Wireless sensor networks under the random pairwise key predistribution scheme: Can resiliency be achieved with small key rings?

Osman Yağan, *Member, IEEE,* and Armand M. Makowski, *Fellow, IEEE,*

***Abstract*—We investigate the resiliency of wireless sensor networks against sensor capture attacks when the network uses the random pairwise key distribution scheme of Chan, Perrig and Song [3]. We present conditions on the model parameters so that the network is (i) *unassailable*, and (ii) *unsplittable*, both with high probability, as the number n of sensor nodes becomes large. Both notions are defined against an adversary who has unlimited computing resources and full knowledge of the network topology, but can only capture a *negligible* fraction $o(n)$ of sensors. We also show that the number of cryptographic keys needed to ensure unassailability and unsplittability under the pairwise key predistribution scheme is an order of magnitude *smaller* than it is under the key predistribution scheme of Eschenauer and Gligor.**

Keywords: Wireless sensor networks, Security, Key predistribution, Resilience against node capture, Unassailability, Unsplittability.

I. Introduction

A. Motivation and Background

SECURITY is widely recognized as a key challenge to the deployment of wireless sensor networks (WSNs) under hostile conditions. Unfortunately, many security schemes developed for general networking environments do not take into account the unique features of WSNs: Public key cryptography is computationally unfeasible due to the severe limitations imposed on the physical memory and power consumption of the individual sensors. Traditional key exchange and distribution protocols are based on trusting third parties, and this makes them inadequate for large-scale WSNs whose topologies are unknown prior to deployment. See the references [2], [14], [17], [18], [19] for discussions of the security challenges in WSN settings.

O. Yağan is with the Department of Electrical and Computer Engineering and CyLab, Carnegie Mellon University, Moffett Field, CA 94035. E-mail:oyagan@ece.cmu.edu

Armand M. Makowski is with the Department of Electrical and Computer Engineering and Institute for Systems Research, University of Maryland, College Park, MD 20742. E-mail:armand@isr.umd.edu

Manuscript received January 15, 2015; revised November 12, 2015; accepted January 7, 2016.

A preliminary version of some of the material was presented at the IEEE 22nd Annual International International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC 2011), held in Toronto (Canada) in September 2011 [23].

Random key predistribution schemes address some of these difficulties by randomly assigning secure keys to sensor nodes prior to network deployment. This idea was first introduced by Eschenauer and Gligor [7] whose scheme, hereafter referred to as the EG scheme, operates as follows: Each of the n sensor nodes is equipped with Σ_{EG} cryptographic keys that are selected independently and uniformly at random from a pool of P keys. Two sensors can then secure a communication link if they have at least one key in common.

Over the past decade, many competing alternatives to the EG scheme have been proposed; see the papers [2], [17], [18], [19] for detailed surveys of various key predistribution schemes for WSNs. In this paper we consider the random pairwise key predistribution scheme of Chan et al. [3]: Before deployment, each of the n sensor nodes is paired (offline) with K distinct nodes which are randomly selected from amongst all other nodes. For each sensor and any sensor paired to it, a unique (pairwise) key is generated and stored in both their memory modules along with their ids. An existing wireless communication link between two nodes can be made secure if at least one of the nodes is paired to the other so that the two nodes have at least one pairwise key in common. Precise implementation details are given in Section II-A. Interest in this scheme stems from its various operational advantages over the EG scheme, e.g., node-to-node authentication and quorum-based revocation without involving a base station; see [3] for more details.

B. Contributions

Given these important advantages, we have found it of interest to assess the performance of the pairwise scheme. A number of issues related to its secure connectivity and to the dimensioning of memory sizes have already been discussed in the recent papers [22], [24], [26], [27], [28]. In the present paper, we explore instead the *resiliency* of the pairwise scheme against node capture attacks. The setup is one where an extremely powerful and knowledgeable adversary captures a subset of the sensor nodes with the goal of severely impairing the functionality of the entire network. As was done for the EG scheme in [12], the main question is whether this objective can be achieved by capturing a (relatively) *small* number of sensors.

This issue is analyzed in the many node regime under the assumption of *full visibility*, namely when all nodes are within transmission range of each other. We first look at the

asymptotic behavior of the *maximum* number $C_r^\star(n;K)$ of edges that can be compromised by capturing r nodes vs. the total number $|E(n;K)|$ of secure edges in the network as the number n of sensors grows unboundedly large – Here K is the parameter specifying the pairwise scheme; see Section II-A for details. Next, we characterize the asymptotic behavior of the size $I_r(n;K)$ of the *largest* subset of sensors whose communications with the rest of the network can be compromised by capturing r nodes. We give conditions on how to scale K with n (i.e., $K = K_n$) so that if $r_n = o(n)$, then with *high probability* the quantity $C_{r_n}^\star(n;K_n)$ (resp. $I_{r_n}(n;K_n)$) grows sub-linearly with $|E(n;K_n)|$ (resp. n). These conditions are highly desirable as they imply that an adversary cannot impair a considerable part of the network without capturing a considerable number of nodes. These two notions were introduced by Mei et al. in [12] under the names of *unassailability* and *unsplittability*, respectively, in the context of the EG scheme. A comparison with the results of Mei et al. [12] shows that under the pairwise scheme both properties can be realized with memory requirements which are order of magnitude *smaller* than the ones needed by the EG scheme.

C. Notation and Conventions

All statements involving limits are understood with n going to infinity. The random variables (rvs) under consideration are all defined on the same probability triple $(\Omega, \mathcal{F}, \mathbb{P})$. Probabilistic statements are made with respect to this probability measure $\mathbb{P}$, and we denote the corresponding expectation operator by $\mathbb{E}$. The indicator function of an event E is denoted by $\mathbf{1}[E]$. Distributional equality is denoted by $=_{st}$, and we use $\xrightarrow{P}_n$ to denote convergence in probability as n gets large. The abbreviation a.a.s. reads asymptotically almost surely, and is understood with n getting large. We shall use $\mathrm{Bin}(n,p)$ to denote a Binomial rv with n trials and success probability p.

When comparing the asymptotic behavior of two sequences $a, b : \mathbb{N}_0 \to \mathbb{R}_+$, we use the standard Landau notation: Thus, $a_n = o(b_n)$ is a shorthand for $\lim_{n\to\infty} \frac{a_n}{b_n} = 0$, whereas $a_n = O(b_n)$ means that there exists $C > 0$ such that $a_n \le C b_n$ for all n sufficiently large. Also, we write $a_n = \Omega(b_n)$ if $b_n = O(a_n)$, or equivalently, if there exists $c > 0$ such that $a_n \ge c b_n$ for all n sufficiently large.

D. Organization of the Paper

The paper is organized as follows: In Section II, we describe the random pairwise key predistribution scheme of Chan et al. (hereafter simply referred to as the pairwise scheme) and the random K-out graph it naturally induces (under full visibility) – Earlier work on its connectivity properties is also recalled. The notions of unassailability and unsplittability are formally introduced in Section III as a precise way to capture network resiliency against node capture attacks; in each case, formal definitions are given, followed by the corresponding results. In Section IV we develop heuristic arguments which shed some light on the results. The impact of the full visibility assumption is briefly discussed In Section V. Some numerical results are presented in Section VI. In Section VII we discuss the required key ring sizes needed to achieve unassailability and unsplittability under the pairwise scheme. A comparison with the EG scheme is given in Section VIII. The proofs of the main results are given in Section XI and Section XII – Key to the analysis are Hoeffding-type bounds which are developed in Section IX and Section X. Section XIII contains the proof of a key result concerning maximal key ring sizes. Conclusions are given in Section XIV where some directions for future research are also outlined.

II. The model

The pairwise scheme and its induced random graph are parametrized by two positive integers n and K such that $K < n$. They are held fixed throughout this section.

A. The random pairwise key predistribution scheme

The network comprises n nodes, labeled $i = 1, \ldots, n$, with unique ids $\mathrm{Id}_1, \ldots, \mathrm{Id}_n$. Write $\mathcal{N}_n = \{1, \ldots, n\}$ and set $\mathcal{N}_{n,-i} = \mathcal{N}_n - \{i\}$ for each $i = 1, \ldots, n$. With node i, we associate a subset $\Gamma_{n,i}(K)$ of K nodes selected uniformly at *random* from $\mathcal{N}_{n,-i}$ – Each of the nodes in $\Gamma_{n,i}(K)$ is said to be paired to node i. Thus, for any subset $A \subseteq \mathcal{N}_{n,-i}$, we require

$$\mathbb{P}\left[\Gamma_{n,i}(K) = A\right] = \begin{cases} \binom{n-1}{K}^{-1} & \text{if } |A| = K \\ 0 & \text{otherwise.} \end{cases} \tag{1}$$

Put differently, the selection of $\Gamma_{n,i}(K)$ is done *uniformly* amongst all subsets of $\mathcal{N}_{n,-i}$ which are of size K. The rvs $\Gamma_{n,1}(K), \ldots, \Gamma_{n,n}(K)$ are assumed to be mutually independent.

Once this *offline* random pairing has been created, we construct the key rings $\Sigma_{n,1}(K), \ldots, \Sigma_{n,n}(K)$, one for each node, as follows: We assume the availability of nK distinct cryptographic keys $\{\omega_{i|\ell},\ i = 1, \ldots, n;\ \ell = 1, \ldots, K\}$. Fix $i = 1, \ldots, n$ and let $\ell_{n,i} : \Gamma_{n,i}(K) \to \{1, \ldots, K\}$ denote a labeling of $\Gamma_{n,i}(K)$. For each node j in $\Gamma_{n,i}(K)$ paired to i, the cryptographic key $\omega_{i|\ell_{n,i}(j)}$ is associated with j. For instance, if the random set $\Gamma_{n,i}(K)$ is realized as $\{j_1, \ldots, j_K\}$ with $1 \le j_1 < \ldots < j_K \le n$, then an obvious labeling consists in $\ell_{n,i}(j_k) = k$ for each $k = 1, \ldots, K$ so that key $\omega_{i|k}$ is associated with node j_k. Of course other labelings are possible. Finally, with node j paired to node i, the pairwise key $\omega_{n,ij}^\star = [\mathrm{Id}_i|\mathrm{Id}_j|\omega_{i|\ell_{n,i}(j)}]$ is constructed and inserted in the memory modules of both nodes i and j. The key $\omega_{n,ij}^\star$ is assigned *exclusively* to the pair of nodes i and j, hence the terminology pairwise predistribution scheme. The key ring $\Sigma_{n,i}(K)$ of node i is the set of keys given by

$$\begin{aligned} &\Sigma_{n,i}(K) \\ &= \left\{\omega_{n,ij}^\star,\ j \in \Gamma_{n,i}(K)\right\} \cup \left\{\omega_{n,ji}^\star,\ \begin{matrix} j = 1, \ldots, n \\ i \in \Gamma_{n,j}(K) \end{matrix}\right\}. \end{aligned} \tag{2}$$

If two nodes, say i and j, are within wireless communication range of each other, they will be able to establish a secure link if and only if $\Sigma_{n,i}(K) \cap \Sigma_{n,j}(K) \neq \emptyset$. This requirement holds if at least one of the events $i \in \Gamma_{n,j}(K)$ or $j \in \Gamma_{n,i}(K)$ takes place, whence

$$\left[\Sigma_{n,i}(K) \cap \Sigma_{n,j}(K) \neq \emptyset\right] = \left[i \in \Gamma_{n,j}(K)\right] \cup \left[j \in \Gamma_{n,i}(K)\right].$$

When both events take place simultaneously, the memory modules of nodes i and j both contain the distinct keys $\omega^{\star}_{n,ij}$ and $\omega^{\star}_{n,ji}$. By construction this scheme supports *distributed* node-to-node authentication.

B. Random K-out graphs

Under full visibility, the pairwise scheme gives rise naturally to the following class of random graphs: The nodes i and j are said to be adjacent, written $i \sim j$, if and only if they have at least one key in common in their key rings, namely,

$$i \sim j \quad \text{iff} \quad \Sigma_{n,i}(K) \cap \Sigma_{n,j}(K) \neq \emptyset. \tag{3}$$

Note that $i \sim i$ cannot occur since by construction i is never contained in $\Gamma_{n,i}(K)$. We denote by $\mathbb{H}(n;K)$ the *undirected* random graph on the vertex set $\{1,\ldots,n\}$ induced by the adjacency notion (3). Obviously there are no self-loops. Throughout let $E(n;K)$ denote the (random) set of undirected edges in $\mathbb{H}(n;K)$.

In the literature on random graphs the random graph $\mathbb{H}(n;K)$ is known as the random K-out graph [1], [10], or as the random K-orientable graph [8]. These references adopt the following definition, which can easily be seen to be equivalent to the symmetric adjacency condition (3): For each of the n vertices assign exactly K arcs to K distinct vertices that are selected uniformly at random, and then ignore the orientation of the arcs. The directed version of this graph (i.e., with the orientation of arcs preserved) has also been studied; e.g., see [15].

C. Connectivity

For future reference we conclude this section with results concerning the *connectivity* of the class of undirected random graphs introduced in the previous section; recall that a graph is said to be connected when there is a path between every pair of vertices. Here and elsewhere, it will be convenient to refer to any mapping $K : \mathbb{N}_0 \to \mathbb{N}_0$ as a *scaling* (for the pairwise scheme) provided the conditions

$$K_n < n, \quad n = 2, 3, \ldots$$

hold.

Theorem 2.1: For any scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ such that $K_n \geq 2$ for all n sufficiently large, it holds that

$$\lim_{n\to\infty} \mathbb{P}[\, \mathbb{H}(n;K_n) \ \textit{is connected}\,] = 1.$$

In fact, we have

$$\lim_{n\to\infty} \mathbb{P}[\, \mathbb{H}(n;K) \ \textit{is connected}\,] = \begin{cases} 0 & \textit{if } K = 1 \\ \\ 1 & \textit{if } K \geq 2. \end{cases} \tag{4}$$

The zero-one law (4) was established independently by Fenner and Frieze [8], and by the authors [24], [27]. In the latter references, the one-law was a by-product of the bound

$$\mathbb{P}[\mathbb{H}(n;K) \ \text{ is connected}] \geq 1 - \frac{155}{n^3}, \qquad \begin{matrix} n \geq 16, \\ K = 2, \ldots, n-1. \end{matrix}$$

With $n = 50$ and $K = 2$ as in Figure 1, this last bound already yields a probability of at least 0.999 that the graph is connected.

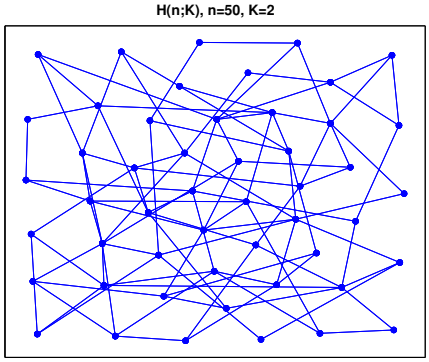

Fig. 1. A realization of the random K-out graph $\mathbb{H}(n;K)$ with $n = 50$ and $K = 2$.

III. Resiliency in WSNs – The main results

As we seek to understand the resiliency of a network against external attacks, we begin by specifying the capabilities of the adversary considered here. To do so we adopt the following model already used in [12] (under full visibility): The adversary (sometimes also called the attacker), upon launching an attack against the network, captures some of its nodes. As a result it now owns the key rings stored at the captured nodes. An edge between two nodes is deemed *compromised* if the adversary is in possession of a key which is stored in *both* their key rings – A compromised edge is therefore one that belongs to $E(n;K)$. By construction, under the pairwise scheme an edge becomes compromised as soon as any of its end nodes is captured. The adversary is assumed to have unlimited computing power; it is also expected to have sufficient knowledge of the network that it is able to minimize the number of nodes which need to be captured in order to compromise a given number of edges.

In many WSN applications, the network as a whole can still be considered functional even though a *small* number of sensors have fallen under the control of the adversary [12]. Hence, in evaluating the level of security provided by a key predistribution scheme, it is natural to ask whether *significant* damage to network functionalities can be inflicted by capturing only a relatively small number of nodes. The next two sections provide ways to formally address this issue.

A. Unassailability

With A being the set of sensor nodes captured by the adversary, let $C_A(n;K)$ denote the total number of (undirected) edges that are compromised as a result of this attack. From earlier remarks it follows that $C_A(n;K)$ is the number of edges in $E(n;K)$ with the property that at least one end of the edge is a node in A, i.e.,

$$C_A(n;K) = \left| \left\{ (i,j) : \begin{matrix} 1 \leq i < j \leq n \\ i \sim j \end{matrix} \ , \ i \in A \vee j \in A \right\} \right|. \tag{5}$$

The adversary considered here is capable of maximizing $C_A(n;K)$ for a given number $|A|$ of nodes to be captured. This leads us to introduce for each $r = 1,\ldots,n-1$, the

maximum number $C_r^\star(n;K)$ of edges that can be compromised by capturing r nodes, namely

$$C_r^\star(n;K) := \max\left(C_A(n;K) : \ A \in \mathcal{P}_{n|r}\right)$$

where $\mathcal{P}_{n|r}$ denotes the collections of all subsets of $\{1,\ldots,n\}$ with exactly r elements.

Under the assumptions made on its capabilities, the powerful and knowledgeable attacker considered here will be able to compromise $C_r^\star(n;K)$ edges by capturing the appropriate set of r nodes – This reflects a worst case mindset from the perspective of the network. Given this definition, it is natural to ask how does the quantity $C_r^\star(n;K)$ behave in relation to the total number $|E(n;K)|$ of edges as n gets large (with K and r possibly scaled with n as K_n and r_n). It is common practice [5], [12] to regard the condition

$$C_{r_n}^\star(n;K_n) = o(|E(n;K_n)|) \quad \text{whenever } r_n = o(n) \tag{6}$$

as indicative of the resiliency of the network against node capture attacks. A crucial implication of (6) is that in the many node regime, an adversary will not be able to compromise $\Omega(|E(n;K_n)|)$ edges by taking over only $o(n)$ nodes. Condition (6) is used as a basis for characterizing the *unassailability* of the pairwise scheme, and is formally understood as the requirement

$$\frac{C_{r_n}^\star(n;K_n)}{|E(n;K_n)|} \xrightarrow{P}_n 0 \quad \text{whenever } r_n = o(n). \tag{7}$$

Conditions are now given for (7) to occur.

Theorem 3.1: For any scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ we have

$$\lim_{n\to\infty} \mathbb{P}\left[C_{r_n}^\star(n;K_n) \geq \varepsilon \cdot |E(n;K_n)|\right] = 0 \tag{8}$$

for every $\varepsilon > 0$ whenever $r_n = o(n)$. The speed of convergence to zero at (8) is captured by the upper bound (57) and occurs faster than exponentially fast in n.

Thus, under the pairwise key predistribution scheme a sensor network is always unassailable, irrespective of how the parameter K scales with n. In particular, it is unassailable for *fixed* values of K. A proof of Theorem 3.1 is given in Section XI.

B. Unsplittability

Condition (8) checks whether an adversary can compromise a considerable fraction of edges by launching an attack on relatively few sensors. However this condition does not reveal anything about the ability of the adversary to *disconnect* or *split* the network. To explore this issue further, we say that the subset S of nodes is *A-splittable* if by capturing the nodes in A the adversary can compromise all the edges from S to its complement $S^c = \mathcal{N}_n - S$. To be more precise, let $E(n;K)(S)$ denote the set of (undirected) edges in $\mathbb{H}(n;K)$ with one end in S and the other in S^c. As per comments made earlier, upon capturing the nodes in A, an edge in $E(n;K)(S)$ is compromised whenever either one of its end nodes belongs to A. The A-splittability of S is therefore characterized by the condition

$$\wedge_{(i,j)\in E(n;K)(S)} \left(i \in A \vee j \in A\right). \tag{9}$$

It is plain that S is A-splittable if and only if its complement S^c (in $\mathcal{N}_n$) is A-splittable.

Next, for each $r = 1,\ldots,n-1$, we say that the set S of nodes is *r-splittable* whenever there *exists* a set A of r nodes such that S is A-splittable. The r-splittability of S corresponds to the conditions

$$\vee_{A\in\mathcal{P}_{n|r}} \left(\wedge_{(i,j)\in E(n;K)(S)} \left(i \in A \vee j \in A\right)\right). \tag{10}$$

Again, if S is r-splittable, then its complement S^c (in $\mathcal{N}_n$) is also r-splittable.

Given the infinite computing power available to it, the attacker can in principle minimize the number of nodes it needs to capture in order to *split* S from the rest of the network. Conversely, this attacker will be able to select a set of r nodes so as to inflict maximal damage. Thus, let $I_r(n;K)$ denote the size of the largest subset S (with size $|S| \leq \frac{n}{2}$) that can be disconnected from the rest of the network by capturing r nodes, namely

$$I_r(n;K) = \max\left\{|S| : S \subseteq \mathcal{N}_n, |S| \leq \frac{n}{2}, \ S \text{ is } r\text{-splittable}\right\}.$$

It is natural to wonder about the behavior of $I_r(n;K)$ as n grows large – It is always the case that $r \leq I_r(n;K) \leq \frac{n}{2}$. From the perspective of the network, it is desirable that the largest subset which can be disconnected be small whenever the number of captured nodes is small. As in [12], again scaling K and r with n, this leads to the condition

$$I_{r_n}(n;K_n) = o(n) \quad \text{whenever } r_n = o(n) \tag{11}$$

as our second characterization of resiliency. This can formally recasts as

$$\frac{I_{r_n}(n;K_n)}{n} \xrightarrow{P}_n 0 \quad \text{whenever } r_n = o(n). \tag{12}$$

The main result along these lines is presented next.

Theorem 3.2: Consider a scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$. For every $\gamma > 0$ we have

$$\lim_{n\to\infty} \mathbb{P}\left[I_{r_n}(n;K_n) \geq \gamma n\right] = 0 \tag{13}$$

whenever $r_n = o(n)$ and the scaling satisfies

$$\lim_{n\to\infty} K_n = \infty. \tag{14}$$

The speed of convergence to zero at (13) is captured by the upper bound (71), and occurs faster than exponentially fast in n.

A proof of Theorem 3.2 can be found in Section XII. Here as well, a careful inspection of the proof shows that the convergence (13) occurs faster than exponentially fast in n. The operational usefulness of (13) derives from the fact that for any subset S of $\mathcal{N}_n$, with $|S| = \Omega(n)$, an adversary must capture *at least* $\Omega(n)$ nodes in order to compromise *all* edges from S to S^c. Unlike unassailability, the unsplittability of the pairwise scheme does not hold irrespective of the scaling of the parameter K; it indeed requires (14) to be satisfied. The implications of the condition (14) on the number of keys that needs to be assigned to each sensor node are discussed in Section VII.

IV. A HEURISTIC ARGUMENT

In this section we present some simple consequences of the model. We then use them to gain some insights into the results, especially Theorem 3.1, through a heuristic argument.

Consider positive integers n and K such that $K < n$. For future reference we write

$$\lambda_n(K) = 2\left(\frac{K}{n-1}\right) - \left(\frac{K}{n-1}\right)^2.$$

A. Link probabilities

Recall that for any pair of nodes $i, j = 1, \ldots, n$, we have $i \sim j$ if and only if $i \in \Gamma_{n,j}(K) \vee j \in \Gamma_{n,i}(K)$. By construction it holds that

$$\mathbb{P}\left[i \in \Gamma_{n,i}(K) \vee i \in \Gamma_{n,i}(K)\right] = 0, \quad i = 1, \ldots, n.$$

Next, consider the case of *distinct* $i, j = 1, \ldots, n$: Elementary set-theoretic arguments readily give

$$\begin{aligned}\mathbb{P}\left[i \in \Gamma_{n,j}(K) \vee j \in \Gamma_{n,i}(K)\right] &= \mathbb{P}\left[i \in \Gamma_{n,j}(K)\right] + \mathbb{P}\left[j \in \Gamma_{n,i}(K)\right] \\ &\quad -\mathbb{P}\left[i \in \Gamma_{n,j}(K), j \in \Gamma_{n,i}(K)\right] \end{aligned} \tag{15}$$

with

$$\mathbb{P}\left[i \in \Gamma_{n,j}(K)\right] = \frac{\binom{n-2}{K-1}}{\binom{n-1}{K}} = \frac{K}{n-1}. \tag{16}$$

The rvs $\Gamma_{n,1}(K), \ldots, \Gamma_{n,n}(K)$ being i.i.d., it follows from (15) that

$$\mathbb{P}\left[i \in \Gamma_{n,j}(K) \vee j \in \Gamma_{n,i}(K)\right] = \lambda_n(K).$$

Collecting these facts we conclude that the link probabilities are given by

$$\begin{aligned}\mathbb{P}\left[i \sim j\right] &= \mathbb{P}\left[i \in \Gamma_{n,j}(K) \vee j \in \Gamma_{n,i}(K)\right] \\ &= (1 - \delta(i,j))\,\lambda_n(K), \quad i, j = 1, \ldots, n. \end{aligned} \tag{17}$$

B. An easy calculation

Pick a subset $A \subseteq \mathcal{N}_n$ of nodes and recall the definition of $C_A(n;K)$ given in (5). Its exact expression

$$\begin{aligned}C_A(n;K) = &\frac{1}{2}\sum_{i\in A}\sum_{j\in A}\mathbf{1}\left[j \in \Gamma_{n,i}(K) \vee i \in \Gamma_{n,j}(K)\right] \\ &+ \sum_{i\in A}\sum_{k\in A^c}\mathbf{1}\left[k \in \Gamma_{n,i}(K) \vee i \in \Gamma_{n,k}(K)\right] \end{aligned} \tag{18}$$

is easily derived. It is also a simple matter to check that

$$|E(n;K)| = \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}\mathbf{1}\left[j \in \Gamma_{n,i}(K) \vee i \in \Gamma_{n,j}(K)\right]. \tag{19}$$

Note that (18) reduces to (19) when $A = \mathcal{N}_n$ (as expected).

Taking expectations in (18) and using (17) we find

$$\begin{aligned}&\mathbb{E}\left[C_A(n;K)\right] \\ &= \frac{1}{2}\sum_{i\in A}\sum_{j\in A}\mathbb{P}\left[j \in \Gamma_{n,i}(K) \vee i \in \Gamma_{n,j}(K)\right] \\ &\quad + \sum_{i\in A}\sum_{k\in A^c}\mathbb{P}\left[k \in \Gamma_{n,i}(K) \vee i \in \Gamma_{n,k}(K)\right] \\ &= \frac{|A|(|A|-1)}{2}\cdot\lambda_n(K) + |A|(n-|A|)\cdot\lambda_n(K) \\ &= \frac{(2n-|A|-1)|A|}{2}\cdot\lambda_n(K). \end{aligned} \tag{20}$$

In a similar way, starting with (19), we have

$$\mathbb{E}\left[|E(n;K)|\right] = \frac{n(n-1)}{2}\cdot\lambda_n(K) \tag{21}$$

as expected. Combining these expressions leads to

$$\begin{aligned}\frac{\mathbb{E}\left[C_A(n;K)\right]}{\mathbb{E}\left[|E(n;K)|\right]} &= \frac{(2n-|A|-1)|A|}{n(n-1)} \\ &= \frac{|A|}{n}\cdot\left(2 - \frac{|A|-1}{n-1}\right). \end{aligned} \tag{22}$$

C. A heuristic based on concentration

We now turn to the situation of Theorem 3.1: Consider a scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$. For each $n = 1, 2, \ldots$, pick a subset $A_n \subseteq \mathcal{N}_n$, and write $r_n = |A_n|$. From (22) we find

$$\frac{\mathbb{E}\left[C_{A_n}(n;K_n)\right]}{\mathbb{E}\left[|E(n;K_n)|\right]} = \frac{r_n}{n}\cdot\left(2 - \frac{r_n - 1}{n-1}\right),$$

an expression where, somewhat surprisingly, K_n does not appear. It is now plain that

$$\lim_{n\to\infty}\frac{\mathbb{E}\left[C_{A_n}(n;K_n)\right]}{\mathbb{E}\left[|E(n;K_n)|\right]} = 0 \text{ if and only if } r_n = o(n),$$

regardless of the behavior of the scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$.

Under the enforced i.i.d. assumptions, it is not unreasonable to expect from the expressions (18) and (19) that concentration results will hold for these quantities: In particular, the rvs $C_{A_n}(n;K_n)$ and $|E(n;K_n)|$ would then be concentrated around their expected values $\mathbb{E}\left[C_{r_n}(n;K_n)\right]$ and $\mathbb{E}\left[|E(n;K_n)|\right]$, respectively, with high probability. By a continuity argument this would lead one to suspect that the ratio

$$\frac{C_{A_n}(n;K_n)}{|E(n;K_n)|}$$

is concentrated around the ratio of the expected values with high probability in the n large limit. In view of earlier remarks it is now only a small step to expect that when $r_n = o(n)$,

$$\frac{C_{A_n}(n;K_n)}{|E(n;K_n)|} \xrightarrow{P}_n 0.$$

In establishing Theorem 3.1 we do in fact show a stronger result, namely

$$\max\left(\frac{C_{A_n}(n;K_n)}{|E(n;K_n)|} : A_n \in \mathcal{P}_{n|r_n}\right) \xrightarrow{P}_n 0 \tag{23}$$

if $r_n = o(n)$.

V. On the impact of the full visibility assumption

The work reported here concerns the unassailability and unsplittability of sensor networks under the full visibility assumption. Although this assumption is unlikely to hold in realistic settings, it allows one to isolate the impact of the pairwise key predistribution protocol on the resulting network resiliency, and makes it possible to give a detailed mathematical analysis of the issues of interest. However, situations where the full visibility assumption does not hold, are of great practical importance and deserve further study.

On the basis of the heuristics given in Section IV we now argue how these more complex situations can be handled as well. Indeed, these heuristic arguments suggest that under full visibility, the unassailability of a network is strongly signaled by the ratio

$$\frac{\mathbb{E}\left[C_A(n;K)\right]}{\mathbb{E}\left[|E(n;K)|\right]} \tag{24}$$

approaching zero as n gets large when the set A of compromised nodes scales as $|A|/n = r_n/n = o(1)$.

When the full visibility assumption is dropped, both the nominator and denominator in (24) will decrease. For a concrete example, consider the *on-off* communication channel model [21], [28]: The channels between pairs of sensors are mutually independent, and each channel is on (resp. off) with probability p (resp. $1-p$). It is also reasonable to assume that the communications processes are independent of the random key distribution scheme. Under this setting, let $C_A(n;K,p)$ and $|E(n;K,p)|$ denote the analog of the quantities $C_A(n;K)$ and $|E(n;K)|$, respectively, under the on-off channel model.

Under the assumed independence, it holds that

$$C_A(n;K,p) =_{st} \text{Bin}\left(C_A(n;K),p\right)$$

and

$$|E(n;K,p)| =_{st} \text{Bin}\left(|E(n;K)|,p\right)$$

conditionally on the randomness induced by the random pairwise scheme. Therefore, $\mathbb{E}\left[C_A(n;K,p)\right] = p\mathbb{E}\left[C_A(n;K)\right]$ and $\mathbb{E}\left[|E(n;K,p)|\right] = p\mathbb{E}\left[|E(n;K)|\right]$, whence

$$\frac{\mathbb{E}\left[C_A(n;K,p)\right]}{\mathbb{E}\left[|E(n;K,p)|\right]} = \frac{\mathbb{E}\left[C_A(n;K)\right]}{\mathbb{E}\left[|E(n;K)|\right]}.$$

Thus, the ratio does not change as we move from full visibility to partial visibility under the on-off channel model, and concentration arguments could again be brought to bear. We might therefore expect that the paper's conclusions are still valid under this communication model, namely, the pairwise scheme achieves unassailability for any choice of K. In fact, by independence and linearity of expectation, most of the arguments given above would also hold for more complicated wireless channel models.

On the other hand, analyzing network unsplittability will be more challenging under partial visibility. The results are likely to differ significantly from those found in the full visibility case, and to be much more sensitive to the underlying communication model being used. To see why this may be so, consider the disk model [13] where sensors can communicate only if their distance is less than some transmission radius $\rho > 0$. For simplicity, assume the n sensors to be independently and randomly deployed on the unit square $[0,1]^2$ and take $\rho < 0.5$:

Imagine that the adversary captures all the nodes located in the rectangular strip $\Gamma(\rho) \equiv [0.5-\rho, 0.5+\rho]\times[0,1]$. The set of compromised nodes, still denoted A as before, is now a random subset of the set of all nodes. Let $\Gamma_-(\rho) \equiv [0, 0.5-\rho]\times[0,1]$ and $\Gamma_+(\rho) \equiv [0.5+\rho, 1]\times[0,1]$ denote the regions in $[0,1]^2$ on each side of $\Gamma(\rho)$.

Obviously, nodes in $\Gamma_-(\rho)$ and $\Gamma_+(\rho)$, respectively, cannot communicate since they are at least at distance 2ρ of each other – No wireless communication is therefore possible between these two components. Note that the expected number of nodes in $\Gamma_\pm(\rho)$ is given by $n(0.5-\rho)$, and can then be construed as large if $\rho = o(1)$. Yet it seems reasonable to argue that this network will indeed be "splittable" regardless of how large the parameter K is selected! The number $|A|$ of sensors involved in this attack is admittedly random; it is distributed like $\text{Bin}(n;2\rho)$ with $\mathbb{E}\left[|A|\right] = 2n\rho$, with $\rho = o(1)$, the condition $r_n = o(n)$ holds in expectation. However, in this case "splittability" was achieved by preventing two large pieces of the network to communicate with each other regardless of whether a pair of nodes, one in each piece, had the requisite keys to secure their communication link, had it be available. This points to the need to refine the notion of unsplittability in such settings, possibly by requiring that the (unsecured) communication network form a connected graph. A more detailed discussion of these issues is beyond the scope of this paper, and will be taken on elsewhere.

VI. Numerical results

It would be desirable to validate the results discussed here by means of numerical simulations, in the process gaining better insights into the notions of unassailability and unsplittability under the pairwise scheme. Unfortunately the attack model assumed in this paper is *not* computationally bounded: The adversary can maximize the number of compromised links or the size of the subgraph that it can split. But implementing such optimal strategies requires exponentially large amount of computing time and resources. Consequently, evaluating $C_r^\star(n;K)$ and $I_r(n;K)$ (and their statistics) is not feasible unless the network comprises very few sensors.

Instead, we rely on the intermediary probability bound (57) (appearing in the proof of Theorem 3.1 in Section XI) for fixed values of n, K and r, as a way to better understand how the fraction $\frac{C_r^\star(n;K)}{|E(n;K)|}$ of compromised links in the network is related to the fraction $\frac{r}{n}$ of captured nodes. With the help of this bound we can answer questions such as "What are the odds that the adversary can compromise at least 15% of the links by capturing just 1% of the sensors?".

Next we provide some numerical results to illustrate how the bound (57) behaves for various parameter values. We consider two scenarios, Scenario 1 and Scenario 2, each with the same number of nodes, namely $n = 1000$. We set $K = 2$ for Scenario 1 and $K = 4$ for Scenario 2. In each case we plot the upper bound on the *logarithm* of the probability that an adversary is able to compromise at least a fraction $\varepsilon = 0.1, 0.2, 0.3$

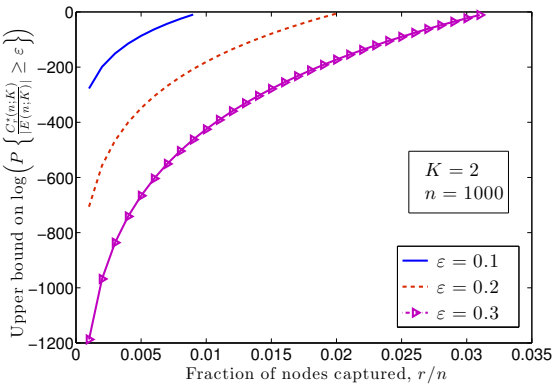

Fig. 2. With $n = 1,000$ and $K = 2$, we plot the logarithm of the upper bound given in (57) for the probability of an adversary compromising more than ε fraction of the links by capturing a fraction r/n of the nodes.

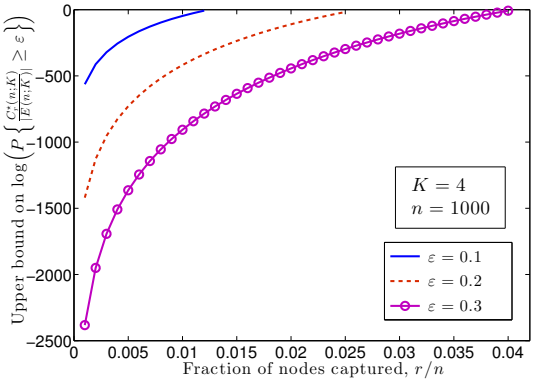

Fig. 3. With $n = 1,000$ and $K = 4$, we plot the logarithm of the upper bound given in (57) for the probability of an adversary compromising more than ε fraction of the links by capturing a fraction r/n of the nodes.

of the links, as a function of the fraction of captured nodes r/n. Figure 2 and Figure 3 correspond to Scenario 1 and Scenario 2, respectively, and give some indication as to how the resilience of the pairwise scheme varies with the parameter K. For instance, even with $K = 4$, an adversary that captures 40 sensors in a network of size 1000 has a negligible chance (e.g., less than 0.05%) of compromising a significant fraction (e.g., 30%) of the network communications.

VII. Resiliency vs. the size of key rings

Theorem 3.1 and Theorem 3.2 give conditions on K for the network to be unassailable and unsplittable, respectively, with high probability; this provides guidelines for *dimensioning* the pairwise scheme to ensure resiliency against node-capture attacks in the many node regime. However, these results do not map in a straightforward manner into the required *number* of cryptographic keys needed in each sensor node. Such information is certainly desirable to help assess how network resiliency under the pairwise scheme is affected by its memory requirements.

A. The key rings are of random and variable size

The difficulty in assessing the number of keys required per sensor can be traced to the fact that the key rings $\Sigma_{n,1}(K), \ldots, \Sigma_{n,n}(K)$ are *not* of constant size – This is in sharp contrast with the EG scheme and its variants (as briefly discussed in Section VIII). Indeed, here the key rings are of random size varying from node to node over the range

$$K \leq |\Sigma_{n,i}(K)| \leq K + n - 1, \quad i = 1, 2, \ldots, n. \tag{25}$$

This is a direct consequence of (2) as we note that

$$\begin{aligned} |\Sigma_{n,i}(K)| &= |\Gamma_{n,i}(K)| + \sum_{j=1, j\neq i}^{n} \mathbf{1}\left[i \in \Gamma_{n,j}(K)\right] \\ &= K + \sum_{j=1, j\neq i}^{n} \mathbf{1}\left[i \in \Gamma_{n,j}(K)\right]. \end{aligned} \tag{26}$$

It follows that

$$|\Sigma_{n,i}(K)| =_{st} K + \text{Bin}\left(n-1, \frac{K}{n-1}\right) \tag{27}$$

because (16) holds for each of the i.i.d. rvs $\Gamma_{n,1}(K), \ldots, \Gamma_{n,n}(K)$.

B. On the average and expected size of key rings

As suggested above, it is of interest to explore the behavior of $|\Sigma_{n,1}(K)|, \ldots, |\Sigma_{n,n}(K)|$ in order to better understand the size of the key rings induced by the conditions of Theorem 3.1 and Theorem 3.2. Beyond operational concerns, this would also allow us to meaningfully compare our findings with those obtained for the EG scheme [12].

To this end, we first observe from the distributional equality (27) that

$$\mathbb{E}\left[|\Sigma_{n,i}(K)|\right] = 2K, \qquad i = 1, \ldots, n. \tag{28}$$

Thus, a simple relation exists between the scheme parameter K and the *expected* number of cryptographic keys stored in a given sensor.

Averaging over the nodes of the network, we also see that the *average* number of cryptographic keys per node is given by

$$|\Sigma|_{n,\text{Avg}}(K) := \frac{|\Sigma_{n,1}(K)| + \cdots + |\Sigma_{n,n}(K)|}{n} = 2K. \tag{29}$$

Indeed, by construction the pairwise scheme provides each of the n sensors with K distinct keys, and a copy of each such key is given to another sensor selected uniformly at random. As a result, there is a total of $2Kn$ keys distributed amongst the n sensors (of which nK are distinct). The relation (29) can also be seen from (26).

The expressions (28) and (29) are encouraging for the following reasons: While key ring sizes can in principle fluctuate over a large interval (given by (25)), potentially being as large as $n + K - 1$, both the expected size of a sensor's key ring and the average key ring size over the network are only $2K$. Given that $K \geq 2$ is already sufficient for connectivity and unassailability (viz. Theorems 2.1 and 3.1), and that any unbounded scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ is enough

to ensure unsplittability (viz. Theorem 3.2), we see that $2K_n$ might possibly be orders of magnitude smaller than $n+K_n-1$ in the parameter regime of interest. This argument can indeed be taken one step further under some conditions on the scaling $K:\mathbb{N}_0\to\mathbb{N}_0$: From (27) we readily check that

$$\mathrm{Var}\left[\frac{|\Sigma_{n,i}(K_n)|}{2K_n}\right]=\frac{1}{4K_n}\left(1-\frac{K_n}{n-1}\right),\qquad \begin{matrix} i=1,\dots,n\\ n=2,3,\dots,\end{matrix}$$

whence

$$\frac{|\Sigma_{n,1}(K_n)|}{2K_n}\xrightarrow{P}_n 1 \tag{30}$$

as soon as the scaling $K:\mathbb{N}_0\to\mathbb{N}_0$ satisfies (14).[1]

C. How big can the biggest key rings be?

From (30) it follows that each key ring size has a propensity to hover about its mean $2K_n$ for large n under the condition (14). However, the deterministic constraint (29) implies that the sizes of the key rings are *negatively* correlated. In fact it is a simple matter to show with the help of (26) that

$$\mathrm{Cov}\left[|\Sigma_{n,i}(K_n)|,|\Sigma_{n,j}(K_n)|\right]\le 0,\qquad \begin{matrix} i\neq j\\ i,j=1,\dots,n\\ n=2,3,\dots\end{matrix}$$

for any scaling $K:\mathbb{N}_0\to\mathbb{N}_0$. In other words, the convergence result (30) does not rule out the possibility of a few sensors having exceptionally large key ring sizes when the network is of large size. Were this to occur, the pairwise scheme would be rendered impractical under the limited memory resources available to each sensor. Of course this discussion assumes that the sensors are all identical in their (limited) capabilities, a likely occurrence with networks consisting of many cheap sensors. In such applications it may be unfeasible to have even a few sensors store and manage a very large number of cryptographic keys.

To explore these worst case scenarios, we need to better understand the asymptotic behavior of the maximal key ring size given by

$$|\Sigma|_{n,\mathrm{Max}}(K):=\max_{i=1,\dots,n}|\Sigma_{n,i}(K)|,\quad n=2,3,\dots.$$

The next result addresses this issue; it is a consequence of [26, Theorem 4.2] and is established in Section XIII.

Theorem 7.1: Consider any scaling $K:\mathbb{N}_0\to\mathbb{N}_0$ such that $K_n=O(\log n)$. Then, there exists $\gamma>0$ such that

$$\lim_{n\to\infty}\mathbb{P}\left[|\Sigma|_{n,\mathrm{Max}}(K_n)>\gamma\log n\right]=0. \tag{31}$$

It follows from (31) that

$$|\Sigma|_{n,\mathrm{Max}}(K_n)=O(\log n)\quad a.a.s.$$

This bound can be improved when the parameter K does not vary with n. The corresponding result was established in [26, Theorem 4.3], and is stated next.

[1]This was established by the authors in [26, Lemma 4.1] using a standard Hoeffding bound [6, Thm. 1.1, p.6] for the Binomial rvs (27).

Theorem 7.2: For each positive integer K and constant $\gamma>1$, we have

$$\lim_{n\to\infty}\mathbb{P}\left[|\Sigma|_{n,\mathrm{Max}}(K)>K+\gamma\frac{\log n}{\log\log n}\right]=0. \tag{32}$$

In other words,

$$|\Sigma|_{n,\mathrm{Max}}(K)=O\left(\frac{\log n}{\log\log n}\right)\quad a.a.s.$$

We refer the reader to [26] for numerical results supporting Theorems 7.1 and 7.2 in the finite n case.

We now turn to the question of how big the key ring sizes are likely to be under the conditions needed for unassailability and unsplittability. In our discussion we rely on the following monotonicity facts which also find use in the proof of Theorem 7.1 in Section XIII, namely the stochastic comparisons

$$|\Sigma_{n,i}(K)|\le_{st}|\Sigma_{n,i}(K+1)|\qquad \begin{matrix} i=1,\dots,n\\ 1\le K<n-1\\ n=2,3,\dots\end{matrix} \tag{33}$$

and

$$|\Sigma|_{n,\mathrm{Max}}(K)\le_{st}|\Sigma|_{n,\mathrm{Max}}(K+1)\qquad \begin{matrix} 1\le K<n-1\\ n=2,3,\dots\end{matrix} \tag{34}$$

where $\le_{st}$ denotes comparison in the strong stochastic order [16, Chapter 8]. See Section XIII for proofs.

We start with unassailability: The largest key ring is stochastically smallest when $K=2$ by virtue of (34), in which case unassailability holds by Theorem 3.1 and the random graph $\mathbb{H}(n;K)$ is a.a.s. connected by Theorem 2.1. Under such conditions it holds that

$$|\Sigma|_{n,\mathrm{Max}}(2)=O\left(\frac{\log n}{\log\log n}\right)\quad a.a.s.$$

by Theorem 7.2.

Next, we turn to unsplittability. This time, we pick a scaling $K:\mathbb{N}_0\to\mathbb{N}_0$ which satisfies the unsplittability condition (14), namely $\lim_{n\to\infty}K_n=\infty$. In view of Theorem 2.1, such a scaling also ensures that $\mathbb{H}(n;K_n)$ is a.a.s. connected (and in fact also unassailable by virtue of Theorem 3.1). It is clear that the scaling can be selected to satisfy both (14) *and* $K_n=O(\log n)$ – Just take $K_n=\lceil a\log n\rceil$ for some $a>0$, in which case

$$|\Sigma|_{n,\mathrm{Max}}(K_n)=O\left(\log n\right)\quad a.a.s.$$

by Theorem 7.1. Thus, the pairwise scheme can ensure unsplittability (together with unassailability and connectivity) with a maximum key ring size being a.a.s. on the order $\log n$, a size deemed feasible for large WSNs [4].

VIII. Comparison with the EG scheme

We now compare the resiliency of sensor networks against node capture attacks under the pairwise scheme with that of the EG scheme. More precisely, we consider the two schemes in terms of the number of cryptographic keys they require (at a minimum) to ensure (i) connectivity and unassailability; and (ii) connectivity and unsplittability. Network connectivity is enforced along with the resiliency metrics since it is a desirable property that is expected to hold in many practical situations.

	Unassailability	Unsplittability
EG – $\Sigma_{\mathrm{EG},n}$	$\Omega(\sqrt{n\log n})$	$\Omega(\sqrt{n\log n})$
Pairwise – $\lvert\Sigma\rvert_{\mathrm{Avg},n}$	4	w_n
Pairwise – $\lvert\Sigma\rvert_{\mathrm{Max},n}$	$O\left(\frac{\log n}{\log\log n}\right)$	$O(\log n)$

Fig. 4. *A comparison of the EG scheme and the pairwise scheme in terms of the minimum number of keys required to achieve unassailability and unsplittability. Here, w_n stands for any function satisfying $\lim_{n\to\infty} w_n = \infty$. The pairwise scheme can ensure both properties with much less memory load on the sensors as compared to the EG scheme.*

The resiliency of WSNs to node capture attacks under the EG scheme was investigated by Mei et al. [12]. They obtained conditions on the scheme parameters to guarantee the appropriate analogs of (8) and (13). Their findings are summarized next.

Let $\mathbb{K}(n;\theta)$ denote the random key graph on the vertex set $\{1,\dots,n\}$ induced by the EG scheme under full visibility [20], [25]; here $\theta = (\Sigma_{\mathrm{EG}}, P)$ collectively stands for the parameters that specify the EG scheme, namely the (fixed) size Σ_{EG} of the key ring of each sensor node and the size P of the key pool. Let $\Sigma_{n,1}(\theta),\dots,\Sigma_{n,n}(\theta)$ denote the key rings associated with nodes $1,\dots,n$, respectively, in the EG scheme. By construction, the rvs $\Sigma_{n,1}(\theta),\dots,\Sigma_{n,n}(\theta)$ are i.i.d. rvs, each of which is uniformly distributed over the collection of all subsets of size Σ_{EG} from a key pool of size P. Thus, by construction we have $|\Sigma_{n,1}(\theta)| = \cdots = |\Sigma_{n,n}(\theta)| = \Sigma_{\mathrm{EG}}$. A scaling for the EG scheme is any pair of mappings $\Sigma_{\mathrm{EG}}, P : \mathbb{N}_0 \to \mathbb{N}_0$ such that

$$\Sigma_{\mathrm{EG},n} \le P_n, \quad n = 2,3,\dots$$

We can now present the main result obtained in [12].

Theorem 8.1: Consider a scaling $\Sigma_{\mathrm{EG}}, P : \mathbb{N}_0 \to \mathbb{N}_0$ for the EG scheme such that $P_n = \lceil n^\alpha \rceil$ for some $\alpha > 0$ and such that

$$\Sigma_{\mathrm{EG},n} \ge \sqrt{(1+\varepsilon)n^{\alpha-1}\log n} \tag{35}$$

for some $\varepsilon > 0$ for all n sufficiently large. If $\alpha \ge 2$, then the conditions (8) and (13) both hold and the random graph $\mathbb{K}(n;\theta)$ is a.a.s. connected.

In [12] it is claimed, but without proofs, that both properties also hold under the weaker conditions $\Sigma_{\mathrm{EG},n} \ge \log n$ and $P_n = \lceil \frac{n}{\log n} \rceil$.

Comparing the two schemes leads to several interesting conclusions. First, it is clear from the discussion in Section VII-C that the pairwise scheme can ensure unassailability and network connectivity with the size of *all* key rings being on the order $\frac{\log n}{\log\log n}$. On the other hand, it follows from Theorem 8.1 that the same properties would seem to require key rings on the order of $\sqrt{n\log n}$ in the EG scheme (since we need $\alpha \ge 2$ in (35)). Similarly, under the pairwise scheme, we see that unsplittability and connectivity can be ensured with all sensors keeping $O(\log n)$ keys, whereas the EG scheme would again require key rings with size $\sqrt{n\log n}$.

These conclusions are summarized in Figure 4. For the sake of completeness, we also include the *average* key ring sizes (see (29)) required in the pairwise scheme to ensure unassailability and unsplittability. Thus the pairwise scheme can ensure both properties with much smaller key ring sizes than would be needed for the EG scheme.

IX. Some basic bounds

Consider positive integers n and K such that $n < K$. Pick a non-empty subset $A \subseteq \mathcal{N}_n$ of nodes with $0 < |A| < n$. The expression (18) for $C_A(n;K)$ being rather cumbersome to use, we will rely instead on the bound

$$C_A(n;K) \le |A|K + L_A(n;K) \tag{36}$$

where we have set

$$L_A(n;K) := \sum_{j\in A^c}\left(\sum_{i\in A}\mathbf{1}\left[i \in \Gamma_{n,j}(K)\right]\right). \tag{37}$$

The validity of (36) can be argued as follows: There are at most $K|A|$ compromised edges which originate from the nodes in A, i.e., at most $K|A|$ edges are created in $\mathbb{H}(n;K)$ as a result of the selections $\{\Gamma_{n,i}(K) : i \in A\}$. On the other hand, there are exactly $L_A(n;K)$ compromised edges originating out of the nodes in A^c.

For future reference we note that

$$\mathbb{E}[L_A(n;K)] = |A|(n-|A|)\frac{K}{n-1}. \tag{38}$$

Next, we derive Hoeffding bounds for the rvs $L_A(n;K)$. Consider the mapping $\Phi : \mathbb{R} \to [0,\infty]$ given by

$$\Phi(x) = \begin{cases} \infty & \text{if } x < -1 \\ (1+x)\log(1+x) - x & \text{if } -1 \le x \end{cases} \tag{39}$$

with the understanding that $t\log t = 0$ if $t = 0$ (by continuity). It is easy to check that $\Phi(x) > 0$ if $x > -1$.

Proposition 9.1: Consider positive integers n and K such that $n < K$. For any non-empty subset $A \subseteq \mathcal{N}_n$ of nodes with $0 < |A| < n$, it holds that

$$\begin{aligned}\mathbb{P}[L_A(n;K) \ge \mathbb{E}[L_A(n;K)] + t] \\ \le\ e^{-\Phi\left(t\mathbb{E}[L_A(n;K)]^{-1}\right)\cdot\mathbb{E}[L_A(n;K)]}\end{aligned} \tag{40}$$

for all $t > 0$. Moreover, we also have the bilateral bound

$$\begin{aligned}\mathbb{P}[|L_A(n;K) - \mathbb{E}[L_A(n;K)]| \ge \varepsilon] \\ \le\ 2e^{-\Phi(\varepsilon)\cdot\mathbb{E}[L_A(n;K)]}\end{aligned} \tag{41}$$

for every $\varepsilon > 0$.

A proof of Proposition 9.1 is given in Appendix B.

X. An easy consequence

In the proofs we will have several opportunities to use the following easy consequence of the bound (40).

Proposition 10.1: Consider positive integers n and K such that $n < K$. With $r = 1,\dots,n-1$, let $\lambda > 0$ satisfy the condition

$$\lambda > \frac{r}{n}\left(1 + \frac{n-r}{n-1}\right). \tag{42}$$

Then, the bound

$$\mathbb{P}\left[C_r^\star(n;K) \ge \lambda nK\right] \le \left(\frac{en}{r}\right)^r e^{-nF_\lambda(n;r)K} \tag{43}$$

holds with

$$\begin{aligned}F_\lambda(n;r) \ =\ & \left(\lambda - \frac{r}{n}\right)\log\left(\frac{\lambda\cdot\frac{n}{r} - 1}{\frac{n-r}{n-1}}\right) \\ & - \left(\lambda - \frac{r}{n}\left(1 + \frac{n-r}{n-1}\right)\right).\end{aligned} \tag{44}$$

Proof. Fix $r = 1, 2, \ldots, n-1$. With $\lambda > 0$ we have

$$\begin{aligned}
&\mathbb{P}\left[C_r^\star(n;K) \geq \lambda nK\right] \\
&= \mathbb{P}\left[\max\left(C_A(n;K) :\ A \in \mathcal{P}_{n|r}\right) \geq \lambda nK\right] \\
&= \mathbb{P}\left[\cup_{A\in\mathcal{P}_{n|r}}\left[C_A(n;K) \geq \lambda nK\right]\right] \\
&\leq \sum_{A\in\mathcal{P}_{n|r}} \mathbb{P}\left[C_A(n;K) \geq \lambda nK\right] \qquad (45)\\
&\leq \sum_{A\in\mathcal{P}_{n|r}} \mathbb{P}\left[L_A(n;K) + K|A| \geq \lambda nK\right] \\
&= \sum_{A\in\mathcal{P}_{n|r}} \mathbb{P}\left[L_A(n;K) \geq (\lambda n - r)\,K\right] \qquad (46)
\end{aligned}$$

where (45) follows by a union bound argument, while the step before last made use of the bound (36).

We write $L_r(n;K)$ for $L_A(n;K)$ when $A = \{1,\ldots,r\}$. Taking note of the fact that the rvs

$$\{L_A(n;K) :\ A \in \mathcal{P}_{n|r}\}$$

are equidistributed, we conclude that

$$\begin{aligned}
&\mathbb{P}\left[C_r^\star(n;K) \geq \lambda nK\right] \\
&\leq |\mathcal{P}_{n|r}|\,\mathbb{P}\left[L_r(n;K) \geq (\lambda n - r)\,K\right] \\
&\leq \left(\frac{en}{r}\right)^r \mathbb{P}\left[L_r(n;K) \geq (\lambda n - r)\,K\right] \qquad (47)
\end{aligned}$$

upon recalling the standard facts

$$|\mathcal{P}_{n|r}| = \binom{n}{r} \leq \left(\frac{en}{r}\right)^r.$$

As we have in mind to use (40) we inquire whether we can indeed find $t > 0$ such that

$$(\lambda n - r)\,K = \mathbb{E}\left[L_r(n;K)\right] + t, \qquad (48)$$

a requirement equivalent to

$$(\lambda n - r)\,K = r(n-r)\frac{K}{n-1} + t.$$

Solving for t we find

$$t = \left(\lambda - \frac{r}{n}\left(1 + \frac{n-r}{n-1}\right)\right)nK. \qquad (49)$$

Under the condition (42), the bound (40) can be used with this value of t (because $t > 0$), yielding

$$\begin{aligned}
&\mathbb{P}\left[L_r(n;K) \geq (\lambda n - r)K\right] \\
&\leq e^{-\Phi\left(t\mathbb{E}[L_r(n;K)]^{-1}\right)\cdot\mathbb{E}[L_r(n;K)]}. \qquad (50)
\end{aligned}$$

Direct inspection shows that

$$\begin{aligned}
&\Phi\left(t\mathbb{E}\left[L_r(n;K)\right]^{-1}\right)\cdot\mathbb{E}\left[L_r(n;K)\right] \qquad (51)\\
&= \left(\mathbb{E}\left[L_r(n;K)\right] + t\right)\log\left(\frac{\mathbb{E}\left[L_r(n;K)\right] + t}{\mathbb{E}\left[L_r(n;K)\right]}\right) - t
\end{aligned}$$

with

$$\mathbb{E}\left[L_r(n;K)\right] + t = \left(\lambda - \frac{r}{n}\right)nK \qquad (52)$$

by virtue of (48) so that

$$\begin{aligned}
\frac{\mathbb{E}\left[L_r(n;K)\right] + t}{\mathbb{E}\left[L_r(n;K)\right]} &= \left(\lambda - \frac{r}{n}\right)\left(\frac{r(n-r)}{n(n-1)}\right)^{-1} \\
&= \left(\lambda\cdot\frac{n}{r} - 1\right)\left(\frac{n-r}{n-1}\right)^{-1}
\end{aligned}$$

Combining these facts we conclude that

$$\Phi\left(t\mathbb{E}\left[L_r(n;K)\right]^{-1}\right)\cdot\mathbb{E}\left[L_r(n;K)\right] = nF_\lambda(n;r)K \qquad (53)$$

with $F_\lambda(n;r)$ given by (44), and the bound

$$\mathbb{P}\left[L_r(n;K) \geq (\lambda n - r)K\right] \leq e^{-nF_\lambda(n;r)K} \qquad (54)$$

holds as a rewrite of (50). The desired conclusion (43) is now a simple consequence of (47). ∎

XI. A proof of Theorem 3.1

The proof proceeds in two steps: First we provide an upper bound on the probability of interest using the auxiliary result presented in Proposition 10.1. Then we let n go to infinity.

A. From keys to edges

Consider the random graph $\mathbb{H}(n;K)$ for positive integers n and K such that $K < n$. By construction each key determines one and only one (undirected) edge in $\mathbb{H}(n;K)$, whereas at most two keys can be associated with any given (undirected) edge. For any edge $i \sim j$, this last scenario occurs when both events $i \in \Gamma_{n,i}(K)$ and $j \in \Gamma_{n,i}(K)$ take place. As a result, we obtain the following bounds

$$\frac{Kn}{2} \leq |E(n;K)| \leq Kn. \qquad (55)$$

Fix $r = 1, 2, \ldots, n-1$. With $\varepsilon > 0$ the lower bound in (55) yields

$$\mathbb{P}\left[C_r^\star(n;K) \geq \varepsilon\cdot|E(n;K)|\right] \leq \mathbb{P}\left[C_r^\star(n;K) \geq \frac{\varepsilon}{2}\cdot nK\right].$$

If $\varepsilon > 0$ satisfies the condition

$$\varepsilon > 2\frac{r}{n}\left(1 + \frac{n-r}{n-1}\right), \qquad (56)$$

then (42) holds for $\lambda = \frac{\varepsilon}{2}$, and Proposition 10.1 yields the bound

$$\mathbb{P}\left[C_r^\star(n;K) \geq \varepsilon\cdot|E(n;K)|\right] \leq \left(\frac{en}{r}\right)^r e^{-nF_{\frac{\varepsilon}{2}}(n;r)K} \qquad (57)$$

where $F_{\frac{\varepsilon}{2}}(n;r)$ is given by (44) (with $\lambda = \frac{\varepsilon}{2}$).

B. Taking the limit with n going to infinity

Consider scalings $K : \mathbb{N}_0 \to \mathbb{N}_0$ and $r : \mathbb{N}_0 \to \mathbb{N}_0$ such that

$$r_n = o(n). \qquad (58)$$

Set

$$t_n = \left(\frac{\varepsilon}{2} - \frac{r_n}{n}\left(1 + \frac{n-r_n}{n-1}\right)\right)nK_n, \quad n = 2, 3, \ldots$$

Under (58), we have $t_n > 0$ for all n sufficiently large, say $n \geq n^\star$ for some positive integer $n^\star$.

On that range, it follows from (57) (with $K = K_n$ and $r = r_n$) that

$$\mathbb{P}\left[C^{\star}_{r_n}(n;K_n) \geq \varepsilon \cdot |E(n;K_n)|\right] \leq \left(\frac{en}{r_n}\right)^{r_n} e^{-F_{\frac{\varepsilon}{2}}(n;r_n)nK_n} = e^{-n(\ldots)} \tag{59}$$

with

$$\ldots = \frac{r_n}{n}\log\left(\frac{1}{e}\frac{r_n}{n}\right) + F_{\frac{\varepsilon}{2}}(n;r_n)K_n.$$

Let n go to infinity in the inequality (59): Under (58) we observe that

$$\lim_{n\to\infty} \frac{r_n}{n}\log\left(\frac{1}{e}\frac{r_n}{n}\right) = 0$$

and that

$$\lim_{n\to\infty} F_{\frac{\varepsilon}{2}}(n;r_n) = \infty,$$

regardless of how the scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ behaves, hence

$$\lim_{n\to\infty}\left(\frac{r_n}{n}\log\left(\frac{1}{e}\frac{r_n}{n}\right) + F_{\frac{\varepsilon}{2}}(n;r_n)K_n\right) = \infty. \tag{60}$$

The desired conclusion (8) is now immediate. ∎

XII. A PROOF OF THEOREM 3.2

Here as well, the proof proceeds in two distinct steps, namely an upper bound followed by a limiting argument.

A. Splittability and compromised edges

As we now turn to establishing (13), fix n and K such that $K < n$. The discussion starts with the following observation: Consider an attack that succeeds in capturing the nodes in A, and let S denote an arbitrary subset of nodes in $\mathcal{N}_n$. If S is A-splittable, then all the edges between the set of nodes S and its complement S^c (in $\mathcal{N}_n$) are compromised by the capture of nodes in A. Hence, the total number $C_A(n;K)$ of edges which are therefore compromised by this attack must be at least $|E(n;K)(S)|$. Therefore, by the characterization (9) of S being A-splittable we have the inclusion

$$[S \text{ is } A\text{-splittable}] \subseteq [C_A(n;K) \geq |E(n;K)(S)|].$$

From the definitions it is plain that (13) holds trivially when $\frac{1}{2} < \gamma$. Thus with each γ in $\left(0,\frac{1}{2}\right]$, let $\mathcal{N}_{n,\gamma}$ denote the collection of all subsets S of $\mathcal{N}_n$ such that $\gamma n \leq |S| \leq \frac{n}{2}$. For each $r = 1,\ldots,n-1$, the definition of the count variable $I_r(n;K)$ and the last inclusion together imply

$$\begin{aligned}
\mathbb{P}\left[I_r(n;K) \geq \gamma n\right] &= \mathbb{P}\left[\bigcup_{S\in\mathcal{N}_{n,\gamma}} [S \text{ is } r\text{-splittable}]\right] \\
&= \mathbb{P}\left[\bigcup_{S\in\mathcal{N}_{n,\gamma}}\left(\bigcup_{A\in\mathcal{P}_{n|r}} [S \text{ is } A\text{-splittable}]\right)\right] \\
&\leq \mathbb{P}\left[\bigcup_{S\in\mathcal{N}_{n,\gamma}}\left(\bigcup_{A\in\mathcal{P}_{n|r}} [C_A(n;K) \geq |E(n;K)(S)|]\right)\right] \\
&= \mathbb{P}\left[\bigcup_{S\in\mathcal{N}_{n,\gamma}}\left[C^{\star}_r(n;K) \geq |E(n;K)(S)|\right]\right] \\
&\leq \sum_{S\in\mathcal{N}_{n,\gamma}} \mathbb{P}\left[C^{\star}_r(n;K) \geq |E(n;K)(S)|\right]
\end{aligned} \tag{61}$$

by a union bound argument in the last step.

Next, pick $\varepsilon > 0$ and δ in $(0,1)$ such that

$$2\varepsilon < (1-\delta)\gamma. \tag{62}$$

The need for doing so will become apparent below. For each S in $\mathcal{N}_{n,\gamma}$, conditioning on the size of $E(n;K)(S)$ relative to εnK, we readily see that

$$\begin{aligned}
&\mathbb{P}\left[C^{\star}_r(n;K) \geq |E(n;K)(S)|\right] \\
&\quad\leq \mathbb{P}\left[C^{\star}_r(n;K) \geq \varepsilon nK\right] + \mathbb{P}\left[|E(n;K)(S)| < \varepsilon nK\right].
\end{aligned} \tag{63}$$

Using this fact with (61) we conclude that

$$\begin{aligned}
\mathbb{P}\left[I_r(n;K) \geq \gamma n\right] &\leq |\mathcal{N}_{n,\gamma}| \cdot \mathbb{P}\left[C^{\star}_r(n;K) \geq \varepsilon nK\right] \\
&\quad + \sum_{S\in\mathcal{N}_{n,\gamma}} \mathbb{P}\left[|E(n;K)(S)| < \varepsilon nK\right].
\end{aligned} \tag{64}$$

Now if condition (42) is satisfied with $\lambda = \varepsilon$, say

$$\varepsilon > \frac{r}{n}\left(1 + \frac{n-r}{n-1}\right), \tag{65}$$

then the auxiliary bound (43) yields

$$\mathbb{P}\left[C^{\star}_r(n;K) \geq \varepsilon nK\right] \leq \left(\frac{en}{r}\right)^{r} e^{-nF_{\varepsilon}(n;r)K}$$

with $F_{\varepsilon}(n;r)$ given by (44) (with $\lambda = \varepsilon$). It then follows that

$$\begin{aligned}
&|\mathcal{N}_{n,\gamma}| \cdot \mathbb{P}\left[C^{\star}_r(n;K) \geq \varepsilon nK\right] \\
&\quad\leq 2^n \cdot \left(\frac{en}{r}\right)^{r} e^{-nF_{\varepsilon}(n;r)K}
\end{aligned} \tag{66}$$

upon using the rough bound $|\mathcal{N}_{n,\gamma}| \leq 2^n$.

As we consider the summation term in the right handside of (64), pick S in $\mathcal{N}_{n,\gamma}$ and observe that

$$\begin{aligned}
|E(n;K)(S)| &= \sum_{j\in S^c}\sum_{i\in S} \mathbf{1}\left[j \in \Gamma_{n,i}(K) \vee i \in \Gamma_{n,j}(K)\right] \\
&\geq L_S(n;K).
\end{aligned} \tag{67}$$

Note that

$$\mathbb{E}\left[L_S(n;K)\right] = |S|\,(n-|S|)\cdot\frac{K}{n-1} \geq \frac{\gamma}{2}\cdot nK \tag{68}$$

since $\gamma n \le |S| \le \frac{n}{2}$ by membership of S in $\mathcal{N}_{n,\gamma}$. From (62) and (68) we automatically have

$$\varepsilon nK < (1-\delta)\mathbb{E}\left[L_{n,S}(K)\right] \tag{69}$$

for *all* $n = 1, 2, \ldots$. Therefore, the bound (67) in combination with the inequality (69) implies

$$\begin{aligned}
&\mathbb{P}\left[|E(n;K)(S)| < \varepsilon nK\right] \\
&\quad\le \mathbb{P}\left[L_S(n;K) < \varepsilon nK\right] \\
&\quad\le \mathbb{P}\left[L_S(n;K) \le (1-\delta)\mathbb{E}\left[L_S(n;K)\right]\right] \\
&\quad\le 2e^{-\Phi(1-\delta)\cdot\mathbb{E}[L_S(n;K)]}
\end{aligned}$$

where the last inequality is a consequence of the bilateral bound (41) given in Proposition 9.1. Exploiting (68) one more time, and noting that $\Phi(x)$ is monotone increasing over the range $0 \le x \le 1$, we finally get

$$\mathbb{P}\left[|E(n;K)(S)| < \varepsilon nK\right] \le 2e^{-\frac{\gamma}{2}\Phi(1-\delta)\cdot nK} \le 2e^{-\frac{\gamma}{2}\Phi(\frac{2\varepsilon}{\gamma})nK}$$

where the last inequality follows from (62). Thus,

$$\begin{aligned}
&\sum_{S\in\mathcal{N}_{n,\gamma}} \mathbb{P}\left[|E(n;K)(S)| < \varepsilon nK\right] \\
&\quad\le 2|\mathcal{N}_{n,\gamma}|e^{-\frac{\gamma}{2}\Phi(\frac{2\varepsilon}{\gamma})\cdot nK} \\
&\quad\le 2^{n+1}\cdot e^{-\frac{\gamma}{2}\Phi(\frac{2\varepsilon}{\gamma})\cdot nK} \\
&\quad= 2\left(2e^{-\frac{\gamma}{2}\Phi(\frac{2\varepsilon}{\gamma})\cdot K}\right)^n.
\end{aligned} \tag{70}$$

Combining the bounds (66) and (70), we get from (64) that

$$\begin{aligned}
\mathbb{P}\left[I_r(n;K) \ge \gamma n\right] \quad &\le \quad 2^n\cdot\left(\frac{en}{r}\right)^r e^{-nF_\varepsilon(n;r)K} \\
&\quad + 2\left(2e^{-\frac{\gamma}{2}\Phi(\frac{2\varepsilon}{\gamma})\cdot K}\right)^n
\end{aligned} \tag{71}$$

provided the conditions (62) and (65) hold; here $F_\varepsilon(n;r)$ is given by (44) with arbitrary $\frac{r}{n}\left(1+\frac{n-r}{n-1}\right) < \varepsilon < \frac{\gamma}{2}$, while $\Phi(x)$ is defined at (39).

B. Taking the limit with n going to infinity

We make use of the bound (71) as follows: Consider scalings $K : \mathbb{N}_0 \to \mathbb{N}_0$ and $r : \mathbb{N}_0 \to \mathbb{N}_0$ such that (58) holds. Pick $\varepsilon > 0$ and δ in $(0,1)$ such that (62) is satisfied. Note that under (58), the condition (65) (with $r = r_n$) will eventually hold for all n sufficiently large, say $n \ge n^\star$ for some positive integer $n^\star$. On that range, the bound (71) therefore holds with $K = K_n$ and $r = r_n$, yielding

$$\begin{aligned}
&\mathbb{P}\left[I_{r_n}(n;K_n) \ge \gamma n\right] \\
&\quad\le e^{-n\left(\frac{r_n}{n}\log\left(\frac{1}{e}\frac{r_n}{n}\right)-\log 2+F_\varepsilon(n;r_n)K_n\right)} \\
&\qquad + 2\left(2e^{-\frac{\gamma}{2}\Phi(\frac{2\varepsilon}{\gamma})\cdot K_n}\right)^n.
\end{aligned} \tag{72}$$

Let n go to infinity in (72): As in the proof of Theorem 3.1, under (58) the limit (60) holds, hence

$$\lim_{n\to\infty}\left(\frac{r_n}{n}\log\left(\frac{1}{e}\frac{r_n}{n}\right) - \log 2 + F_\varepsilon(n;r_n)K_n\right) = \infty$$

regardless of the behavior of the scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$, while the condition (14) ensures

$$\lim_{n\to\infty} 2e^{-\frac{\gamma}{2}\Phi(\frac{2\varepsilon}{\gamma})\cdot K_n} = 0.$$

The desired conclusion (13) is now immediate. ∎

XIII. A PROOF OF THEOREM 7.1

A. A monotonicity result

We begin by first establishing the monotonicity results (33) and (34). Fix positive integers K and n such that $K < n$. Note from (26) that

$$|\Sigma_{n,i}(K)| = K + X_{n,i}(K), \quad i = 1, \ldots, n \tag{73}$$

with $X_{n,i}(K)$ defined by

$$X_{n,i}(K) = \sum_{j=1, j\ne i}^{n} \mathbf{1}\left[i \in \Gamma_{n,j}(K)\right].$$

For each $i = 1, \ldots, n$, the rvs $X_{n,i}(K)$ and $X_{n,i}(K+1)$ are Binomial rvs $\mathrm{Bin}(n-1, \frac{K}{n-1})$ and $\mathrm{Bin}(n-1, \frac{K+1}{n-1})$, respectively.

The comparison $X_{n,i}(K) \le_{st} X_{n,i}(K+1)$ holds by well-known facts and properties concerning the stochastic ordering $\le_{st}$ (e.g., see [16, Chapter 8]), whence

$$\begin{aligned}
K + X_{n,i}(K) \quad &\le_{st} \quad K + X_{n,i}(K+1) \\
&\le_{st} \quad K + 1 + X_{n,i}(K+1)
\end{aligned} \tag{74}$$

and the conclusion

$$|\Sigma_{n,i}(K)| \le_{st} |\Sigma_{n,i}(K+1)| \tag{75}$$

follows.

Unfortunately, as discussed already in Appendix A, the rvs $|\Sigma_{n,1}(K)|, \ldots |\Sigma_{n,n}(K)|$ are not independent; they are in fact negatively correlated; see Section VII-C. As a result, the one-dimensional comparisons (75) do not necessarily imply the desired result (34). A stronger version of (75) (in the usual pointwise sense) needs to be established through a *coupling* argument we now develop: With K and n such that $K+1 < n$, consider the i.i.d. random sets $\Gamma_{n,1}(K+1), \ldots, \Gamma_{n,n}(K+1)$. For each $i = 1, \ldots, n$, let $U_{n,i}(K)$ denote a rv $\Omega \to \mathcal{N}_{n,-i}$ which is uniformly distributed over the set $\Gamma_{n,i}(K+1)$ conditionally on $\Gamma_{n,1}(K+1), \ldots, \Gamma_{n,n}(K+1)$ with

$$\begin{aligned}
&\mathbb{P}\left[U_{n,i}(K) = \ell \mid \Gamma_{n,1}(K+1), \ldots, \Gamma_{n,n}(K+1)\right] \\
&\quad= \begin{cases} \frac{1}{K+1} & \text{if } \ell \in \Gamma_{n,i}(K+1) \\ 0 & \text{if } \ell \notin \Gamma_{n,i}(K+1). \end{cases}
\end{aligned} \tag{76}$$

Possibly by enlarging the probability triple $(\Omega, \mathcal{F}, \mathbb{P})$, this construction can be carried out so that the rvs $U_{n,1}(K+1)), \ldots, U_{n,n}(K+1)$ are mutually independent given $(\Gamma_{n,1}(K+1), \ldots, \Gamma_{n,n}(K+1))$, *and* the pointwise constraints

$$U_{n,i}(K+1) \in \Gamma_{n,i}(K+1), \quad i = 1, \ldots, n \tag{77}$$

are simultaneously satisfied.[2]

[2]Such a construction can be achieved as follows: Introduce a collection of i.i.d. $\{1, \ldots, K+1\}$-valued rvs $\{V_1(K+1), \ldots, V_n(K+1)\}$ which are (i) independent of the rvs $\{\Gamma_{n,1}(K+1), \ldots, \Gamma_{n,n}(K+1)\}$ and (ii) uniformly distributed on $\{1, \ldots, K+1\}$. If $V_i(K+1) = k$ for some $k = 1, \ldots, K+1$, then set $U_{n,i}(K+1)$ to be the k^{th} largest value in $\Gamma_{n,i}(K+1)$.

Fix $i = 1, \ldots, n$. In view of (77), we can now define the random set $\widetilde{\Gamma}_{n,i}(K)$ as the set obtained by removing $U_{n,i}(K+1)$ from $\Gamma_{n,i}(K+1)$, i.e.,

$$\widetilde{\Gamma}_{n,i}(K) = \Gamma_{n,i}(K+1) - \{U_{n,i}(K+1)\}.$$

By construction, under (77) we have

$$\widetilde{\Gamma}_{n,i}(K) \subseteq \Gamma_{n,i}(K+1) \tag{78}$$

with $|\widetilde{\Gamma}_{n,i}(K)| = K$. Under the enforced conditional independence given $(\Gamma_{n,1}(K+1), \ldots, \Gamma_{n,n}(K+1))$, it is easy to check that the rvs $\widetilde{\Gamma}_{n,1}(K), \ldots, \widetilde{\Gamma}_{n,n}(K)$ are mutually independent. Furthermore, we now show that for each $i = 1, \ldots, n$, the distributional equality $\widetilde{\Gamma}_{n,i}(K) =_{st} \Gamma_{n,i}(K)$ holds.

Indeed, by construction the set $\widetilde{\Gamma}_{n,i}(K)$ is a subset of $\mathcal{N}_n$ which does not contain i and which has exactly K elements in it. Thus, for any subset $S \subseteq \mathcal{N}_{n,-i}$ with $|S| = K$, we have

$$\begin{aligned}
&\mathbb{P}\left[\widetilde{\Gamma}_{n,i}(K) = S\right] \\
&= \mathbb{P}\left[\Gamma_{n,i}(K+1) - \{U_{n,i}(K+1)\} = S\right] \\
&= \sum_{T \subseteq \mathcal{N}_{n,-i},\ |T|=K+1} \mathbb{P}\left[\begin{array}{c} \Gamma_{n,i}(K+1) = T, \\ T - \{U_{n,i}(K+1)\} = S \end{array}\right] \\
&= \sum_{\ell \in \mathcal{N}_{n,-i},\ \ell \notin S} \mathbb{P}\left[\begin{array}{c} \Gamma_{n,i}(K+1) = S \cup \{\ell\}, \\ U_{n,i}(K+1) = \ell \end{array}\right] \\
&= |\mathcal{N}_{n,-i} \cap S^c| \cdot \frac{1}{K+1} \cdot \frac{1}{\binom{n-1}{K+1}} \\
&= \frac{n-(K+1)}{K+1} \cdot \frac{1}{\binom{n-1}{K+1}} \\
&= \frac{1}{\binom{n-1}{K}}
\end{aligned} \tag{79}$$

as desired.

Now set

$$\widetilde{X}_{n,i}(K) = \sum_{j=1, j\neq i}^{n} \mathbf{1}\left[i \in \widetilde{\Gamma}_{n,j}(K)\right], \quad i = 1, \ldots, n.$$

By construction (and earlier remarks), the random vector $\left(\widetilde{\Gamma}_{n,1}(K), \ldots, \widetilde{\Gamma}_{n,n}(K)\right)$ has the same distribution as the random vector $(\Gamma_{n,1}(K), \ldots, \Gamma_{n,n}(K))$. It is now plain from (73) that the random vector $\left(K + \widetilde{X}_{n,1}(K), \ldots, K + \widetilde{X}_{n,n}(K)\right)$ has the same distribution as the random vector $(|\Sigma_{n,1}(K)|, \ldots, |\Sigma_{n,n}(K)|)$, so that

$$\max_{i=1,\ldots,n} \left(K + \widetilde{X}_{n,i}(K)\right) =_{st} |\Sigma|_{n,\mathrm{Max}}(K). \tag{80}$$

However, the inclusions (78) also imply

$$\widetilde{X}_{n,i}(K) \leq X_{n,i}(K+1), \quad i = 1, \ldots, n$$

and the pointwise comparison

$$\max_{i=1,\ldots,n} \left(K + \widetilde{X}_{n,i}(K)\right) \leq |\Sigma|_{n,\mathrm{Max}}(K+1)$$

follows. We readily conclude (34) with the help of (80). ■

B. Proving Theorem 7.1

It is known [26, Thm. 4.2] (and the discussion following it) that if a scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ satisfies $K_n \sim \lambda \log n$ for some $\lambda \geq 2.6$, then

$$\lim_{n\to\infty} \mathbb{P}\left[|\Sigma|_{n,\mathrm{Max}}(K_n) > (c+2)K_n\right] = 0 \tag{81}$$

for any $c \geq 1$.

Now, pick an arbitrary scaling $K : \mathbb{N}_0 \to \mathbb{N}_0$ such that $K_n = O(\log n)$. This amounts to the existence of a constant $a > 0$ such that $K_n \leq a \log n$ for all n sufficiently large, say $n \geq n_a$ for some finite integer n_a. Define the auxiliary scaling $\tilde{K}_a : \mathbb{N}_0 \to \mathbb{N}_0$ by setting $\tilde{K}_{a,n} = \lceil a \log n \rceil$ for all $n = 1, 2, \ldots$. Note that $K_n \leq \tilde{K}_{a,n}$ for all $n \geq n_a$ with $\tilde{K}_{a,n} \sim a \log n$.

Two cases are possible: If $a \geq 2.6$, then putting $c = 1$ in (81) yields

$$\lim_{n\to\infty} \mathbb{P}\left[|\Sigma|_{n,\mathrm{Max}}(\tilde{K}_{a,n}) > 3\tilde{K}_{a,n}\right] = 0,$$

whence

$$\lim_{n\to\infty} \mathbb{P}\left[|\Sigma|_{n,\mathrm{Max}}(\tilde{K}_{a,n}) > (3a+1)\log n\right] = 0, \tag{82}$$

since $\tilde{K}_{a,n} \leq a \log n + 1 \leq (a + \frac{1}{3}) \log n$ for all n sufficiently large. Using the stochastic comparison (34) with K_n and $\tilde{K}_{a,n}$ we conclude

$$\begin{aligned}
&\mathbb{P}\left[|\Sigma|_{n,\mathrm{Max}}(K_n) > (3a+1)\log n\right] \\
&\leq \mathbb{P}\left[|\Sigma|_{n,\mathrm{Max}}(\tilde{K}_{a,n}) > (3a+1)\log n\right]
\end{aligned} \tag{83}$$

whenever $n \geq n_a$. Letting n go to infinity in this last inequality and using (82), we obtain the desired result (31) with $\gamma = 3a + 1$.

If $a < 2.6$, then the same arguments as above show that $K_n \leq \tilde{K}_{a,n} \leq \tilde{K}_{2.6,n}$ for all $n \geq n_a$. Applying (82) and (83) with $a = 2.6$ yields the desired result (31) with $\gamma = 7.8$. ■

XIV. Future Work

The research presented in this paper can be extended in several directions. Firstly, the analysis of resiliency properties of sensor networks has only been done under the full visibility assumption. Future research should address situations where wireless communication connectivity is explicitly taken into account. Secondly, it might be worthwhile extending the analysis to key predistribution schemes other than the EG scheme and the pairwise scheme. A good candidate would be the q-composite scheme introduced in [3], which is a direct extension of the EG scheme. Finally, one might revisit the analysis with a less powerful attacker model and see how the required key ring sizes are affected by the capabilities of the potential adversary.

Acknowledgment

This work was supported in part by NSF Grant CCF-0729093, in part by the Department of Electrical and Computer Engineering at Carnegie Mellon, and in part by a gift from Persistent Systems, Inc. The paper was completed during Fall 2014 while A.M. Makowski was a Visiting Professor

with the Department of Statistics of the Hebrew University of Jerusalem with the support of a fellowship from the Lady Davis Trust.

REFERENCES

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

[2] S. A. Çamtepe and B. Yener, *Key Distribution Mechanisms for Wireless Sensor Networks: a Survey*, Technical Report TR-05-07, Renselaer Polytechnic Institute, Computer Science Department, Troy (NY), March 2005.

[3] H. Chan, A. Perrig and D. Song, "Random key predistribution schemes for sensor networks," in Proceedings of 2003 IEEE Symposium on Security and Privacy (SP 2003), Oakland (CA), May 2003.

[4] R. Di Pietro, L.V. Mancini, A. Mei, A. Panconesi and J. Radhakrishnan, "Redoubtable sensor networks," *ACM Transactions on Information and System Security* **TISSEC 11** (2008), pp. 1-22.

[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.

[6] D. Dubhashi and A. Panconesi, *Concentration of Measure for the Analysis of Randomized Algorithms*, Cambridge University Press, New York (NY), 2009.

[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. 2008), pp. 155-163.

[8] T.I. Fenner and A.M. Frieze, "On the connectivity of random m-orientable graphs and digraphs," *Combinatorica* **2** (1982), pp. 347-359.

[9] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *Journal of the American Statistical Association* **58** (1963), pp. 13-30.

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

[11] K. Joag-Dev and F. Proschan, "Negative association of random variables, with applications," *The Annals of Statistics* **11** (1983), pp. 266-295.

[12] A. Mei, A. Panconesi and J. Radhakrishnan, "Unassailable sensor networks," in Proceedings of SecureComm 2008, Istanbul (Turkey), September 2008.

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

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

[15] T. Philips, D. Towsley and J. Wolf, "On the diameter of a class of random graphs," *IEEE Transactions on Information Theory* **IT-36** (1990), pp. 285-288.

[16] S. Ross, *Stochastic Processes*, J. Wiley & Sons, New York (NY), 1984.

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

[18] Y. Wang, G. Attebury and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys & Tutorials* **8** (2006), pp. 2-23.

[19] Y. Xiao, V.K. Rayi, B. Sun, X. Du, F. Hu and M. Galloway, "A survey of key management schemes in wireless sensor networks," *Computer Communications* **30** (2007), pp. 2314-2341.

[20] O. Yağan, *Random Graph Modeling of Key Distribution Schemes in Wireless Sensor Networks*, Ph.D. Thesis, Department of Electrical and Computer Engineering, University of Maryland, College Park (MD), June 2011.

[21] O. Yağan, "Performance of the Eschenauer-Gligor key predistribution scheme under an on-off channel." *IEEE Transactions on Information Theory* **IT-58** (2012), pp. 3821-3835.

[22] O. Yağan and A. M. Makowski, "On the gradual deployment of random pairwise key distribution schemes," in Proceedings of the 9th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt 2011), Princeton (NJ), May 2011.

[23] O. Yağan and A. M. Makowski, "On the resiliency of sensor networks under the pairwise key distribution scheme," in Proceedings of the 22nd Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2011), Toronto (ON), September 2011.

[24] O. Yağan and A. M. Makowski, "Connectivity results for sensor networks under a random pairwise key predistribution scheme," in Proceedings of the IEEE International Symposium on Information Theory (ISIT 2012), Boston (MA), July 2012.

[25] O. Yağan and A.M. Makowski, "Zero-one laws for connectivity in random key graphs," *IEEE Transactions on Information Theory* **IT-58** (2012), pp. 2983-2999.

[26] O. Yağan and A. M. Makowski, "On the scalability of the random pairwise key distribution scheme: Gradual deployment and key ring sizes," *Performance Evaluation* **70** (2013), pp. 493-512.

[27] O. Yağan and A. M. Makowski, "On the connectivity of sensor networks under random pairwise key predistribution," *IEEE Transcations on Information Theory* **IT-59** (2013), pp. 5754-5762.

[28] F. Yavuz, J. Zhao, O. Yağan and V. Gligor, "Towards k-connectivity of the random graph induced by a pairwise key predistribution scheme with unreliable links," *IEEE Transactions on Information Theory* **IT-61** (2015), pp. 6251-6271.

Osman Yağan (S'07-M'12) received the B.S. degree in Electrical and Electronics Engineering from the Middle East Technical University, Ankara (Turkey) in 2007, and the Ph.D. degree in Electrical and Computer Engineering from the University of Maryland, College Park, MD in 2011. He is an Assistant Research Professor of Electrical and Computer Engineering (ECE) at Carnegie Mellon University (CMU) with an appointment in the Silicon Valley Campus. Prior to joining the faculty of the ECE department in August 2013, he was a Postdoctoral Research Fellow in CyLab at CMU. He has also held a visiting Postdoctoral Scholar position at Arizona State University during Fall 2011. His research interests include wireless communication networks, security, social and information networks, and cyber-physical systems.

Armand M. Makowski (M'83-SM'94-F'06) received the Licence en Sciences Mathématiques from the Université Libre de Bruxelles in 1975, the M.S. degree in Engineering-Systems Science from U.C.L.A. in 1976 and the Ph.D. degree in Applied Mathematics from the University of Kentucky in 1981. In August 1981, he joined the faculty of the Electrical Engineering Department at the University of Maryland College Park, where he is Professor of Electrical and Computer Engineering. He has held a joint appointment with the Institute for Systems Research since its establishment in 1985. Armand Makowski was a C.R.B. Fellow of the Belgian-American Educational Foundation (BAEF) for the academic year 1975-76; he is also a 1984 recipient of the NSF Presidential Young Investigator Award and became an IEEE Fellow in 2006. His research interests lie in applying advanced methods from the theory of stochastic processes to the modeling, design and performance evaluation of engineering systems, with particular emphasis on communication systems and networks.

APPENDIX
PROOF OF PROPOSITION 9.1

A. Negative association

In what follows we will need upper bounds on the probabilities of various events where the rv $L_A(n;K)$ deviates from its expected value $\mathbb{E}[L_A(n;K)]$. Returning to the expression (37), we note that the $\{0,1\}$-valued rvs

$$\left\{ \mathbf{1}\left[i \in \Gamma_{n,j}(K) \right], \quad \begin{matrix} i \neq j \\ i,j = 1,\ldots,n \end{matrix} \right\} \tag{A.1}$$

are *identically distributed* but *not* mutually independent, thereby precluding a direct use of standard Hoeffding bounds to obtain the desired bounds [6], [10].

However, we shall show shortly that the usual bounds still hold by leveraging the negative association of the rvs involved: Let $\xi_1,\ldots,\xi_m$ be a collection of $\mathbb{R}$-valued rvs. Following Joag-Dev and Proschan [11], we say that the rvs $\xi_1,\ldots,\xi_m$ are *negatively associated* if for any disjoint subsets A and B of $\{1,\ldots,m\}$ and for any non-decreasing mappings $f:\mathbb{R}^{|A|}\to\mathbb{R}$ and $g:\mathbb{R}^{|B|}\to\mathbb{R}$, we have

$$\mathbb{E}\left[f(\boldsymbol{\xi}_A) g(\boldsymbol{\xi}_B) \right] \leq \mathbb{E}\left[f(\boldsymbol{\xi}_A) \right] \mathbb{E}\left[g(\boldsymbol{\xi}_B) \right] \tag{A.2}$$

with rvs $\boldsymbol{\xi}_A = (\xi_a,\ a \in A)$ and $\boldsymbol{\xi}_B = (\xi_b,\ b \in B)$, provided the expectations all exist.

Proposition A.1: The collection (A.1) of $\{0,1\}$-valued rvs form a collection of negatively associated rvs.

Proof. Fix $j = 1,2,\ldots,n$. The rvs

$$\left\{ \mathbf{1}\left[i \in \Gamma_{n,j}(K) \right], \quad \begin{matrix} i \neq j \\ i = 1,\ldots,n \end{matrix} \right\}$$

are negatively associated rvs [11, P2, p. 288]. The desired result is now a consequence of Property (P7) in [11, p. 288] according to which the union of independent sets of negatively associated rvs is also negatively associated. ∎

B. A proof of Proposition 9.1

Fix $t > 0$. With $\theta > 0$ given, the usual Chernoff bound yields

$$\begin{aligned} &\mathbb{P}\left[L_A(n;K) \geq \mathbb{E}\left[L_A(n;K) \right] + t \right] \\ &\quad \leq \quad e^{-\theta(\mathbb{E}[L_A(n;K)]+t)} \mathbb{E}\left[e^{\theta L_A(n;K)} \right]. \end{aligned}$$

The derivation of the various classical Hoeffding bounds proceeds by providing simpler expressions for the best possible Chernoff bound, namely

$$\inf\left\{ e^{-\theta(\mathbb{E}[L_A(n;K)]+t)} \mathbb{E}\left[e^{\theta L_A(n;K)} \right] :\ \theta > 0 \right\}. \tag{A.3}$$

Historically, key to the success of this approach has been the underlying assumption that the $\{0,1\}$-valued summands defining $L_A(n;K)$ are mutually independent: Indeed, under this independence assumption, the simplification

$$\mathbb{E}\left[e^{\theta L_A(n;K)} \right] = \prod_{j \in A^c} \left(\prod_{i \in A} \mathbb{E}\left[e^{\theta \mathbf{1}[i \in \Gamma_{n,j}(K)]} \right] \right) \tag{A.4}$$

would then take place. This factored form then permits various compact upper bounds to (A.3) to be derived; for details we refer the reader to Hoeffding's original paper [9] or to Chapter 2 in [10].

Here the lack of mutual independence mentioned earlier precludes (A.4) to hold. Yet, by Proposition A.1 the rvs in the collection (A.1) being negatively associated, it follows from (A.2) that the upper bound

$$\mathbb{E}\left[e^{\theta L_A(n;K)} \right] \leq \prod_{j \in A^c} \left(\prod_{i \in A} \mathbb{E}\left[e^{\theta \mathbf{1}[i \in \Gamma_{n,j}(K)]} \right] \right) \tag{A.5}$$

holds. Consequently, the best Chernoff bound in the i.i.d. case will also serve as a bound (probaby not the sharpest) to

$$\mathbb{P}\left[L_A(n;K) \geq \mathbb{E}\left[L_A(n;K) \right] + t \right], \tag{A.6}$$

and any bound derived from it will therefore act as an upper bound to the probability (A.6). The bound (40) then follows from a similar bound derived under i.i.d. assumptions, namely the first bound in [10, Eqn. 2.5, p. 26].

Upper bounds to the probabilities

$$\mathbb{P}\left[L_A(n;K) \leq \mathbb{E}\left[L_A(n;K) \right] - t \right], \quad t \geq 0$$

are obtained *mutatis mutandi* by similar aguments; see Section 2.1 of [10, p. 26] for a discussion in the i.i.d.. case. In particular, the first bound in [10, Eqn. 2.6, p. 26] also holds here, and [10, Corollary 2.3, p. 27] can be invoked to validate (41). ∎