

Key Predistribution and Random Intersection Graphs

Simon R. Blackburn

Joint work with Stefanie Gerke

Royal Holloway, University of London

25th June 2008

Overview

Wireless Sensor Networks

Key predistribution

Random graphs

A theorem

Sketch proofs

Open problems

Wireless Sensor Networks (WSNs)

Characteristics of a Wireless Sensor Network:

- ▶ Small, low power nodes with wireless capability
- ▶ Each node generates sensor data
- ▶ Aim to form a secure connected network
- ▶ No prior knowledge of network structure
- ▶ Use predistributed keys (as PKC too expensive)

Simple key predistribution schemes

Two simple predistribution schemes:

1. Every node given the same key.
2. Every pair u, v of nodes given a different key k_{uv} .

Simple key predistribution schemes

Two simple predistribution schemes:

1. Every node given the same key.
Problem: node capture/compromise.
2. Every pair u, v of nodes given a different key k_{uv} .

Simple key predistribution schemes

Two simple predistribution schemes:

1. Every node given the same key.
Problem: node capture/compromise.
2. Every pair u, v of nodes given a different key k_{uv} .
Problem: node stores lots of keys.

Eschenauer–Gligor key predistribution

Let V be a set of n nodes.

Let M be a pool of m secret keys.

Each node $u \in V$ is randomly assigned a set $F_u \subseteq M$ of keys, where $|F_u| = k$.

A pair of nodes $u_1, u_2 \in V$ can communicate securely if:

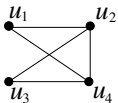
- ▶ they are in communication range, and
- ▶ they share at least one key: $F_{u_1} \cap F_{u_2} \neq \emptyset$.

A small example

Four nodes, eight keys in the pool, each node receives 3 keys:

Node u	F_u
u_1	$\{s_1, s_2, s_3\}$
u_2	$\{s_3, s_4, s_5\}$
u_3	$\{s_4, s_5, s_6\}$
u_4	$\{s_1, s_4, s_7\}$

Draw edges between nodes if they share one or more keys:



Uniform random intersection graphs

Let V be a set of n nodes. Let M be a set of m colours. Let $k \geq 2$.

Definition

The **uniform random intersection graph** $G(n, m, k)$ is constructed as follows. For each node $u \in V$, assign a set F_u of k distinct colours from M uniformly at random. Join $u_1, u_2 \in V$ by an edge if and only if

$$F_{u_1} \cap F_{u_2} \neq \emptyset.$$

Uniform random intersection graphs

Let V be a set of n nodes. Let M be a set of m colours. Let $k \geq 2$.

Definition

The **uniform random intersection graph** $G(n, m, k)$ is constructed as follows. For each node $u \in V$, assign a set F_u of k distinct colours from M uniformly at random. Join $u_1, u_2 \in V$ by an edge if and only if

$$F_{u_1} \cap F_{u_2} \neq \emptyset.$$

Question

For which parameters is $G(n, m, k)$ likely to be connected?

Note: The application gives us n and k . We can vary m as we wish.

Erdős–Renyi random graphs

Let n be an integer. Let $p = p(n) \in [0, 1]$ be some function of n .

Definition

The **Erdős–Renyi graph** $G_{n,p}$ has n nodes. Add an edge between each pair of vertices with probability p (independently).

Erdős–Renyi random graphs

Let n be an integer. Let $p = p(n) \in [0, 1]$ be some function of n .

Definition

The **Erdős–Renyi graph** $G_{n,p}$ has n nodes. Add an edge between each pair of vertices with probability p (independently).

The probability of an edge in $G(n, m, k)$ is

$$p = 1 - \frac{\binom{m-k}{k}}{\binom{m}{k}} \approx \frac{k^2}{m},$$

so Eschenauer and Gligor model $G(n, m, k)$ by $G_{n,p}$.

Connectivity of random graphs

The graph $G_{n,p}$ is connected as long as $p > \frac{\log n}{n}$:

Theorem

Let $\omega \rightarrow \infty$ as $n \rightarrow \infty$.

- (i) When $p = \frac{\log n + \omega}{n}$, then almost surely $G_{n,p}$ is connected.
- (ii) When $p = \frac{\log n - \omega}{n}$, then almost surely $G_{n,p}$ is disconnected.

Connectivity of random graphs

The graph $G_{n,p}$ is connected as long as $p > \frac{\log n}{n}$:

Theorem

Let $\omega \rightarrow \infty$ as $n \rightarrow \infty$.

- (i) When $p = \frac{\log n + \omega}{n}$, then almost surely $G_{n,p}$ is connected.
- (ii) When $p = \frac{\log n - \omega}{n}$, then almost surely $G_{n,p}$ is disconnected.

So we hope that $G(n, m, p)$ is connected when

$$p = \frac{k^2}{m} > \frac{\log n}{n}.$$

The two random graph models are different

The probability that three vertices form a triangle in $G_{n,p}$ is p^3 .

The probability that three vertices form a triangle in $G(n, m, 2)$ is approx $\frac{1}{2}p^2$.

So there are many more triangles in $G(n, m, k)$ than in $G_{n,p}$.

Why should the connectivity threshold be the same in the two models?

Our main theorem

Theorem

Let $\alpha \in \mathbb{R}$ be positive. Let $k \geq 2$ be a function of n , and let $m = \lfloor n^\alpha \rfloor$.

(i) When

$$\liminf_{n \rightarrow \infty} \frac{k^2 n}{m \log n} > 1$$

then almost surely $G(n, m, k)$ is connected.

(ii) When

$$\limsup_{n \rightarrow \infty} \frac{k^2 n}{m \log n} < 1$$

then almost surely $G(n, m, k)$ is disconnected.

We can drop the condition that $m = \lfloor n^\alpha \rfloor$ when $m \geq n$ or when $m = o(n/\log n)$.

Proving $G(n, m, k)$ is disconnected

Assume that

$$\limsup_{n \rightarrow \infty} \frac{k^2 n}{m \log n} < 1.$$

The expected number of isolated vertices is

$$n \left(\frac{\binom{m-k}{k}}{\binom{m}{k}} \right)^{n-1} \rightarrow \infty \text{ as } n \rightarrow \infty.$$

The standard deviation of the number of isolated vertices grows more slowly than the expected number.

These two facts imply (by the 2nd moment method) that there is at least one isolated vertex almost surely.

Proving that $G(n, m, k)$ is connected: $m \geq n$

Let $S \subseteq V$ be a set of vertices of size s .

S is assigned about ks colours with very high probability.

Given that S is assigned almost ks colours, the probability that S is a component of $G(n, m, k)$ is at most (approx)

$$\left(\frac{\binom{m-ks}{k}}{\binom{m}{k}} \right)^{n-s}$$

which tends to 0 very rapidly.

So S is very unlikely to be a component: indeed the probability that there is any component is extremely small.

Proving that $G(n, m, k)$ is connected: $m < n$

- ▶ Reduce to the case when $k = 2$: $G(n, m, 2)$ is less likely to be connected than $G(n, m, k)$.
- ▶ Define the colour graph H : vertices are the m colours; colours are joined when there is a node of $G(n, m, 2)$ assigned both colours.
- ▶ $G(n, m, 2)$ is connected if and only if H consists of a connected component plus a (possibly empty) set of isolated vertices.
- ▶ The edges of H are chosen independently: can model as a classical random graph.
- ▶ Use the known threshold for a random graph to consist of a connected component plus isolated vertices.

Open problems

- ▶ Remove the condition that $m = \lfloor n^\alpha \rfloor$ from the theorem.

Open problems

- ▶ Remove the condition that $m = \lfloor n^\alpha \rfloor$ from the theorem.
- ▶ Prove a tighter threshold of

$$\frac{k^2 n}{m} = (\log n) \pm \omega$$

where $\omega \rightarrow \infty$ as $n \rightarrow \infty$.

Open problems

- ▶ Remove the condition that $m = \lfloor n^\alpha \rfloor$ from the theorem.
- ▶ Prove a tighter threshold of

$$\frac{k^2 n}{m} = (\log n) \pm \omega$$

where $\omega \rightarrow \infty$ as $n \rightarrow \infty$.

- ▶ Prove good results on the emergence of the giant component in $G(n, m, k)$ (something is already known).

Open problems

- ▶ Remove the condition that $m = \lfloor n^\alpha \rfloor$ from the theorem.
- ▶ Prove a tighter threshold of

$$\frac{k^2 n}{m} = (\log n) \pm \omega$$

where $\omega \rightarrow \infty$ as $n \rightarrow \infty$.

- ▶ Prove good results on the emergence of the giant component in $G(n, m, k)$ (something is already known).
- ▶ Prove results on the k -connectivity and chromatic number of $G(n, m, k)$.

Links

Our paper can be obtained from the arXiv:

<http://arxiv.org/abs/0805.2814>

This talk can be downloaded from my homepage:

<http://www.cs.rhul.ac.uk/~simonb/>