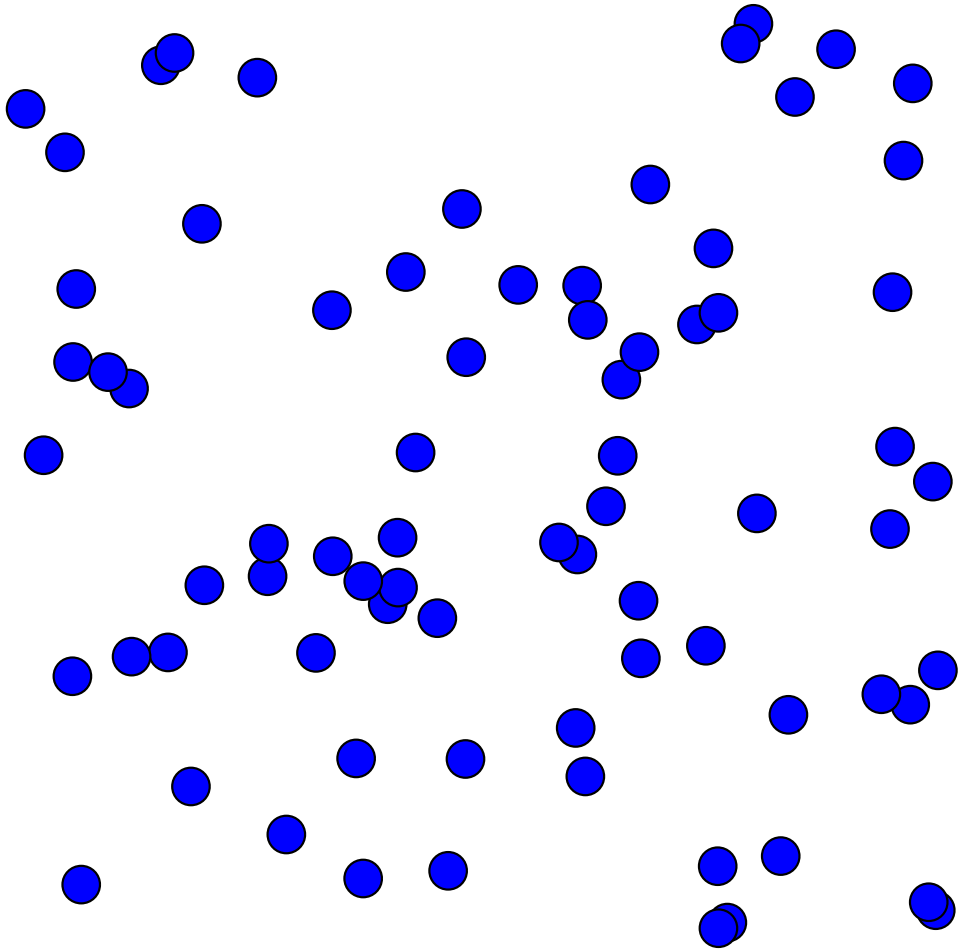
Information Security Group
Royal Holloway, University of London

4 September 2009

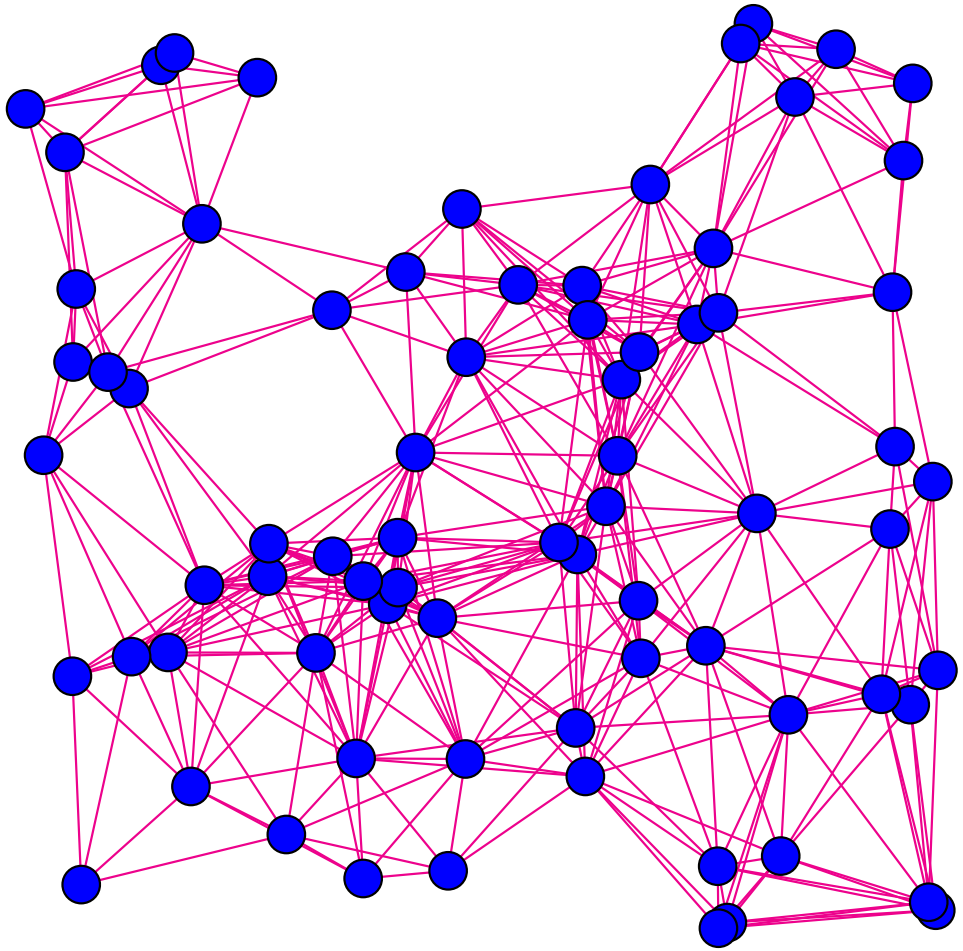
Outline

'Traditional' View of a WSN

'Traditional' View of a WSN



'Traditional' View of a WSN



Oil/Gas/Water Pipelines are Critical Infrastructure

photo credit: Chris Sauerwald, `http://www.flickr.com/people/afterfate/`

Pipeline Monitoring

- Pipelines are used to transport valuable resources over long distances through isolated areas.

Pipeline Monitoring

- Pipelines are used to transport valuable resources over long distances through isolated areas.
- Detection of leaks, measurement of seismic activity, detection of theft or sabotage...

Pipeline Monitoring

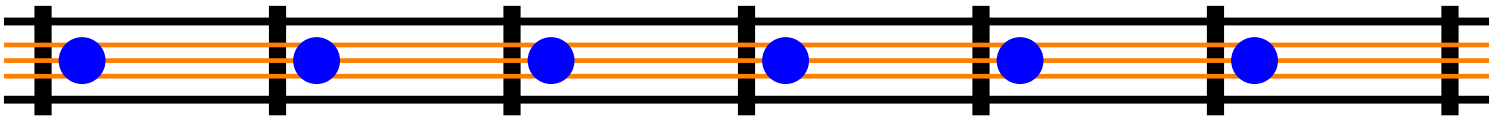
- Pipelines are used to transport valuable resources over long distances through isolated areas.
- Detection of leaks, measurement of seismic activity, detection of theft or sabotage...
- Also bridges, railway lines, roads...

Pipeline Monitoring

- Pipelines are used to transport valuable resources over long distances through isolated areas.
- Detection of leaks, measurement of seismic activity, detection of theft or sabotage...
- Also bridges, railway lines, roads...
- Perimeter surveillance requires sensors in a ring.

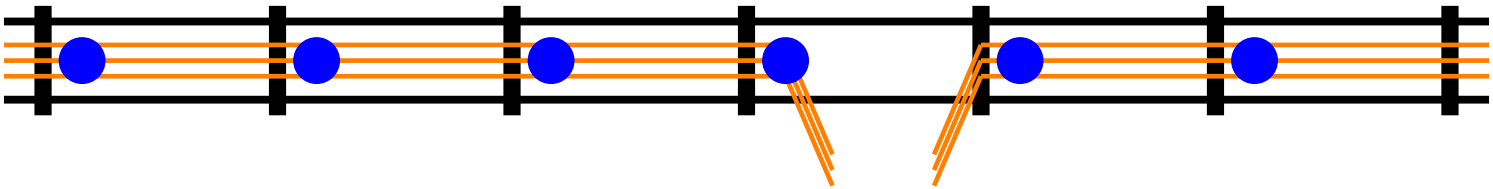
WSNs are Well-Suited to Monitoring Linear Infrastructure

- ease of deployment
- ease of maintenance
- increased reliability



WSNs are Well-Suited to Monitoring Linear Infrastructure

- ease of deployment
- ease of maintenance
- increased reliability



Characteristics of One-Dimensional WSNs

We assume the network consists of an arbitrary number of nodes, each with communication range r.

- Restricted number of neighbours
  (proportional to r, rather than r^2)
- Location knowledge
  (In particular, the order of nodes along the pipe is known.)
- Density of node deployment
  (required to ensure adequate sensing coverage)

Key Predistribution

key predistribution scheme (KPS)

- nodes are assigned keys before deployment
- nodes that share keys can communicate securely

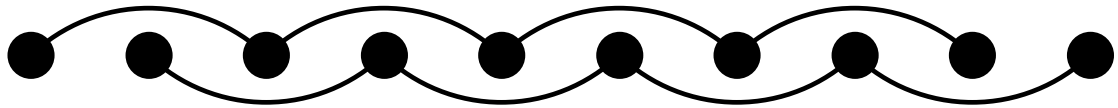
e.g. Eschenauer and Gligor: Each node draws m keys uniformly (without replacement) from a keypool $\mathcal{K}$

Security Metrics for KPSs for Traditional WSNs

- Number of keys stored by each node.
- Connectivity: Pr_1:=probability that two neighbouring nodes share a key
- Resilience: $\mathrm{fail}(s)$:=number of links between uncaptured nodes that are compromised when an adversary captures s nodes

Major Security Threat for One-Dimensional WSNs: Disconnection of the Network

- We need to prevent large sections of the network from becoming disconnected.
- Small numbers of isolated nodes are not a problem.



New Security Metric for One-Dimensional WSNs

Definition

A KPS for a one-dimensional network consisting of a set $\mathcal{N}$ of n nodes, where n is arbitrary, is s-fallible if

New Security Metric for One-Dimensional WSNs

Definition

A KPS for a one-dimensional network consisting of a set $\mathcal{N}$ of n nodes, where n is arbitrary, is s-fallible if

1. After the capture of any $s-1$ nodes, there exists a set $\mathcal{E} \subset \mathcal{N}$ of size at most $O(1)$ such that $\mathcal{N} \setminus \mathcal{E}$ is connected.

New Security Metric for One-Dimensional WSNs

Definition

A KPS for a one-dimensional network consisting of a set $\mathcal{N}$ of n nodes, where n is arbitrary, is s-fallible if

1. After the capture of any $s-1$ nodes, there exists a set $\mathcal{E} \subset \mathcal{N}$ of size at most $O(1)$ such that $\mathcal{N} \setminus \mathcal{E}$ is connected.
2. It is possible to choose s nodes whose capture partitions the network into two (or more) isolated networks of size $\Omega(n)$.

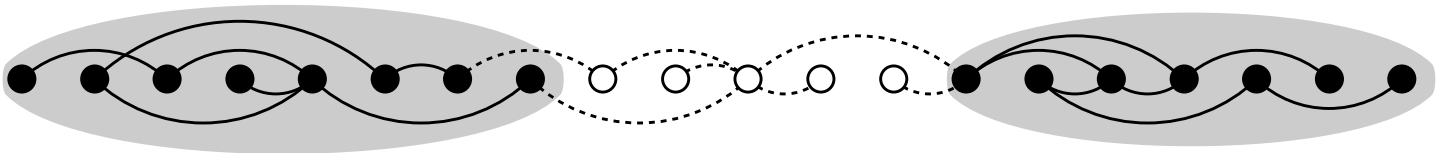
Upper Bounds For s-Fallibility

Theorem

If a KPS for a one-dimensional WSN in which the nodes have communication range r yields a connected network, then it is s-fallible for some $1 \leq s \leq r$.

Theorem

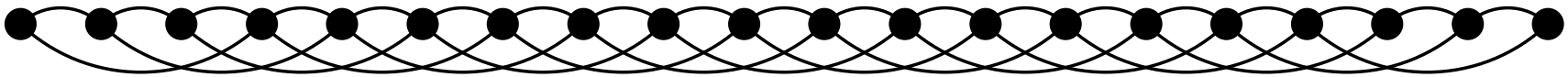
Suppose a KPS that yields a connected network assigns keys to nodes such that the largest distance between two nodes that share a key is b. Then it is s-fallible for some $1 \leq s \leq b$.



Basic Construction

We assign keys to the nodes such that:

- all pairs of nodes at distance r share a key;
- all pairs of nodes at distance 1 share a key.



e.g. $r = 3$

The Basic Construction is r-Fallible

(sketch...)

- Label nodes sequentially $0, 1, \ldots, n$.
- Suppose $r - 1$ nodes are captured.
- There exists $x \in \mathbb{Z}$ such that no node with a label equivalent to $x \pmod{r}$ has been captured.
- Let Ψ_1, Ψ_2 be nodes at distance at least $r + 1$ from some captured node. We can find a secure path between them:

The Basic Construction is r-Fallible

(sketch...)

- Label nodes sequentially $0, 1, \ldots, n$.
- Suppose $r-1$ nodes are captured.
- There exists $x \in \mathbb{Z}$ such that no node with a label equivalent to $x \pmod{r}$ has been captured.
- Let Ψ_1, Ψ_2 be nodes at distance at least $r+1$ from some captured node. We can find a secure path between them:
  1. Take hops of length 1 from Ψ_1 to Ψ_2 until a node with label equivalent to $x \pmod{r}$ is reached.

The Basic Construction is r-Fallible

(sketch...)

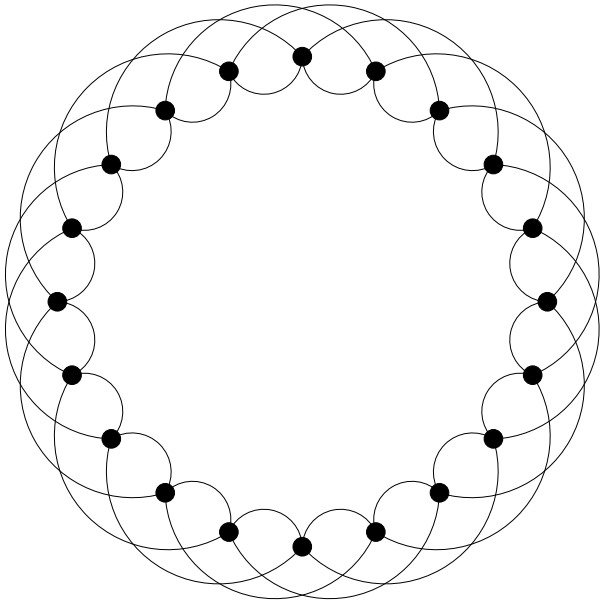
- Label nodes sequentially $0, 1, \ldots, n$.
- Suppose $r-1$ nodes are captured.
- There exists $x \in \mathbb{Z}$ such that no node with a label equivalent to $x \pmod r$ has been captured.
- Let Ψ_1, Ψ_2 be nodes at distance at least $r+1$ from some captured node. We can find a secure path between them:
  1. Take hops of length 1 from Ψ_1 to Ψ_2 until a node with label equivalent to $x \pmod r$ is reached.
  2. Take hops of length r towards Ψ_2 until a node at distance less than r from Ψ_2 is reached.

The Basic Construction is r-Fallible

(sketch...)

- Label nodes sequentially $0, 1, \ldots, n$.
- Suppose $r-1$ nodes are captured.
- There exists $x \in \mathbb{Z}$ such that no node with a label equivalent to $x \pmod r$ has been captured.
- Let Ψ_1, Ψ_2 be nodes at distance at least $r+1$ from some captured node. We can find a secure path between them:
  1. Take hops of length 1 from Ψ_1 to Ψ_2 until a node with label equivalent to $x \pmod r$ is reached.
  2. Take hops of length r towards Ψ_2 until a node at distance less than r from Ψ_2 is reached.
  3. Complete the path by hops of length 1.

Construction for Ring Topologies



thankyou

http://www.isg.rhul.ac.uk/~martin/wsn.html