Random Key Predistribution for Wireless Sensor Networks Using Deployment Knowledge

Michał Ren, Adam Mickiewicz University, Poznań, Poland
Joint work with Jerzy Jaworski and Katarzyna Rybarczyk

Sensor networks, that is networks of nodes with sensing ability, and wireless communication capacity are proving very useful in fields of environment and industrial monitoring, as well as security. Since the nodes are assumed to be as cheap as possible (with the so far unattained ideal being "smart dust"), and have limited energy capacity (batteries), they can not perform many operations nor standard protocols used to ensure security in more capable devices. Of particular interest is the problem of key distribution in wireless sensor networks, made difficult by lack of, or very limited, ability to perform public-key operations as well as vulnerability to node compromise – the nodes can not be tamper-resistant, so physical compromise of a node compromises all of its key material. Previous work in this area has mostly concentrated on the so-called random key predistribution methods, introduced by Eschenauer and Gligor [10].

Numerous enhancements to the random key predistribution methods have been proposed, chief among them the utilization of Blom's scheme [1] to decrease the memory consumption and communication overhead as well as ensuring that as long as the number of compromised nodes remains under a certain threshold, the scheme remains secure [8], or using polynomial-based threshold schemes [5] to achieve the same improvements [12].

An interesting class of approaches to the problem has emerged, which aims to improve the properties of key distribution schemes by utilizing deployment knowledge, that is knowledge of the physical location of the nodes. The most commonly considered schemes make use of threshold key predistribution schemes based on Blom's scheme, and use a square deployment grid [9]. Only a few proposals exist for non-square deployment grid models with no analytical results but rather simulation ones, some utilizing Blom's scheme [14], and some utilizing polynomial threshold schemes [11, 15].

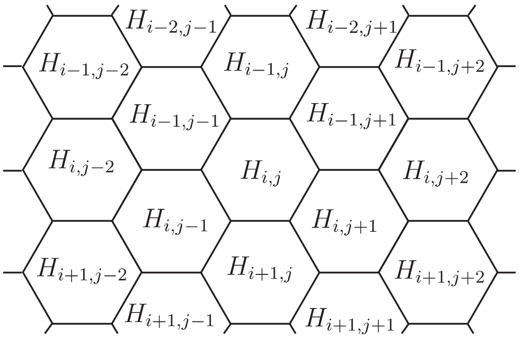

Figure 1. Arrangement of hexagonal clusters

We consider the following model of the sensor grid. The area on which sensor nodes are deployed consists of hexagons (see fig. 1), with sensor deployment points corresponding to centers of the hexagons. It is assumed that the communication range (both for sending and receiving) of sensor nodes is equal to the circumradius of the hexagon. More precisely, lest s be communication range, let $\mathcal{H}$ be the division of the deployment area into hexagons, each with edge length of $\frac{s}{2}$. We will call $\mathcal{H}$ a hexagon grid. Let $\mathcal{H}^+$ be $\mathcal{H}$ with added hexagons, adjacent to the border hexagons of $\mathcal{H}$. To each of the hexagons in $\mathcal{H}$ and $\mathcal{H}^+$ we may assign coordinates $(i,j) \in I$ and $(i,j) \in I^+$, respectively (see fig. 1). To each hexagon $H_{i,j} \in \mathcal{H}^+$ we will assign a set $S_{i,j}$ of m keys (for different heksagons those sets will be disjoint) and we will attribute a set $V_{i,j}$ of N sensors to each hexagon $H_{i,j} \in \mathcal{H}$. Moreover, each sensor $v \in V_{i,j}$ will be deployed over a middle point of a hexagon $H_{i,j}$. We will assume that the place in the deployment area in which it lands will be given according to Gaussian distribution with arbitrary parameters (in fact all the calculations work for any distribution with the center of symmetry in the middle point of the hexagon).

Each cluster $H_{i,j}$ is assigned a key pool $S_{i,j}$, which is a disjoint subset of keys from the total network key pool. Every sensor node deployed over the center of cluster $H_{i,j}$ is randomly assigned d keys from each of the key pools: $S_{i-1,j-1}, S_{i-1,j}, S_{i-1,j+1}, S_{i,j-1}, S_{i,j}, S_{i,j+1}, S_{i+1,j}$. No keys from other pools are assigned to the nodes, and every node ends up with exactly $7d$ keys. We assume that two nodes can communicate if they are in wireless communication range and they share at least one key. We are interested in assuring that with high probability, a large fraction of the nodes can communicate. Communication must be assured both between the nodes in every hexagonal cluster and between nodes of neighboring clusters, in order to enable global and local connectivity of the network. Therefore we are interested in the connectivity of the random graph defined as follows:

Definition 1. The Wireless Sensor Network Graph G_{WSN} we will call a random graph with the vertex set $\bigcup_{(i,j)\in I} V_{i,j}$ and the edge set $E_{WSN} = \{(v,v') : v, v' \in \bigcup_{(i,j)\in I} V_{i,j}, D(v) \cap D(v') \neq \emptyset \text{ and } d(v,v') \leq s\}$ where $D(v)$ is a set of keys assigned to $v \in V_{i,j}$, according to the following procedure: For every $(i,j) \in I$, every $v \in V_{i,j}$ will be assigned a pool of d keys from each of the key pools $S_{i-1,j-1}, S_{i-1,j}, S_{i-1,j+1}, S_{i,j-1}, S_{i,j}, S_{i,j+1}, S_{i+1,j}$. For a given key pool $S \in \{S_{i-1,j-1}, S_{i-1,j}, S_{i-1,j+1}, S_{i,j-1}, S_{i,j}, S_{i,j+1}, S_{i+1,j}\}$ d keys will be chosen uniformly at random from all d-element subsets of S independently of all other key pools and sensors.

For analysis of local connectivity, that is communication inside the hexagonal cluster where all nodes are within wireless communication range, we use the random intersection graph model. It has only recently been used to model sensor network connectivity properties [4, 13], and while it is more difficult to analyze, it represents the random predistribution model for sensor networks much more accurately than the $G(n,p)$ model [10] previously used in literature. Our model and its analysis differ from [4, 13] in that nodes are not assigned keys from the common pool – two different nodes in one hexagonal cluster can have keys chosen from different pools if their intended deployment points were different. Although, due to their wide application, many other generalized models of random intersection graph have been studied recently (for example [2, 3, 6, 7]), all of them assume that each node chooses its keys from the same key pool. In our work we give preliminary results regarding connectivity and the diameter (the number of hops that messages have to pass through to travel through the network) of the random intersection graph corresponding to the hexagonal cluster. We establish relations between the key pool size $|S|$, the number of chosen keys d and number of nodes, which ensures efficient communication in the cluster.

For analysis of global connectivity we will use the results of the local connectivity, and an estimation of probability of the possibility of communication between nodes in neighboring hexagons. We will therefore give asymptotic results showing how to pick parameters (key pool size $|S|$, the number of chosen keys d) depending on the number of deployed nodes in order to assure global connectivity of the network, and estimate the diameter of the network for the given parameters.

We prove the following two theorems:

Theorem 1. *Let $\varepsilon > 0, d = \lceil \sqrt{m \ln m} \rceil, N \leq m, 2d < m$. Then, with probability at least*

(1)
$$1 - \frac{h(\mathcal{H})(N+3)}{m^4} - 6h(\mathcal{H})\left(1-p''\right)^N - h(\mathcal{H})\left(1-p\right)^N - e^{-\frac{\varepsilon^2}{2}N(h(\mathcal{H})-b(\mathcal{H}))(p+6p')} - e^{-\frac{\varepsilon^2}{2}Nb(\mathcal{H})(p+3p')}$$

the giant component of G_{WSN} is of size at least

$$(1-\varepsilon)N((p+6p')h(\mathcal{H}) - 3p'b(\mathcal{H})) \tag{2}$$

and has diameter at most $2\,diam(\mathcal{H}) + 3$.

Theorem 2. *Let $N \to \infty, N \ln N = o(m), b(\mathcal{H}) = o(h(\mathcal{H})), h(N) = h(\mathcal{H})$ be any function tending to infinity but slower than N^δ for any $\delta > 0$. If*

$$\liminf_{N\to\infty} \frac{d^2 N}{m \ln N}\,(4p + 20p') > 1$$

then with probability tending to one as $N \to \infty$ the largest connected component is of size at least

$$(1 - o(1))Nh(N)(p + 6p')$$

Where $diam(\mathcal{H})$ is the diameter of the hexagonal grid graph (i.e. number of the edges between hexagons that should be crossed to travel between two most distant hexagons), $h(\mathcal{H})$ – the number of hexagons in $\mathcal{H}$, $b(\mathcal{H})$ – the number of border hexagons in $\mathcal{H}$, p – the probability that a sensor will end up in the hexagon over which it was deployed, p' – the probability that a sensor will end up in the given hexagon neighboring to the one over which it was deployed and p'' – the probability that a sensor will end up in the hexagon over which it was deployed and in addition lands in a circle with a center point in the middle point of an edge shared with a given neighboring hexagon.

As far as we are aware, no analytical results for hexagonal random key predistribution schemes for sensor networks have previously appeared in literature. Moreover, we consider the random intersection graph as our theoretical model, which has never been considered in any random key predistribution scheme with deployment knowledge. We are also basing our considerations on a very general key distribution model in which the keys are simply chosen from a key pool, so the results should be applicable for many schemes derived from it.

References

[1] R. Blom, *An optimal class of symmetric key generation systems*, Proc. of the EUROCRYPT 84 workshop on Advances in cryptology: theory and application of cryptographic techniques (New York, NY, USA), Springer-Verlag New York, Inc., 1985, pp. 335–338.

[2] Mindaugas Bloznelis, *Component evolution in a general random intersection graph*, (to appear).

[3] ———, *Degree distribution of a typical vertex in a general random intersection graph*, (to appear).

[4] Mindaugas Bloznelis, Jerzy Jaworski, and Katarzyna Rybarczyk, *Component evolution in a secure wireless sensor networks*, Networks **(to appear)** (2008).

[5] Carlo Blundo, Alfredo De Santis, Ugo Vaccaro, Amir Herzberg, Shay Kutten, and Moti Yong, *Perfectly secure key distribution for dynamic conferences*, Inf. Comput. **146** (1998), no. 1, 1–23.

[6] Tom Britton, Maria Deijfen, Andreas Nordvall Lageras, and Mathias Lindholm, *Epidemics on random graphs with tunable clustering*, arXiv:0708.3939v1 [math.PR] **(submitted)** (2007).

[7] M. Deijfen and W. Kets, *Random intersection graphs with tunable degree distribution and clustering*, CentER Discussion Paper Series **(submitted)** (2007).

[8] Wenliang Du, Jing Deng, Yunghsiang S. Han, Pramod K. Varshney, Jonathan Katz, and Aram Khalili, *A pairwise key predistribution scheme for wireless sensor networks*, ACM Trans. Inf. Syst. Secur. **8** (2005), no. 2, 228–258.

[9] Wenliang Du, Wenliang Du, Jing Deng, Y.S. Han, and P.K. Varshney, *A key predistribution scheme for sensor networks using deployment knowledge*, IEEE Transactions on Dependable and Secure Computing **3** (2006), no. 1, 62–77.

[10] Laurent Eschenauer and Virgil D. Gligor, *A key-management scheme for distributed sensor networks*, CCS '02: Proceedings of the 9th ACM conference on Computer and communications security (New York, NY, USA), ACM Press, 2002, pp. 41–47.

[11] Guorui Li, Guorui Li, Jingsha He, and Yingfang Fu, *A hexagon-based key predistribution scheme in sensor networks*, Proc. ICPP 2006 Workshops Parallel Processing Workshops 2006 International Conference on (Jingsha He, ed.), 2006, pp. 6 pp.–.

[12] Donggang Liu and Peng Ning, *Establishing pairwise keys in distributed sensor networks*, CCS '03: Proceedings of the 10th ACM conference on Computer and communications security (New York, NY, USA), ACM Press, 2003, pp. 52–61.

[13] Roberto Di Pietro, Luigi Mancini, Alessandro Mei, Alessandro Panconesi, and Jaikumar Radhakrishnan, *How to design connected sensor networks that are provably secure*, Proceedings of SecureComm 2006, the 2nd IEEE/CreateNet International Conference on Security and Privacy in Communication Networks, 2006.

[14] Zhou Yun, Zhou Yun, Zhang Yanchao, and Fang Yuguang, *Key establishment in sensor networks based on triangle grid deployment model*, Proc. IEEE Military Communications Conference MILCOM 2005 (Yanchao Zhang, ed.), 2005, pp. 1450–1455 Vol. 3.

[15] ———, *LLK: a link-layer key establishment scheme for wireless sensor networks*, Proc. IEEE Wireless Communications and Networking Conference (Yanchao Zhang, ed.), vol. 4, 2005, pp. 1921–1926 Vol. 4.