Reliability of Wireless Sensor Networks under a Heterogeneous Key Predistribution Scheme

Rashad Eletreby* and Osman Yağan

Dept. of ECE
Carnegie Mellon University

Supported by NSF CCF #1617934 and by a generous gift from Persistent Systems, Inc.
Wireless sensor networks (WSNs)

- Distributed collection of sensor nodes that are of low-cost, small-size, and limited capabilities
- Facilitate a broad range of applications, e.g., medical, environmental, industrial, military, etc.
- WSNs may be deployed in hostile environments → eavesdropping and node-capture attacks are possible

Cryptographic protection is needed

- Asymmetric (Public-key) cryptosystems → excessive energy consumption and computation overhead
- Symmetric cryptosystems → faster, energy-efficient, feasible choice for securing wireless sensor networks\(^1\)

\(^1\)Laurent Eschenauer and Virgil D. Gligor “A key-management scheme for distributed sensor networks” (ACM CCS ’02)
Key management

**Key predistribution**: practical option for key distribution of large-scale sensor networks

- Single mission key $\rightarrow$ an adversary can compromise the whole network by capturing one node
- Pair-wise keys $\rightarrow$ huge memory, severely limits network dynamics, requires $\binom{n}{2}$ keys in total
- Location-dependent key predistribution $\rightarrow$ unknown network topology prior to deployment
Random key predistribution schemes

- Introduced in the seminal work of Eschenauer-Gligor\(^1\)
- Each node is assigned \(K\) cryptographic keys at random from a key pool of size \(P\)
- Two nodes can securely communicate only if they share a key

---

\(^{1}\text{Laurent Eschenauer and Virgil D. Gligor. 2002. “A key-management scheme for distributed sensor networks” (ACM CCS ’02)}\)
The heterogeneous random key predistribution scheme

- Proposed by Yaşan\(^1\) as a generalization to the classical Eschenauer-Gligor scheme
- Facilitates networks with varying level of resources, connectivity and security requirements, e.g., regular nodes and cluster heads
- Each node is randomly assigned to one of \(r\) possible classes
- A class-\(i\) node selects \(K_i\) keys at random from a large key pool of size \(P\)
- Two nodes can securely communicate only if they share a key

Shared-key connectivity: A crucial requirement

- Given the randomness involved $\implies$ A pair of nodes may not share a key $\implies$ Is the resulting network connected?
- If the network is connected, then there is a secure path between every pair of nodes

How should we adjust the number of keys and the size of the key pool $P$ to ensure shared-key connectivity?
Shared-key connectivity: A crucial requirement

How should we adjust the number of keys and the size of the key pool $P$ to ensure shared-key connectivity?

- Yağan\(^1\) proposed scaling conditions on $K_1, \ldots, K_r, P$ as functions of the network size $n$ such that the network is connected with high probability as $n$ gets large.

Shared-key connectivity is not sufficient

- Shared-key connectivity is **crucial**, but it assumes that all wireless links are available and **reliable**
- A wireless link connecting a pair of key-sharing nodes may fail for various reasons

**Shared-key connectivity** $\not\iff$ **Actual network connectivity**

The failure of this link renders the network disconnected
The notion of reliability

- A network is reliable if it preserves its operation despite the failure of some wireless links $\iff$ remains connected.

- **A simple model:** Assume that each wireless link fails with probability $1 - \alpha$ independently.

  Does the network remain connected?
Objective

- How should the number of keys $K_1, K_2, \ldots, K_r$ and the size of the key pool $P$ be selected to ensure network **reliability** against random link-failures?

How can we scale $K_1, K_2, \ldots, K_r, P, \alpha$ with the network size $n$ such that

$$\lim_{n \to \infty} P[\text{NETWORK RELIABILITY}] = 1$$
Approach: Random graph modeling and analysis

Our approach is based on:

▶ Modeling the network by an appropriate random graph

▶ Establishing scaling conditions on the model parameters such that the network is reliable with high probability
Random graphs

- **Sampling viewpoint**: A random graph is a graph that is obtained by randomly sampling from a collection of graphs, e.g., $G(n, m)$

- **Construction viewpoint**: Start with a vertex set then connect edges according to a probabilistic rule, e.g., $G(n, p)$
The inhomogeneous random key graph 
\( \mathbb{K}(n; \mu, K, P) \)^1

- Models the heterogeneous random key predistribution scheme
- Vertex set \( V = \{v_1, \ldots, v_n\} \) where \( n \) denotes the graph size
- Given \( r \) classes, each vertex \( v_x \) is classified as class-\( i \) with probability \( \mu_i > 0 \) \( \implies \sum_{i=1}^{r} \mu_i = 1 \)
- A class-\( i \) vertex \( v_x \) is given set \( \Sigma_x \) of \( K_i \) objects drawn uniformly at random (without replacement) from an object pool of size \( P \)

Two distinct nodes \( v_x \) and \( v_y \) are adjacent, denoted by the event \( K_{xy} \), if they share an object \( \implies K_{xy} := [\Sigma_x \cap \Sigma_y \neq \emptyset] \)

---

Edge probability of $\mathbb{K}(n; \mu, K, P)$

- Let $t_x$ denote the class of an arbitrary node $v_x$ and $p_{ij} := \mathbb{P}[K_{xy} | t_x = i, t_y = j]$

- $(\frac{P - K_j}{K_i}) / (\frac{P}{K_i}) \implies$ probability that a random subset of $K_i$ objects is disjoint from a subset of $K_j$ objects

- We have

$$p_{ij} = 1 - \left( \frac{P - K_j}{K_i} \right) / \left( \frac{P}{K_i} \right)$$
Let $\lambda_i$ denote the edge probability of an arbitrary class-\(i\) node in $\mathbb{K}$. We have

$$
\lambda_i = \mathbb{P} [ K_{xy} \mid t_x = i ]
$$

$$
= \sum_{j=1}^{r} \mathbb{P} [ K_{xy} \mid t_x = i, t_y = j ] \mathbb{P} [ t_y = j ]
$$

$$
= \sum_{j=1}^{r} \mu_j p_{ij}
$$
Erdős-Rényi graph $\mathbb{G}(n; \alpha)$

- A simple model for random link-failures
- Vertex set $\mathcal{V} = \{v_1, v_2, \ldots, v_n\}$
- Start with a complete graph on $\mathcal{V}$. Then, remove each edge independently with probability $1 - \alpha$

Two distinct nodes $v_x$ and $v_y$ are adjacent, denoted by the event $C_{xy}$ if the edge connecting them was not deleted

$$\mathbb{P}[C_{xy}] = \alpha$$

- Class-independent
The composite graph $\mathbb{H}(n; \mu, K, P, \alpha)$

- We consider a composite graph
  \[ \mathbb{H}(n; \mu, K, P, \alpha) := K(n; \mu, K, P) \cap G(n; \alpha) \]

- Two nodes are adjacent in $\mathbb{H}(n; \mu, K, P, \alpha)$ if and only if they are adjacent in both $K(n; \mu, K, P)$ and $G(n; \alpha)$
The composite graph $\mathbb{H}(n; \mu, K, P, \alpha)$

- The intersection of $\mathbb{K}(n; \mu, K, P)$ with $G(n; \alpha)$ models the case when each link of $\mathbb{K}(n; \mu, K, P)$ fails independently with probability $1 - \alpha$.
- If $\mathbb{H}(n; \mu, K, P, \alpha)$ is connected $\implies \mathbb{K}(n; \mu, K, P)$ remains connected despite the random failure of links.

**Network Reliability $\equiv$ Connectivity of $\mathbb{H}(n; \mu, K, P, \alpha)$**

- A graph is connected when there is a path between every pair of vertices.
Edge probability of $\mathbb{H}(n; \mu, K, P, \alpha)$

- Recall that $t_x$ denotes the class of an arbitrary node $v_x$

  Two arbitrary nodes $v_x$ and $v_y$ are adjacent in the intersecting graph $\mathbb{H}$, denoted by the event $E_{xy}$, if they are adjacent in both $K$ and $G$ \( \implies E_{xy} := [K_{xy} \cap C_{xy}] \)

- We have

  \[
  \mathbb{P} \left[ E_{xy} \mid t_x = i, t_y = j \right] = \mathbb{P} \left[ C_{xy} \cap K_{xy} \mid t_x = i, t_y = j \right] \\
  = \mathbb{P} \left[ C_{xy} \right] \mathbb{P} \left[ K_{xy} \mid t_x = i, t_y = j \right] \\
  = \alpha p_{ij}
  \]
Edge probability of \( \mathbb{H}(n; \mu, K, P, \alpha) \)

- Let \( \Lambda_i \) denote the edge probability of an arbitrary class-\( i \) node in \( \mathbb{H} \). We have

\[
\Lambda_i = \mathbb{P} \left[ E_{xy} \mid t_x = i \right]
\]

\[
= \sum_{j=1}^{r} \mathbb{P} \left[ E_{xy} \mid t_x = i, t_y = j \right] \mathbb{P} [t_y = j]
\]

\[
= \sum_{j=1}^{r} \mu_j \alpha P_{ij} = \alpha \mathbb{P} \left[ K_{xy} \mid t_x = i \right] = \alpha \lambda_i
\]

where \( \lambda_i \) denotes the edge probability of an arbitrary class-\( i \) node in \( \mathbb{K} \)

- \( K_1 \leq \ldots \leq K_r \implies \lambda_1 \leq \ldots \leq \lambda_r \implies \Lambda_1 \leq \ldots \leq \Lambda_r \)
A zero-one law for connectivity of \( \mathcal{H}(n; \mu, K, P, \alpha) \)

Theorem

Consider a probability distribution \( \mu = \{\mu_1, \ldots, \mu_r\} \) with \( \mu_i > 0 \) for \( i = 1, \ldots, r \), a scaling \( K, P : \mathbb{N}_0 \rightarrow \mathbb{N}_0^{r+1} \), and a scaling \( \alpha : \mathbb{N}_0 \rightarrow (0, 1) \) such that

\[
\Lambda_1(n) = \alpha_n \lambda_1(n) \sim c \log n \frac{\log n}{n}
\]

edge prob. of class-1 nodes

holds for some \( c > 0 \). Then, we have

\[
\lim_{n \rightarrow \infty} \mathbb{P}[\mathcal{H}(n; \mu, K_n, P_n, \alpha_n) \text{ is connected}] = \begin{cases} 
0 & \text{if } c < 1 \\
1 & \text{if } c > 1 
\end{cases}
\]

under few extra conditions.

\(^1\)R. Eletreby and O. Yağan, “On the network reliability problem of the heterogeneous key predistribution scheme” (IEEE CDC 2016)
Equivalent scaling

- If $\lambda_1(n) = o(1)$, we can express our scaling condition in simple terms, namely

$$\frac{K_{\min,n} K_{\text{avg},n}}{P_n} \sim c \frac{\log n}{n^{\alpha_n}}$$

- If all links are reliable, i.e., $\alpha_n = 1$ for $n = 1, 2, \ldots$, our scaling condition reduces to the scaling condition given by Yağan¹ for the shared-key connectivity

$$\frac{K_{\min,n} K_{\text{avg},n}}{P_n} \sim c \frac{\log n}{n}$$

---

The finite case: Probability of connectivity

Recall that
\[ \frac{K_{1,n}K_{\text{avg},n}}{P_n} \sim c \frac{\log n}{n^{\alpha_n}} \]

Figure: Empirical probability that \( \mathbb{H}(n; \mu, K, P, \alpha) \) is connected with \( n = 500, \mu = (1/4, 1/4, 1/4, 1/4), K = (K_1, K_1 + 5, K_1 + 10, K_1 + 15), \) and \( P = 10^4. \) For each parameter pair \((K, \alpha)\), 200 independent samples of the graph \( \mathbb{H}(n; \mu, K, P, \alpha) \) are generated.
The finite case: Importance of $K_1$

- Recall that $\frac{K_1, nK_{\text{avg}}, n}{P_n} \sim c \frac{\log n}{n^{\alpha n}}$

---

**Figure:** Empirical probability that $\mathbb{H}(n; \mu, K, P, \alpha)$ is connected with $n = 500$, $\mu = (1/2, 1/2)$, and $P = 10^4$; we consider four choices of $K = (K_1, K_2)$ each with the same mean. For each parameter pair $(K, \alpha)$, 200 independent samples of the graph $\mathbb{H}(n; \mu, K, P, \alpha)$ are generated.
Ongoing and future work

- **A stronger notion of reliability**\(^1\) \implies \text{Reliability against both link and node failures}
  - If \(\mathbb{H}(n; \mu, K, P, \alpha)\) is \(k\)-connected with high probability, then the network is reliable against i) the random failure of each link and ii) the failure of any \(k - 1\) nodes

- **A general model for random link failures**\(^2\)
  - A link between nodes of class-\(i\) and class-\(j\) fails with probability \(1 - \alpha_{ij}\) independently \(\implies \alpha = [\alpha_{ij}]\)
  - \(\mathbb{H}(n; \mu, K, P, \alpha) := K(n; \mu, K, P) \cap G(n; \alpha)\)

- **A new approach to modeling complex networks**
  \implies Using graph union and intersection to generate network models with a rich mixture of structural properties

---

\(^1\)IEEE ISIT 2016 and IEEE ISIT 2017

\(^2\)Allerton 2016 and IEEE ISIT 2017
Thank You!

www.andrew.cmu.edu/~reletreb