Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2012, Article ID 847805, 12 pages
doi:10.1155/2012/847805

Research Article

Secrecy Transfer

Zhihong Liu,[1] Jianfeng Ma,[1] Yong Zeng,[1] Li Yang,[1] and YoungHo Park[2]

[1] *School of Computer Science and Technology, Xidian University, Xi'an 710071, China*
[2] *Department of Electrical Engineering, Kyungpook National University, Daegu 702-701, Republic of Korea*

Correspondence should be addressed to Zhihong Liu, liuzhihong@mail.xidian.edu.cn

Received 7 March 2012; Revised 8 June 2012; Accepted 10 June 2012

Academic Editor: Mihui Kim

Suppose that n nodes with n_0 acquaintances per node are randomly deployed in a two-dimensional Euclidean space with the geographic restriction that each pair of nodes can exchange information between them directly only if the distance between them is at most r, the acquaintanceship between nodes forms a random graph, while the physical communication links constitute a random geometric graph. To get a fully connected and secure network, we introduce secrecy transfer which combines random graph and random geometric graph via the propagation of acquaintanceship to produce an acquaintanceship graph G_{n,n_0}, a kind of random geometric graph with each edge representing an acquaintanceship between two nodes. We find that components of graph G_{n,n_0} that undergoes a phase transition from small components to a giant component when n_0 is larger than a threshold, the threshold for G_{n,n_0} to be a connected graph is derived. In addition, we present its implementation method and applications in wireless sensor networks.

1. Introduction

Suppose at a classroom with n students, each of whom initially has n_0 acquaintances who are randomly chosen among them. Students can only communicate with its direct neighbors. At first, students are isolated. If two adjacent students are acquainted with each other, a link forms between them. As time goes on, some small acquaintance groups emerge. Two stranger students, say Alice and Bob, belonging to different groups may be adjacent, but if there are students in the two groups, respectively, familiar with each other, Alice and Bob may use them as introducers to establish a link between them. By repeating this process, students will be increasingly interwoven by such links, creating a web of acquaintances. We denote this construction as *secrecy transfer* and the resulting network as the *acquaintanceship graph* G_{n,n_0}. We are here interested in the question: for which critical threshold of n_0 is there likely to be a connected acquaintanceship graph?

At first glance, the acquaintanceship graph is a kind of social networks, such as the patterns of friendships between individuals. Technically, the acquaintanceship graph is a combination of random graph [1] and random geometric graph [2]. A random geometric graph $G_{n,r}$ is a graph resulting from placing n nodes randomly in a plane and connecting each pair of nodes if their distance is at most the radius r, while a random graph $G_{n,p}$ is a graph with n nodes in which each edge (out of the $\binom{n}{2}$ possible edges) is chosen independently at random with an edge probability p. The acquaintanceship graph G_{n,n_0} has both properties of random graph and random geometric graph. Initially, n nodes are placed randomly on a plane, every node has n_0 acquaintances. In the view of acquaintanceship, it can be considered logically as a random graph $G_{n,p}$ without geographical position restriction. If graph G_{n,n_0} is connected, everyone can make the acquaintance of arbitrary nodes in the graph. Intuitively, we think that there is a threshold value. If n_0 is larger than that value, the graph G_{n,n_0} may be connected. If the communication between any pair of acquaintances is considered secure and trusted, through the introduction of acquaintances, any one can extend his circle of acquaintance and eventually get secure communication with arbitrary nodes in the graph G_{n,n_0}.

Random graphs and random geometric graphs have been studied extensively, but in a separate way. Random graph and its variations have been used as models of social structure in, for example, epidemiology [3], while random geometric graph is always viewed as a wireless communication network

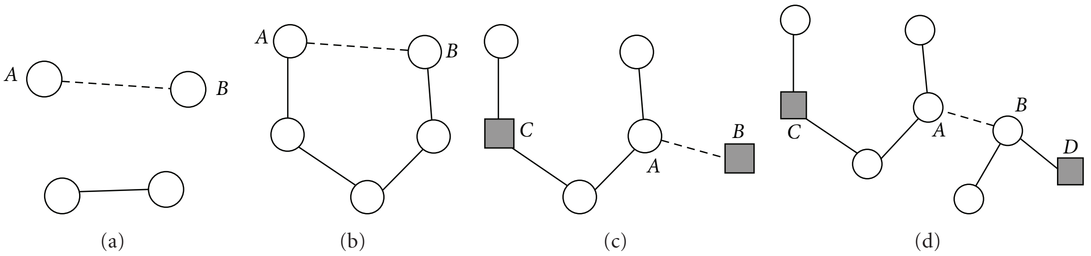


Figure 1: Secrecy transfer.

[4, 5], such as Ad hoc, Mesh, or sensor networks. In fact, random graphs and random geometric graphs have different structural properties. Any two nodes in a random graph can be connected by a link with certain probability regardless of their geographical position. Random key graphs have been recently been used by Di Pietro et al. [6] to model the random key predistribution scheme of Eschenauer and Gligor [7]. The random key graph is a random graph obtained as follows: n nodes, each assigned a subset of keys, are distributed uniformly at random on a given field. An edge is added if two nodes are within a radius r and share at least one common key. Formally, the resulting graph, matching a random graph with identical link probability to a random geometric graph, can be considered as the initial graph of the acquaintanceship graph G_{n,n_0}, if two nodes, sharing one common key, are referred to as acquaintances. Note that, unlike random key graphs, secrecy transfer is a *growth* model and can be considered as a stochastic process. We are interested in the crucial property, connectivity, of the resulting acquaintanceship graph. In [8], we use secrecy transfer to enhance the security performance of key infection [9]. In fact, secrecy transfer in [8] only focuses on key establishment between adjacent nodes who are in a connected component; otherwise, key infection is applied to establish a secret link key. Obviously, it is a tradeoff between key infection and secrecy transfer discussed in this paper. In this paper, some results are given and complemented by simulations, especially the connectivity threshold.

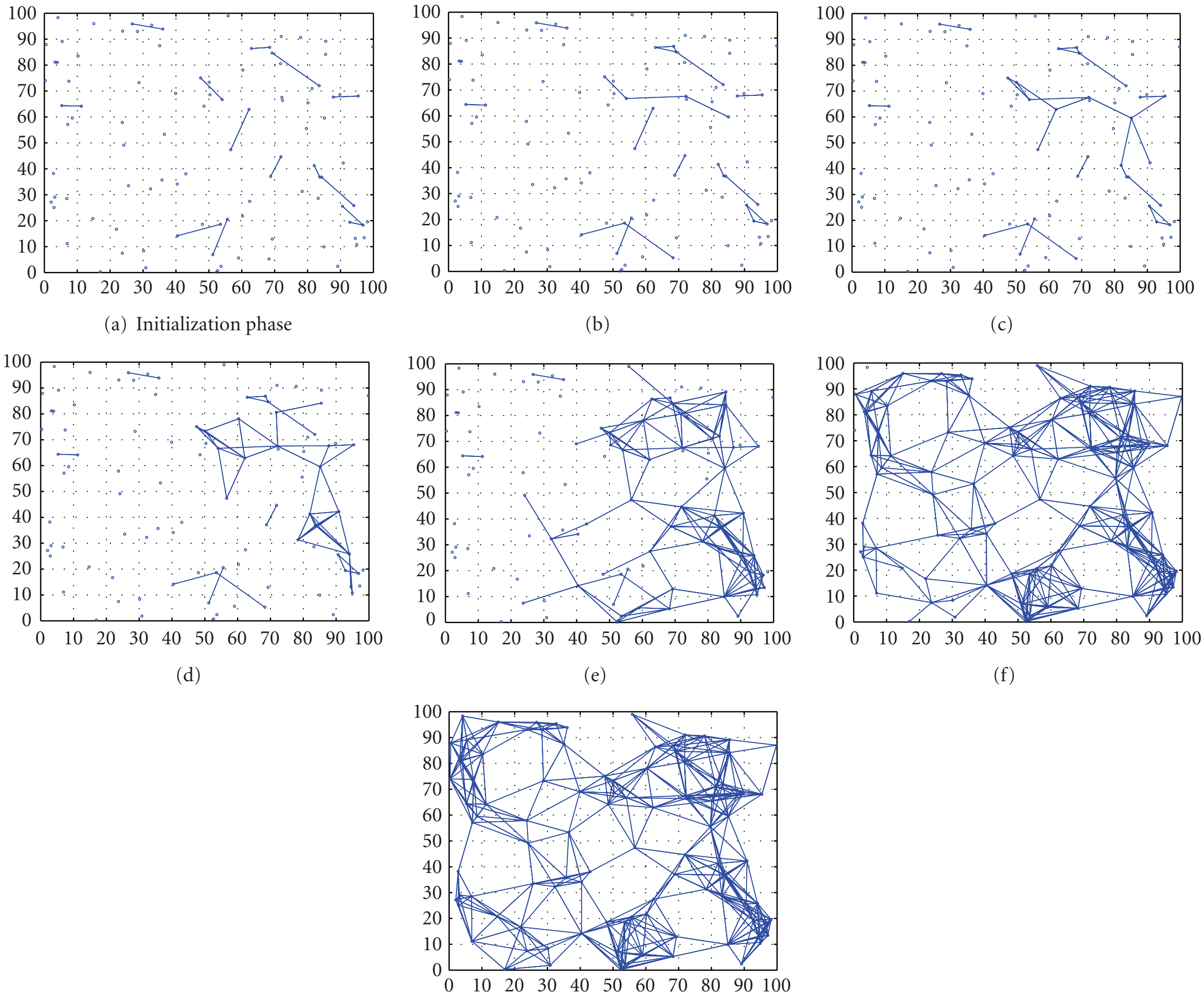
Organization. First, secrecy transfer is presented in Section 2. We derive the connectivity threshold of value n_0 in Section 3. Next, in Section 4, we present the analysis of secrecy transfer in heterogeneous networks. Section 5 gives an implementation method of secrecy transfer. In Section 6, some applications are given. Finally, we conclude the paper in Section 7.

2. Secrecy Transfer

Let n nodes be distributed uniformly and independently at random in a field $[0,1]^2$, each of them has n_0 acquaintances. A pair of nodes are adjacent only if the distance between them is at most the radius r. Suppose nodes A and B are adjacent, that is, the distance between them $|A-B| < r$. Initially, A and B are connected if they are acquainted with each other (*initialization phase*, see Figure 1(a)). If nodes A and B are connected by a path, an edge $A-B$ is added (see Figure 1(b)). As time goes on, the graph G_{n,n_0} evolves continuously, and gradually consists of some components. If node A belongs to a component C_A, and B has acquaint with at least one of nodes in the component C_A, say node C in C_A, we connect A and B by a new edge (see Figure 1(c)). For the case where A and B belong to different component C_A and C_B, if there exist two acquaintance nodes C and D in C_A and C_B, respectively, we introduce an edge between A and B; Otherwise, A and B are disconnected at present stage. If there is no new edge is added for any pair of adjacent nodes, secrecy transfer reaches the *stable state* and the algorithm terminates. Continuing this process, we can get a acquaintanceship graph G_{n,n_0}.

As depicted in Figure 2, 100 nodes are randomly distributed over a $100 \times 100\,\mathrm{m}^2$ field, $n_0 = 4$, and the radius $r = 20\,\mathrm{m}$. At first, two adjacent nodes connect with the probability $p = n_0/n = 0.04$, and we get the initial acquaintanceship graph G_{n,n_0}, as illustrated in Figure 2(a). After repeating secrecy transfer process on the graph G_{n,n_0}, it gradually evolves into the graph shown in Figure 2(g), which approximates to the underly random geometric graph $G_{n,r}$.

One of our goals is to design a *security mechanism* to enable any two adjacent nodes to establish a pairwise key after they are deployed in a field. More specifically, suppose that every node in the network has been preloaded before its deployment with n_0 secret keys, each of which is shared with one of its acquaintances. Let nodes A and B be two adjacent nodes, $|A-B| < r$. If nodes A and B happen to be acquaintances, they share a key K_{AB} which can be used to protect their communication link. If A and B are not acquaintances, but are connected by a path (Figure 1(b)), A can generate a new key K_{AB} and send it to B along the path. As more secure edges are added to the graph G_{n,n_0}, larger components emerge. Suppose node A belongs to a component C_A, (as plotted in Figure 1(c)) if node B acquaints with a node $C \in C_A$, which means that nodes B and C have a shared key K_{BC}. In this case, node A randomly generates a key K_{AB} and sends it along a path in the component C_A to node C. Node C encrypts K_{AB} with the key K_{BC}, that is, $\{K_{AB}\}_{K_{BC}}$ and sends the result back to A. Node A, then, sends $\{K_{AB}\}_{K_{BC}}$ to B via the unsecure channel. Finally, node B can get key K_{AB}, for it has the key K_{BC}. In another case, where nodes A and B belong to different components C_A and C_B, but node $C \in C_A$ acquaints with node $D \in C_B$, as shown in Figure 1(d). Node A first sends a key K_{AB} to node C. Node C encrypts K_{AB} with key K_{CD} which is shared with



(a) Initialization phase

(b)

(c)

(d)

(e)

(f)

(g) Stable state

Figure 2: An example of secrecy transfer process, with $n = 100$ nodes randomly distributed over a $100 \times 100\,\text{m}^2$ field, $n_0 = 4$, and $r = 20\,\text{m}$.

node D and sends $\{K_{AB}\}_{K_{CD}}$ to node D via nodes A and B. For node D has K_{CD}, it can decrypt the message $\{K_{AB}\}_{K_{CD}}$ to obtain K_{AB}.

Given a randomly deployed network with n nodes, we can view it as a random geometric graph $G_{n,r}$ with each edge representing a possible communication link. Without the protection of a secret key, an adversary can eavesdrop conversations between nodes. If each node has several trusted nodes initially, the trust relationship can be considered as a random graph $G_{n,p}$ with each edge connecting a pair of nodes which have shared a secret key. However, random graph does not consider the transmission radius of nodes, but simply assumes any two nodes have the same probability p to establish a connection. When the distance between two nodes is larger than the transmission radius r, they cannot communicate directly. Roughly speaking, $G_{n,p}$ reflects the *logical* trust relationship between nodes, while $G_{n,r}$ depicts the *physical* communication structure of nodes in the network. Secrecy transfer constructs a graph G_{n,n_0} from $G_{n,r}$ and $G_{n,p}$ (where $p = n_0/n$) and turns it to a *secure* random geometric graph by adding secure edges to it.

The construction of secrecy transfer above reveals that, the graph G_{n,n_0} is robust against eavesdrop attack, for each edge is added via the existing trustiness between nodes. If cryptographic attacks are considered impractical, the adversary cannot break $\{K_{AB}\}_{K_{CD}}$ to get the key K_{AB}, for the key K_{CD} shared between C and D is loaded initially.

3. Connectivity Threshold

The component structure of the graph G_{n,n_0} changes gradually as secrecy transfer is applied. As illustrated in Figure 2(a), after the initialization phase, the greatest component of G_{n,n_0} is tree of small order. Gradually, a giant component emerges, swallowing the whole network, provided the underly random geometric graph $G_{n,r}$ is connected and n_0 is large enough.

Suppose two adjacent components, C_A and C_B, have, respectively, m_1 and m_2 vertices, nodes A in C_A and B in C_B

are adjacent. We first estimate the probability P_{m_1,m_2} that two adjacent components C_A and C_B may get connected to form a larger component.

Let random variable $\mathbb{X}$ be the total number of nodes with whom nodes in component C_A are familiar, $\mathbf{X}_i$ be a bernoulli random variable, where $\mathbf{X}_i = 1$ when the circle of acquaintances of node i includes at least one node in the component C_A, $\mathbf{X}_i = 0$ otherwise. Therefore,

$$\mathbb{X} = \mathbf{X}_1 + \mathbf{X}_2 + \cdots + \mathbf{X}_n. \tag{1}$$

If component C_A consists of m_1 nodes, we have the probability of $\mathbf{X}_i = 1$,

$$\mathbb{P}(\mathbf{X}_i = 1) = 1 - (1 - P)^{m_1}, \tag{2}$$

where $P = n_0/n$.

Thus, the expectation of random variable $\mathbf{X}_i$ is $\mathbb{E}(\mathbf{X}_i) = 1 - (1 - P)^{m_1}$.

For $\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_n$ are mutually independent, the expectation of $\mathbb{X}$ is

$$\mathbb{E}(\mathbb{X}) = \sum_{i=1}^{n} \mathbb{E}(\mathbf{X}_i) = n\left[1 - (1 - P)^{m_1}\right], \tag{3}$$

which means that, for a component of order m_1, the circle of acquaintances of this component may consist of $n[1 - (1 - P)^{m_1}]$ nodes on average. Let $a = n[1 - (1 - P)^{m_1}]$, the probability P_{m_1,m_2} that there is at least one common acquaintance between components C_A and C_B is

$$P_{m_1,m_2} = 1 - \left(1 - \frac{a - m_1}{n - m_1}\right)^{m_2}. \tag{4}$$

For example, one may see that, for a network $n = 10,000$, $m_1 = 200$, and $m_2 = 1$, the probability P_{m_1,m_2} tends to 1 when $P > 0.02$. This provides intuition that, a component of order 200 is *attractive* and will *swallow* nodes nearby to form a larger component, a kind of "*rich get richer*" phenomenon. For two components of order $m_1 = m_2 = 50$, the probability P_{m_1,m_2} approximates 1 if $P > 0.002$. In general, the larger the components are, the more likely they are to be mixed together.

In a random graph $G_{n,N}$ with n vertices and N edges, if $N \sim cn$ with $c \geq 1/2$, the greatest component has (with probability tending to 1 for $n \to +\infty$) approximately $n^{2/3}$ vertices [10]. As a special case, when $n = 10,000$, $n^{2/3} \approx 464$, such large component in graph G_{n,n_0} will swallow the whole network with high probability.

Next, we investigate the relationship between the connectivity property of graph G_{n,n_0} and value n_0. To determine the value n_0 which will guarantee the connectivity of graph G_{n,n_0}, we employ a well-known algorithm to generate random graphs $G_{n,p}$ with a given degree distribution [11]. Each graph generated has n nodes and $n_0 = np$ links per node. The algorithm may lead to a multigraph, either by connecting a node to itself or by connecting two nodes together more than once. However, as n increases, these events become rare and their number becomes statistically insignificant.

We first generate a random graph with n nodes and n_0 links per node, then deploy the nodes into a square region to obtain a random topology. For $n = 500$, $r = 35\,\text{m}$, and n_0 varying, we repeat our simulations 50 times to yield an acceptable confidence of results. For each simulation, we measure empirical values for the maximum component and the second component for each trial, averaged over 50 random topologies. In Figure 3, an interesting phenomenon observed is a "*phase transition*" as n_0 increases. There is a critical value of n_0, above which the graph will almost surely be connected. The maximum component grows rapidly from a component of small size to a giant component when $n_0 > 10$. On the contrary, the size of the second component decreases as $n_0 > 10$.

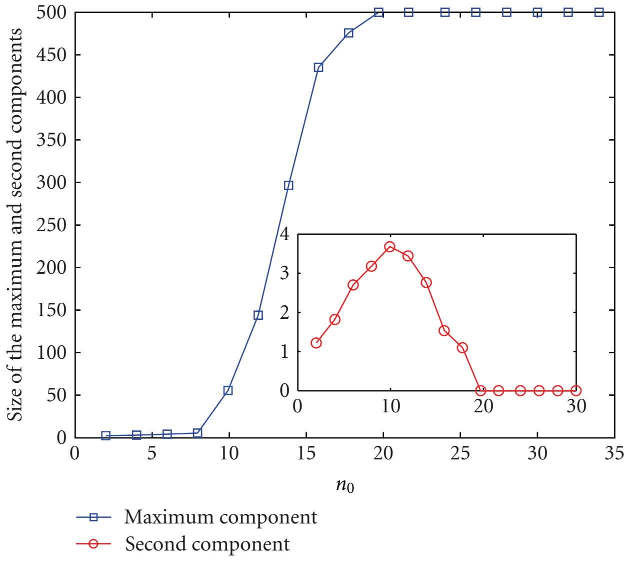


FIGURE 3: Size of the maximum and second components in graph G_{n,n_0} for $n = 500$, $r = 35\,\text{m}$.

Within this context, we want to know, under what conditions is the graph G_{n,n_0} be connected? How can we choose n_0 such that the graph G_{n,n_0} constructed by secrecy transfer will be connected with high probability? The answer to this question is crucial in determining the number of acquaintances that an arbitrary node should have initially.

3.1. Lower Bound of Connectivity Threshold. To get a fully connected graph G_{n,n_0}, two conditions must be satisfied. First, the graph $G_{n,r}$ must be connected, which means that, given the value n and a deployment region, the value r should be large enough to guarantee a connected random geometric graph $G_{n,r}$. Assume n nodes are uniformly deployed in a unit square $[0,1]^2$, the well-known connectivity threshold $r_c = \sqrt{(\log n \pm O(1))/\pi n}$ [5]. Second, the value n_0 must be large enough to get the random graph $G_{n,p}$ fully connected. Consider an arbitrary pair of adjacent nodes A and B in graph G_{n,n_0} which have not established secret key between them. For $G_{n,p}$ is connected, there is at least one path in graph $G_{n,p}$, say $P_{AB} = Ax_0x_1 \cdots x_kB$ between nodes A and B. Given any adjacent nodes in path P_{AB}, say x_i and x_{i+1}, there must exist a path $P' = x_iy_1y_2 \cdots y_tx_{i+1}$ from x_i to x_{i+1} in graph $G_{n,r}$, for graph $G_{n,r}$ is connected.

For a random graph $G_{n,p}$, when p is zero, the graph does not have any edge, whereas when p is one, the graph is fully connected. Bollobás showed that, for monotone properties, there exists a value of p such that the property moves from "nonexistent" to "certainly true" in a very large random graph [1]. The function defining p is called the *threshold function* of a property. Given a desired probability P_c for graph connectivity, the threshold function p of $G_{n,p}$ is defined by

$$P_c = \lim_{n \to \infty} P_r \left[G_{n,p} \text{ is connected} \right] = e^{e^{-c}}, \tag{5}$$

where $p = \ln(n)/n + c/n$ and c is any real constant.

Therefore, given n we can find p for which the resulting graph $G_{n,p}$ is connected with desired probability P_c. Thus, the lower bound of connectivity threshold of n_0 is

$$n_0 = p \times (n-1) = \frac{n-1}{n} [\ln(n) - \ln(-\ln(P_c))]. \tag{6}$$

3.2. Analysis Results of Connectivity Threshold. Notice that when n_0 is below the lower bound of connectivity threshold mentioned above, the graph $G_{n,p}$ is not connected with high probability, and hence the graph G_{n,n_0} also is not connected with high probability. However, a greater n_0 above the lower bound cannot guarantee a connected graph G_{n,n_0} when n' is small, where n' is the average number of neighbors of a node. For a tighter bound of n_0, correlated with n, n', is not known yet, we only present some analysis results of n_0 below.

After the initialization phase of secrecy transfer, we get a random graph. Erdös and Rényi showed that for random graphs, a giant component exists if the average degree of node $\langle k \rangle > 1$[10] . If $\langle k \rangle < 1$ only small components exist, and the size of the largest component is proportional to $\ln n$ (n is the number of nodes in the graph). Exactly at the threshold, $\langle k \rangle = 1$, a component whose size is proportional to $n^{2/3}$ emerges. In the sequel, when $n = 10,000$, $n' = 10$, and $n_0 = 200$, after the initialization phase of secrecy transfer, the average degree of nodes in the graph G_{n,n_0}, $\langle k \rangle = n'(n_0/n) = 10 \times (200/10000) = 0.2$. In this occasion, the initial graph G_{n,n_0} only consists of small components, such as trees of small size. As the simulation results of initialization phase shown in Figure 2(a), the graph G_{n,n_0} only contains small isolated trees. Our goal is to determine how many such components exist, and the probability that they will be connected to form a giant component.

Let the graph G_{n,n_0} in the initialization phase contains components $C_1, C_2, \dots, C_i$, such that the size of component C_i is $|C_i| = \lambda_i$, and $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_i \geq 2$. For two components C_i and C_j of order λ_i and λ_j, if they are adjacent, the probability that they will be connected through secrecy transfer is

$$P_{\lambda_1,\lambda_2} = 1 - \left(1 - \frac{a - \lambda_1}{n - \lambda_1}\right)^{\lambda_2}, \tag{7}$$

where $a = n[1 - (1-P)^{\lambda_1}]$, $P = n_0/n$.

When secrecy transfer is applied, the graph G_{n,n_0} will evolve continuously. A larger component is more attractive and will swallow nodes nearby to form a larger component with high probability. *Popularity is attractive.* If a component can absorb nodes nearby by secrecy transfer, it is termed as *expandable*. Next we estimate the asymptotic probability $P_{\text{expandable}}$ that at least one component in $C_1, C_2, \dots, C_i$ is expandable. At first we estimate the number of neighbors n'_λ of a component of size λ.

Suppose n nodes distributed uniformly and independently at random in a unit area S, that is, $S = 1$. Let a component C of size $|C| = \lambda$ lie inside a circle of radius R, n'_λ neighbors of the component C lie outside the circle and be at distance at most r from nodes in the component. Let S' be a subarea in the deployment area S, $S' \ll S$. The probability that a node is placed within area S' is $P = S'/S = S'$. Then, the probability $P(x)$ that of t nodes are placed in the area S' is

$$P(x = t) = \binom{n}{t} P^t (1-P)^{n-t}. \tag{8}$$

When $n \gg 1$ and $S' \ll S$, we can approximate it with a Poisson distribution,

$$P(x = t) \approx \frac{e^{-nP} \cdot (np)^t}{t!} = \frac{e^{-nS'} (nS')^t}{t!}, \tag{9}$$

and the average number of nodes within area S' is

$$t = nS'. \tag{10}$$

In the initial graph G_{n,n_0}, any component of size λ is small ($\lambda \ll n$), and the area S' it occupied is also small, that is, $S' \ll S = 1$. Therefore, we have approximately

$$\lambda = n\pi R^2, \qquad n' = n\pi r^2. \tag{11}$$

Thus,

$$n'_\lambda = n\left[(R+r)^2 \pi - r^2 \pi\right] = n' + 2\sqrt{\lambda n'}. \tag{12}$$

Therefore, the probability P_λ that a component of size λ is expandable is

$$P_\lambda = 1 - (1 - P_{\lambda,1})^{n'_\lambda}, \tag{13}$$

where $P_{\lambda,1} = (a - \lambda)/(n - \lambda)$, $a = n[1 - (1-P)^\lambda]$, $P = n_0/n$.

For a set of components $C_1, C_2, \dots, C_i$, $|C_i| = \lambda_i$, the probability $P_{\text{expandable}}$ can be calculated as

$$\begin{aligned} &P_{\text{expandable}} \\ &\quad = 1 - (1 - P_{\lambda_1})(1 - P_{\lambda_2}) \cdots (1 - P_{\lambda_i}) \\ &\quad = 1 - (1 - P_{\lambda_1,1})^{n'_{\lambda_1}} (1 - P_{\lambda_2,1})^{n'_{\lambda_2}} \cdots (1 - P_{\lambda_i,1})^{n'_{\lambda_\mathrm{i}}} \\ &\quad \approx 1 - \exp\left\{ -\left(n'_{\lambda_1} P_{\lambda_1,1} + n'_{\lambda_2} P_{\lambda_2,1} + \ldots + n'{}_{\lambda_i} P_{\lambda_i,1} \right) \right\}. \end{aligned} \tag{14}$$

Note that for two sets of components $\mathbb{C} = \{C_1, C_2, \dots, C_i\}$ ($|C_i| = \lambda_i$) and $\mathbb{C}' = \{C'_1, C'_2, \dots, C'_i\}$ ($|C'_i| = \lambda'_i$), if $\lambda_1 \geq \lambda'_1$, $\lambda_2 \geq \lambda'_2$,$\ldots \lambda_i \geq \lambda'_i$, then

$$\begin{gathered} n'_{\lambda_1} \geq n'_{\lambda'_1}, \dots, n'_{\lambda_\mathrm{i}} \geq n'_{\lambda'_i}, \\ P_{\lambda_1,1} \geq P_{\lambda'_1,1}, \dots, P_{\lambda_i,1} \geq P_{\lambda'_i,1}. \end{gathered} \tag{15}$$

Therefore, the probability $P_{\text{expandable}}$ that at least one component in set $\mathbb{C}$ is expandable is greater than that in set $\mathbb{C}'$.

Given parameters n, n', and n_0, after the initialization phase of secrecy transfer, the graph G_{n,n_0} may contain some components $C_1, C_2, \ldots, C_i$. The expandable probability of this component set $P_{\text{expandable}} \rightarrow 1$, implies that at least one component in $C_1, C_2, \ldots, C_i$ is expandable and will grow larger with high probability. Let a component C_1 be expandable and become a larger component C_1' by swallowing nodes nearby. For $|C_1'| > |C_1|$, the expandable probability $P'_{\text{expandable}}$ of components $C_1', C_2, \ldots, C_i$ is greater than the expandable probability $P_{\text{expandable}}$ of components $C_1, C_2, \ldots, C_i$, that is,

$$P'_{\text{expandable}} > P_{\text{expandable}} \longrightarrow 1. \tag{16}$$

Thus, if the expandable probability $P_{\text{expandable}}$ of the initial graph approximates 1, it will become even greater almost surely, and the graph G_{n,n_0} will eventually evolve into a connected graph with high probability if both $G_{n,p}$ and $G_{n,r}$ are connected graphs. However, small expandable probability of the initial graph G_{n,n_0} cannot guarantee a connected graph with high probability and secrecy transfer will terminate with isolated components.

However, exact results of the critical threshold n_0 are not known yet, we only present some analysis results below.

In an Erdös-Rényi random graph $G_{n,N}$ with n nodes and N links [10], if $N \sim l \cdot n^{(k-2)/(k-1)}$ where $l > 0$, then the number of trees of order k contained in $G_{n,N}$ has in the limit for $n \rightarrow +\infty$ a Poisson distribution with mean value

$$\bar{\lambda} = \frac{(2l)^{k-1} k^{k-2}}{k!}. \tag{17}$$

Among these trees, the probability $P_{\text{expandable}}$ that at least one tree of order k is expandable is

$$P_{\text{expandable}} = 1 - (1 - P_k)^{\bar{\lambda}}, \tag{18}$$

where P_k is the probability that a tree of order k is expandable, $P_k = 1 - (1 - P_{k,1})^{n_k'}$, $n_k' = n' + 2\sqrt{kn'}$, $P_{k,1} = (a-k)/(n-k)$, $a = n[1-(1 - n_0/n)^k]$, and $\bar{\lambda} = (2l)^{k-1} k^{k-2}/k!$.

For the graph G_{n,n_0} after the initialization phase of secrecy transfer, the number of links in G_{n,n_0} is

$$N = \frac{1}{2} n \cdot n' P = \frac{1}{2} n \cdot n' \frac{n_0}{n} = \frac{1}{2} n' n_0 \sim l \cdot n^{(k-2)/(k-1)}, \tag{19}$$

which yields the result

$$k \sim 1 + \frac{\ln n}{\ln(2ln/n' n_0)}. \tag{20}$$

Using the above considerations, we can estimate the expandable probability $P_{\text{expandable}}$ of the components (trees) of order k.

We see that, for $n = 10,000$, $n' = 10$, and $n_0 = 100$, the probability $P_{\text{expandable}} \approx 0.6991$; for $n_0 = 200$, the probability $P_{\text{expandable}} \approx 1$. This indicates that, in this occasion, for $n_0 \geq 200$, the graph G_{n,n_0} will eventually evolve into a connected graph by secrecy transfer with high probability. However, for $n_0 < 100$, the graph G_{n,n_0} may be fragmented and contains no giant component of order n. Furthermore, the critical threshold of n_0 is rather sensitive to n'. For $n = 100,000$, $n' = 30$, and $n_0 = 200$, the probability $P_{\text{expandable}} \approx 0.9337$. If we reduce n' to 5, then $P_{\text{expandable}} \approx 0.5391$. This is because the decline in n' will result in the decline in the number of neighbors of a component, so does the expandable probability.

On the other hand, the probability P_0 that secrecy transfer cannot take place after the initialization phase is

$$P_0 = \left[\left(1 - \frac{n_0}{n}\right)^{n'} \right]^n = \left(1 - \frac{n_0}{n}\right)^{n \cdot n'} \approx e^{-n_0 \cdot n'}, \tag{21}$$

which is only dependent on n_0 and n'. Less n_0 or n', higher the probability P_0.

4. Heterogeneous Network

Consider graph $G_{n,r}$ of n nodes with n_0 acquaintances per node randomly selected among the nodes in the graph, we are also interested in the number of rounds needed for secrecy transfer to reach a *stable state*. It is shown in Section 3 that a necessary condition for graph G_{n,n_0} to be connected is that graphs $G_{n,p}$ and $G_{n,r}$ must be fully connected. However, the speed of the convergence of secrecy transfer depends on the values of n_0, r for given n. To gain insight, we first consider the value r and perform a simulation-based study of it. Employing a uniform random generator, we position $n = 500$ nodes in a square planar region of $500 \times 500\,\text{m}^2$, following our deployment from Section 3. For each random topology, we estimate the speed of the convergence of secrecy transfer as the number of rounds that it needs to perform to reach its stable state. At each round, each pair of adjacent nodes in the graph G_{n,n_0} employ secrecy transfer to try to get connected. If there is no new edge is added in this round, secrecy transfer reaches its stable state and terminates. We observe from Figure 4 that, as the value r increases, the stable state is reached with a faster speed, and for value n_0, the number of rounds reaches its peak when n_0 approximates to its connectivity threshold.

Conventionally, a wireless network consists of some nodes as supernodes with greater communication radius than normal nodes. The use of these supernodes lead to important characteristics of complex networks [12]: a small average shortest path length between all nodes, and a high-cluster coefficient, which help us saving network resources, avoiding excessive communication, and reducing the time to data delivery. Figure 5 depicts plots of secrecy transfer with $n = 500$ nodes deployed over a $500 \times 500\,\text{m}^2$ field, $n_0 = 20$, and $r = 35\,\text{m}$, among them there are 25 supernodes (squares in the figures) with a larger communication radius $R = 150\,\text{m}$ and only bidirectional links are considered.

From the simulation results illustrated in Figure 6, we conclude that, compared to the homogeneous network case, for a heterogeneous network with supernodes, as the radius R of supernodes grows, the value of n_0 required to maintain

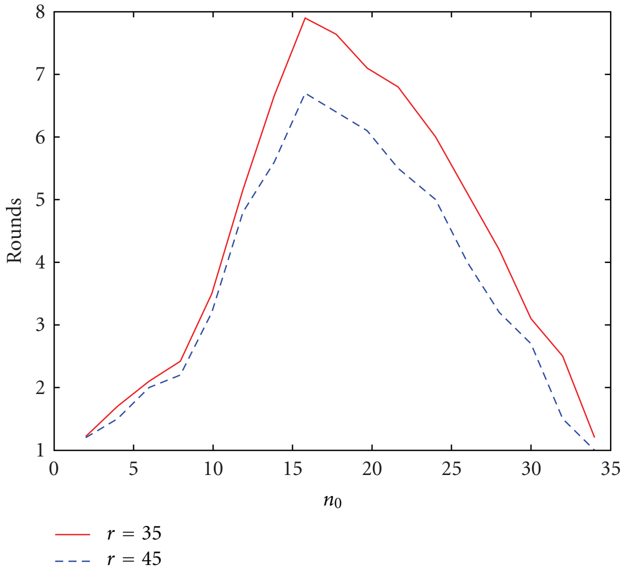


Figure 4: Value n_0 versus. number of rounds of secrecy transfer for various values of the radius r.

connectivity of graph G_{n,n_0} decreases, the speed of the convergence of secrecy transfer accelerates. Hierarchically, supernodes can form a higher layer, while normal nodes constitute a lower layer of the network. An implication of a heterogeneous network is that it has better performance with regard to improving energy, power and topology control, scalability, and fault-tolerance and routing efficiency.

One of the most important properties of a network is the degree distribution, or the fraction $P(k)$ of nodes having k connections (degree k). Although the degree distribution alone is not enough to characterize the network, it has great influence on the network's structure and behavior. A well-known result for Erdös-Rényi random graph is that the degree distribution is Poissonian, $P(k) = e^{-\lambda}\lambda^k/k!$, where $\lambda = \langle k\rangle$ is the average degree. For many real networks, such as the Internet, WWW, citations of scientific articles, airline networks, and many more, they often exhibit a scale-free degree distribution, $P(k) = Ck^{-\gamma}$, $k = m, \dots, K$, where $C \approx (\gamma - 1)m^{\gamma-1}$ is a normalization faction, and m and K are the lower and upper cutoffs for the degree of a node, respectively. A scale-free network with $2 < \gamma < 3$ and N nodes have diameter $d \sim \ln\ln N$ and can be considered as "ultra small-world" network. In fact, the diameter of network is relevant in many fields regarding communication and computer networks, such as routing, searching, and transport of information. All these processes become more efficient when the diameter is smaller.

Intuitively, compared to homogeneous networks, a heterogeneous network with supernodes has a degree distribution different from Poisson distribution. Next, we discuss the degree distribution of heterogeneous networks. Let n nodes and s supernodes be distributed uniformly and independently at random in a square of area 1, $[0,1]^2$, the communication radii of nodes and supernodes are r and R ($r < R$), respectively, and only bidirectional links are taken into considerations.

For a heterogeneous network, there are two degree distributions, one for each type of nodes. For normal nodes with radii r, the degree distribution $P_n(k)$ is Poissonian,

$$P_n(k) = \frac{e^{-\lambda_n}{\lambda_n}^k}{k!}, \quad \text{where } \lambda_n = \langle k\rangle = \pi(n+s)r^2, \tag{22}$$

whereas the degree distribution of supernodes is

$$P_s(k) = \frac{e^{-\lambda_s}{\lambda_s}^k}{k!}, \quad \text{where } \lambda_s = \langle k\rangle = \pi\left(nr^2 + sR^2\right). \tag{23}$$

Therefore, the degree distribution $P_{2-h}(k)$ of the heterogeneous network is

$$P_{2-h}(k) = \frac{n}{n+s}P_n(k) + \frac{s}{n+s}P_s(k). \tag{24}$$

From the degree distribution $P_{2-h}(k)$ derived above, we depict and compare it with two different networks. In Figure 7(a) we show the degree distribution of a heterogeneous network with $n = 9{,}000$, $s = 1{,}000$, $r = 0.01$, and $R = 0.1$. In Figure 7(b), we compare $P_{2-h}(k)$ with power law $P(k) = k^{-2}$ and Poisson distribution $P(k) = \lambda^k e^{-\lambda}/k!$, where $\lambda = (n+s)\pi r^2$. As the figures shown, the degree distribution of a heterogeneous network with two peaks is different from a Poisson distribution and right-skewed to a power law. The results imply that the behavior of a heterogeneous network has some characteristics of scale-free network, such as small diameter.

Now consider the placement of nodes with more types. Suppose that the network contains t types of nodes, denoted as $T_1, T_2, \dots, T_t$. For nodes of type T_i, the number of nodes $|T_i|$ in it and node's communication radius r_i satisfy the conditions,

$$\begin{gathered} r_1 < r_2 < \cdots < r_t, \\ |T_1| > |T_2| > \cdots > |T_t|. \end{gathered} \tag{25}$$

For simplicity, let n denote the total number of nodes in the network, and

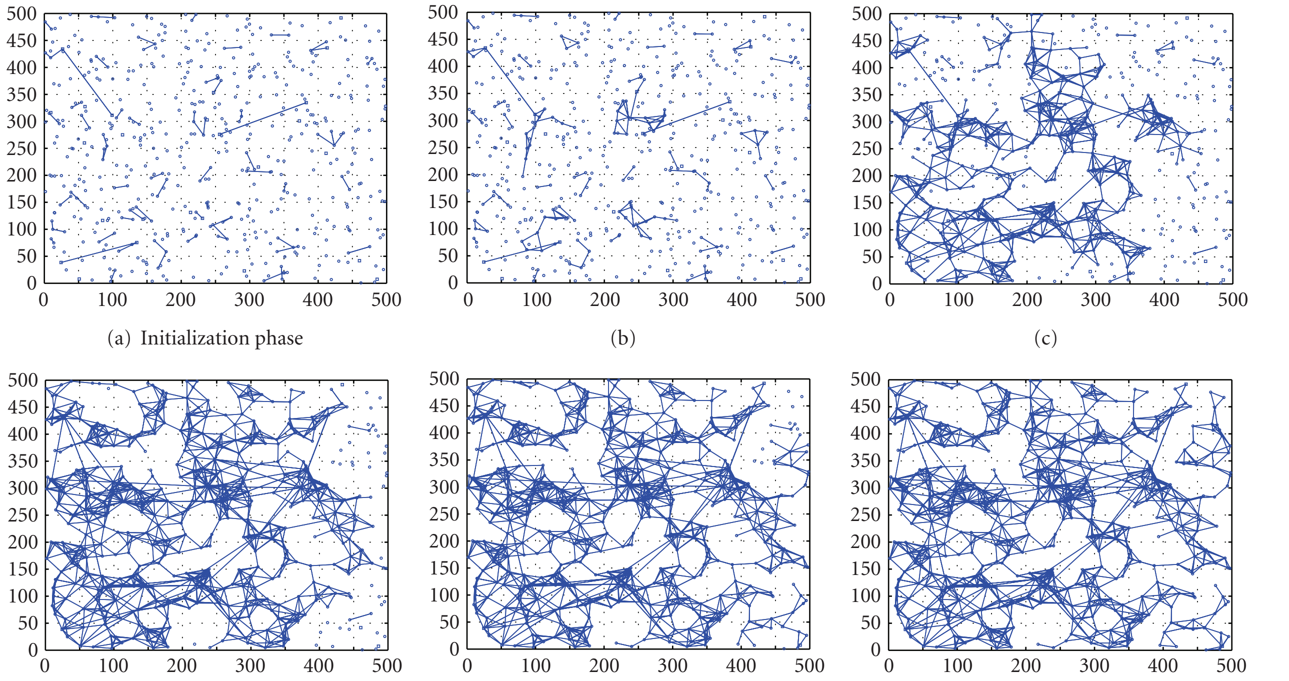
$$|T_1| = \frac{n}{2}, \qquad |T_2| = \frac{n}{2^2}, \dots, \qquad |T_t| = \frac{n}{2^t}. \tag{26}$$

It is clear that when $n \to +\infty$ and $t \to +\infty$,

$$|T_1| + |T_2| + \cdots + |T_t| = n \cdot \sum_{i=1}^{t} \frac{1}{2^i} \longrightarrow n. \tag{27}$$

Recall that the degree of each type of nodes has a Poisson distribution with different mean value. To derive the degree distribution $P_{t-h}(k)$ of the network, we first determine the degree distribution $P_i(k)$ of nodes of type T_i,

$$P_i(k) = \frac{e^{-\lambda_i}\lambda_i^k}{k!}, \quad (i = 1, \dots, t), \tag{28}$$



(a) Initialization phase

(b)

(c)

(d)

(e)

(f) stable state

Figure 5: Secrecy transfer process in a heterogeneous network, $n = 500$, $s = 25$, $r = 35$ m, and $R = 150$ m.

where,

$$\begin{aligned}
\lambda_1 &= \pi r_1^2 n,\\
\lambda_2 &= \pi \frac{r_1^2 + r_2^2}{2} n,\\
\lambda_3 &= \pi \frac{2r_1^2 + r_2^2 + r_3^2}{4} n,\\
\lambda_4 &= \pi \frac{4r_1^2 + 2r_2^2 + r_3^2 + r_4^2}{8} n,\\
\lambda_5 &= \pi \frac{8r_1^2 + 4r_2^2 + 2r_3^2 + r_4^2 + r_5^2}{16} n,\\
&\cdots\cdots .
\end{aligned} \tag{29}$$

Therefore, the degree distribution of the heterogeneous network with t types of nodes is

$$\begin{aligned}
P_{t-h}(k) &= \frac{1}{2} P_1(k) + \frac{1}{4} P_2(k) + \cdots + \frac{1}{2^t} P_t(k)\\
&= \frac{1}{k!}\left(\frac{1}{2} e^{-\lambda_1}\lambda_1^k + \frac{1}{4} e^{-\lambda_2}\lambda_2^k + \cdots + \frac{1}{2^t} e^{-\lambda_t}\lambda_t^k\right).
\end{aligned} \tag{30}$$

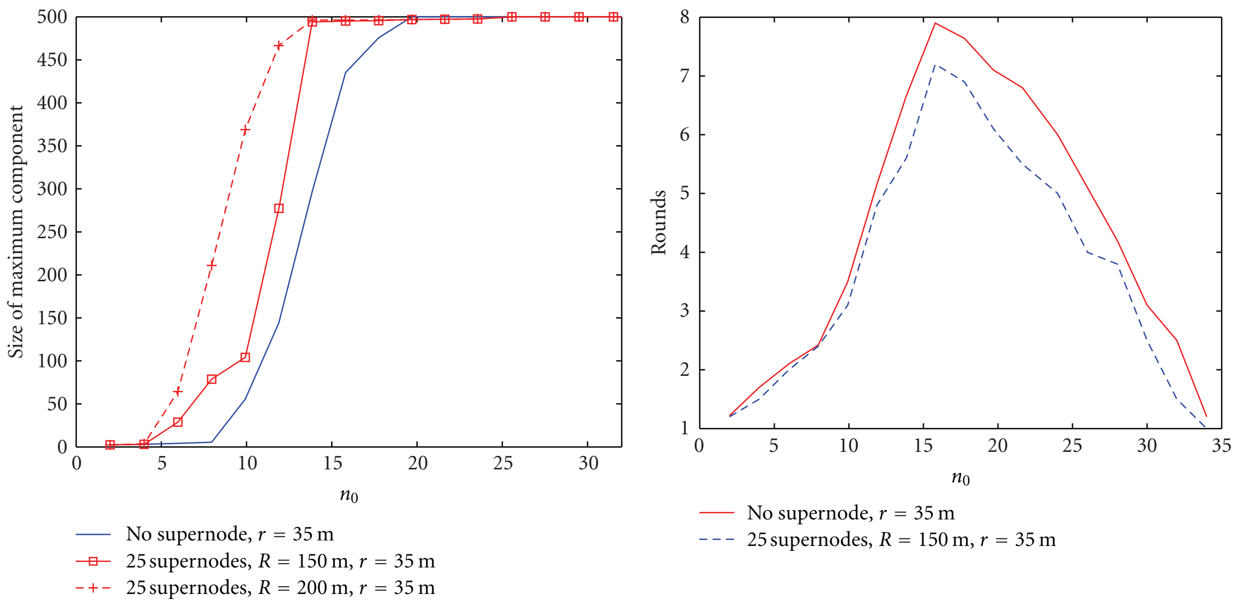
For $P_{t-h}(k)$ is complicated, we present some numerical results on it. Figure 8 shows the degree distribution $P_{t-h}(k)$ for $r_1 = 0.01$, $r_2 = 0.03$, $r_3 = 0.05$, $r_4 = 0.07$, $r_5 = 0.09$, $r_6 = 0.11$, $r_7 = 0.13$, and $r_8 = 0.2$. As expected, the degree distribution of the heterogeneous network approaches power law $P(k) \propto k^{-2}$. This implies that heterogeneous network maintains some statistical properties of a scale-free network. Therefore, it is plausible that the convergence speed of secrecy transfer in a heterogeneous network is faster than that in a homogeneous network.

5. Implementation of Secrecy Transfer

In this section, we elaborate the implementation method of secrecy transfer. The method contains three phases: the initialization phase, the secrecy transfer phase, and the update phase. To implement secrecy transfer efficiently, we use Bloom Filter [13] for membership queries.

Bloom Filter. A Bloom Filter is a popular data structure used for membership queries. It represents a set $S = [s_1, \ldots, s_n]$ using k independent hash functions $h_1, \ldots, h_k$ and a string of m bits, each of which is initially set to 0. For each $s \in S$, we hash it with all the k hash functions and obtain their values $h_i(s)$ $(1 \le i \le k)$. The bits corresponding to these values are then set to 1 in the string. To determine whether an item s' is in S, bits $h_i(s')$ are checked. If all these bits are 1s, s' is considered to be in S.

Since multiple hash values may map to the same bit, Bloom Filter may yield false positives. That is, an element is not in S but its bits $h_i(s)$ are collectively marked by elements in S. If the hash is uniformly random over m values, the probability that a bit is 0 after all the n elements are hashed and their bits marked is $(1 - 1/m)^{kn} \approx e^{-kn/m}$. Therefore, the probability for a false positive is $(1 - (1 - 1/m)^{kn})^k \approx (1 - e^{-kn/m})^k$. The right hand side is minimized when $k = (m/n) \ln 2$ in which case it becomes $(1/2)^k = (0.6185)^{m/n}$.



(a)

(b)

Figure 6: The maximum component and rounds of secrecy transfer in heterogeneous networks.

5.1. Initialization Phase. We first generate a random graph with n nodes and n_0 links per node. For each link a secret key is assigned to it. Each node stores the ID of its neighbors and the corresponding secret key between them. For instance, if node i has n_0 neighbors $i_1, \ldots, i_{n_0}$, it constructs an *acquaintanceship set*

$$A_i = \left\{ \left(i_1, K_{i,i_1}\right), \ldots, \left(i_{n_0}, K_{i,i_{n_0}}\right) \right\}, \tag{31}$$

where K_{i,i_1} is the assigned secret key between node i and its neighbor i_1.

After that nodes are deployed randomly over a field.

5.2. Secrecy Transfer Phase. Suppose two adjacent components, C_A and C_B, have, respectively, m_1 and m_2 nodes, nodes $A \in C_A$ and $B \in C_B$ are adjacent. For component C_A, a *component head* (at first after initialization phase, each node is a component head of its own since all nodes are isolated. After several rounds of secrecy transfer process, some large components emerge. To reduce the communication cost, a node is selected to be a component head according to its centrality in the component. To simply the procedure, the node with the highest degree is chosen to be the component head) is selected. He stores all the ID of nodes belonging to the component C_A in a *component member set*

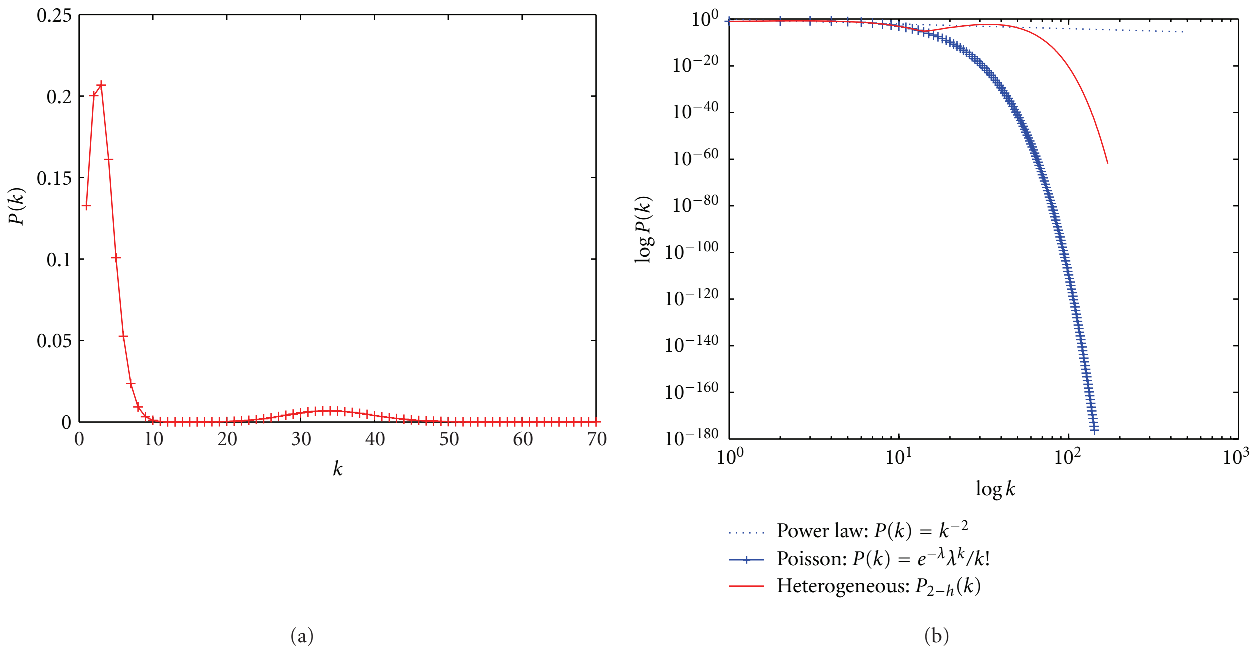
$$\mathrm{CM}_{C_A} = \{a_1, \ldots, a_{m_1}\}, \tag{32}$$

where $a_i \in C_A$.

Each node stores a Bloom Filter BF_{C_A} which contains all the nodes in the acquaintance circle of C_A. That is, the nodes in C_A and the acquaintances of node i for all $i \in C_A$. If an adjacent node k is added to C_A, the Bloom Filter BF_k of node k is inserted into BF_{C_A}, that is, a new Bloom Filter $\mathrm{BF}_{C'_A}$ for the new component $C'_A = C_A + k$ is created, that is, $\mathrm{BF}_{C'_A} = \mathrm{BF}_{C_A} + \mathrm{BF}_k$.

If two components C_A and C_B get connected and melt into a larger component C_{AB}, a new Bloom Filter of component C_{AB}, $\mathrm{BF}_{C_{AB}} = \mathrm{BF}_{C_A} + \mathrm{BF}_{C_B}$, is created and stored in nodes of C_{AB}. To further improve the performance, not all nodes in C_A or C_B need to update its BF_{C_A} or BF_{C_B} to $\mathrm{BF}_{C_{AB}}$, only nodes whose neighbors are not all connected to them need to store the updated Bloom Filter $\mathrm{BF}_{C_{AB}}$ of the new component C_{AB}. As depicted in Figure 9, C_A and C_B melt into a larger component C_{AB}, an isolated node E is adjacent to nodes A, B, F, and G. After C_A and C_B get connected, only nodes A, B, F, and G in C_{AB} have unconnected neighbor. Therefore, they need to store the new $\mathrm{BF}_{C_{AB}}$ and will broadcast it later.

Next, we give an overview of the operations of secrecy transfer. In general, the operation of secrecy transfer is initiated by a new created component. Let C_A be a new component that has "swallowed" node H, nodes A and F have already updated their BF_{C_A} (to insert the ID of node H into it), and let C_B be an adjacent component of C_A. After that, nodes A and F broadcast BF_{C_A} to their adjacent nodes B and E. On receiving the BF_{C_A} from component C_A, node B sends a query message containing BF_{C_A} to the component head of C_B, say node I, where the component member set of C_B, $\mathrm{CM}_{C_B} = \{b_1, \ldots, b_{m_2}\}$, is stored. The component head I then determines whether the nodes in set CM_{C_B} are in the Bloom Filter BF_{C_A}. If a node, say $D \in \mathrm{CM}_{C_B}$, is found in the Bloom Filter BF_{C_A}, node I answers node B by sending D to it. Node B then tells A that there is a node $D \in C_B$ belonging to the acquaintance circle of component C_A. After that, nodes A broadcasts a query message with the ID of node D in component C_A. Each node in C_A verifies whether node D belongs to its acquaintanceship set. As illustrated in Figure 9,



(a)

(b)

Figure 7: Degree distributions for different networks. The horizontal axis is node degree k (or $\log k$), and the vertical axis is the probability distribution $P(k)$ (or $\log P(k)$) of degrees, that is, the fraction of nodes that have degree greater than or equal to k. The network shown in (a) is a heterogeneous network with two types of nodes, three networks (of power law, heterogeneous, and Poisson distribution) are depicted in (b) with a logarithmic degree scale.

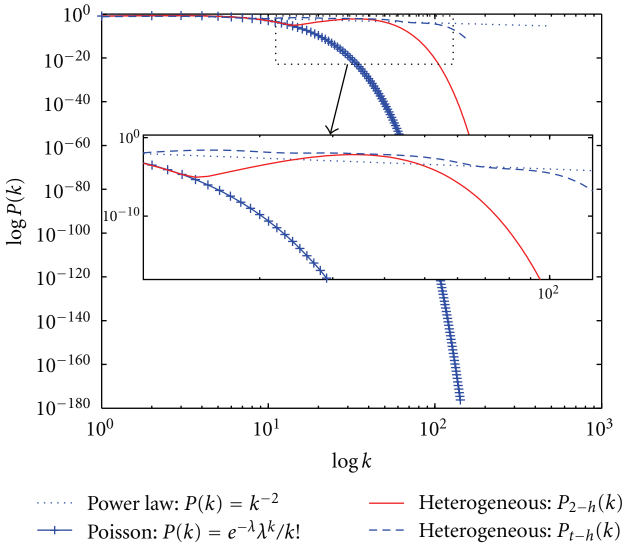


Figure 8: Degree distributions.

if the acquaintanceship set of node $C \in C_A$ contains node D, that is, $A_C = \{\ldots,(D,K_{CD}),\ldots\}$, the node C transmits a response message (C, D) to node A. After obtaining the acquaintance node pair (C, D) from C, node A knows that nodes $C \in C_A$ and $D \in C_B$ are acquaint with each other (they have a shared key K_{CD}). Now nodes A and B can establish a secret key K_{AB} as mentioned in Section 2.

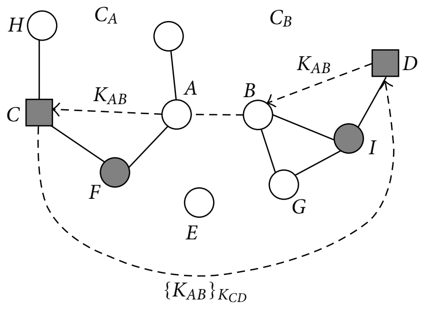


Figure 9: Secrecy transfer phase.

5.3. Updated Phase. After the secret key K_{AB} between nodes A and B is established, two components become a larger component C_{AB}, we then should update the acquaintance circle of C_{AB} for nodes who have unconnected neighbors. A new component head is also need to be selected according to the degree distribution of nodes in C_{AB}. As to the network in Figure 9, if node I is the new component head of C_{AB}, the component member set is updated to be

$$\mathrm{CM}_{A_B} = \mathrm{CM}_{C_A} + \mathrm{CM}_{C_B} = \{a_1,\ldots,a_{m_1},b_1,\ldots,b_{m_2}\}. \quad (33)$$

Finally, if nodes have updated their Bloom Filter $\mathrm{BF}_{C_{AB}}$, they broadcast the new $\mathrm{BF}_{C_{AB}}$ to their neighbors to find chances for new links. Recursively, this procedure is applied until there is no node has updated its Bloom Filter.

5.4. Security Analysis. As discussed in Section 2, secrecy transfer is robust against eavesdrop attack, for each edge is added via the existing trustiness between nodes. In this subsection, we study the resilience of secrecy transfer against the node compromise attack. Let n_c denote the number of nodes that have been captured. Suppose the compromised nodes are independently and random distributed among the entire deployment region.

Theoretically, as depicted in Figure 9, if any node in the paths $A-F-C$ and $D-I-B$ is compromised, the key K_{AB} between nodes A and B is not secure. Suppose that the length of two paths are l_1 and l_2, respectively. It is easy to estimate the probability that a new established key K_{AB} is compromised as the following:

$$P\{K_{AB}\,\text{is compromised}\} = 1 - \frac{\binom{l_1+l_2}{n-n_c}}{\binom{l_1+l_2}{n}}, \qquad (34)$$

where n is the number of node in the network.

Unfortunately, even if all nodes in two paths are not compromised, the key K_{AB} may be unsecure. For instance, let a path from A to C be $A-H_1-H_2-H_3-H_4-C$, and all nodes in the path have not been compromised. Node A sends K_{AB} to H_1 by sending $\{K_{AB}\}_{K_{AH_1}}$, H_1 then transmits $\{K_{AB}\}_{K_{H_1H_2}}$ to node H_2 until K_{AB} reaches the last node C. If $K_{AH_1}, K_{H_1H_2}, \ldots, K_{H_4C}$ are not compromised, K_{AB} is still secure after it is transmitted across the path. However, if a key, such as $K_{H_1H_2}$, is compromised, an adversary may eavesdrop on the communication flows between nodes H_1 and H_2 to obtain $\{K_{AB}\}_{K_{H_1H_2}}$, thus K_{AB} is leaked.

In general, if there are compromised nodes in the network, any key established by secrecy transfer between two neighbors H_1 and H_2 may be unsecure unless nodes H_1 and H_2 are acquaint with each other initially. For any pair of acquaintance nodes, the secret key between them is preloaded before the network is deployed and is considered unbreakable (unless the node is compromised). As to any key established by secrecy transfer, compromised nodes may degrade its security since lots of nodes are involved in the process of the negotiation of a new link key.

In order to set up a more secure channel between nodes A and C, it is reasonable to use the acquaintanceship set of nodes. Suppose in a path $A-H_1-H_2-H_3-H_4-C$, (A, H_3), (H_1, H_3), and (H_1, C) are three pair of acquaintances. To send a secret key K_{AB} to C, node A can send $\{K_{AB}\}_{K_{AH_3}}$ to H_3, H_3 then sends $\{K_{AB}\}_{K_{H_1H_3}}$ to H_1. At last, node C can get $\{K_{AB}\}_{K_{H_1C}}$ from H_1. The advantage of this method is that all communications are encrypted with predistributed keys. If nodes A, C, H_1, and H_3 are not compromised, the key K_{AB} is secure after the transmission. However, such a secure logical path in a set of nodes may not exist. For a path of l nodes, their initial acquaintanceship can be viewed as a random graph $\widehat{G}_{n,p}$, where $n = l$ and $p = n_0/n$. If $\widehat{G}_{n,p}$ is connected, a logical path exists.

If an adversary is not present at the network before secrecy transfer has completed, or it takes more time than a secure interval to compromise nodes, the communication links established by secrecy transfer are secure; otherwise, undetected malicious nodes may degrade the security of secrecy transfer and jeopardize the network. In [14], authors investigated the potentially disastrous threat of node compromise spreading (via communication and preestablished mutual trust) in wireless sensor networks and proposed an epidemiological model to investigate the probability of a breakout. This model can be adapted to analyze the spread of malicious behavior of compromised nodes in the process of secrecy transfer. But how to design efficient countermeasures is still unknown.

5.5. Storage Overhead. A node, say i, needs to store

(1) an *acquaintanceship set*

$$A_i = \left\{(i_1, K_{i,i_1}), (i_2, K_{i,i_2}), \ldots, \left(i_{n_0}, K_{i,i_{n_0}}\right)\right\}, \qquad (35)$$

where $i_1, i_2, \ldots, i_{n_0}$ are the acquaintances of node i, $K_{i,i_1}, K_{i,i_2}, \ldots, K_{i,i_{n_0}}$ are the corresponding secret keys with each acquaintance, respectively.

(2) n' secret keys established with its neighbors,

(3) a Bloom Filter BF_{C_A} $(i \in C_A)$.

For a component head j $(j \in C_A)$, in addition to the secret values a normal node stores, it also stores a *component member set*

$$\text{CM}_{C_A} = \{a_1, \ldots, a_m\}, \qquad (36)$$

where $a_1, \ldots, a_m$ are the members of component C_A, m is the cardinality of the component.

6. Applications of Secrecy Transfer

The need for untethered distributed communications and computing continues to drive advances in mobile communications and wireless networking. To serve this purpose, wireless sensor networks have been envisioned to consist of groups of lightweight sensor nodes that may be randomly and densely deployed to observe data within a physical region of interest [15].

In many applications, such as target tracking, battlefield surveillance, and intruder detection, sensor networks are often deployed in hostile environments. To protect the sensitive data, secret keys should be established to achieve data confidentially, integrity, and authentication between communicating parties [16–19]. The first practical key predistribution scheme for sensor network is random key predistribution scheme introduced by Eschenauer and Gligor [7]. Its operation can be briefly described as follows. A random pool S of keys is selected from the key space. Each sensor node receives a random subset of m keys (key ring) from the key pool before deployment. Any two nodes able to find one common key within their respective subsets can use that key as their shared secret to initiate communication. Moreover, the network can be viewed as a random graph $G_{n,p}$, each edge added if two adjacent nodes can find one common key within their key rings. A major advantage of this scheme is the exclusion of base stations in key management, but a fixed number of compromised sensors causes a fraction of the remaining network to become insecure. Successive sensor captures enable the adversary to reveal network key pool and use them to attack other sensors. In addition, the storage overhead is still high for lightweight sensor nodes. As mentioned previously, secrecy transfer can turn a random graph to a secure random geometric graph. If secrecy transfer is applied with the random key predistribution scheme, the storage overhead of nodes is lower and it can achieve better resilience against node capture attack.

In [20], an asymmetric key predistribution scheme AKPS for sensor networks was proposed. Each nodes only store two secret values initially, a large amount of storage is shifted to keying material servers (KMS). Since AKPS needs to provide public keying material for any pair of nodes, a KMS should store $\binom{n}{2}$ public keying material for a network of n nodes. Roughly speaking, AKPS is not viable for arbitrary large network. We find that, if secrecy transfer is used, a KMS does not need to be preloaded with $\binom{n}{2}$ public keying material. Specially, suppose n^* out of $\binom{n}{2}$ public keying material are randomly picked, the initial probability that two arbitrary sensors can establish a secret key is $p = n^*/\binom{n}{2} = 2n^*/n(n-1)$, which means that, any nodes has $n_0 = n \times p = 2n^*/(n-1)$ "acquaintances" on average. As before, if n_0 is larger than the connectivity threshold, we can repeat the construction process of secrecy transfer to get a connected graph G_{n,n_0} which will guarantee that any pair of adjacent nodes can establish secret keys.

7. Conclusion

This work presented a secrecy transfer algorithm which is directly based on the idea that networks form primarily by people introducing pairs of their acquaintances to one another. The resulting network, showing both properties of random graph and random geometric graph, cannot only model the introduction process in social networks, but also be used to protect the network.

Acknowledgments

This work is supported by Program for Changjiang Scholars and Innovative Research Team in University (IRT1078), the Key Program of NSFC-Guangdong Union Foundation (U1135002), Major national S&T program (2011ZX03005-002), National Natural Science Foundation of China (61173135, 61100230, 61100233), and the Natural Science Basic Research Plan in Shaanxi Province of China (2011JM8004). It is also supported partly by Mobile Network Security Technology Research Center of Kyungpook National University, Republic of Korea.

References

[1] B. Bollobás, *Random Graphs*, Cambridge University Press, 2nd edition, 2001.

[2] M. Penrose, *Random Geometric Graphs*, Oxford Studies in Probability, Oxford University Press, Oxford, UK, 2003.

[3] M. Altmann, "Susceptible-infected-removed epidemic models with dynamic partnerships.," *Journal of Mathematical Biology*, vol. 33, no. 6, pp. 661–675, 1995.

[4] C. Bettstetter, "On the minimum node degree and connectivity of a wireless multihop network," in *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC '02)*, pp. 80–91, ACM, June 2002.

[5] P. Gupta and P. R. Kumar, "The capacity of wireless networks," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 388–404, 2000.

[6] R. Di Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan, "Redoubtable sensor networks," *ACM Transactions on Information and System Security*, vol. 11, no. 3, article 13, 2008.

[7] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 41–47, November 2002.

[8] Z. Liu, J. Ma, Q. Pei, L. Pang, and Y. Park, "Key infection, secrecy transfer, and key evolution for sensor networks," *IEEE Transactions on Wireless Communications*, vol. 9, no. 8, pp. 2643–2653, 2010.

[9] R. Anderson, H. Chan, and A. Perrig, "Key infection: smart trust for smart dust," in *Proceedings of the 12th IEEE International Conference on Network Protocols (ICNP '04)*, pp. 206–215, Berlin, Germany, October 2004.

[10] P. Erdös and A. Rényi, "On the evolution of random graphs," *Publication of the Mathematical Institute of the Hungarian Academy of Sciences*, vol. 5, pp. 17–61, 1960.

[11] B. Bollobás, "A probability proof of an asymptotic formula for the number of labelled regular graphs," *European Journal of Combinatorics*, vol. 1, pp. 311–316, 1980.

[12] M. E. J. Newman, "The structure and function of complex networks," *SIAM Review*, vol. 45, no. 2, pp. 167–256, 2003.

[13] B. H, Bloom, "Space/time trade-offs in hash coding with allowable errors," *Communications of the ACM*, vol. 13, no. 7, pp. 422–426, 1970.

[14] P. De, Y. Liu, and S. K. Das, "Deployment-aware modeling of node compromise spread in wireless sensor networks using epidemic theory," *ACM Transactions on Sensor Networks*, vol. 5, no. 3, pp. 1–33, 2009.

[15] N. M. Freris, H. Kowshik, and P. R. Kumar, "Fundamentals of large sensor networks: connectivity, capacity, clocks, and computation," *Proceedings of the IEEE*, vol. 98, no. 11, pp. 1828–1846, 2010.

[16] V. C. Giruka, M. Singhal, J. Royalty, and S. Varanasi, "Security in wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 8, no. 1, pp. 1–24, 2008.

[17] J. Jeong and Z. J. Haas, "Predeployed secure key distribution mechanisms in sensor networks: current state-of-the-art and a new approach using time information," *IEEE Wireless Communications*, vol. 15, no. 4, pp. 42–51, 2008.

[18] L. Ma, X. Cheng, F. Liu, F. An, and J. Rivera, "iPAK: an in-situ pairwise key bootstrapping scheme for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 18, no. 8, pp. 1174–1184, 2007.

[19] J. C. Lee, V. C. M. Leung, K. H. Wong, J. Cao, and H. C. B. Chan, "Key management issues in wireless sensor networks: current proposals and future developments," *IEEE Wireless Communications*, vol. 14, no. 5, pp. 76–84, 2007.

[20] Z. Liu, J. Ma, Q. Huang, and S. Moon, "Asymmetric Key Predistribution Scheme for sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1366–1372, 2009.

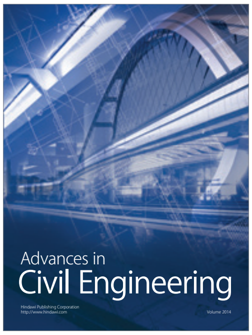
Journal of
Engineering

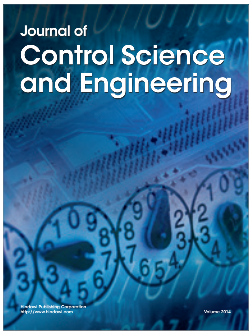
The Scientific World Journal

International Journal of
Rotating Machinery

Journal of
Sensors

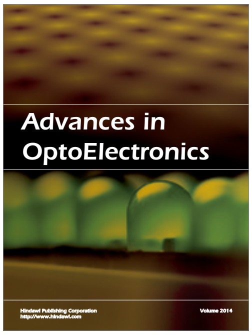
International Journal of
Distributed Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science and Engineering

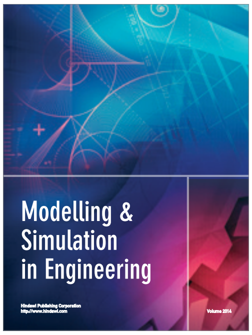
Journal of
Robotics

Journal of
Electrical and Computer Engineering

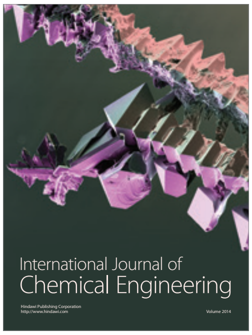

Advances in
OptoElectronics

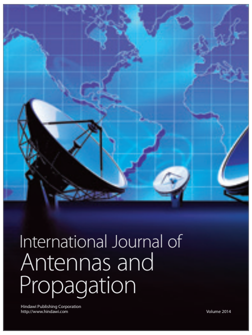
VLSI Design

International Journal of
Navigation and Observation

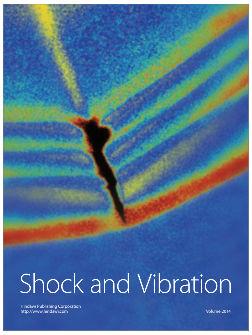

Modelling & Simulation in Engineering

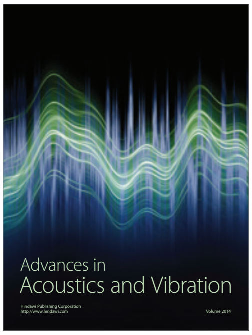
International Journal of
Aerospace Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration