Modeling Key Infection in Large-Scale Sensor Networks

Feiyang Peng, Zhihong Liu(✉), Yong Zeng, and Jialei Wang

School of Cyber Engineering, Xidian University, Xi'an, China
liuzhihong@mail.xidian.edu.cn

Abstract. Key infection is a lightweight security protocol suitable for large-scale sensor networks. In this paper, we first derive a probabilistic model to analyze the security of key infection, then propose a group based key infection to improve its security performance.

Keywords: Key management · Key infection · Secrecy amplification
Sensor networks

1 Introduction

Typically, a sensor network is composed of a large number of sensor nodes; each sensor node is a small, inexpensive wireless device with limited battery power, memory storage, data processing capacity and short radio transmission range. Additionally, sensor networks are often operated on an unattended mode and sensors are not tamper resistant. This makes sensor networks more vulnerable than traditional wireless networks.

The first practical key predistribution scheme [1,2] for sensor networks is random key pre-distribution scheme introduced by Eschenauer and Gligor [3] and was investigated by Yağan and Makowski [4]. A major advantage of this scheme is the exclusion of the base station in key management. Another category scheme is location based key pre-distribution [5,6], which takes advantage of sensor deployment information to improve the network performance. Location based schemes can reach the same connectivity with fewer keys stored in sensors than previous schemes.

In this paper, we are interested in very simple sensors and a large number of them in a network. The number is such that it is infeasible to deploy every sensor node manually. Deployment in batches implies self-organizing network that is automatically and autonomously established upon physical deployment. Large number of sensors make it also hard to change code or data stored in every sensor, it is much easier to mass-produce sensors that are identical even on firmware and data level.

Key infection [7] is a lightweight security protocol suitable for large-scale sensor networks and is based on the assumption that, during the network deployment phase, the adversary can monitor only a fixed percentage of communication

S. Qing et al. (Eds.): ICICS 2017, LNCS 10631, pp. 265–275, 2018.
https://doi.org/10.1007/978-3-319-89500-0_24

channels. Sensors simply broadcast keys in clear to all their neighbors. The plaintext key exchange is not much useful in common scenarios but when this process starts in hundred thousands instances at a time, it becomes extremely difficult for the adversary to compromise large fraction keys of the network.

To analyze key infection protocol, we propose a probability model of key infection. This model can help designers to evaluate key infection and adapt it to their needs. Then, a group based key infection protocol is proposed to improve the security performance of key infection.

2 Network Model and Security Assumptions

We consider a large-scale uniformly and densely distributed sensor network that monitors a vast terrain via a large number of static sensors, which can be deployed through approaches such as aerial scattering. No topology information is available before deployment. Eavesdroppers are also distributed uniformly over the same field. As depicted in Fig. 1, a sensor transmits a key in plaintext to its neighbor, any eavesdropper located in the transmission range can learn this key. However, a global passive adversary that can monitor all communications everywhere in the deployment region at all times is a too-strong security model. We adopt the attacker model [7] as follows:

- The attacker can deploy some eavesdroppers in the field and is able to monitor only a small proportion of the communications of the sensor network during the deployment phase. After key exchange is complete, she is able to monitor all communications at will;
- The attacker is passive, and does not execute active attacks (such as jamming or flooding) during the deployment phase.

Throughout the sequel, sensors are deployed randomly with locations assumed to be drawn independently from the uniform distribution in the field. The distance between two sensors i and j is denoted as $\|i - j\|$.

Let $\mathbf{X}$ be the point in the field, for $r \geq 0$, let $\mathbb{R}_i(r) = \{\mathbf{X} : \|\mathbf{X} - i\| \leq r\}$ for the disk of radius r centered at i, and in a slight abuse of notation, for

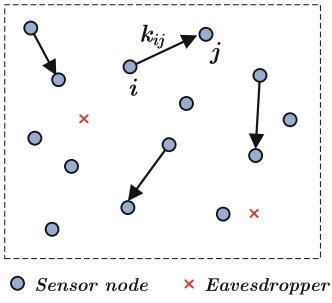


Fig. 1. Example of key infection.

any $r_1, r_2 \geq 0$, write $\mathbb{R}_{ij}(r_1, r_2) = \{\mathbf{X} : \|\mathbf{X} - i\| \leq r_1 \text{ and } \|\mathbf{X} - j\| \leq r_2\}$ for the overlap region of $\mathbb{R}_i(r_1)$ and $\mathbb{R}_j(r_2)$, write $\mathbb{R}_{i\bar{j}}(r_1, r_2) = \{\mathbf{X} : \|\mathbf{X} - i\| \leq r_1 \text{ and } \|\mathbf{X} - j\| > r_2\}$ for the region $\mathbb{R}_i(r_1) \backslash \mathbb{R}_j(r_2)$, write $\mathbb{R}_{ij\bar{k}}(r_1, r_2, r_3) = \{\mathbf{X} : \|\mathbf{X} - i\| \leq r_1, \|\mathbf{X} - j\| \leq r_2 \text{ and } \|\mathbf{X} - k\| > r_3\}$ for the region $\mathbb{R}_{ij}(r_1, r_2) \backslash \mathbb{R}_k(r_3)$. If $r_1 = r_2 = r$, write $\mathbb{R}_{ij}(r_1, r_2) = \mathbb{R}_{ij}(r)$ for short. We also write $\mathbb{A}_i(r)$ for the area of region $\mathbb{R}_i(r)$, $\mathbb{A}_{ij}(r_1, r_2)$ for the area of region $\mathbb{R}_{ij}(r_1, r_2)$. In an extension of this notation, $\mathbb{A}_{ij\bar{k}}(r_1, r_2, r_3)$ denotes the area of the region $\mathbb{R}_{ij\bar{k}}(r_1, r_2, r_3) = \mathbb{R}_{ij}(r_1, r_2) \backslash \mathbb{R}_k(r_3)$.

3 Background of Key Infection

Basic Key Infection. The idea of basic key infection (B-KI) [7] is to propagate keying material after deployment: each sensor simply chooses a key and broadcasts it in plaintext to its neighbors.

Assume sensor i, when it comes to rest after deployment, broadcasts a key k_i and is heard by sensor j. Sensor j then generates a key k_{ji} and sends to i: $\{j, k_{ji}\}_{k_i}$. Later on, the key k_{ji} can be used to protect communication link between sensors i and j.

Whispering Key Infection. Whispering key infection (W-KI) [7] makes a small change to improve the performance of the basic key infection. Instead of each sensor broadcasting a key as loudly as it can, it starts off transmitting very quietly and steadily increases the power until a response is heard. This whispering key infection ensures that two sensors W_1 or W_2 within the range of each other will exchange a secure key provided that an eavesdropper is further away from either W_1 or W_2 than the distance between W_1 and W_2.

Secrecy Amplification. Secrecy amplification (SA-KI) [7] utilizes multipath key establishment to improve the security of basic key infection. Suppose that sensors W_1, W_2, and W_3 are neighbors. W_1 and W_2 share key k_{12}, W_1 and W_3 share key k_{13}, W_2 and W_3 share key k_{23}. To amplify the secrecy of key k_{12}, W_1 ask W_3 to exchange an additional key with W_2 as following:

$$\begin{aligned} W_1 \rightarrow W_3 &: \{W_1, W_2, N_1\}_{k_{13}} \\ W_3 \rightarrow W_2 &: \{W_1, W_2, N_1\}_{k_{23}} \\ W_2 \text{ computes} &: k'_{12} = H(k_{12}||N_1) \\ W_2 \rightarrow W_1 &: \{N_1, N_2\}_{k'_{12}} \\ W_1 \rightarrow W_2 &: \{N_2\}_{k'_{12}} \end{aligned}$$

where N_1 and N_2 are nonces, $\{M\}_{k_i}$ represents the encrypted message M using key k_i, and $H(.)$ is a hash function. After the protocol terminates, W_1 and W_2 update their key from k_{12} to $k'_{12} = H(k_{12}||N_1)$.

4 Probability Model of Key Infection

4.1 Basic Key Infection

Let n sensors with communication radius R be distributed over a field of size S, t be the number of eavesdroppers in the field. As depicted in Fig. 2, two adjacent sensors i and j exploit B-KI to establish a secure key. The adversary, in order to eavesdrop the key setup process, should place at least one eavesdropper in region $\mathbb{R}_{ij}(R)$, or one eavesdropper in region $\mathbb{R}_{i\bar{j}}(R)$ and another in region $\mathbb{R}_{\bar{i}j}(R)$ simultaneously.

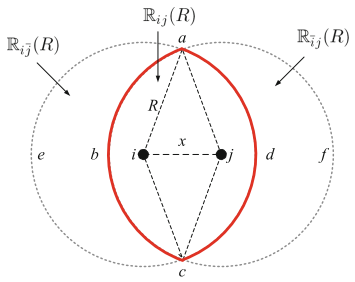


Fig. 2. Two adjacent sensors i and j in B-KI.

Let $\|i-j\| = x$, the cumulative distribution function of x is given by $F(x) = \mathbf{P}\{\|i-j\| \le x\} = x^2/R^2$, and its probability density function is $f(x) = F'(x) = 2x/R^2$. The area of the overlap region $\mathbb{R}_{ij}(R)$ is $\mathbb{A}_{ij}(R) = 2R^2 \cos^{-1}\frac{x}{2R} - x\sqrt{R^2 - \frac{x^2}{4}}$, and its expectation is

$$\mathbf{E}[\mathbb{A}_{ij}(R)] = \int_0^R \mathbb{A}_{ij}(R)\frac{2x}{R^2}\mathrm{d}x = \left(\pi - \frac{3\sqrt{3}}{4}\right)R^2 \approx 0.5865\pi R^2.$$

Therefore, the probability $\mathbf{P}\{b\}$ that there are exactly b eavesdroppers in the overlap region $\mathbb{R}_{ij}(R)$ is

$$\mathbf{P}\{b\} = \binom{t}{b}\left(\frac{\mathbf{E}[\mathbb{A}_{ij}(R)]}{S}\right)^b\left(1 - \frac{\mathbf{E}[\mathbb{A}_{ij}(R)]}{S}\right)^{t-b},$$

and the probability of at least one eavesdropper located inside the interior of region $\mathbb{R}_{ij}(R)$ is

$$\begin{aligned}\mathbf{P}_{\mathbb{R}_{ij}(R)} &= 1 - \mathbf{P}\{b=0\} = 1 - \left(1 - \frac{\mathbf{E}[\mathbb{A}_{ij}(R)]}{S}\right)^t \\ &\approx 1 - \left(1 - \frac{0.5865\pi R^2}{S}\right)^t.\end{aligned}$$

Let n' denote the average number of neighbors of a sensor. Because the sensors are distributed over the field uniformly, when $n \gg n'$ and $S \gg \pi R^2$, we have $\frac{\pi R^2}{S} = \frac{n'+1}{n} \approx \frac{n'}{n}$. It follows that, the probability $\mathbf{P}_{\mathbb{R}_{ij}(R)}$ can be approximated as $\mathbf{P}_{\mathbb{R}_{ij}(R)} = 1 - (1 - 0.5865 \cdot \frac{n'}{n})^t$.

Again, as estimated above, we can obtain $\mathbf{E}[\mathbb{A}_{i\bar{j}}(R)] = \mathbf{E}[\mathbb{A}_{\bar{i}j}(R)] = \pi R^2 - \mathbf{E}[\mathbb{A}_{ij}(R)] = 0.4135\pi R^2$, and

$$\mathbf{P}_{\mathbb{R}_{i\bar{j}}(R)} = \mathbf{P}_{\mathbb{R}_{\bar{i}j}(R)} = 1 - \left(1 - 0.4135 \cdot \frac{n'}{n}\right)^t.$$

Let $\mathbb{B}_{ij}$, $\mathbb{B}_{i\bar{j}}$, and $\mathbb{B}_{\bar{i}j}$ be events that the adversary has placed eavesdroppers in regions $\mathbb{R}_{ij}(R)$, $\mathbb{R}_{i\bar{j}}(R)$, and $\mathbb{R}_{\bar{i}j}(R)$, respectively. Clearly, $\mathbb{B}_{ij}$, $\mathbb{B}_{i\bar{j}}$, and $\mathbb{B}_{\bar{i}j}$ are independent. Therefore, the event $\mathbb{B}$ that the link key between i and j is broken in B-KI is $\mathbb{B} = \mathbb{B}_{ij} \cup (\mathbb{B}_{i\bar{j}} \cap \mathbb{B}_{\bar{i}j})$. Therefore

$$\mathbf{P}\{\mathbb{B}\} = \mathbf{P}\{\mathbb{B}_{ij}\} + \mathbf{P}\{\mathbb{B}_{i\bar{j}}\mathbb{B}_{\bar{i}j}\} - \mathbf{P}\{\mathbb{B}_{ij}\mathbb{B}_{i\bar{j}}\mathbb{B}_{\bar{i}j}\}.$$

Thus, as to the basic key infection B-KI, the outage probability $\mathbf{P}_{B-KI}$ that the link key between a pair of sensors is compromised, is equal to the probability that event $\mathbb{B}$ occurs. More preciously,

$$\mathbf{P}_{B-KI} = \mathbf{P}_{\mathbb{R}_{ij}(R)} + \mathbf{P}_{\mathbb{R}_{i\bar{j}}(R)} \cdot \mathbf{P}_{\mathbb{R}_{\bar{i}j}(R)} - \mathbf{P}_{\mathbb{R}_{ij}(R)} \cdot \mathbf{P}_{\mathbb{R}_{i\bar{j}}(R)} \cdot \mathbf{P}_{\mathbb{R}_{\bar{i}j}(R)}.$$

It will be convenient to introduce a new notation, $\varphi(x_1, x_2, \ldots, x_n) = \varphi(x_1) \cdot \varphi(x_2) \cdots \varphi(x_n)$, where $\varphi(x) = 1 - (1 - x \cdot \frac{n'}{n})^t$. Then, the outage probability $\mathbf{P}_{B-KI}$ can be expressed as

$$\mathbf{P}_{B-KI} = \varphi(0.5865) + \varphi^2(0.4135) - \varphi(0.5865)\varphi^2(0.4135). \tag{1}$$

4.2 Whispering Key Infection

Whispering key infection (W-KI) [7] makes a small change to improve the performance of the basic key infection. Sensor starts off transmitting very quietly and steadily increases the power until a response is heard. We begin by considering the case (denoted as W-KI(2)) that both parties exploit whispering key infection to establish a link key. Consider Fig. 3(a), where $\|i - j\| = x$, we have $\mathbb{A}_{ij}(x) = (\frac{2\pi}{3} - \frac{\sqrt{3}}{2})x^2$, and its expectation

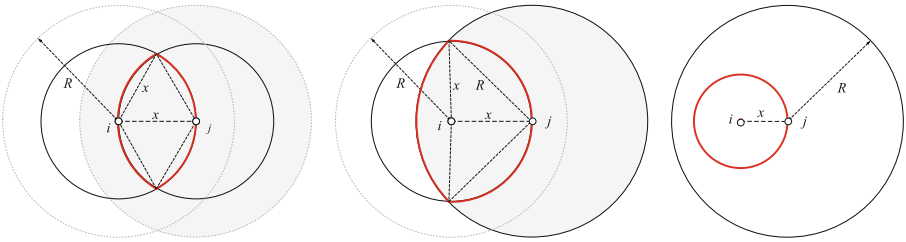
$$\mathbf{E}[\mathbb{A}_{ij}(x)] = \int_0^R \mathbb{A}_{ij}(x)\frac{2x}{R^2}\mathrm{d}x = \left(\frac{\pi}{3} - \frac{\sqrt{3}}{4}\right)R^2 \approx 0.1955\pi R^2.$$

Again, we have $\mathbb{A}_{i\bar{j}}(x) = \mathbb{A}_{\bar{i}j}(x) = (\frac{\pi}{3} + \frac{\sqrt{3}}{2})x^2$, and

$$\mathbf{E}[\mathbb{A}_{i\bar{j}}(x)] = \mathbf{E}[\mathbb{A}_{\bar{i}j}(x)] = \int_0^R \mathbb{A}_{ij}(x)\frac{2x}{R^2}\mathrm{d}x = \left(\frac{\pi}{6} + \frac{\sqrt{3}}{4}\right)R^2 \approx 0.3045\pi R^2.$$

For two parties whispering key infection, W-KI(2), the outage probability $\mathbf{P}_{W-KI(2)}$ that the key is compromised is

$$\begin{aligned}\mathbf{P}_{W-KI(2)} &= \mathbf{P}_{\mathbb{R}_{ij}(x)} + \mathbf{P}_{\mathbb{R}_{i\bar{j}}(x)}\mathbf{P}_{\mathbb{R}_{\bar{i}j}(x)} - \mathbf{P}_{\mathbb{R}_{ij}(x)}\mathbf{P}_{\mathbb{R}_{i\bar{j}}(x)}\mathbf{P}_{\mathbb{R}_{\bar{i}j}(x)} \\ &= \varphi(0.1955) + \varphi^2(0.3045) - \varphi(0.1955)\varphi^2(0.3045) \end{aligned} \tag{2}$$



(a) W-KI(2) (b) W-KI(1) (c) W-KI(1)

Fig. 3. Two adjacent sensors in W-KI(2) and W-KI(1).

Now considering the case that only one party applies whispering key infection, denoted as W-KI(1). As depicted in Fig. 3(b) and (c), sensor i uses whispering key infection to communicate with sensor j, but j communicates with i using the maximum communication radius R. In this case, the area of the lenticular overlap region $\mathbb{R}_{ij}(x, R)$ is

$$\mathbb{A}_{ij}(x,R) = \begin{cases} \pi x^2 & 0 < x \le \frac{R}{2}, \\ g(x) & \frac{R}{2} < x \le R. \end{cases}$$

where, $g(x) = 2x^2 \sin^{-1}\frac{R}{2x} + R^2\cos^{-1}\frac{R}{2x} - \frac{R}{2}\sqrt{4x^2 - R^2}$.

$$\mathbf{E}[\mathbb{A}_{ij}(x,R)] = \int_0^R \mathbb{A}_{ij}(x,R)\frac{2x}{R^2}\mathrm{d}x = \int_0^{\frac{R}{2}} \pi x^2 \frac{2x}{R^2}\mathrm{d}x + \int_{\frac{R}{2}}^R g(x)\frac{2x}{R^2}\mathrm{d}x \approx 0.2932\pi R^2.$$

When $R/2 < x \le R$, $\mathbb{A}_{i\bar{j}}(x,R) = \pi x^2 - g(x)$. So we have

$$\mathbf{E}[\mathbb{A}_{i\bar{j}}(x,R)] = \int_{\frac{R}{2}}^R \mathbb{A}_{i\bar{j}}(x,R)\frac{2x}{R^2}\mathrm{d}x \approx 0.2068\pi R^2,$$

$$\mathbf{E}[\mathbb{A}_{\bar{i}j}(x,R)] = \pi R^2 - \mathbf{E}[\mathbb{A}_{ij}(x,R)] = 0.7068\pi R^2.$$

In consequence, the probability that a key is broken in W-KI(1) is

$$\begin{aligned}\mathbf{P}_{W-KI(1)} &= \mathbf{P}_{\mathbb{R}_{ij}(x,R)} + \mathbf{P}_{\mathbb{R}_{i\bar{j}}(x,R)} \cdot \mathbf{P}_{\mathbb{R}_{\bar{i}j}(x,R)} \\ &\quad - \mathbf{P}_{\mathbb{R}_{ij}(x,R)} \cdot \mathbf{P}_{\mathbb{R}_{i\bar{j}}(x,R)} \cdot \mathbf{P}_{\mathbb{R}_{\bar{i}j}(x,R)} \\ &= \varphi(0.2932) + \varphi(0.2068, 0.7068) \\ &\quad - \varphi(0.2932, 0.2068, 0.7068). \end{aligned} \tag{3}$$

4.3 Secrecy Amplification

Secrecy amplification (SA-KI) [7] utilizes multipath key establishment to make the adversary's job harder. As depicted in Fig. 4, sensors i, j use intermediate sensor k to update their initial key. The communication radius is R, the distances between i and j, i and k, j and k are x, y, z, respectively. We first estimate the area of overlap region $\mathbb{R}_{ijk}(R)$ among three neighboring sensors.

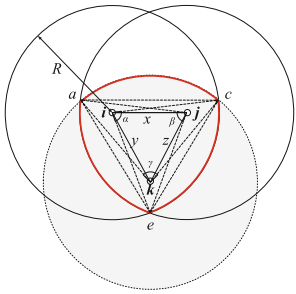


Fig. 4. Three adjacent sensors i, j, and k in SA-KI.

Let $\alpha = \angle cie$, $\beta = \angle aje$, and $\gamma = \angle akc$. Then, $\alpha = \cos^{-1}\frac{x}{2R} + \cos^{-1}\frac{y}{2R} - \cos^{-1}\frac{x^2+y^2-z^2}{2xy}$, $\beta = \cos^{-1}\frac{x}{2R} + \cos^{-1}\frac{z}{2R} - \cos^{-1}\frac{x^2+z^2-y^2}{2xz}$, $\gamma = \cos^{-1}\frac{y}{2R} + \cos^{-1}\frac{z}{2R} - \cos^{-1}\frac{y^2+z^2-x^2}{2yz}$, and the area of $\triangle ace$ is $S_{\triangle ace} = \sqrt{l(l-ce)(l-ae)(l-ac)}$, where $l = \frac{1}{2}(ce + ae + ac)$, $ce = 2R\sin(\alpha/2)$, $ae = 2R\sin(\beta/2)$, $ac = 2R\sin(\gamma/2)$.

The area of region $\mathbb{R}_{ijk}(R)$ shown in Fig. 4 is $\mathbb{A}_{ijk}(R) = S_{\triangle ace} + \frac{R^2}{2}(\alpha + \beta + \gamma - \sin\alpha - \sin\beta - \sin\gamma)$, and

$$\mathbf{E}[\mathbb{A}_{ijk}(R)] = \iiint_0^R \mathbb{A}_{ijk}(R) f(x) f(y) f(z) \mathrm{d}x\mathrm{d}y\mathrm{d}z \approx 0.4942\pi R^2,$$

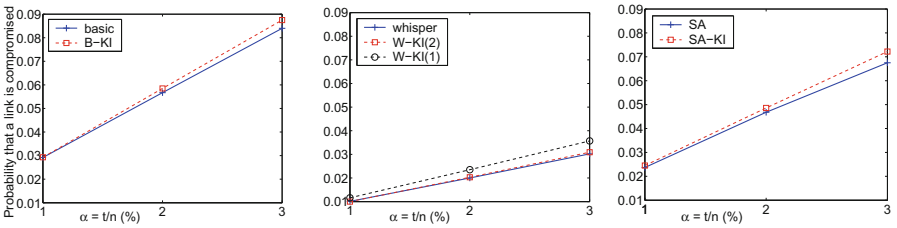
where $f(x) = 2x/R^2$, $f(y) = 2y/R^2$, and $f(z) = 2z/R^2$.

According to Subsect. 4.1, $\mathbf{E}[\mathbb{A}_{ij}(R)] = \mathbf{E}[\mathbb{A}_{ik}(R)] = \mathbf{E}[\mathbb{A}_{jk}(R)] = 0.5865\pi R^2$, $\mathbf{E}[\mathbb{A}_{i\bar{j}}(R)] = \mathbf{E}[\mathbb{A}_{\bar{i}j}(R)] = 0.4135\pi R^2$, $\mathbf{E}[\mathbb{A}_{ij\bar{k}}(R)] = \mathbf{E}[\mathbb{A}_{ij}(R)] - \mathbf{E}[\mathbb{A}_{ijk}(R)] = 0.5865\pi R^2 - 0.4942\pi R^2 = 0.0923\pi R^2$, $\mathbf{E}[\mathbb{A}_{\bar{i}\bar{j}k}(R)] = \pi R^2 - \mathbf{E}[\mathbb{A}_{ik}(R)] - \mathbf{E}[\mathbb{A}_{jk}(R)] + \mathbf{E}[\mathbb{A}_{ijk}(R)] = 0.3212\pi R^2$.

Let events $\mathbf{A} = \mathbb{B}_{ijk}$, $\mathbf{B} = \mathbb{B}_{i\bar{j}}$, $\mathbf{C} = \mathbb{B}_{\bar{i}j}$, $\mathbf{D} = \mathbb{B}_{\bar{i}\bar{j}k}$, and $\mathbf{E} = \mathbb{B}_{ij\bar{k}}$, the event $\mathbb{B}$ that a key is broken after secrecy amplification is $\mathbb{B} = \mathbf{A} \cup (\mathbf{BCD}) \cup (\mathbf{DE})$. Therefore, the outage probability of SA-KI is

$$\begin{aligned}\mathbf{P}_{SA-KI} = \mathbf{P}\{\mathbb{B}\} &= \mathbf{P}\{\mathbf{A}\} + \mathbf{P}\{\mathbf{BCD}\} + \mathbf{P}\{\mathbf{DE}\} - \mathbf{P}\{\mathbf{ABCD}\} \\ &\quad - \mathbf{P}\{\mathbf{ADE}\} - \mathbf{P}\{\mathbf{BCDE}\} + \mathbf{P}\{\mathbf{ABCDE}\} \\ &= \varphi(a) + \varphi(b,c,d) + \varphi(d,e) - \varphi(a,b,c,d) \\ &\quad - \varphi(a,d,e) - \varphi(b,c,d,e) + \varphi(a,b,c,d,e). \end{aligned} \tag{4}$$

where $a = 0.4942$, $b = c = 0.4135$, $d = 0.3212$, and $e = 0.0923$.



(a) Basic key infection (b) Whispering key infection (c) Secrecy amplification

Fig. 5. The outage probability of simulation results [7] vs. the probability model. For each subfigure, the solid line with marker + is the simulation results given in [7], the dotted line represents the result of the probability model proposed in this paper. Here, $n' = 5$, $\alpha = t/n$.

The analytical results of the probability model for key infection are given in Fig. 5. Our results of probability model approximate to the simulation results in [7]. Therefore, this model can help designers to evaluate key infection and adapt it to their needs.

5 Group Based Key Infection

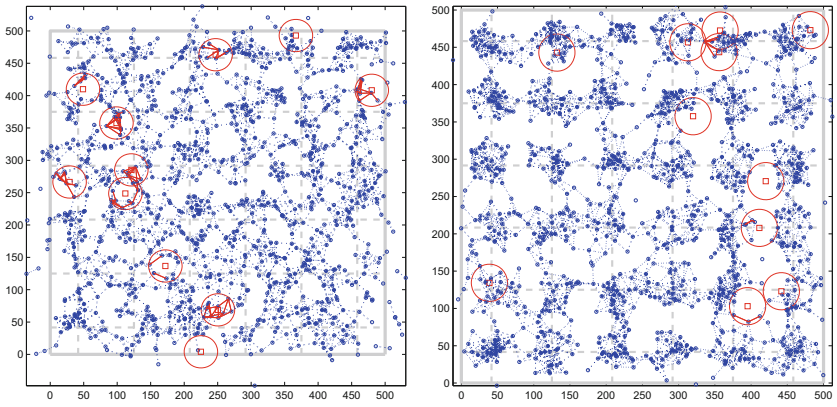
In practice, it is quite common that sensors are deployed in groups. Consider several canisters of sensors deployed via an artillery shell into enemy territory, sensors within a canister are more likely to be close to each other *a priori*. In this section, we present a group based key infection scheme, G-KI, to improve the security of key infection.

Group Based Key Infection. The scheme consists of two steps:

Step 1: *In-group key establishment*. Before deployment, sensors are first pre-arranged into small groups, and sensors apply key infection to establish pairwise keys with all the other sensors in the same group.
Step 2: *Cross-group key establishment*. After deployment, if two adjacent sensors have not established a secret key, they use key infection to negotiate a key. Secrecy amplification could be applied jointly if needed.

Evaluation of G-KI. Group based key infection is trivially secure if an adversary arrives after the cross-group key establishment phase. Only link between two sensors belong to different groups can be broken by eavesdroppers. In our analysis and simulations, we use the following setup:

– The number of sensors in the network is $n = 1080$. The deployment area is $500\,\mathrm{m} \times 500\,\mathrm{m}$, and is divided into a grid of size $36 = 6 \times 6$. The center of



(a) G-KI ($\sigma = 30, R = 25$) (b) G-KI ($\sigma = 20, R = 25$)

Fig. 6. Deployment examples of G-KI with different σ. Red squares and blue circles denote eavesdroppers and sensors, respectively. Red lines are the links compromised by the adversary, blue dot lines are the secure links. The big red circles are eavesdropping regions of eavesdroppers. (Color figure online)

each grid cell is the deployment point. Any sensor in the deployment group G_i follows a two-dimensional Gaussian distribution centered at a deployment point (x_i, y_i) with the standard deviation σ.

Figure 6 shows two deployment examples of G-KI with different σ. Figure 7 illustrates the probability that a link key is compromised for different standard deviation σ and communication radius R. Clearly, smaller σ, lower the probability that a link key is compromised. This indicates that G-KI can improve the security of key infection as long as the nodes in a group are close to each other after deployment.

Assume two sensors i and j which belong to the same group G_k are deployed independently from the two-dimensional Gaussian distribution centered at a deployment point (a_k, b_k) with location $(\mathbf{X}_i, \mathbf{Y}_i)$ and $(\mathbf{X}_j, \mathbf{Y}_j)$ respectively. For $\mathbf{X}_i$, $\mathbf{X}_j$, $\mathbf{Y}_i$, and $\mathbf{Y}_j$ are independent normal random variables which have the distributions $\mathbf{X}_i, \mathbf{X}_j \sim \mathcal{N}(a_k, \sigma^2)$, $\mathbf{Y}_i, \mathbf{Y}_j \sim \mathcal{N}(b_k, \sigma^2)$, then, random variables $\mathbf{X} = \mathbf{X}_i - \mathbf{X}_j \sim \mathcal{N}(0, 2\sigma^2)$, $\mathbf{Y} = \mathbf{Y}_i - \mathbf{Y}_j \sim \mathcal{N}(0, 2\sigma^2)$, and

$$f_{\mathbf{X},\mathbf{Y}}(x, y) = \frac{1}{4\pi\sigma} e^{-\frac{x^2+y^2}{4\sigma^2}}, -\infty < x, y < \infty$$

Therefore, the distance between nodes i and j, $\mathbf{Z} = \sqrt{\mathbf{X}^2 + \mathbf{Y}^2}$ has the *Rayleigh* distribution, $\mathbf{Z} = \sqrt{\mathbf{X}^2 + \mathbf{Y}^2} \sim Rayleigh(\sqrt{2}\sigma)$, and the probability distribution function of $\mathbf{Z}$ is given by $F_{\mathbf{Z}}(z) = 1 - e^{-\frac{z^2}{4\sigma^2}}$, $(z \geq 0)$. Therefore, the probability that two sensors in the same group are adjacent after deployment is $\mathbf{P}\{\mathbf{Z} \leq R\} = 1 - e^{-\frac{R^2}{4\sigma^2}}$.

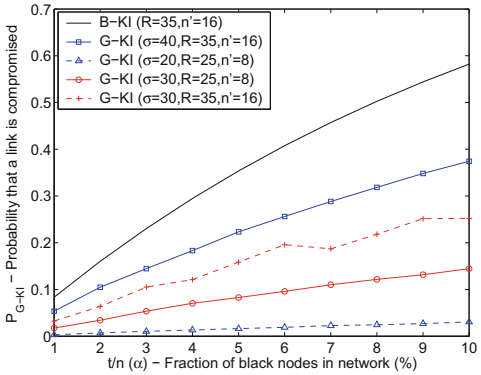


Fig. 7. Probability that a link is compromised in G-KI.

As Fig. 6 depicted, when the deviation σ increases, the sensors are more evenly distributed, but the benefits introduced by G-KI diminish monotonically, because the sensors in the same group are not close to each other. An appropriate σ is a trade-off between the security and the suitable distribution of the network.

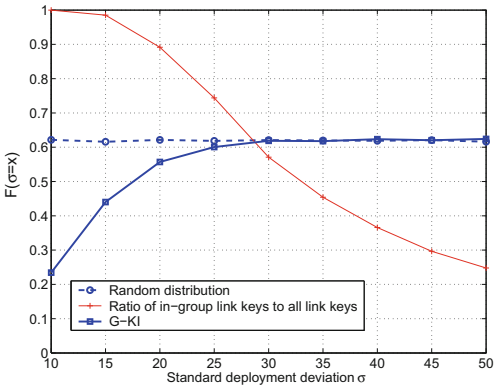


Fig. 8. How a distribution of G-KI with different deviation σ approximates random distribution in the field.

To tackle this contradiction, we evaluate how the distribution of sensors approximates to the random distribution over the deployment field. We first divide the whole deployment field into very small equal size cells, and calculate the deviation $Var(\sigma = x)$ of the number of sensors in each cell[1] when

[1] In our simulation, the field is divided into 50×50 square cells $cell(i,j), 1 \leq i \leq 50, 1 \leq j \leq 50$ with equal size. The number of sensors in each cell is calculated except the cells located at edges. Let the number of sensors in $cell(i,j)$ is $|cell(i,j)|$, the $Var(\sigma = x)$ is estimated as following: $\mu = \frac{1}{48\times48}\sum_{i=2}^{49}\sum_{j=2}^{49}|cell(i,j)|$, $Var(\sigma = x) = \frac{1}{48\times48}\sum_{i=2}^{49}\sum_{j=2}^{49}(\mu - |cell(i,j)|)^2$.

$\sigma = x$. Then, we define a function $F(x) = e^{-Var(\sigma=x)}$. If $F(x_1) > F(x_2)$, the distribution with $\sigma = x_1$ is more approximate to random distribution than the distribution with $\sigma = x_2$. Figure 8 depicts the simulation results of $F(x)$ with different σ. When $\sigma \geq 30$, the distribution of G-KI asymptotic approximates to random distribution.

6 Conclusions

Although key infection may seem extremely counterintuitive, it is remarkably simple and efficient. As can be anticipated, a one-fit-all solution does not work for all kinds of sensor networks, key infection provides a viable way to trade off security for cost and usability. Our probability model can help network designers to evaluate the security of key infection and adapt it to their needs. On occasions where more security is needed, group based key infection can be applied to further improve its security performance.

Acknowledgments. This work was supported by the National Key Research and Development Program of China (2016YFB0800601), the National Natural Science Foundation of China (61671360, 61173135), and in part by the Natural Science Basic Research Plan in Shaanxi Province of China (2017JM6082).

References

1. Ding, J., Bouabdallah, A., Tarokh, V.: Key pre-distributions from graph-based block designs. IEEE Sens. J. **16**(6), 1842–1850 (2016)
2. Bechkit, W., Challal, Y., Bouabdallah, A., Tarokh, V.: A highly scalable key pre-distribution scheme for wireless sensor networks. IEEE Trans. Wirel. Commun. **12**(2), 948–959 (2013)
3. Eschenauer, L., Gligor, V.: A key-management scheme for distributed sensor networks, In: Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 41–47. ACM Press, Washington (2002)
4. Yağan, O., Makowski, A.M.: Wireless sensor networks under the random pairwise key predistribution scheme: can resiliency be achieved with small key rings? IEEE/ACM Trans. Netw. **24**(6), 3383–3396 (2016)
5. Du, W., Deng, J., Han, Y.S., Chen, S., Varshney, P.K.: A key management scheme for wireless sensor networks using deployment knowledge. In: INFOCOM 2004, pp. 586–597. IEEE Press, New York (2004)
6. Choi, J., Bang, J., Kim, L., Ahn, M., Kwon, T.: Location-based key management strong against insider threats in wireless sensor networks. IEEE Syst. J. **11**(2), 494–502 (2017)
7. Anderson, R., Chan, H., Perrig, A.: Key infection: smart trust for smart dust. In: IEEE International Conference on Network Protocols, pp. 206–215. IEEE Press, New York (2004)