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

Osman Yagan and Armand M. Makowski

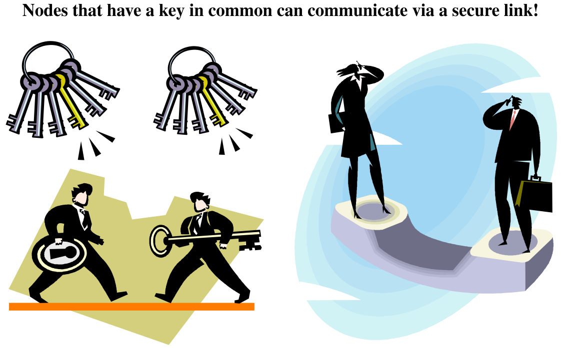
## WSNs and security

- 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.
- Public key cryptography is impractical due to computational and communication limitations.
- Internet style key exchange and distribution protocols based on trusting third parties are **inadequate** for **large-scale** WSNs due to unknown network topology prior to deployment.
- A possible solution: Random key predistribution!

## A random key predistribution scheme (Eschenauer and Gligor 2002)

- **Initialization phase:** 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.
- **Key setup phase:** After discovering their **wireless neighbors**, nodes mutually authenticate the shared keys to verify that the other party owns it. Now, they can communicate securely in one hop.
- **Path-key identification phase:** The key rings being randomly selected, some pairs of wireless neighbors may not share a key. If a path of nodes sharing keys pairwise exists between them, this (secure) path can be used to exchange a **path-key** to establish a direct (and secure) link between them.

**Nodes that have a key in common can communicate via a secure link!**



**Q:** Given integers $P$ and $K$ with $K < P$, how do we select the parameters $P$ and $K$ to make the probability of secure connectivity as large as possible?

## Random key graph, $\mathbb{K}(n;\theta)$

- $n$: The number of nodes.
- $P$: The size of the key pool.
- $K$: The size of each key ring.
- With $\theta \equiv (P,K)$, let $K_i(\theta)$ denote the **random** set of $K$ **distinct** keys assigned to node $i$. Assume the random sets $K_1(\theta),\ldots,K_n(\theta)$ to are **i.i.d.** with

$$\mathbb{P}[K_i(\theta)=S] = \binom{P}{K}^{-1}, \quad S \in \mathcal{P}_K$$

- Not equivalent to Erdős-Renyi graph $\mathbb{G}(n;p)$ since edge assignments may be correlated.
- Quantities of interest

$$\begin{aligned} P^\star(n;\theta) &:= \mathbb{P}[\mathbb{K}(n;\theta) \text{ is connected}] \\ P(n;\theta) &:= \mathbb{P}[\mathbb{K}(n;\theta) \text{ contains no isolated nodes}] \end{aligned}$$

## Main results

**Theorem 1** *For any admissible pair $P,K:\mathbb{N}_0 \to \mathbb{N}$, we have*

$$\lim_{n\to\infty} P(n;K_n,P_n) = \begin{cases} 0 & \text{if } \lim_{n\to\infty}\alpha_n = -\infty \\ 1 & \text{if } \lim_{n\to\infty}\alpha_n = +\infty \end{cases}$$

*where the function $\alpha:\mathbb{N}_0 \to \mathbb{R}$ is determined through*

$$\frac{K_n^2}{P_n} = \frac{\log n + \alpha_n}{n}, \quad n = 1,2,\ldots$$

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

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

*for some $c>0$, we have*

$$\lim_{n\to\infty} P(n;K_n,P_n) = \begin{cases} 0 & \text{if } 0<c<1 \\ 1 & \text{if } 1<c. \end{cases}$$

Treating absence of isolated nodes is **useful** because

$$P^\star(n;\theta) \le P(n;\theta).$$

Corollary 1 already establishes the **zero law** for connectivity (see conjecture) since

$$\lim_{n\to\infty} P^\star(n;\theta_n) = 0$$

whenever $0<c<1$.

## Related work and a conjecture

**Previously:** Di Pietro et al. (2004-2006): For $n$ large, they show that the random key graph will be connected with very high probability if $P_n$ and $K_n$ are selected such that

$$P_n \ge n \quad \text{and} \quad \frac{K_n^2}{P_n} \sim c\frac{\log n}{n} \quad (n\to\infty)$$

as soon as $c > 16$.

**Conjecture** *For any admissible pair $P,K:\mathbb{N}_0 \to \mathbb{N}$ such that*

$$\frac{K_n^2}{P_n} \sim c\frac{\log n}{n} \quad (n\to\infty)$$

*for some $c>0$, we have*

$$\lim_{n\to\infty} P^\star(n;P_n,K_n) = \begin{cases} 0 & \text{if } 0<c<1 \\ 1 & \text{if } 1<c. \end{cases}$$

**Motivation:** Zero-one laws for graph connectivity in Erdős-Renyi graphs $\mathbb{G}(n;p)$ $(0<p<1)$: Whenever

$$p_n \sim c\frac{\log n}{n} \quad (n\to\infty)$$

for some $c>0$, we have

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

with critical threshold for connectivity in $\mathbb{G}(n;p)$ given by

$$p_n^\star := \frac{\log n}{n}, \quad n=1,2,\ldots$$

**Analogy:** With $\mathbb{P}[K_i(\theta)\cap K_j(\theta)=\emptyset] = \frac{\binom{P-K}{K}}{\binom{P}{K}} = q(\theta)$, we have

$$1-q(\theta_n) \sim \frac{K_n^2}{P_n} = c\frac{\log n}{n} \quad (n\to\infty),$$

and although

$$\mathbb{K}(n;\theta) \not\equiv \mathbb{G}(n;p) \quad \text{even with } p = 1-q(\theta),$$

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

## References


† O. Yagan and A. M. Makowski, “On the random graph induced by a random key predistribution scheme under full visibility,” Submitted to the IEEE International Symposium on Information Theory (ISIT 2008), Toronto (Canada), July 2008.