APPLICATIONS OF RANDOM INTERSECTION GRAPHS TO SECURE SENSOR NETWORKS – CONNECTIVITY RESULTS

Jun Zhao, Osman Yağan, Virgil Gligor
Carnegie Mellon University
Emails: {junzhao, oyagan, gligor}@cmu.edu

SIAM Workshop on Network Science 2015
May 16-17 · Snowbird, Utah, USA

Summary

Random intersection graphs have received much attention and been used in diverse applications including secure sensor networks. We discuss the applications of random intersection graphs to different secure sensor networks in order to derive the results of network connectivity.

Random Intersection Graphs and Their Applications

Random intersection graphs was introduced by Singer-Cohen [6]. These graphs have recently received considerable attention in the literature and been used in diverse applications [1, 2, 7–13]. In a general random intersection graph, each node is assigned a set of items in some *random* manner, and any two nodes establish an *undirected* edge in between if and only if they have at least a certain number of items in common. In this paper, we consider random s-intersection graphs defined as follows. In a random s-intersection graph with n nodes, each node selects K_n distinct items uniformly at random from the same item pool that has P_n different items, and any two nodes have an edge in between upon sharing at least s items, where $1 \leq s \leq K_n \leq P_n$ holds, and K_n and P_n are functions of n for generality. We denote a random s-intersection graph by $G_s(n, K_n, P_n)$.

Random intersection graphs have numerous application areas including secure wireless sensor networks [8, 10, 11, 13], social networks [1], cryptanalysis [2], and clustering [12]. We detail the use of random intersection graphs to model secure sensor networks.

Use of Random Intersection Graphs to Model Secure Sensor Networks

We first explain that random 1-intersection graphs naturally capture the Eschenauer–Gligor (EG) key predistribution scheme [5], which is a recognized approach to ensure secure communications in wireless sensor networks (citation: 3700+ as of 01/07/2015). In the EG scheme for an n-size sensor network, cryptographic keys are predistributed to sensors before sensors get deployed; in particular, before deployment, each sensor is assigned a set of K_n distinct cryptographic keys selected uniformly at random from a key pool containing P_n different keys. After deployment, two sensors establish secure communication over an existing link if and only if they have at least one common key. We say that a secure sensor network has *full visibility* if secure communication between two sensors only require the key sharing and does not have link constraints (examples of link constraints include the links being reliable and the distance between sensors being small enough). Then the topology of a sensor network with the EG scheme under full visibility is given by a random 1-intersection graph $G_1(n, K_n, P_n)$.

The full visibility model explained above does not capture link constraints, but wireless links in practice might be unreliable due to the presence of physical barriers in between or because of harsh environmental conditions severely impairing transmission. Moreover, in real–world implementations of sensor networks, two sensors have to be within a certain distance from each other to communicate. Therefore, in our analysis of secure sensor networks, we consider two types of link constraints: *link unreliability* and *transmission constraints*. In the link unreliability model, each link between two sensors is independently active with probability t_n and inactive with probability $(1 - t_n)$. For transmission constraints, we use the widely adopted disk model: each node's transmission area is a disk with a transmission radius r_n so two nodes must have a distance at most r_n for direct communication. In terms of the node distribution, we consider that the n sensors are independently and uniformly deployed in a region $\mathcal{A}$, where $\mathcal{A}$ is *either* a torus $\mathcal{T}$ without any boundary or a *square* $\mathcal{S}$ with boundaries, each with a unit area.

This abstract summarizes some of the results that appear in our work [7–13].

Graphs	Results
$G_1(n, K_n, P_n)$	k-connectivity [7]
$G_1(n, K_n, P_n) \cap G(n, t_n)$	k-connectivity [8,9]
$G_1(n, K_n, P_n) \cap G_{\mathcal{A}}(n, r_n)$	connectivity [10]
$G_s(n, K_n, P_n)$	k-connectivity [11]
$G_s(n, K_n, P_n) \cap G(n, t_n)$	k-connectivity [12]
$G_s(n, K_n, P_n) \cap G_{\mathcal{A}}(n, r_n)$	connectivity [13]

Table 1: *Graphs and their results.*

Note that t_n and r_n are functions of n for generality. The link unreliability induces an *Erdős–Rényi graph* [4] denoted by $G(n, t_n)$, and the model of transmission constraints yields a *random geometric graph* denoted by $G_{\mathcal{A}}(n, r_n)$. In consideration of the EG scheme and the link constraints, the topology of a sensor network with the EG scheme under link unreliability is given by the intersection of a random 1-intersection graph $G_1(n, K_n, P_n)$ and an Erdős–Rényi graph $G(n, t_n)$, where for graphs G_1 and G_2, two nodes have an edge in between in $G_1 \cap G_2$ if and only if these two nodes have an edge in G_1 and also an edge in G_2. Similarly, the topology of a sensor network with the EG scheme under transmission constraints is given by the intersection of a random 1-intersection graph $G_1(n, K_n, P_n)$ and a random geometric graph $G_{\mathcal{A}}(n, r_n)$.

The EG scheme was further extended to the Chan–Perrig–Song (CPS) scheme [3] (citation: 3000+ as of 01/07/2015). The only difference between the two schemes is that in the CPS scheme, a secure link between two sensors requires the sharing of at least s different keys rather than just one key. Then from the analysis on the EG scheme above and recalling the graph notation, we immediately obtain that: (i) the topology of a sensor network with the CPS scheme under full visibility is given by $G_s(n, K_n, P_n)$; (ii) the topology of a sensor network with the CPS scheme under link unreliability is given by $G_s(n, K_n, P_n) \cap G(n, t_n)$; and (iii) the topology of a sensor network with the CPS scheme under transmission constraints is given by $G_s(n, K_n, P_n) \cap G_{\mathcal{A}}(n, r_n)$.

We have derived (k-)connectivity results of the aforementioned graphs, as summarized in Table 1, where a graph is k-connected if each pair of nodes has at least k internally node-disjoint path(s) between them, and connectivity just means 1-connectivity. As an example, we present the following theorem for k-connectivity results of a random s-intersection graph $G_s(n, K_n, P_n)$.

Theorem 1 *For a random s-intersection graph $G_s(n, K_n, P_n)$ which models a secure sensor network with the CPS scheme under full visibility, under $P_n = \Omega(n)$, if*

$$\frac{1}{s!} \cdot \frac{{K_n}^{2s}}{{P_n}^{s}} = \frac{\ln n + (k-1) \ln \ln n + \alpha_n}{n} \tag{1}$$

for a sequence α_n with $\lim_{n\to\infty} \alpha_n = \alpha^* \in [-\infty, \infty]$, then

$$\lim_{n\to\infty} \mathbb{P}[\text{ Graph } G_s(n, K_n, P_n) \text{ is } k\text{-connected.}\,] = e^{-\frac{e^{-\alpha^*}}{(k-1)!}}.$$

In Theorem 1 above, the term $\frac{1}{s!} \cdot \frac{{K_n}^{2s}}{{P_n}^{s}}$ in Equation (1) is an asymptotics of the edge probability (i.e., the probability for the existence of an edge between two nodes). If we replace (1) by the condition of the edge probability being $\frac{\ln n + (k-1) \ln \ln n + \alpha_n}{n}$, Theorem 1 still follows. Theorem 1 shows that random s-intersection graphs exhibit a phase transition for k-connectivity, and in view of the above, a critical threshold of the edge probability for k-connectivity is $\frac{\ln n + (k-1) \ln \ln n}{n}$, which is the same as Erdős–Rényi graphs [4].

References

[1] F. Ball, D. Sirl, and P. Trapman, "Epidemics on random intersection graphs," *The Annals of Applied Probability*, vol. 24, pp. 1081–1128, 2014.

[2] S. Blackburn, D. Stinson, and J. Upadhyay, "On the complexity of the herding attack and some related attacks on hash functions," *Designs, Codes and Cryptography*, vol. 64, no. 1-2, pp. 171–193, 2012.

[3] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *IEEE Symposium on Security and Privacy*, 2003.

[4] P. Erdős and A. Rényi, "On the strength of connectedness of random graphs," *Acta Mathematica Academiae Scientiarum Hungaricae*, pp. 261–267, 1961.

[5] L. Eschenauer and V. Gligor. A key-management scheme for distributed sensor networks. In *ACM Conference on Computer and Communications Security*, 2002.

[6] K. Singer-Cohen, *Random intersection graphs*. PhD thesis, Department of Mathematical Sciences, The Johns Hopkins University, 1995.

[7] J. Zhao, O. Yağan, and V. Gligor. On the strengths of connectivity and robustness in general random intersection graphs. In *IEEE Conference on Decision and Control*, 2014.

[8] J. Zhao, O. Yağan, and V. Gligor. Secure k-connectivity in wireless sensor networks under an on/off channel model. In *IEEE International Symposium on Information Theory*, 2013.

[9] J. Zhao, O. Yağan, and V. Gligor. On asymptotically exact probability of k-connectivity in random key graphs intersecting Erdős–Rényi graphs, *arXiv*, 1409.6022 [math.CO], 2014.

[10] J. Zhao, O. Yağan, and V. Gligor. Connectivity in secure wireless sensor networks under transmission constraints. In *Allerton Conference on Communication, Control, and Computing*, 2014.

[11] J. Zhao, O. Yağan, and V. Gligor. On topological properties of wireless sensor networks under the q-composite key predistribution scheme with on/off channels. In *IEEE International Symposium on Information Theory*, 2014.

[12] J. Zhao, O. Yağan, and V. Gligor. On k-connectivity and minimum vertex degree in random s-intersection graphs. In *SIAM Meeting on Analytic Algorithmics and Combinatorics*, 2015.

[13] J. Zhao, O. Yağan, and V. Gligor. Designing securely and reliably connected wireless sensor networks, *arXiv*, 1501.01826 [cs.CR], 2015.