

On the random graph induced by a random key predistribution scheme under full visibility

Osman Yağın

(Joint work with Armand M. Makowski)

ECE & ISR/HyNet

University of Maryland at College Park

oyagan@umd.edu

WSNs and security

- WSNs are **distributed** collections of sensors with **limited** capabilities for computations and wireless communications
- Deployed in **hostile** environments where communications are monitored, and nodes are subject to capture and surreptitious use by an adversary
- **Cryptographic protection** needed to ensure secure communications, as well as to enable sensor-capture detection, key revocation and sensor disabling
- Traditional key exchange and distribution protocols based on trusting third parties are **inadequate** for **large-scale** WSNs

A random key predistribution scheme (Eschenauer and Gligor 2002)

- Before network deployment, each node **randomly** selects a set of K **distinct** keys from a pool of P keys. These K keys form the **key ring** of the node, and are inserted into its memory.
- A secure link will be established between nodes who share at least one key in their key rings.

$$\begin{aligned} \mathbb{P}[\text{link assignment between any two sensors}] &= 1 - \frac{\binom{P-K}{K}}{\binom{P}{K}} \\ &\sim \frac{K^2}{P} \end{aligned}$$

A basic question

Given the randomness involved, for any pair of integers P and K with $K < P$, there is a **positive** probability that secure connectivity will **not** be achieved

This so even when the communication graph is itself connected!

Q: How do we select the parameters P and K to make the probability of secure connectivity as large as possible?

The random key graph $\mathbb{K}(n; \theta)$

- Constructing the random graph with vertex set $\{1, \dots, n\}$
 - sensors \Rightarrow nodes
 - links \Rightarrow edges
 - $\theta \equiv (P, K)$
- \mathbb{P} [edge assignment between any two nodes] $\sim \frac{K^2}{P}$

Q: How do we select P and K so that $\mathbb{K}(n; \theta)$ is connected with very high probability?

The Erdős-Renyi graph $\mathbb{G}(n; p)$

Random link assignment encoded through **i.i.d.** $\{0, 1\}$ -valued rvs

$$\{\xi_{ij}(p), i < j; i, j = 1, \dots, n\}$$

with

$$\mathbb{P}[\xi_{ij}(p) = 1] = p$$

for some $0 < p < 1$.

Also known as Bernoulli graphs

Zero-one laws for graph connectivity in Erdős-Renyi graphs

$\mathbb{G}(n; p)$ ($0 < p < 1$): Whenever

$$p_n \sim c \frac{\log n}{n}$$

for some $c > 0$, we have

$$\lim_{n \rightarrow \infty} \mathbb{P}[\mathbb{G}(n; p_n) \text{ is connected}] = \begin{cases} 0 & \text{if } 0 < c < 1 \\ 1 & \text{if } 1 < c \end{cases}$$

Critical threshold for graph connectivity:

$$p_n^* := \frac{\log n}{n}, \quad n = 1, 2, \dots$$

But $\mathbb{K}(n; \theta) \not\equiv \mathbb{G}(n; p)$!

Despite **strong similarities**,

$$\mathbb{K}(n; \theta) \not\equiv \mathbb{G}(n; p),$$

even with

$$p = \frac{K^2}{P}$$

For n large, Di Pietro et al. show that $\mathbb{K}(n; \theta_n)$ will be connected with very high probability if P_n and K_n are selected such that

$$P_n \geq n \quad \text{and} \quad \frac{K_n^2}{P_n} \sim c \frac{\log n}{n}$$

as soon as $c > 16$.

Zero-one law for absence of isolated nodes

$P(n; \theta) := \mathbb{P} [\mathbb{K}_n(\theta) \text{ contains no isolated nodes}]$

Theorem 1 *For any admissible pair $P, K : \mathbb{N}_0 \rightarrow \mathbb{N}$ such that*

$$\frac{K_n^2}{P_n} \sim c \frac{\log n}{n}$$

for some $c > 0$, we have

$$\lim_{n \rightarrow \infty} P(n; \theta_n) = \begin{cases} 0 & \text{if } 0 < c < 1 \\ 1 & \text{if } 1 < c \end{cases}$$

Zero-one law for connectivity

Theorem 2 For any admissible pair $P, K : \mathbb{N}_0 \rightarrow \mathbb{N}$ such that

$$\frac{K_n^2}{P_n} \sim c \frac{\log n}{n}$$

and $P_n \geq n$, we have

$$\lim_{n \rightarrow \infty} \mathbb{P} [\mathbb{K}_n(\theta) \text{ is connected}] = \begin{cases} 0 & \text{if } 0 < c < 1 \\ 1 & \text{if } 1 < c \end{cases}$$

Yağan and Makowski (To be submitted)

Consequently

Although

$$\mathbb{K}(n; \theta) \not\cong \mathbb{G}(n; p),$$

$\mathbb{K}_n(\theta)$ and $\mathbb{G}(n; p)$ exhibit related asymptotic behavior for graph connectivity!

Look for other graph properties!