International Journal of Networked and Distributed Computing, Vol. 4, No. 2 (April 2016), 75-84

Percolation Thresholds on Tree-Based Communities of Wireless Sensor Networks*

Qiao Li[1] †, Zhendong Niu[1], Baihai Zhang[2], Lingguo Cui[2], Bin Wu[3]

[1] *School of Computer Science and Technology, Beijing Institute of Technology, No. 5 South Zhong Guan Cun Street, Beijing, 100081, China*

E-mail: liqiao2012@outlook.com, zniu@bit.edu.cn

[2] *School of Automation, Beijing Institute of Technology, No. 5 South Zhong Guan Cun Street, Beijing, 100081, China*

E-mail: smczhang@bit.edu.cn, cuilingguo@bit.edu.cn

[3] *Science and Technology on Space Physics Laboratory, No. 1 South Da Hong Men Street, Beijing, 100076, China*

E-mail: wubin_005@163.com

Abstract

Many efficient deployments of large-scale wireless sensor networks based on the tree-based community rise into view recently. Sensor nodes are severely resource constrained, and lack sophisticated defense mechanisms to fight virus attacks. Cyber viruses spread through node populations over the networks, and a number of results about the prevalence have been derived in recent years by exploiting epidemic behaviors and the percolation processes on networks. A network model based on the Cayley tree is proposed to depict the underlying tree-based architectures of the network and the community. The percolation thresholds are calculated and analyzed in two cases. Due to random links in the communities, the sensor virus extends drastically on the network. The analysis and evaluation shows that the percolation threshold keeps decreasing with the increase of the shortcut probability. There is the smallest percolation threshold in a random network, where the virus easily attacks the network from one side to another. The conclusions can further our understanding of epidemic dynamics on tree-based communities of wireless sensor networks.

Keywords: Cayley tree; community; epidemic; percolation threshold

* This work is supported by the National Natural Science Foundation of China under Grant No. 61203144, the General Financial Grant from the China Postdoctoral Science Foundation under Grant No. 2013M540869, and the Open Fund of Guangdong Provincial Digital Signal and Image Processing Technologies Key Laboratory under Grant No. 2013GDDSIPL-06.

† Corresponding author.

1. Introduction

Recent years have seen the deployments of large-scale wireless sensor networks in a variety of applications including habitat and environmental monitoring,[1] precision agriculture,[2] security surveillance,[3] etc. New features and design trends have emerged in large-scale wireless sensor networks, making those networks appeal not only to the scientific community but also to the industry. One such trend is the running of different applications on heterogeneous sensor nodes deployed in multiple networks in order to better exploit the expensive physical network infrastructure. It is crucial to design mechanisms which effectively coordinate available resources to optimize the resource utilization while meeting different application requirements. Many efficient deployments based on the community rise into view recently.[4,5,6]

The community is one of the common properties (Other properties include the small world effect,[7] the right-skewed degree distribution,[8] the clustering,[9] et al.) of the network. Qualitatively, the community is defined as a subset of nodes within the graph such that connections between the nodes are denser than connections with the rest of the network. ZIGBEE and IEEE Std. 802.15.4 can construct tree-based communities in a broad deployment area if every node is the Full Function Device (FFD).[10] F. Wei et al. proposed an autonomous community construction technology to achieve real-time transmission in the multiple emergencies' situation.[11] Emergency information can be transmitted in the community and protected from the interference of other information's transmission. J. Y. Wu et al. proposed a routing protocol called community structure clustering routing protocol (CSCR).[12] CSCR divides the network into densely connected subgroups through the algorithm of detecting community structure. It balances the energy consumption and extends the lifetime of wireless sensor networks. T. Y. Chuang and K. C. Chen developed an information-centric processing methodology based on the community structure to achieve self-organizing sensor networks.[13] Combining the community structure with the data recovery algorithms, a self-organizing management scheme was proposed to mitigate the sensor maintenance costs.

Compared with regular computer systems, the large-scale wireless sensor network is even easier for sensors to be compromised by virus attacks.[14,15,16] The sensor node does not have complicated hardware architecture or operating system to protect its safety due to cost and resource constraints. The cyber attack by the worm presents one of the most dangerous threats to the security and integrity of the wireless sensor network. In according to the percolation theory, there exists a percolation threshold in the network.[17] B. Wang et al. proposed a random clique network model which was composed of different orders of cliques to study two interacting diseases spreading in networks with community structures.[18] Y. Feng et al. considered a pair of homogeneous diseases spreading concurrently on uniform networks based on the Susceptible-Infectious-Susceptible (SIS) model.[19] A new model describing the transmission process of the interacting diseases was established. C. H. Li et al. studied the spreading of infections in complex heterogeneous networks based on a Susceptible-Infectious-Recovered-Susceptible (SIRS) epidemic model with birth and death rates.[20] They found that the dynamics of the network-based SIRS model were completely determined by a threshold value. X. L. Peng et al. analyzed the influence of the effective vaccination intervention on the threshold and prevalence in the hybrid network.[21] They found that the vaccination could linearly decrease the epidemic prevalence in hybrid networks. The immunization is one of the most common and successful strategies for combating the outbreak of infectious diseases.[22]

The network is represented by a graph in which vertices are individuals and undirected edges are contacts. The epidemic begins with a single individual and spreads along the contacts. We assume a generalized Susceptible-Infectious (SI) dynamic for the cyber virus in which the virus spreads on the network with a infection probability h. This dynamic can be mapped onto a site percolation process on the wireless sensor network. The connected clusters of nodes in the percolation process correspond to the groups of individuals who would be infected by the epidemic starting with any node within that cluster.

Typically, there are only a small number of infected nodes in the network for the small value of h, and the virus will die naturally in the prevalence. But above some critical h_c an extensive spanning cluster or giant component appears. Once such a giant component is present, the cyber virus attacks the network from one side to another and thereby reaches an extensive fraction of the network. The value of h_c at which the giant component first forms is called the percolation threshold. We focus on tree-based communities of large-scale wireless sensor networks and analyze the spatial-temporal dynamics of the virus prevalence in this paper. The contributions include the following aspects. A network model based on the Cayley tree[23] is proposed to depict the underlying tree-based architectures of the network and the community. The percolation thresholds are calculated in two cases. The analysis and evaluation shows that the percolation threshold keeps decreasing with the increase of the shortcut probability in the tree-based communities of wireless sensor networks. There is the smallest percolation threshold in a random network, where the virus easily attacks the network from one side to another.

The rest of the paper is organized as follows. The network model and preliminaries are proposed in Section 2. Percolation thresholds are calculated in Section 3. The evaluation and analysis is presented in Section 4. The paper concludes in Section 5.

2. Network Model and Preliminaries

We consider the following two problems which motivate our study:

- *Problem* 1. The efficient deployments result in variable network architectures. How should we abstract the main structure characteristics to describe the hierarchical architectures.
- *Problem* 2. How should we describe the cyber virus propagations[24] on the hierarchical architectures and calculate the percolation thresholds.

A community is generally thought as a part of a network where internal connections are denser than external ones. Many possible definitions of communities exist in the literature. The basic quantity to consider is k_i, the degree of a generic node i, which in terms of the adjacency matrix $A_{i,j}$ of the network G is $k_i = \sum_j A_{i,j}$. If we consider a subgraph $V \subset G$, to which node i belongs, we can split the total degree in two contributions: $k_i(V) = k_i^{in}(V) + k_i^{out}(V)$.[5] $k_i^{in}(V) = \sum_{j \in V} A_{i,j}$ is the number of edges connecting node i to other nodes belonging to V. $k_i^{out}(V) = \sum_{j \notin V} A_{i,j}$ is the number of connections toward nodes in the rest of the network.

Definition of community in a strong sense

The subgraph V is a community in a strong sense if

$$k_i^{in}(V) > k_i^{out}(V), \quad \forall i \in V. \tag{1}$$

In a *strong* community each node has more connections within the community V than with the rest of the graph.

Definition of community in a weak sense

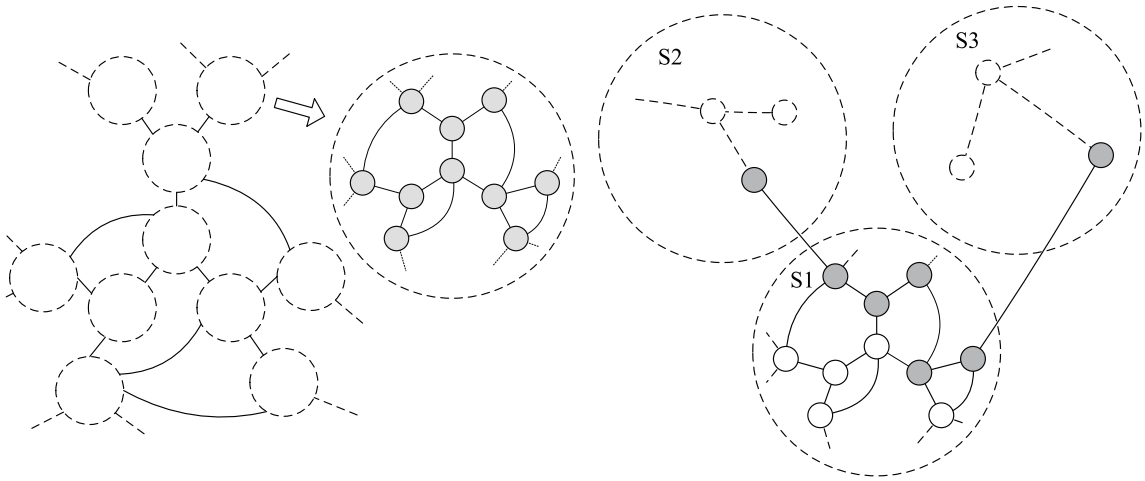
The subgraph V is a community in a weak sense if

$$\sum_{i \in V} k_i^{in}(V) > \sum_{i \in V} k_i^{out}(V). \tag{2}$$

In a *weak* community the sum of all degrees within the community V is larger than the sum of all degrees toward the rest of the network.

Clearly a community in a strong sense is also a community in a weak sense, while the converse is not true. Community structures can be defined and identified. The investigation of community structures in networks is an important issue in many domains and disciplines. Several algorithms which are self-contained exist for revealing community structures in networks.[25,26]

In our research, the underlying architecture of the tree-based community network is abstracted as the Cayley tree, and the underlying deployment of sensors within the community is also the Cayley tree. Random links are added to the two underlying architectures, and the community model has a hybrid structure with regular bonds and random bonds. Fig. 1(a) shows our network model describing the network architecture and the deployment of sensors within the community. The Cayley tree, where every node i has the same degree $k_i = z + 1$ (except for leaf nodes on the boundary which possess $k = 1$), is a regular graph with no loops. It can be constructed by first starting from



(a) (b)

Fig.1. (a) The abstract of the community network based on the Cayley tree. Communities (denoted by dashed circles) with dense internal connections are linked together with external connections. Curves denote random links between two nodes (in the community) or two communities. (b) The virus attacking behaviors on the community network. The virus spreads from the infected nodes (the grey ones) to susceptible neighbors (the white ones) in the community and susceptible ones in other communities along external connections.

a root node at generation $g = 0$, giving that node $z+1$ child nodes, and then repeatedly giving each new child z children of its own. This process continues for a fixed number of generations g. The Cayley tree can grow either in width (via z) or in depth (via g). The number of nodes in generation $g > 0$ is $n(g) = (z+1)z^{g-1}$, and the total number of nodes is $N(g) = 1 + \sum_{g'=1}^{g} n(g')$. The total number of links is $M(g) = N(g) - 1 = (z+1)(z^g - 1)/(z-1)$ in the Cayley tree. Since the bulk of the graph is regular, the Cayley tree has no density fluctuations (all connected subgraphs of the same size have the same number of links). The parameter p is defined as the average number of shortcuts per bond on the underlying structure, and the shortcuts has two sources: the first comes from the random links within the community, and the second comes from the random links outside of the community. Considering that a community is defined as a subset of nodes within the graph that connections between the nodes are denser than connections with the rest of the network, the parameter p is defined as

$$p = \begin{cases} p^{in} & \forall i, j \in V \\ p^{out} & \forall i \in V, j \notin V, \end{cases} \tag{3}$$

where $p^{in} > p^{out}$. Our community model conforms to the definition of community in a weak sense above.

Traditionally, the hierarchical network architecture is abstracted as the random graph or the regular graph in the analysis of the prevalence. In a hypothetical scene that all nodes move randomly or flood messages under no rule, the random graph is suitable for depicting the network architecture. On the base of the mean-field theory, the virus propagation is analyzed as the random process.[24] On the other way, the epidemic on the regular graph is a standard percolation problem.[17] The proposed network model in this paper depicts the hierarchical tree-based communities, and indicates complex structure characteristics of wireless sensor networks. Our research focuses on the spatial-temporal dynamics of the virus prevalence and calculates perco-

lation thresholds of tree-based communities of wireless sensor networks. Fig. 1(b) shows the virus attacking behaviors on the community network. $S1$, $S2$ and $S3$ are three communities of the network. The virus spreads from the infected nodes (the grey ones) to susceptible neighbors (the white ones) in the community and susceptible ones in other communities along external connections. The epidemic propagation is a SI process if there is no immune mechanism.[27]

3. Percolation Thresholds

The wireless sensor network is vulnerable to sensor worms.[28,29] The high-density deployment of wireless sensor nodes implies that any virus can be highly contagious. Sensor nodes are severely resource constrained, and lack sophisticated defense mechanisms to fight virus attacks. Due to shortcuts in tree-based communities, the epidemic propagation becomes much drastic. In our network model, shortcuts are added uniformly to the underlying structure with $p^{in} > p^{out}$.

A certain fraction h of nodes in the community network is assumed to be susceptible to the virus, and the bonds represent the physical contacts by which the virus can spread. The epidemic propagation begins with a single infected node. The nodes will be infected (occupied) or not depending on whether they are susceptible to the virus. If the distribution of infected nodes is random, the problem when an epidemic occurs becomes equivalent to a standard percolation problem.[17] The node is denoted by a site in the graph. The percolation probability h_c, at which the outbreak of the epidemic occurs, can be calculated. If h is above the threshold with $h > h_c$, the epidemic spreads. Below it with $h < h_c$, the epidemic dies out naturally. The epidemic threshold is actually equivalent to a critical point in a nonequilibrium phase transition. The investigation of the percolation threshold is nontrivial in the study of epidemics on tree-based communities of wireless sensor networks. In this paper, the site percolation is only considered.

The network G is split into subgraphs $G_0, G_1, G_2 \cdots G_m$ in terms of the deployment of the communities. $N_0, N_1, N_2 \cdots N_m$ is the number of nodes belonging to each subgraph with $N = N_0 + N_1 + N_2 + \cdots + N_m$. Given the network G is split into N_c subgraphs with the same size, each subgraph includes $N_0 = N/N_c$ nodes. The probability that two sites chosen randomly within the community V have a shortcut between them is calculated as

$$\begin{aligned} \psi^{in} &= 1 - (1 - \frac{2}{N_0^2})^{p(N_0-1)} \\ &\approx \frac{2p(N_0-1)}{N_0^2} \\ &\approx \frac{2p}{N_0}, \end{aligned} \tag{4}$$

where $N_0 = (z+1)(z^{g_0}-1)/(z-1)+1$ (g_0 is the number of generations of the nodes within the community) is the number of nodes of the community, and $p = p^{in}$ is the shortcut probability within the community V.

The probability that one site is connected to another one chosen randomly outside of its community by an additional shortcut is calculated as

$$\begin{aligned} \psi^{out} &= 1 - (1 - \frac{2}{N(N-N_0)})^{p(N_c-1)} \\ &\approx \frac{2p(N_c-1)}{N(N-N_0)} \\ &= \frac{2p}{NN_0}, \end{aligned} \tag{5}$$

where $N_c = (z+1)(z^{g_c}-1)/(z-1)+1$ (g_c is the number of generations of the communities) is the number of the communities, $N = N_c N_0$ is the total number of nodes of the network, and $p = p^{out}$ is the external shortcut probability.

So, the probability that two sites (node i and node j) chosen randomly in the network have a shortcut between them is presented as

$$\psi = \begin{cases} \psi^{in} & \forall i, j \in V \\ \psi^{out} & \forall i \in V, j \notin V. \end{cases} \tag{6}$$

Under the attack of the sensor virus, occupied sites will be connected together by the near-neighbor bonds to construct the local clusters on the community network. The average number of local clusters

of size i on the underlying architecture can be calculated by

$$X_i = h^i(1-h)^{2+(z-1)i}N_0. \tag{7}$$

The spreading of the epidemic is analyzed starting from a localized virus source. In order to construct a so-called giant component as in the random graph,[27] we start with one particular local cluster in some community and add all other clusters to it, which can be reached by traveling along a single shortcut. Two sources contribute to the giant component, one is the occupied clusters within the community, and the other is the occupied clusters reachable via shortcuts outside of the community. Then all other clusters, which can be reached by traveling along a single shortcut, are added to the new ones. This process continues until the connected cluster, the giant component, is constructed.

In order to calculate the percolation threshold h_c, a vector V is defined at each step in this process, whose component v_i is the probability that a local cluster of size i is added to the overall connected cluster. Another vector $V^{'}$, whose component $v_i^{'}$ can be gotten in terms of the value of V at the previous step, is defined. At or below the percolation threshold the component v_i is small and we can calculate the vector $V^{'}$ using a transition matrix M. The following formula reflects the relationship between V and $V^{'}$

$$v_i^{'} = \sum_{j=1}^{N} M_{ij}v_j, \tag{8}$$

where

$$M_{ij} = X_i[1-(1-\psi)^{ij}]. \tag{9}$$

X_i is the number of local clusters of size i as before. $[1-(1-\psi)^{ij}]$ is the probability of a shortcut from one local cluster of size i to another of size j, and there are ij possible pairs of sites by which these can be connected.

The largest eigenvalue λ of the transition matrix M is considered. For $\lambda < 1$, the vector V tends to 0 according to Eq. (8). The rate at which new local clusters are added falls off exponentially, and the connected clusters are finite with an exponential size distribution. Conversely, for $\lambda > 1$, V keeps growing until the size of the connected cluster becomes limited by the size of the whole network. The percolation threshold occurs at the point $\lambda = 1$.

It is difficult to find the largest eigenvalue of the transition matrix M for finite N. If p is a constant, ψ tends to 0 with $N_0 \to \infty$ ($N \to \infty$). Eq. (9) can be simplified through the relation

$$M_{ij} = ij\psi X_i. \tag{10}$$

If we set $v_i^{'} = \lambda v_i$, Eq. (8) is rewritten as

$$\lambda v_i = i\psi X_i \sum_{j=1}^{\infty} jv_j. \tag{11}$$

Then,

$$v_i = C\lambda^{-1} i\psi X_i, \tag{12}$$

where $C = \sum_{j=1}^{\infty} jv_j$ is a constant. And

$$\begin{aligned}
\sum_{i=1}^{\infty} v_i &= C\lambda^{-1}\psi \sum_{i=1}^{\infty} iX_i, \\
\sum_{i=1}^{\infty} iv_i &= C\lambda^{-1}\psi \sum_{i=1}^{\infty} i^2X_i, \\
C &= C\lambda^{-1}\psi \sum_{i=1}^{\infty} i^2X_i, \\
\lambda &= \psi \sum_{i=1}^{\infty} i^2X_i.
\end{aligned} \tag{13}$$

For general z, the average number of local clusters of size i in the network X_i can be rewritten as

$$X_i = h^i(1-h)^{2+(z-1)i}N_0 = (1-h)^2[h(1-h)^{z-1}]^iN_0. \tag{14}$$

From Eqs. (13) and (14), λ is calculated by

$$\lambda = \frac{\psi N_0 h(1-h)^{z+1}[1+h(1-h)^{z-1}]}{[1-h(1-h)^{z-1}]^3}. \tag{15}$$

The percolation threshold can be analyzed in two cases.

a) Percolation threshold of case 1

If we ignore the difference between the shortcut probability within the community and that outside of the community, the network is transformed into a small world network with $p = p^{in} = p^{out}$. The network is not homogeneous in this status unless the range of the community expands to the whole network with $N = N_0$. On the latter assumption, it generates a homogeneous network. Since all nodes have approximately the same number of links, they

all contribute equally to the network's diameter, thus the infection of each node causes the same amount of damage to the network. There is no substantial difference whether the nodes are infected randomly or in decreasing order of the connectivity. When a fraction of nodes are infected by the virus, it is like that the fraction of nodes are removed from the network. The network displays unusual behavior at the percolation threshold h_c, where it falls apart and the main cluster breaks into small pieces.

From Eqs. (4) and (15), λ is rewritten as

$$\lambda = \frac{2ph(1-h)^{z+1}[1+h(1-h)^{z-1}]}{[1-h(1-h)^{z-1}]^3}. \qquad (16)$$

We set $\lambda = 1$ to get the value of p at the percolation threshold h_c with

$$p = \frac{[1-h_c(1-h_c)^{z-1}]^3}{2h_c(1-h_c)^{z+1}[1+h_c(1-h_c)^{z-1}]}, \qquad (17)$$

where p is a constant. The percolation threshold h_c for general z can be calculated on the basis of Eq. (17). From the result we can see that the percolation threshold h_c is not related to the size of the network or the community. But it is closely related to the shortcut probability and the underlying structure (z reveals the characteristic).

If the epidemic only occurs in the community with the shortcut probability $p = p^{in}$ and it dose not extends to other communities, the giant component will not arise in the whole network considering the limit of the size of the community. In this case the percolation threshold h_c can not be analyzed on the basis of Eq. (17) unless the range of the community expands to the whole network.

b) Percolation threshold of case 2

If it is assumed that the local clusters are linked together to construct the giant component only by external shortcuts between the communities, from Eqs. (5) and (15) λ is rewritten as

$$\lambda = \frac{2ph(1-h)^{z+1}[1+h(1-h)^{z-1}]}{N[1-h(1-h)^{z-1}]^3}. \qquad (18)$$

We set $\lambda = 1$ to get the value of p at the percolation threshold h_c with

$$p = \frac{N[1-h_c(1-h_c)^{z-1}]^3}{2h_c(1-h_c)^{z+1}[1+h_c(1-h_c)^{z-1}]}, \qquad (19)$$

where $p = p^{out}$ is the external shortcut probability. From Eq. (19) we can see that the percolation threshold h_c is closely related to the shortcut probability, the underlying structure and the size of the network.

The percolation threshold of the network depends on the deployment and structure, and it becomes more complex in reality. it is difficult to calculate the accurate percolation threshold of a real network with complex hierarchical structure although it exists certainly.

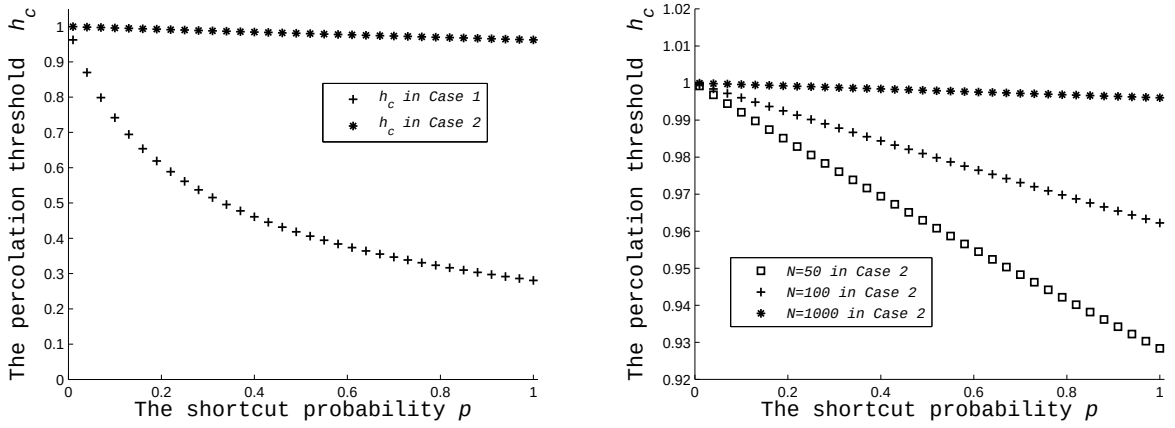
4. Evaluation and Analysis

4.1. Percolation thresholds

The evaluation of the percolation threshold at which the outbreak of the epidemic occurs is presented. The percolation threshold in Case 1 can be calculated as $h_c = \frac{\sqrt{(2p+1)^2+8p}-(2p+1)}{4p}$ with $z = 1$. As shown in Fig. 2(a), the percolation threshold h_c keeps decreasing with the increase of the shortcut probability p in Case 1 and Case 2 ($N = 1000$). Despite the relation of the percolation threshold h_c with the size of the network N, h_c decreases with the increase of the shortcut probability p in Case 2. As shown in Fig. 2(b), the larger the size of the network N is, the larger the percolation threshold h_c is.

For $z > 1$, it is difficult to solve Eqs. (17) and (19), but the variety of h_c is similar with that with $z = 1$. When the shortcut probability p increases, the percolation threshold h_c keeps decreasing. At $p = 1$, there exists the smallest percolation threshold in the complex network.

The results coincide with the reality. Due to shortcuts in the community, the epidemic propagation becomes drastic when the shortcut probability p increases. The percolation threshold decreases simultaneously. There is a small percolation threshold in the random network, where the virus easily attacks the network from one side to another.



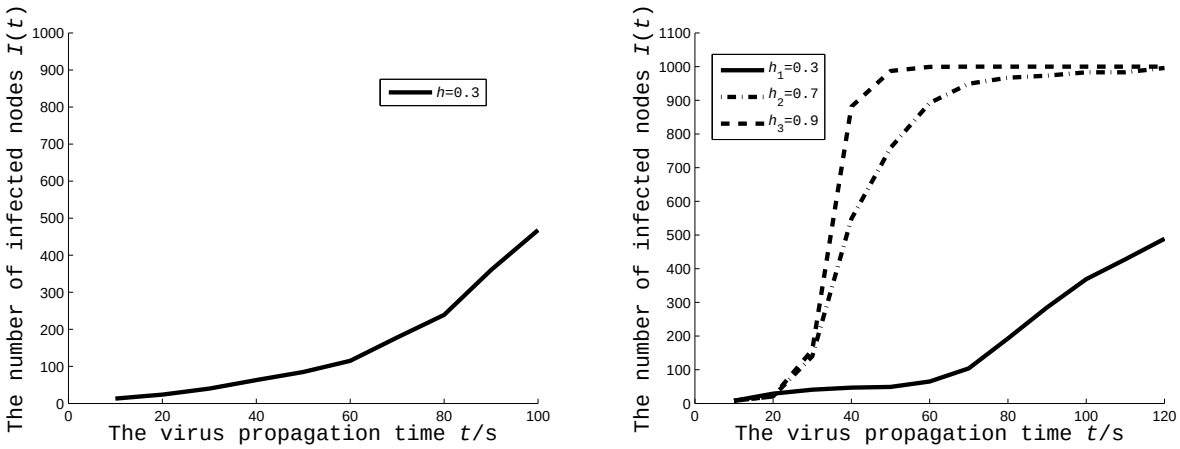
(a) (b)

Fig.2. The variety of the percolation threshold h_c. Here the lines depict the variety of the percolation threshold h_c with the increase of the shortcut probability p in (a) Case 1 and Case 2 ($N = 1000$), (b) Case 2 with $N = 50$, $N = 100$, and $N = 1000$.

4.2. Real architecture evaluation of virus propagations

Evaluations of epidemic propagations on the communities of Zigbee are presented in this section. Zigbee can construct tree-based communities in a broad deployment area if every node is the FFD. The parameters and specifications from Ref. 10 are used in the real architecture evaluation. The time evolution of infected numbers in the network is observed by using a large number of experiments assuming that there is a small section of infectious nodes in the initial stage. We assume that node i is susceptible, it is infected with the infection probability h if there are infectious neighbors. It will be infected eventually as the infection spreads in the experiments. The spatial-temporal dynamics of the epidemic prevalence on the hierarchical architecture are analyzed.

Fig. 3(a) and (b) show the time evolution of infected numbers on the communities of Zigbee. The effect of the infection probability h on the epidemiological process is tested in the experiment. There is only one infected community in the initial stage. In the experiment, 1000 nodes are randomly deployed in a $1000m \times 1000m$ surveillance area. In the construction of the network architecture, the inner connection probability of the community δ_{in} is 0.9, and the external connection probability of the community δ_{out} is 0.3. There are maximum 15 individuals in one community of the network. Other parameters from Ref. 10 are used in the evaluations. The infection probability h is 0.3 in Fig. 3(a). The figure shows that the epidemic spreads slowly with the small infection probability in most time on the hierarchical architecture of the wireless sensor network. At 100s, about 500 nodes are infected in Fig. 3(a). Fig. 3(b) shows the time evolution of the infected number with the infection probability $h_1 = 0.3$, $h_2 = 0.7$ and $h_3 = 0.9$. The epidemic expands at different speeds when the infection probability h varies. The figure shows that the epidemic spreads rapidly with a large infection probability in most time on the hierarchical network. In the late phase of the propagation, the prevalence experiences a decline due to the reduction of remaining susceptible nodes in the network. At 120s, all nodes are infected with $h_2 = 0.7$ and $h_3 = 0.9$, about 500 nodes are infected with $h_1 = 0.3$. h_2 and h_3 are above the percolation threshold h_c, the infected number keeps increasing rapidly in the network until the whole network is infected. h_1 is below the percolation threshold h_c, the epidemic expands more slowly on the network. The experiments reveal the impressive influence of percolation thresholds on the virus prevalence.



(a) (b)

Fig.3. Epidemiological propagations on the communities of Zigbee in the case of $N = 1000$, $\delta_{in} = 0.9$, and $\delta_{out} = 0.3$. Here the lines represent the time evolution of the infected number on communities with (a) $h = 0.3$, (b) $h_1 = 0.3$, $h_2 = 0.7$ and $h_3 = 0.9$.

5. Conclusions

The tree-based community is frequently used in the deployments of large-scale wireless sensor networks. The epidemic dynamics on tree-based communities of large-scale wireless sensor networks are studied in this paper, and they becomes more drastic due to random links in communities. The underlying architecture of the network or the community is abstracted as the Cayley tree, and random links are added to it to construct the tree-based communities. Percolation thresholds of two cases are calculated based on the network model. The analysis and evaluation shows that the percolation threshold keeps decreasing with the increase of the shortcut probability in the tree-based community network. There exists the smallest percolation threshold in a random network, where the virus will easily extend to the whole network. The existence of random links is equivalent to the addition of neighbors to the relevant population. The sensor virus infects the neighbor nodes on the underlying architecture and attacks neighbors in other communities along external links, which accelerate the virus propagation. The conclusions can further our understanding of epidemic dynamics on tree-based communities of wireless sensor networks.

References

1. E. Kampianakis, J. Kimionis, K. Tountas, C. Konstantopoulos, E. Koutroulis, and A. Bletsas, Wireless environmental sensor networking with analog scatter radio and timer principles, *IEEE Sensors Journal*, **14** (10) (2014) 3365–3376.
2. T. R. Rao, D. Balachander, N. Tiwari, and M. V. S. N. Prasad, Ultra-high frequency near-ground short-range propagation measurements in forest and plantation environments for wireless sensor networks, *IET Wireless Sensor Systems*, **3** (1) (2012) 80–84.
3. S. Roy, M. Conti, S. Setia, and S. Jajodia, Secure data aggregation in wireless sensor networks: filtering out the attacker's impact, *IEEE Transactions on Information Forensics and Security*, **9** (4) (2014) 681–694.
4. M. E. J. Newman and T. P. Peixoto, Generalized communities in networks, *Physical Review Letters*, **115** (8) (2015) 088701–1–5.
5. H. J. Li and J. J. Daniels, Social significance of community structure: statistical view, *Physical Review E*, **91** (1) (2015) 012801–1–10.
6. S. Kundu and S. K. Pal, Fuzzy-rough community in social networks, *Pattern Recognition Letters*, **67** (2015) 145-152.
7. J. W. Duncan, *Small Worlds, the Dynamics of Networks between Order and Randomness*, (Princeton University Press, Princeton, 1999).
8. A. L. Barabási, Scale-free networks: a decade and beyond, *Science*, **325** (2009) 412–413.
9. J. Bodlaj and V. Batagelj, Hierarchical link clustering algorithm in networks, *Physical Review E*, **91** (6)

(2015) 062814–1–17.
10. C. Pham, Communication performances of IEEE 802.15.4 wireless sensor motes for data-intensive applications: a comparison of WaspMote, Arduino MEGA, TelosB, MicaZ and iMote2 for image surveillance, *Journal of Network and Computer Applications*, **46** (2014) 48–59.
11. F. Wei, M. E. Haque, X. D. Lu, and K. Mori, Autonomous community construction and coordination technology to achieve real-time transmission in multiple emergencies' situation, *Telecommunication Systems*, **54** (1) (2013) 61–78.
12. J. Y. Wu, X. Y. Shao, and H. P. Zhu, A novel clustering routing protocol with community structure detection for wireless sensor networks, *Applied Mechanics and Materials*, **472** (2014) 460–465.
13. T. Y. Chuang and K. C. Chen, Information centric sensor network management via community structure, *IEEE Communications Letters*, **19** (5) (2015) 767–770.
14. F. D. Sahneh and C. Scoglio, Competitive epidemic spreading over arbitrary multilayer networks, *Physical Review E*, **89** (6) (2014) 062817–1–15.
15. C. Comaniciu, On energy-security tradeoffs and cooperation for wireless Ad Hoc networks, *Journal of Cyber Security and Mobility*, **1** (2012) 53–64.
16. P. S. Romualdo, C. Castellano, P. V. Mieghem, and A. Vespignani, Epidemic processes in complex networks, *Reviews of Modern Physics*, **87** (3) (2015) 925–979.
17. S. Dietrich and A. Ammon, *Introduction to Percolation Theory*, (Burgess Science Press, Great Britain, 1992).
18. B. Wang, L. Cao, H. Suzuki, and K. Aihara, Impacts of clustering on interacting epidemics, *Journal of Theoretical Biology*, **304** (2012) 121–130.
19. Y. Feng, Q. L. Fan, L. Ma, and L. Ding, Epidemic spreading on uniform networks with two interacting diseases, *Physica A: Statistical Mechanics and Its Applications*, **393** (2014) 277–285.
20. C. H. Li, C. C. Tsai, and S. Y. Yang, Analysis of epidemic spreading of an SIRS model in complex heterogeneous networks, *Communications in Nonlinear Science and Numerical Simulation*, **19** (4) (2014) 1042–1054.
21. X. L. Peng, X. J. Xu, X. C. Fu, and T. Zhou, Vaccination intervention on epidemic dynamics in networks, *Physical Review E*, **87** (2013) 022813–1–10.
22. C. Granell, S. Gómez, and A. Arenas, Competing spreading processes on multiplex networks: awareness and epidemics, *Physical Review E*, **90** (1) (2014) 012808–1–7.
23. J. P. Bagrow, Communities and bottlenecks: trees and treelike networks have high modularity, *Physical Review E*, **85** (6) (2012) 066118–1–9.
24. R. V. D. Bovenkamp and P. V. Mieghem, Survival time of the susceptible-infected-susceptible infection process on a graph, *Physical Review E*, **92** (3) (2015) 032806–1–16.
25. V. A. Traag, R. Aldecoa, and J. C. Delvenne, Detecting communities using asymptotical surprise, *Physical Review E*, **92** (2) (2015) 022816–1–11.
26. R. K. Darst, D. R. Reichman, P. Ronhovde, and Z. Nussinov, Algorithm independent bounds on community detection problems and associated transitions in stochastic block model graphs, *Journal of Complex Networks*, **3** (3) (2015) 333-360.
27. T. J. Norman, *The Mathematical Theory of Infectious Diseases*, (Hafner Press, New York, 1975).
28. S. Bonaccorsi, S. Ottaviano, F. D. Pellegrini, A. Socievole, and P. V. Mieghem, Epidemic outbreaks in two-scale community networks, *Physical Review E*, **90** (1) (2014) 012810–1–11.
29. B. K. Mishra and N. Keshri, Mathematical model on the transmission of worms in wireless sensor network, *Applied Mathematical Modelling*, **37** (6) (2013) 4103–4111.