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

Osman Yağan and Armand M. Makowski
Department of Electrical and Computer Engineering
and the Institute for Systems Research
University of Maryland at College Park
College Park, Maryland 20742
oyagan@umd.edu, armand@isr.umd.edu

Abstract— **We consider the random graph induced by the random key predistribution scheme of Eschenauer and Gligor under the assumption of full visibility. We show the existence of a zero-one law for the absence of isolated nodes, and complement it by a Poisson convergence for the number of isolated nodes. Leveraging earlier results and analogies with Erdős-Renyi graphs, we explore similar results for the property of graph connectivity.**

Keywords: Wireless sensor networks, Key predistribution, Secure connectivity, Absence of isolated nodes, Zero-one laws, Poisson convergence.

I. Introduction

Wireless sensor networks (WSNs) are distributed collections of sensors with limited capabilities for computations and wireless communications. It is envisioned that such networks will be deployed in hostile environments where communications are monitored, and nodes are subject to capture and surreptitious use by an adversary. Under these circumstances, cryptographic protection will be needed to ensure secure communications, as well as to support sensor-capture detection, key revocation and sensor disabling. However, traditional key exchange and distribution protocols based on trusting third parties are inadequate for large-scale WSNs, e.g., see [7, 13, 15] for discussions of some of the challenges to be encountered.

A. A random key predistribution scheme

Recently, Eschenauer and Gligor [7] have proposed a key management solution better suited to WSN environments. This scheme, hereafter called the EG scheme, is based on *random* key predistribution and operates in three phases: Consider a collection of n sensor nodes equipped with wireless transmitters, and assume available a large set of P cryptographic keys, also known as the *key pool*.

(i) Initialization phase: Before network deployment, each node randomly selects a set of K *distinct* keys from the pool. These K keys form the *key ring* of the node, and are inserted into its memory. Key rings are selected independently across nodes.

(ii) Key setup phase: After deployment, each node discovers its *wireless neighbors*, i.e., those nodes which are within its wireless communication range. When a node finds a wireless neighbor with whom it shares a key, they mutually authenticate the key to verify that the other party actually owns it. At the end of this phase, wireless neighbors which have keys in common can now communicate securely with each other in one hop.

(iii) Path-key identification phase: The key rings being randomly selected, there is a possibility that some pairs of wireless neighbors may not share a key. If a path made up of nodes sharing keys pairwise exists between such a pair of wireless neighbors, this (secure) path can be used to exchange a *path-key* to establish a direct (and secure) link between them.

B. Dimensioning for secure connectivity

A basic question concerning the EG scheme is its ability to achieve *secure connectivity* among participating nodes in the sense that a *secure path* exists between any pair of nodes. Given the randomness involved, for any pair of integers P and K such that $K < P$, there is a positive probability that secure connectivity will *not* be achieved – This will be so even in the best of cases when the communication graph is itself connected.[1] Hence, there arises the need to understand how to select the parameters P and K in order to make the probability of secure connectivity as large as possible.

This issue was addressed by Eschenauer and Gligor in their original paper under two simplifying assumptions, namely *full visibility* and *mutual independence* of secure link allocations; more on this second assumption in Section III. Full visibility refers to the situation where two nodes are always able to communicate with each other, irrespective of their relative positions or the quality of the wireless links that may exist between them. In that case, the shared key discovery process allows every pair of nodes to determine whether their key rings have keys in common. This makes it possible to model the EG scheme with the help of a class of random graphs, introduced in Section II and hereafter referred to as *random key graphs*.

For sure, the assumption of full visibility does away with the wireless nature of the communication infrastructure supporting WSNs. In return, this simplification allows us to focus on how randomizing the key selections affects the establishment

[1] The communication graph refers to the graph induced by the communication process whereby two nodes are adjacent if they are wireless neighbors, e.g., the disk model or the SINR graph.

978-1-4244-2571-6/08/$25.00 ©2008 IEEE

of secure links. It is this aspect of the EG scheme that we study here, as we develop various properties for the random key graph. We do so with an eye towards understanding how proper parameter selection in the EG scheme may lead to secure connectivity with very high probability.

C. Contributions

For the class of random key graphs, we establish a zero-one law for the absence of isolated nodes, and identify the corresponding critical thresholds; see Theorem 4.1. We complement this result by a Poisson convergence for the number of isolated nodes; see Theorem 4.4. These results already imply a zero law for the property of graph connectivity. Next, starting with earlier results by Di Pietro et al. [4], we leverage analogies with Erdős-Renyi graphs (and attending zero-one laws) to conjecture the form of zero-one laws for graph connectivity in random key graphs. We also give conditions for the corresponding "double exponential" result. Implications for secure connectivity can be found in Section III. The proofs of Theorems 4.1 and 4.4 are outlined in Sections V and VI, respectively, with full details in the extended version [16].

II. Random key graphs

The model is parametrized by the number n of nodes, the size P of the key pool and the size K of each key ring with $K < P$. To lighten the notation we often group the integers P and K into the ordered pair $\theta \equiv (P, K)$. With $\mathcal{P}$ the set of all cryptographic keys, let $\mathcal{P}_K$ to denote the collection of all subsets of $\mathcal{P}$ which contain exactly K elements – Obviously, we have $|\mathcal{P}| = P$ and $|\mathcal{P}_K| = \binom{P}{K}$.

For each node $i = 1, \ldots, n$, let $\boldsymbol{K}_i(\theta)$ denote the random set of K distinct keys assigned to node i. We can think of $\boldsymbol{K}_i(\theta)$ as an $\mathcal{P}_K$-valued rv. Under the EG scheme, the rvs $\boldsymbol{K}_1(\theta), \ldots, \boldsymbol{K}_n(\theta)$ are assumed to be *i.i.d.* rvs which are *uniformly* distributed over $\mathcal{P}_K$ with

$$\mathbb{P}\left[\boldsymbol{K}_i(\theta) = S\right] = \binom{P}{K}^{-1}, \quad S \in \mathcal{P}_K \tag{1}$$

for all $i = 1, \ldots, n$. This corresponds to selecting keys randomly and *without* replacement from the key pool.

The key set-up phase in the EG scheme suggests a natural notion of adjacency between nodes: Distinct nodes $i, j = 1, \ldots, n$ are said to be adjacent if they share at least one key in their key rings, namely

$$\boldsymbol{K}_i(\theta) \cap \boldsymbol{K}_j(\theta) \neq \emptyset. \tag{2}$$

In that case, an undirected link is assigned between nodes i and j. The resulting random graph defines the *random key graph* on the vertex set $\{1, \ldots, n\}$, hereafter denoted $\mathbb{K}(n; \theta)$. For distinct $i, j = 1, \ldots, n$, it is a simple matter to check that

$$\mathbb{P}\left[\boldsymbol{K}_i(\theta) \cap \boldsymbol{K}_j(\theta) = \emptyset\right] = q(\theta) \tag{3}$$

with

$$q(\theta) := \frac{\binom{P-K}{K}}{\binom{P}{K}}. \tag{4}$$

Random key graphs form a subclass in the family of random graphs known in the literature as *random intersection* graphs. However, the model adopted here differs from the random graphs discussed by Singer-Cohen et al. in [11, 14] where each node is assigned a key ring, one key at a time according to a Bernoulli-like mechanism (so that each key ring has a random size and has positive probability of being empty).

Despite strong similarities, the random graph $\mathbb{K}(n; \theta)$ is *not* an Erdős-Renyi graph $\mathbb{G}(n; p)$ [10] *even* if we take

$$p = 1 - q(\theta). \tag{5}$$

This is so because edge assignments are correlated in $\mathbb{K}(n; \theta)$ but independent in $\mathbb{G}(n; p)$: For distinct $i, j = 1, \ldots, n$, define the edge assignment rvs as the indicators rvs given by

$$\xi_{ij}(\theta) := \mathbf{1}\left[\boldsymbol{K}_i(\theta) \cap \boldsymbol{K}_j(\theta) \neq \emptyset\right].$$

Then, for distinct triplets $i, j, k = 1, \ldots, n$, the rvs $\xi_{ij}(\theta)$, $\xi_{jk}(\theta)$ and $\xi_{ik}(\theta)$ are *not* mutually independent (although they are *pairwise* independent).

Let $P^\star(n; \theta)$ denote the probability that the random graph $\mathbb{K}(n; \theta)$ is connected, namely

$$P^\star(n; \theta) := \mathbb{P}\left[\mathbb{K}(n; \theta) \text{ is connected}\right].$$

In the full visibility case assumed here, $P^\star(n; \theta)$ coincides with the probability of secure connectivity mentioned earlier.

III. Related work

We wish to select P and K so that $P^\star(n; \theta)$ is as large (i.e., as close to one) as possible. This issue naturally draws attention to zero-one laws for graph connectivity in random key graphs when P and K are appropriately scaled with n. Such zero-one laws are known to hold for the Erdős-Renyi graphs $\mathbb{G}(n; p)$ $(0 < p < 1)$ [6, 10]: Whenever[2]

$$p_n \sim c\, \frac{\log n}{n} \tag{6}$$

for some $c > 0$, it holds that

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}(n; p_n) \text{ is connected}\right] = \begin{cases} 0 & \text{if } \ 0 < c < 1 \\ \\ 1 & \text{if } \ 1 < c. \end{cases} \tag{7}$$

However, given that no such zero-one laws for random key graphs were available to them, Eschenauer and Gligor instead replaced $\mathbb{K}(n; \theta)$ with the *proxy* Erdős-Renyi graph $\mathbb{G}(n; p)$ where p is given by (5), thereby leading to the approximation

$$P^\star(n; \theta) \simeq \mathbb{P}\left[\mathbb{G}(n; 1 - q(\theta)) \text{ is connected}\right]. \tag{8}$$

An additional benefit of this approach lies in the availability of the celebrated "double exponential" result of Erdős and Renyi [2, 6]: For every scalar γ, it is well known that

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{G}(n; p_{n,\gamma}) \text{ is connected}\right] = e^{-e^{-\gamma}} \tag{9}$$

with

$$p_{n,\gamma} = \frac{\log n}{n} + \frac{\gamma + o(1)}{n}, \quad n = 2, 3, \ldots \tag{10}$$

[2] In this paper, all statements involving limits, including asymptotic equivalences, are always understood with n going to infinity.

Thus, if we select P and K as functions of n, say P_n and K_n, so that

$$1 - q(\theta_n) = \frac{\log n}{n} + \frac{\gamma + o(1)}{n}, \quad n = 2, 3, \ldots \tag{11}$$

then a reasonable approximation in the form

$$P^\star(n; \theta_n) \simeq e^{-e^{-\gamma}}$$

suggests itself for large n. A refinement of this approach, still based on the theory of Erdős-Renyi graphs, is given by Hwang and Kim [9] for the EG as well as for a number of other random key predistribution schemes, including schemes by Chan et al. [3] and by Du et al. [5].

In [4], Di Pietro et al. argue that edge assignments in the random key graph (2) are not mutually independent (as was already indicated earlier) but may in fact be strongly correlated for reasonable values of the parameters K and P. Therefore, an analysis based on Erdős-Renyi graphs may not provide a reliable guide for properly dimensioning the EG scheme. This prompted these authors to investigate the connectivity properties of random key graphs (*without* the independence assumption on the edge assignments). They showed [4, Thm. 4.6] that for large n, the random key graph will be connected with very high probability if P_n and K_n are selected such that

$$P_n \geq n \quad \text{and} \quad \frac{K_n^2}{P_n} \sim c\, \frac{\log n}{n} \tag{12}$$

as soon as $c > 16$.

IV. The results

What happens when $0 < c \leq 16$? This is where we pick up the trail: Ideally, for reasons that should be apparent from the discussion of Section III, one would like to establish a zero-one law for graph connectivity in random key graphs, together with the appropriate version of an attending "double exponential" result. In view of the results of Di Pietro et al., we expect such a zero-one law to hold in the form

$$\lim_{n\to\infty} P^\star(n; \theta_n) = \begin{cases} 0 & \text{if } \ 0 < c < 1 \\ \\ 1 & \text{if } \ 1 < c \end{cases} \tag{13}$$

whenever

$$\frac{K_n^2}{P_n} \sim c\, \frac{\log n}{n} \tag{14}$$

for some $c > 0$ (possibly with some additional conditions).

This is not too farfetched for the following reasons: First of all, the results in [4, Thm. 4.6] already confirm the one-law in the range $c > 16$. Next, although it is certainly true that random key graphs do not coincide with Erdős-Renyi graphs, they certainly appear to be somewhat related – In both cases the edge assignments are pairwise independent. Therefore, the zero-one law (6)-(7) for Erdős-Renyi graphs may be viewed as indirect additional support for the validity of (13) under (14). In fact, such a "transfer" is not without precedent: In the class of random intersection graphs studied by Singer et al. [11, 14], Fill et al. [8] have shown equivalence with Erdős-Renyi graphs in a strong sense for some asymptotic regimes of interest.

In the present paper we report on results that further suggest the validity of (13) under (14). As with Erdős-Renyi graphs [2, 6], we do so by considering the property that the random key graph contains no isolated nodes: Fix $n = 2, 3, \ldots$ and consider $\theta = (P, K)$ with positive integers K and P such that $K < P$. We then define

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

If the random key graph $\mathbb{K}(n; \theta)$ is connected, then it does not contain isolated nodes, whence

$$P^\star(n; \theta) \leq P(n; \theta). \tag{15}$$

A. Zero-one laws

With any pair of functions $P, K : \mathbb{N}_0 \to \mathbb{N}$, we associate a function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ through the relation

$$\frac{K_n^2}{P_n} = \frac{\log n + \alpha_n}{n}, \quad n = 1, 2, \ldots \tag{16}$$

Just set

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

A pair of functions $P, K : \mathbb{N}_0 \to \mathbb{N}$ is said to be *admissible* if $K_n < P_n$ for all $n = 1, 2, \ldots$. Our main result is the following zero-one law for the absence of isolated nodes.

Theorem 4.1: *For any admissible pair of functions $P, K : \mathbb{N}_0 \to \mathbb{N}$, it holds that*

$$\lim_{n\to\infty} P(n; \theta_n) = \begin{cases} 0 & \text{if } \lim_{n\to\infty} \alpha_n = -\infty \\ \\ 1 & \text{if } \lim_{n\to\infty} \alpha_n = +\infty \end{cases} \tag{17}$$

where the function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ is determined through (16).

Theorem 4.1, whose proof is outlined in Section V, readily implies the following zero-one law.

Corollary 4.2: *Consider any admissible pair of functions $P, K : \mathbb{N}_0 \to \mathbb{N}$ such that (14) holds for some $c > 0$. Then it holds that*

$$\lim_{n\to\infty} P(n; \theta_n) = \begin{cases} 0 & \text{if } 0 < c < 1 \\ \\ 1 & \text{if } 1 < c. \end{cases} \tag{18}$$

Indeed, it suffices to use Theorem 4.1 with any admissible pair of functions $P, K : \mathbb{N}_0 \to \mathbb{N}$ whose function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ satisfies

$$\alpha_n = (c - 1)\,(1 + o(1)) \cdot \log n, \quad n = 1, 2, \ldots$$

With the help of (15), it is now plain from Corollary 4.2 under (14) that

$$\lim_{n\to\infty} P^\star(n; \theta_n) = 0 \quad \text{if } \ 0 < c < 1. \tag{19}$$

This already establishes the zero-law in (13) under (14). In fact, Theorem 4.1 also implies the stronger statement

$$\lim_{n\to\infty} P^\star(n; \theta_n) = 0 \quad \text{if } \ \lim_{n\to\infty} \alpha_n = -\infty.$$

Taking our cue from existing results for Erdős-Renyi graphs [2, 6, 10] (as well as for geometric random graphs, e.g., see

[12]), we expect that again for random key graphs, graph connectivity and the absence of isolated nodes are *asymptotically equivalent* graph properties (for large n). This leads to the following conjecture which is currently under investigation:

Conjecture 4.3: *For any admissible pair of functions $P, K : \mathbb{N}_0 \to \mathbb{N}$, it holds that*

$$\lim_{n\to\infty} P^\star(n;\theta_n) = \begin{cases} 0 & \text{if } \lim_{n\to\infty}\alpha_n = -\infty \\ \\ 1 & \text{if } \lim_{n\to\infty}\alpha_n = +\infty \end{cases} \tag{20}$$

with function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ determined through (16).

As before, by virtue of (15), the zero-law in Conjecture 4.3 readily follows from Theorem 4.1.

B. Poisson convergence

Stronger results can be contemplated: Consider $\theta = (P, K)$ with positive integers K and P such that $K < P$. Fix $n = 2, 3, \ldots$ and write

$$\chi_{n,i}(\theta) := \mathbf{1}\left[\text{Node } i \text{ is isolated in } \mathbb{K}_n(\theta)\right], \quad i = 1, \ldots, n.$$

The number of isolated nodes in $\mathbb{K}_n(\theta)$ is simply given by

$$I_n(\theta) := \sum_{i=1}^{n} \chi_{n,i}(\theta).$$

The random graph $\mathbb{K}_n(\theta)$ has no isolated nodes if $I_n(\theta) = 0$, in which case

$$P(n;\theta) = \mathbb{P}\left[I_n(\theta) = 0\right]. \tag{21}$$

Let $\Pi(\mu)$ denote a Poisson rv with parameter μ. Using the Stein-Chen method we can derive a Poisson approximation result which yields convergence to a Poisson rv.

Theorem 4.4: *Consider an admissible pair of functions $P, K : \mathbb{N}_0 \to \mathbb{N}$ whose function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ determined through (16) satisfies*

$$\lim_{n\to\infty} \alpha_n = \gamma \tag{22}$$

for some scalar γ. Then, the convergence

$$I_n(\theta_n) \Longrightarrow_n \Pi(e^{-\gamma}) \tag{23}$$

holds with $\Longrightarrow_n$ denoting convergence in distribution (as n goes to infinity).

The attending "double exponential" result is now immediate from (21), and takes the form

$$\lim_{n\to\infty} P(n;\theta_n) = e^{-e^{-\gamma}} \tag{24}$$

for any admissible pair of functions $P, K : \mathbb{N}_0 \to \mathbb{N}$ satisfying the assumptions of Theorem 4.4. This last convergence also implies Theorem 4.1 by an easy monotonicity argument. Finally, the conjectured asymptotic equivalence of graph connectivity and absence of isolated nodes, which underlies Conjecture 4.3, would now lead to the desired "double exponential" result

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

under the assumptions required for (24) to hold.

V. A proof of Theorem 4.1 (Outline)

Fix $n = 2, 3, \ldots$ and consider $\theta = (P, K)$ with positive integers K and P such that $K < P$. The equivalence (21) provides the basis for applying the *method of first and second moments* [10, p. 55], an approach which relies on the well-known bounds

$$1 - \mathbb{E}\left[I_n(\theta)\right] \le \mathbb{P}\left[I_n(\theta) = 0\right] \le 1 - \frac{\left(\mathbb{E}\left[I_n(\theta)\right]\right)^2}{\mathbb{E}\left[I_n(\theta)^2\right]}.$$

The rvs $\chi_{n,1}(\theta), \ldots, \chi_{n,n}(\theta)$ being exchangeable, we find

$$\mathbb{E}\left[I_n(\theta)\right] = n\mathbb{E}\left[\chi_{n,1}(\theta)\right] \tag{25}$$

and

$$\begin{aligned} \mathbb{E}\left[I_n(\theta)^2\right] &= n\mathbb{E}\left[\chi_{n,1}(\theta)\right] \\ &\quad + n(n-1)\mathbb{E}\left[\chi_{n,1}(\theta)\chi_{n,2}(\theta)\right] \end{aligned} \tag{26}$$

by the binary nature of the rvs involved, whence

$$\frac{\mathbb{E}\left[I_n(\theta)^2\right]}{\left(\mathbb{E}\left[I_n(\theta)\right]\right)^2} = \frac{1}{\mathbb{E}\left[I_n(\theta)\right]} + \frac{n-1}{n} \cdot \frac{\mathbb{E}\left[\chi_{n,1}(\theta)\chi_{n,2}(\theta)\right]}{\left(\mathbb{E}\left[\chi_{n,1}(\theta)\right]\right)^2}.$$

The proof of Theorem 4.1 is easily completed once the next two technical lemmas are established.

Lemma 5.1: *For any admissible pair of functions $P, K : \mathbb{N}_0 \to \mathbb{N}$, it holds that*

$$\lim_{n\to\infty} \mathbb{E}\left[I_n(\theta_n)\right] = \begin{cases} 0 & \text{if } \lim_{n\to\infty}\alpha_n = +\infty \\ \\ \infty & \text{if } \lim_{n\to\infty}\alpha_n = -\infty \end{cases} \tag{27}$$

where the function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ is determined through (16).

Lemma 5.2: *For any admissible pair of functions $P, K : \mathbb{N}_0 \to \mathbb{N}$, it holds that*

$$\lim_{n\to\infty} \frac{\mathbb{E}\left[\chi_{n,1}(\theta_n)\chi_{n,2}(\theta_n)\right]}{\left(\mathbb{E}\left[\chi_{n,1}(\theta_n)\right]\right)^2} = 1 \tag{28}$$

whenever the function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ determined through (16) satisfies the condition $\lim_{n\to\infty}\alpha_n = -\infty$.

Details as to how Lemmas 5.1 and 5.2 can be used to establish Theorem 4.1 are available in [16]. As we now turn to proving Lemmas 5.1 and 5.2, for positive integers K and P such that $3K < P$, we write

$$A(P,K) := \frac{\binom{P-K}{K}}{\binom{P}{K}} \quad \text{and} \quad B(P,K) := \frac{\binom{P-2K}{K}}{\binom{P}{K}}.$$

Fix $n = 2, 3, \ldots$. Under the enforced independence assumptions, it is a simple matter to see that

$$\mathbb{E}\left[\chi_{n,i}(\theta)\right] = A(P,K)^{n-1}$$

for all $i = 1, \ldots, n$, whence

$$\mathbb{E}\left[I_n(\theta)\right] = nA(P,K)^{n-1}. \tag{29}$$

Similarly, for distinct $i, j = 1, \ldots, n$, we have

$$\mathbb{E}\left[\chi_{n,i}(\theta)\chi_{n,j}(\theta)\right] = A(P,K)B(P,K)^{n-2}$$

and the expression

$$\frac{\mathbb{E}\left[\chi_{n,i}(\theta)\chi_{n,j}(\theta)\right]}{\left(\mathbb{E}\left[\chi_{n,i}(\theta)\right]\right)^2} = \frac{1}{A(P,K)}\left(\frac{\binom{P-2K}{K}}{\binom{P-K}{K}}\frac{\binom{P}{K}}{\binom{P-K}{K}}\right)^{n-2} \tag{30}$$

follows.

Next, if we use the inequalities $P-K < P-(K-1) < \ldots < P-1 < P$ in the expression

$$A(P,K) = \frac{\binom{P-K}{K}}{\binom{P}{K}} = \prod_{\ell=0}^{K-1}\left(1-\frac{K}{P-\ell}\right),$$

we obtain the bounds

$$\left(1-\frac{K}{P-K}\right)^K \le A(P,K) \le \left(1-\frac{K}{P}\right)^K. \tag{31}$$

Replacing P by $P-K$ in this last argument yields

$$\left(1-\frac{K}{P-2K}\right)^K \le \frac{\binom{P-2K}{K}}{\binom{P-K}{K}} \le \left(1-\frac{K}{P-K}\right)^K. \tag{32}$$

To establish Lemma 5.1, use (29) and the bound (31), while the proof of Lemma 5.2 relies on (30) with bounds (31) and (32).

VI. A proof of Theorem 4.4 (Outline)

Fix $n = 2, 3, \ldots$ and consider $\theta = (P,K)$ with positive integers K and P such that $K < P$. By a coupling argument, the rvs $\chi_{n,1}(\theta), \ldots, \chi_{n,n}(\theta)$ can be shown to be *negatively related* (in the technical sense given in [1, p. Defn. 2.1.1, p. 24]). As a result, the basic Stein-Chen inequality [1, Cor. 2.C.2, p. 26] takes on the simpler form

$$d_{TV}(I_n(\theta); \Pi(\mathbb{E}\left[I_n(\theta)\right])) \le \frac{\mathbb{E}\left[I_n(\theta)\right] - \mathrm{Var}[I_n(\theta)]}{\mathbb{E}\left[I_n(\theta)\right]} \tag{33}$$

where d_{TV} denotes the total variation distance. The triangular inequality for the total variation distance yields

$$\begin{aligned} d_{TV}(I_n(\theta); \Pi(e^{-\gamma})) \quad &\le \quad d_{TV}(I_n(\theta); \Pi(\mathbb{E}\left[I_n(\theta)\right])) \\ &\quad + d_{TV}(\Pi(\mathbb{E}\left[I_n(\theta)\right]); \Pi(e^{-\gamma})) \end{aligned} \tag{34}$$

while we have the well-known estimate

$$d_{TV}(\Pi(\mathbb{E}\left[I_n(\theta)\right]); \Pi(e^{-\gamma})) \le |\mathbb{E}\left[I_n(\theta)\right] - e^{-\gamma}|. \tag{35}$$

Direct substitution from (25) and (26) gives

$$\begin{aligned} &\mathbb{E}\left[I_n(\theta)\right] - \mathrm{Var}[I_n(\theta)] \\ = \quad &\mathbb{E}\left[I_n(\theta)\right] - \left(\mathbb{E}\left[I_n(\theta)^2\right] - \mathbb{E}\left[I_n(\theta)\right]^2\right) \\ = \quad &\left(n\mathbb{E}\left[\chi_{n,1}(\theta)\right]\right)^2 - n(n-1)\mathbb{E}\left[\chi_{n,1}(\theta)\chi_{n,2}(\theta)\right] \end{aligned}$$

whence

$$\begin{aligned} &\frac{\mathbb{E}\left[I_n(\theta)\right] - \mathrm{Var}[I_n(\theta)]}{\mathbb{E}\left[I_n(\theta)\right]} \\ = \quad &n\mathbb{E}\left[\chi_{n,1}(\theta)\right] - (n-1)\frac{\mathbb{E}\left[\chi_{n,1}(\theta)\chi_{n,2}(\theta)\right]}{\mathbb{E}\left[\chi_{n,1}(\theta)\right]} \\ = \quad &n\left(\frac{\binom{P-K}{K}}{\binom{P}{K}}\right)^{n-1} - (n-1)\left(\frac{\binom{P-2K}{K}}{\binom{P-K}{K}}\right)^{n-2} \end{aligned}$$

upon making use of the expressions developed in Section V.

In these expressions we now substitute θ by θ_n by means of an admissible pair of functions $P, K : \mathbb{N}_0 \to \mathbb{N}$ whose function $\alpha : \mathbb{N}_0 \to \mathbb{R}$ satisfies (22) for some scalar γ: It is a simple matter to check that $\lim_{n\to\infty}\mathbb{E}\left[I_n(\theta_n)\right] = e^{-\gamma}$ while

$$\lim_{n\to\infty}\frac{\mathbb{E}\left[I_n(\theta_n)\right] - \mathrm{Var}[I_n(\theta_n)]}{\mathbb{E}\left[I_n(\theta_n)\right]} = 0.$$

Combining these observations with (33), (34) and (35), we get

$$\lim_{n\to\infty} d_{TV}(I_n(\theta_n); \Pi(\mathbb{E}\left[I_n(\theta_n)\right])) = 0,$$

and the convergence (23) follows because the modes of convergence in distribution and in total variation are equivalent for discrete rvs. Details can be found in [16].

Acknowledgment

This work was supported by NSF Grant CCF-07290.

References

[1] A. D. Barbour, L. Holst and S. Janson, *Poisson Approximation*, Oxford Studies in Probability **2**, Oxford University Press, Oxford (UK), 1992.

[2] B. Bollobás, *Random Graphs*, Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge (UK), 2001.

[3] H. Chen, A. Perrig and D. Song, "Random key predistribution schemes for sensor networks," in Proceedings of the 2003 IEEE Symposium on Security and Privacy (S&P 2003), Oakland (CA), May 2003, pp. 197-213.

[4] R. Di Pietro, L.V. Mancini, A. Mei, A. Panconesi and J. Radhakrishnan, "Sensor networks that are provably secure," in Proceedings of SecureComm 2006, the 2nd IEEE/CreateNet International Conference on Security and Privacy in Communication Networks, Baltimore (MD), August 2006.

[5] W. Du, J. Deng, Y.S. Han and P.K. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," in Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS 2003), Washington (DC), October 2003, pp. 42-51.

[6] P. Erdös and A. Rényi, "On the evolution of random graphs," *Publ. Math. Inst. Hung. Acad. Sci.* **5** (1960), pp. 17-61.

[7] L. Eschenauer and V.D. Gligor, "A key-management scheme for distributed sensor networks," in Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS 2002), Washington (DC), November 2002, pp. 41-47.

[8] J. Fill, E.R. Schneinerman and K.B. Cohen-Singer, "Random intersection graphs when $m = \omega(n)$: An equivalence theorem relating the evolution of the $G(n,m,p)$ and $G(n,p)$ models, *Random Structures and Algorithms* **16** (2000), pp. 249-258.

[9] J. Hwang and Y. Kim, "Revisiting random key pre-distribution schemes for wireless sensor networks," in the Proceedings of the Second ACM Workshop on Security of Ad Hoc And Sensor Networks (SASN 2004), Washington (DC), October 2004.

[10] S. Janson, T. Łuczak and A. Ruciński, *Random Graphs*, Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons, 2000.

[11] M.K. Karoński, E.R. Schneinerman, and K.B. Singer-Cohen, "On random intersection graphs: The subgraph problem," *Combinatorics, Probability and Computing* **8** (1999), pp. 131-159.

[12] M.D. Penrose, *Random Geometric Graphs*, Oxford Studies in Probability **5**, Oxford University Press, New York (NY), 2003.

[13] A. Perrig, J. Stankovic and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM* **47** (2004), pp. 53–57.

[14] K.B. Singer, *Random Intersection Graphs*, Ph.D. Thesis, Department of Mathematical Sciences, The Johns Hopkins University, Baltimore (MD), 1995.

[15] D.-M. Sun and B. He, "Review of key management mechanisms in wireless sensor networks," *Acta Automatica Sinica* **12** (2006), pp. 900-906.

[16] O. Yağan and A.M. Makowski, "On the random graph induced by a random key predistribution scheme under full visibility (Extended version)," Available online at http://hdl.handle.net/1903/7498, January 2008.