Mathematical Analysis of Secrecy Amplification in Key Infection*

Dae Hyun YUM(a), Member

SUMMARY Key infection is a lightweight key-distribution protocol for partially compromised wireless sensor networks, where sensor nodes send cryptographic keys in the clear. As the adversary is assumed to be present partially at the deployment stage, some keys are eavesdropped but others remain secret. To enhance the security of key infection, secrecy amplification combines keys propagated along different paths. Two neighbor nodes $W_1$ and $W_2$ can use another node $W_3$ to update their key. If $W_3$ is outside of the eavesdropping region of the adversary, the updated key is guaranteed to be secure. To date, the effectiveness of secrecy amplification has been demonstrated only by simulation. In this article, we present the first mathematical analysis of secrecy amplification. Our result shows that the effectiveness of secrecy amplification increases as the distance between the two neighbor nodes decreases.

key words: sensor network, smart dust, key management, key infection

1. Introduction

A wireless sensor network consists of a large number of tiny, cheap, and resource-constrained sensor nodes. For example, ‘smart dust’ with a volume of one cubic millimeter can be distributed in large numbers by random scattering (e.g., from an airplane)[1]. When a large number of sensor nodes are deployed, it is often difficult for an adversary to eavesdrop on all of the communication.

Anderson, Chan, and Perrig proposed ‘key infection’ to deal with the key distribution problem in environments with a partially present adversary [2]. At the deployment stage, keys are sent in the clear but the partially present adversary cannot eavesdrop on all the keys. Therefore, some keys are compromised but others remain secret.

Secrecy amplification is a post-deployment technique to establish an updated key from multiple old keys propagated along different paths. Let $k_{12}$ be the key established between two neighbor nodes $W_1$ and $W_2$. If the adversary can eavesdrop on $W_1$ and $W_2$ at the deployment stage, $k_{12}$ is compromised. To update $k_{12}$, $W_1$ and $W_2$ can ask a neighbor node $W_3$ to deliver messages between $W_1$ and $W_2$. If $W_3$ is outside of the eavesdropping region of the adversary, $k_{12}$ can be updated to a new secure key.

Previous works on key infection show the effectiveness of secrecy amplification based on simulations (e.g., [3]) and no rigorous mathematical analysis has been performed. In this article, we provide the first mathematical analysis of secrecy amplification. We compute the probability of effective secrecy amplification (i.e., the probability of updating a compromised key to a secure key) as a function of the distance between two neighbor nodes $W_1$ and $W_2$. The analysis shows that secrecy amplification is more effective for near nodes than for distant nodes.

2. Preliminaries

For a point $P$, $P_x$ and $P_y$ denote the $x$- and $y$-coordinate. $C_P$ denotes a circle centered at $P$. Circle $C_P$ with radius $R$ is the set $C_P = \{(x, y) \in \mathbb{R}^2 : (x - P_x)^2 + (y - P_y)^2 = R^2\}$. For two circles $C_{P_1}$ and $C_{P_2}$, $I[C_{P_1}, C_{P_2}] = C_{P_1} \cap C_{P_2}$ denotes the intersection points of $C_{P_1}$ and $C_{P_2}$. To distinguish between (two) intersection points, $I^\ast[C_{P_1}, C_{P_2}]$ denotes the intersection point in quadrant $\xi$. For two circles $C_{P_1}$ and $C_{P_2}$ with the radius $R$ where $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$,

\[
C_{P_1} : (x - x_1)^2 + (y - y_1)^2 = R^2
\]

\[
C_{P_2} : (x - x_2)^2 + (y - y_2)^2 = R^2
\]

the intersection points $I[C_{P_1}, C_{P_2}]$ can be expressed as

\[
x = x_1 + R \cos \theta \quad \text{and} \quad y = y_1 + R \sin \theta.
\]

By substituting Eq. (3) into Eq. (2), we can have

\[
\theta = \tan^{-1} \frac{y_2 - y_1}{x_2 - x_1} \pm \cos^{-1} \frac{\sqrt{(x_2-x_1)^2 + (y_2-y_1)^2}}{2R}.
\]

By Eq. (3)–(4), $I[C_{P_1}, C_{P_2}] = (x, y)$ is given by

\[
x = x_1 + R \cos \left( \tan^{-1} \frac{y_2 - y_1}{x_2 - x_1} \pm \cos^{-1} \frac{\sqrt{(x_2-x_1)^2 + (y_2-y_1)^2}}{2R} \right),
\]

\[
y = y_1 + R \sin \left( \tan^{-1} \frac{y_2 - y_1}{x_2 - x_1} \pm \cos^{-1} \frac{\sqrt{(x_2-x_1)^2 + (y_2-y_1)^2}}{2R} \right).
\]

For a point $P = (P_x, P_y)$, $D_P$ denotes a disk centered at $P$. Disk $D_P$ with radius $R$ is the set $D_P = \{(x, y) \in \mathbb{R}^2 : (x - P_x)^2 + (y - P_y)^2 \leq R^2\}$. For disks $D_{P_1}$ and $D_{P_2}$, $I[D_{P_1}, D_{P_2}] = D_{P_1} \cap D_{P_2}$ denotes the intersection region of $D_{P_1}$ and $D_{P_2}$.

Manuscript received January 1, 2016.

Manuscript publicized March 28, 2016.

1 The author is with the Department of Information and Communication Engineering, Myongji University, Yongin, Gyeonggi-do, 449–728, Republic of Korea.

2 This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (NRF-2013R1A1A1009630).

a) E-mail: dhyum@mju.ac.kr
DOI: 10.1587/transinf.2016EDL8001

Copyright © 2016 The Institute of Electronics, Information and Communication Engineers
3. Secrecy Amplification

At the deployment stage of key infection, a key is established between each pair of neighbor sensor nodes in a partially compromised network. Let $W_1$ and $W_2$ be honest (or white) neighbor nodes and $B$ be an adversarial (or black) node. Let $R$ be the maximum range of the radio. Nodes are assumed to transmit at the maximum strength all the time; we do not consider nodes adjusting transmission power adaptively (e.g., whispering mode). The security of $k_{12}$ depends on the relative positions of $W_1$, $W_2$, and $B$. If $B$ is located within the transmission ranges of both $W_1$ and $W_2$ at the deployment stage, i.e., $B \in I[D_{W_1}, D_{W_2}]$, then $B$ can compromise $k_{12}$. Since the attacker in commodity sensor networks is able to monitor only a small proportion ($\alpha$) of the communications of the sensor network during the deployment phase (e.g., $\alpha = 1 \sim 3\%$) [2], we assume that there is at most one black node within the common transmission ranges of two white nodes (i.e., $|\{B \mid B \in I[D_{W_1}, D_{W_2}]\}| \leq 1$).

To update $k_{12}$, $W_1$ and $W_2$ can use another neighbor node $W_3$. Let $k_{ij}$ be the key established between $W_i$ and $W_j$ at the deployment stage. During the secrecy amplification, each message sent between $W_i$ and $W_j$ is encrypted with the established key $k_{ij}$. Unless the black node $B$ is able to eavesdrop on all the communication channels between $W_1$, $W_2$, and $W_3$ (i.e., $B$ already knows $k_{12}$, $k_{13}$, and $k_{23}$), the old key $k_{12}$ can be updated to a new secure key.

4. Mathematical Analysis

To measure the effectiveness of secrecy amplification, we compute the probability that a compromised key $k_{12}$ is updated to a secure key. All circles and disks in this section will have radius $R$ and thus we often omit the radius.

The first sub-figure of Fig. 1 shows two white nodes $W_1 = (W_{1x}, W_{1y}) = (-\lambda/2, 0)$ and $W_2 = (W_{2x}, W_{2y}) = (\lambda/2, 0)$ on the $x$-axis, where $\lambda$ is the distance between $W_1$ and $W_2$. The coordinates of $P_1, P_2, \ldots, P_6$ are as follows.

$$
P_1 = (R + \lambda/2, 0), \quad P_2 = (R - \lambda/2, 0),
$$
$$
P_3 = (0, \sqrt{R^2 - (\lambda/2)^2}), \quad P_4 = (0, -\sqrt{R^2 - (\lambda/2)^2}),
$$
$$
P_5 = (-R - \lambda/2, 0), \quad P_6 = (-R + \lambda/2, 0).
$$

A black node $B \in I[D_{W_1}, D_{W_2}]$ is located in the intersection region of two disks $D_{W_1}$ and $D_{W_2}$, i.e., the shape $\psi$ bounded by points $P_2, P_3, P_4, P_5$. To update $k_{12}$, $W_1$ and $W_2$ hire another neighbor node $W_3 \in I[D_{W_1}, D_{W_2}]$ that is able to communicate with both $W_1$ and $W_2$. To update $k_{12}$ to a secure key, $B$ should not be able to eavesdrop on $W_3$, i.e., $W_3 \notin D_B$. Therefore, the probability of effective secrecy amplification is equal to the conditional probability $\psi = \Pr[W_3 \notin D_B \mid B \in I[D_{W_1}, D_{W_2}] \land W_3 \in I[D_{W_1}, D_{W_2}]]$. From the symmetry of $I[D_{W_1}, D_{W_2}]$ in Fig. 1, we can compute the probability $\psi_B$ by assuming that $B$ is in quadrant I.

Let $\psi_B$ be the probability of effective secrecy amplification $\psi$ for a fixed black node $B$. Then, for a black node $B \in I[D_{W_1}, D_{W_2}]$ in quadrant I, the probability $\psi_B$ can be computed by a ratio of areas

$$
\psi_B = \frac{\Pr[W_3 \in I[D_{W_1}, D_{W_2}] \land W_3 \notin D_B]}{\Pr[W_3 \in I[D_{W_1}, D_{W_2}] li]\frac{Area[I[D_{W_1}, D_{W_2}] - D_B]}{Area[I[D_{W_1}, D_{W_2}]]},
$$

(7)

where $Area[\cdot]$ denotes the area of the argument region and
\[ \text{Area}(l[D_W, D_W]) = 4\int_0^{R/2} \int_0^{\sqrt{R^2 - (x+y/2)^2}} dydx. \]

Since \[ \text{Area}(l[D_W, D_W] \cap D_B) = \text{Area}(l[D_W, D_W]) \]
depends on the position of \( B \), we divide \( l[D_W, D_W] \) of quadrant I into six regions.

**Region-0.** This region is bounded by the \( x \)-axis, the \( y \)-axis, and arc \( W_5P_7 \) of \( C_{P_1} \), where \( P_7 = (0, -\sqrt{R^2 - (\lambda/2)^2}) \). If \( B \) is in Region-0, it holds that \( |B - P_i| \leq R \) for \( i = 2, 3, 4, 5 \) and \( l[D_W, D_W] \subset D_B \). Therefore, \[ \text{Area}(l[D_W, D_W] - D_B) = 0 \]
and from (7), we have

\[ \psi_{\text{Region-0}} = 0. \]  

(8)

In other words, \( B \) in Region-0 can eavesdrop on any \( W_3 \in l[D_W, D_W] \) and secrecy amplification always fails.

**Region-1.** This region is bounded by the \( y \)-axis, arc \( W_2P_7 \) of \( C_{P_1} \), and arc \( W_2P_8 \) of \( C_{P_2} \), where \( P_7 = (0, -\sqrt{R^2 - (\lambda/2)^2}) \) and \( P_8 = (0, \sqrt{R^2 - (\lambda/2)^2}) \). We use the center of three points \( W_2, P_7, P_8 \) as the representative position of \( B \) in Region-1, which approximates Region-1 to triangle \( \triangle W_2P_7P_8 \).

\[ B = (B_x, B_y) = \left( \frac{\lambda/2 - R - \sqrt{R^2 - (\lambda/2)^2} + \sqrt{R^2 - (\lambda/2)^2}}{3}, \frac{\sqrt{R^2 - (\lambda/2)^2}}{3} \right) \]

By Eq. (5), we can compute the \( x \)-coordinates of intersection points \( Q = l'|C_{W_1}, C_B \) and \( Q' = l'|C_{W_2}, C_B \), where \( W_1 = (\lambda/2, 0) \) and \( W_2 = (\lambda/2, 0) \). In Region-1 of Fig. 1, we have \( Q_x \geq Q_y \) and \( Q_x \leq Q_y \) because \( B \) stays over \( W_2P_7 \) of \( C_{P_1} \). We have \( Q_x \leq 0 \) and \( Q_y \leq 0 \) because \( B \) stays below \( W_2P_8 \) of \( C_{P_2} \) and satisfies that \( |P_2 - P_8| = |P_5 - P_8| = R \). Therefore, \( Q \) and \( Q' \) belong to quadrant IV and quadrant III, respectively.

For a circle \( C_f : (x - P_x)^2 + (y - P_y)^2 = R^2 \), we denote explicit solutions as \( f_{C_f}(x) = P_x + \sqrt{R^2 - (x - P_x)^2}, f_{C_f}(y) = P_y - \sqrt{R^2 - (y - P_y)^2} \), \( f_{C_f}(x) = P_x - \sqrt{R^2 - (x - P_x)^2}, f_{C_f}(y) = P_y + \sqrt{R^2 - (y - P_y)^2} \), and \( f_{C_f}(x) = P_x + \sqrt{R^2 - (x - P_x)^2}, f_{C_f}(y) = P_y - \sqrt{R^2 - (y - P_y)^2} \).

For secrecy amplification to succeed, \( W_3 \) should be in \( l[D_W, D_W] \) that is bounded by points \( Q, Q', P_4 \). By Eq. (7), the probability of effective secrecy amplification in Region-1 can be computed as follows.

\[ \psi_{\text{Region-1}} = \frac{1}{\text{Area}(l[D_W, D_W])} \times \text{Area}(l[D_W, D_W] - D_B) \]

\[ = \frac{1}{\text{Area}(l[D_W, D_W])} \times \left( \int_{Q_x}^{Q_x'} 2f_{C_f}(x)dx + \int_{Q_y}^{Q_y'} f_{C_f}(x) - f_{C_f}(x)dx + \int_{Q_y}^{Q_y'} f_{C_f}(x) - f_{C_f}(x)dx \right) \]

\[ \times \left( \int_{Q_x}^{Q_x'} B_x - \sqrt{R^2 - (x-B_x)^2} + \sqrt{R^2 - (x+\lambda/2)^2}dx \right) \]

\[ \times \left( \int_{Q_y}^{Q_y'} B_x - \sqrt{R^2 - (x-B_x)^2} + \sqrt{R^2 - (x+\lambda/2)^2}dx \right) \]

\[ + \int_{Q_y}^{Q_y'} B_y - \sqrt{R^2 - (x-B_y)^2} + \sqrt{R^2 - (x+\lambda/2)^2}dx \]

(9)

**Region-2.** This region is bounded by the \( y \)-axis, arc \( P_3P_{12} \) of \( C_{P_3} \), and arc \( P_8P_{12} \) of \( C_{P_1} \), where \( P_{12} = l'[C_{W_1}, C_{P_1}] = ((R - \lambda)/2, \sqrt{R^2 - (\lambda/2)^2}) \). We use the center of three points \( P_3, P_8, P_{12} \) as the representative position of \( B \) in Region-2, which approximates Region-2 to triangle \( \triangle P_3P_8P_{12} \).

\[ B = (B_x, B_y) = \left( \frac{P_3 + P_8 + P_{12}}{3}, \frac{\sqrt{R^2 - (\lambda/2)^2}}{3} \right) \]

By Eq. (5), we can compute the \( x \)-coordinates of intersection points \( Q = l'[C_{W_1}, C_B] \) and \( Q' = l'[C_{W_2}, C_B] \). In Region-2 of Fig. 1, we have \( Q_x \geq 0 \) and \( Q_y \leq 0 \) because \( B \) stays over \( P_2P_8 \) of \( C_{P_1} \) in quadrant I and it holds that \( |P_8 - P_2| = |P_{12} - P_2| = |P_8 - P_3| = R \).

By Eq. (7), the probability of effective secrecy amplification in Region-2 can be computed as follows.

\[ \psi_{\text{Region-2}} = \frac{1}{\text{Area}(l[D_W, D_W])} \times \text{Area}(l[D_W, D_W] - D_B) \]

\[ = \frac{1}{\text{Area}(l[D_W, D_W])} \times \left( \int_{Q_x}^{Q_x'} 2f_{C_f}(x)dx + \int_{Q_y}^{Q_y'} f_{C_f}(x) - f_{C_f}(x)dx + \int_{Q_y}^{Q_y'} f_{C_f}(x) - f_{C_f}(x)dx \right) \]

\[ \times \left( \int_{Q_x}^{Q_x'} B_x - \sqrt{R^2 - (x-B_x)^2} + \sqrt{R^2 - (x+\lambda/2)^2}dx \right) \]

\[ \times \left( \int_{Q_y}^{Q_y'} B_x - \sqrt{R^2 - (x-B_x)^2} + \sqrt{R^2 - (x+\lambda/2)^2}dx \right) \]

\[ \times \left( \int_{Q_y}^{Q_y'} B_x - \sqrt{R^2 - (x-B_x)^2} + \sqrt{R^2 - (x+\lambda/2)^2}dx \right) \]

\[ \times \left( \int_{Q_y}^{Q_y'} 2\sqrt{R^2 - (x+\lambda/2)^2}dx \right) \]

(10)

**Region-3.** This region is bounded by arc \( P_8P_{12} \) of \( C_{P_1} \), arc \( W_2P_9 \) of \( C_{P_2} \), arc \( W_2P_9 \) of \( C_{P_1} \), and arc \( P_9P_{12} \) of \( C_{W_1} \), where \( P_9 = (R/2, \sqrt{R^2 - (R/2 + \lambda/2)^2}) \). We cannot use the center of four points \( P_3, P_8, W_2, P_9 \) as the representative position of \( B \) in Region-3, because it gets out of Region-3 as \( \lambda \to R \). Instead, we use the middle point of the Region-3 segment of \( C_{P_1} \), where \( P_{11} = (-R/2, 0) \) is the middle point of line \( \triangle P_5W_1 \).

The \( x \)-coordinates of the intersection points \( V = l'[C_{P_3}, C_{P_1}] \) and \( V' = l'[C_{P_3}, C_{P_1}] \) are \( V_x = \frac{R+\lambda}{4} \) and \( V_x' = \frac{R-\lambda}{4} \) by Eq. (5). We use the middle point of arc \( VV' \) of
$C_{P_i}$ as the representative position of $B$ in Region-3.

$$B = (B_x, B_y) = (R \cos \theta - R/2, R \sin \theta)$$

where the angle (in radians) between $x$-axis and $P_1' B$ is $\theta = \angle P_1 P_1' B = \frac{1}{2} (\angle P_1 P_1' V + \angle P_1 P_1' V') = \frac{1}{2} \left( \cos^{-1} \frac{V_x + R/2}{R} + \cos^{-1} \frac{V_y + R/2}{R} \right)$.

By Eq. (5), we can compute the $x$-coordinates of intersection points $Q = I^V\{C_{P_i}, C_{B}\}$ and $Q' = I^H\{C_{P_i}, C_{B}\}$. In Region-3 of Fig. 1, we have $Q_1 \leq 0$ because $B$ stays under $P_8 P_{12}$ of $C_{P_i}$ and it holds that $|P_8 - P_2| = |P_{12} - P_2| = R$. We have $Q_2' \geq 0$ because $B$ stays to the right of $W_2 P_8$ of $C_{P_i}$ and it holds that $|W_2 - P_5| = |P_8 - P_5| = R$. Therefore, $Q$ and $Q'$ belong to quadrant IV and quadrant II, respectively.

By Eq. (7), the probability of effective secrecy amplification in Region-3 can be computed as follows.

$$\psi_{\text{Region-3}} = \frac{1}{\text{Area}[I[D_{W_1},D_{W_2}]]} \times \text{Area}[I[D_{W_1},D_{W_2}] - D_B]$$

$$= \left( \int_{\theta=0}^{\theta=\pi/2} \int_{r=R}^{r=\sqrt{R^2 - x^2}} \frac{r^2}{2} \sin \theta dr d\theta \right)$$

Region-4. This region is bounded by arc $W_2 P_9$ of $C_{P_i}$, arc $W_2 P_{10}$ of $C_{P_i}$, and arc $P_9 P_{10}$ of $C_{W_i}$. We use the center of three points $W_2, P_9, P_{10}$ as the representative position of $B$ in Region-4, which approximates Region-4 to a triangle.

$$B = (B_x, B_y) = \left( \frac{W_{2x} + P_{9x} + P_{10x}}{3}, \frac{W_{2y} + P_{9y} + P_{10y}}{3} \right)$$

where $W_2 = (W_{2x}, W_{2y}) = (\lambda/2, 0)$, $P_9 = (P_{9x}, P_{9y}) = (R/2, \sqrt{R^2 - (R/2 + \lambda/2)^2})$, $P_{10} = (P_{10x}, P_{10y}) = \left( \frac{\pi}{4} + R \cos \left( \tan^{-1} \frac{\sqrt{R^2 - (\lambda/2)^2}}{\lambda/2} - \frac{\pi}{2} \right), R \sin \left( \tan^{-1} \frac{\sqrt{R^2 - (\lambda/2)^2}}{\lambda/2} - \frac{\pi}{2} \right) \right)$.

By Eq. (6), we can compute the $y$-coordinates of intersection points $Q = I^V\{C_{W_i}, C_{B}\}$ and $Q' = I^H\{C_{W_i}, C_{B}\}$. In Region-4 of Fig. 1, we have $Q_1 \geq 0$ because $B$ stays below $W_2 P_{10}$ of $C_{P_i}$ and to the right of $W_2$, $P_9$ satisfies $|P_9 - W_2| = R$. Therefore, $Q$ and $Q'$ belong to quadrant IV and quadrant II, respectively.

By Eq. (7), the probability of effective secrecy amplification in Region-4 can be computed as follows.

$$\psi_{\text{Region-4}} = \frac{1}{\text{Area}[I[D_{W_1},D_{W_2}]]} \times \text{Area}[I[D_{W_1},D_{W_2}] - D_B]$$

$$= \left( \int_{\theta=0}^{\theta=\pi/2} \int_{r=R}^{r=\sqrt{R^2 - x^2}} \frac{r^2}{2} \sin \theta dr d\theta \right)$$

Region-5. This region is bounded by the $x$-axis, arc $W_2 P_{10}$ of $C_{P_i}$, and arc $P_9 P_{10}$ of $C_{W_i}$. We use the center of three points $W_2, P_9, P_{10}$ as the representative position of $B$ in Region-5.

$$B = (B_x, B_y) = \left( \frac{W_{2x} + P_{9x} + P_{10x}}{3}, \frac{W_{2y} + P_{9y} + P_{10y}}{3} \right)$$

By Eq. (6), we can compute the $y$-coordinates of intersection points $Q = I^V\{C_{W_i}, C_{B}\}$ and $Q' = I^H\{C_{W_i}, C_{B}\}$. In Region-5 of Fig. 1, we have $Q_1 \geq 0$ because $B$ stays below $W_2 P_{10}$ of $C_{P_i}$ and to the right of $W_2$, $P_9$ satisfies $|P_9 - W_2| = R$. Therefore, $Q$ and $Q'$ belong to quadrant IV and quadrant II, respectively.

By Eq. (7), the probability of effective secrecy amplification in Region-5 can be computed as follows.

$$\psi_{\text{Region-5}} = \frac{1}{\text{Area}[I[D_{W_1},D_{W_2}]]} \times \text{Area}[I[D_{W_1},D_{W_2}] - D_B]$$

$$= \left( \int_{\theta=0}^{\theta=\pi/2} \int_{r=R}^{r=\sqrt{R^2 - x^2}} \frac{r^2}{2} \sin \theta dr d\theta \right)$$
\[ + \int_{Q_0}^{R_0} \sqrt{R^2 - x^2} \left( 2 \left( \sqrt{R^2 - y^2} - \frac{1}{2} \right) dy \right) \]

(13)

We compute the area of Region-1 \( \mathcal{A}_i = \text{Area}[\text{Region-}i] \) and the sum of six areas \( \mathcal{A} = \sum_{i=0}^{5} \mathcal{A}_i \) as follows.

\[ \mathcal{A} = \frac{1}{4} \text{Area}[I[D_{W_1}, D_{W_2}]] = \int_{0}^{R-1/2} \int_{0}^{\sqrt{R^2-x^2}} dydx \]

\[ \mathcal{A}_0 = \int_{0}^{\sqrt{R^2-x^2}} dydx \]

\[ \mathcal{A}_1 = \int_{0}^{\sqrt{R^2-x^2}} dydx \]

\[ \mathcal{A}_2 = \int_{0}^{\sqrt{R^2-(x-1/2)^2}} dydx \]

\[ \mathcal{A}_3 = \int_{0}^{\sqrt{R^2-(x-3/2)^2}} dydx \]

\[ \mathcal{A}_4 = \int_{0}^{\sqrt{R^2-(x-5/2)^2}} dydx \]

\[ \mathcal{A}_5 = \int_{0}^{\sqrt{R^2-(x-7/2)^2}} dydx \]

Finally, the probability of effective secrecy amplification is

\[ \psi = \sum_{i=0}^{5} \Pr(B \in \text{Region-}i) \psi_i = \sum_{i=0}^{5} \frac{\mathcal{A}_i}{\mathcal{A}} \psi_i \]

(14)

where \( \psi_i \) for \( i = 0, \ldots, 5 \) are given by Eq. (8)–(13).

To verify the validity of Eq. (14), we also performed Monte Carlo simulations for various distances \( \frac{1}{R} = 0.1 \times j \) where \( j = 1, 2, \ldots, 10 \). For each \( \frac{1}{R} \), we first fixed \( W_1 \) and \( W_2 \) and then randomly generated a black node \( B \) and 100,000 white nodes \( W_3 \) in the rectangular area \( \{(x, y) : -\frac{1}{2} - R \leq x \leq \frac{1}{2} + R, \ -R \leq y \leq R\} \). If \( B \) belongs to \( I[D_{W_1}, D_{W_2}] \), the probability of effective secrecy amplification was computed with neighbor nodes \( W_3 \in I[D_{W_1}, D_{W_2}] \). This step was repeated by randomly generating the black node 100,000 times. The average value of the probability over all \( B \in I[D_{W_1}, D_{W_2}] \) is the simulation result. Numerical values of Eq. (14) and Monte Carlo simulations are given in Fig. 2. The two graphs show the tendency that secrecy amplification is more effective for nodes with small distances. Approximately, the effectiveness of secrecy amplification for near nodes can be 30–40% and that for distant nodes can be 10–20%. The maximum difference between the two graphs in Fig. 2 is 0.0535 at \( \frac{1}{R} = 1 \), where the probability of effective secrecy amplification is 0.0496 by Eq. (14) and 0.1031 by the simulation result. Generally, the difference is less than 0.0535 and thus Eq. (14) seems to be valid (and useful) for most practical applications.

5. Conclusion

Key infection with secrecy amplification is a very efficient key distribution protocol. Our mathematical analysis of secrecy amplification shows that near nodes can enjoy higher levels of security. The analysis was performed under the assumption that the transmission power of each node is fixed (i.e., \( R \)). We leave the analysis of secrecy amplification where nodes can adjust transmission power adaptively (e.g., whispering mode) as an open problem.

Acknowledgements

The author would like to thank Junyeun Kim, Seung Hoon Choi, and Jin Seok Kim, for their collaboration on this work. The author would also like to thank the IEICE reviewer for the helpful comments and suggestions.

References

