Critical behavior of blind spots in sensor networks

Liang Huang
Department of Electrical Engineering, Arizona State University, Tempe, Arizona 85287

Ying-Cheng Lai
Department of Electrical Engineering, Arizona State University, Tempe, Arizona 85287
and Department of Physics and Astronomy, Arizona State University, Tempe, Arizona 85287

Kwangho Park, Junshan Zhang, and Zhifeng Hu
Department of Electrical Engineering, Arizona State University, Tempe, Arizona 85287

(Received 11 January 2007; accepted 9 May 2007; published online 29 June 2007)

Blind spots in sensor networks, i.e., individual nodes or small groups of nodes isolated from the rest of the network, are of great concern as they may significantly degrade the network's ability to collect and process information. As the operations of many types of sensors in realistic applications rely on short-lifetime power supplies (e.g., batteries), once they are used up ("off"), replacements become necessary ("on"). This off-and-on process can lead to blind spots. An issue of both theoretical and practical interest concerns the dynamical process and the critical behavior associated with the occurrence of blind spots. In particular, there can be various network topologies, and the off-and-on process can be characterized by the probability that a node functions normally, or the occupying probability of a node in the network. The question to be addressed in this paper concerns how the dynamics of blind spots depend on the network topology and on the occupying probability. For regular, random, and mixed networks, we provide theoretical formulas relating the probability of blind spots to the occupying probability, from which the critical point for the occurrence of blind spots can be determined. For scale-free networks, we present a procedure to estimate the critical point. While our theoretical and numerical analyses are presented in the framework of sensor networks, we expect our results to be generally applicable to network partitioning issues in other networks, such as the wireless cellular network, the Internet, or transportation networks, where the issue of blind spots may be of concern. © *2007 American Institute of Physics*.

[DOI: 10.1063/1.2745232]

Recent years have witnessed an increasing use of sensor networks in a wide range of applications.[1] Examples include monitoring and collection of information on objects ranging from plankton colonies,[2] endangered species,[3] soil and air contaminants[4] to traffic flow,[5] biomedical subjects,[6] building and bridges,[7] etc. Sensor networks also find critical applications in homeland defense such as detection of chemical or biological agents and pattern recognition.[1] In a sensor network, the issue of blind spots is of particular importance as the power supplies maintaining the normal operation of the sensors are usually of finite lifetime. As a result, blind spots, i.e., isolated nodes or isolated clusters of nodes, can occur. A central question concerns the onset of blind spots and its dependence on network topologies, i.e., What type of networks are more resilient or more susceptible to blind spots? Here we address this question by investigating four types of sensor network topologies: regular, random, mixed, and heterogeneous. Based on the degree-distributions of these networks, we have obtained, for the first three types of networks, explicit formulas for the critical value of the occupying probability, below which blind spots are likely. For heterogeneous networks, we have derived a computational procedure that allows the critical occupying probability to be determined implicitly. Excellent agreement has been found between the theoretical predictions and numerical simulations. We expect our results to be useful not only for designing specific sensor networks, but also for deriving control strategies to restore the networks from catastrophic events as in the aftermath of a large-scale attack.

I. INTRODUCTION

Wireless sensor networks have increasingly been deployed in various applications that are important for improving the quality of life in a modern society.[1] In many applications, sensors are powered by sources that have relatively short lifetime, such as batteries, for which routine replacement or recharging is necessary.[8] Because of this requirement, at any given time a number of sensors in the network are not operational, or are in an "off" state, and another group of sensors are turned back on. The off-and-on process can be characterized by the probability that a node functions normally, or the occupying probability of a node in the network. Intuitively, if the number of "off" sensors is small, we expect the network to remain fully connected, which is desired. However, as the number becomes large, situations can arise where some of the sensors in the network, while still functional, become isolated from other sensors. These are the *blind spots*.[9,10] The occurrence of blind spots can be a serious issue of concern, as they may result in loss or interruption of critical data or information.

There is vast engineering literature on sensor networks, but results on blind-spot dynamics are scarce. In particular, there has been no study of the interplay between the dynamics and the network architecture. Our point is that this dynamics problem can be addressed by using tools from statistical physics, e.g., percolation theory.[11] A network is integrable and functional if a substantial fraction of nodes are connected. Theoretically, the problem can be treated in the framework of percolation where one can ask, for instance, under what conditions a global spanning cluster of nodes, which contains a considerable fraction of the active nodes, can be formed.[12–15] Intuitively, one may expect that networks with a stronger ability to form spanning clusters should be more capable of "absorbing" isolated nodes and, hence, such networks should be more robust against the occurrence of blind spots. In the language of percolation, this is to say that networks with smaller percolation thresholds should be more easily to be fully connected as the occupying probability is increased through the threshold. However, our recent brief work on blind-spot dynamics in scale-free networks[10] results in a finding that is contrary to the intuitive thinking: blind spots are more probable in networks that are more susceptible to percolation for the same type of networks.[10] Retrospectively, this can be understood by noting that, the percolation threshold is generally smaller for relatively more heterogeneous networks, when the average degree is fixed, there is also a higher probability for these networks to possess more small-degree nodes, making more difficult a full connection.

Sensor networks, a typical class of networks in which the nodes exhibit an on-off behavior due to finite power supply, are not necessarily scale free. Due to practical constraints, a sensor network can be random or regular with a homogeneous degree distribution. In this paper, we shall present a systematic study of the occurrence of blind spots on several different types of sensor networks. Since larger networks are more susceptible to blind spots, we pay special attention to the dependence of the critical condition for the occurrence of blind spots on the network size. That is, scaling laws underlying the blind-spot occurrence with respect to the network size are our focus. In particular, we shall demonstrate that from the statistical point of view, the occurrence of blind spots can be characterized by the occupying probability; i.e., the probability that a node is "on" or "off" for a static case, which can be studied via ensemble statistics. Therefore, the main issue of interest concerns how the number of blind spots depends on the occupying probability for any given network architecture, and what the scaling laws should be between the critical values for the occurrence of blind spots and the network size, and how they depend on the network structure. We shall adopt the basic analytic scheme introduced in Ref. 10 and develop more detailed analysis for four different types of sensor networks: regular, random, mixed, and heterogeneous. Based on a few simple assumptions, the degree distribution for each type of sensor network can be obtained, yielding the desirable scaling laws. For the first three types of networks, explicit formulas can be obtained for the critical value of the occupying probability, below which blind spots are likely. Numerical simulations are carried out and compared with the theories. For heterogeneous networks, a computational procedure is derived, which allows the critical occupying probability to be determined implicitly. These results should be useful not only for designing specific sensor networks, but also for deriving control strategies to restore the networks from catastrophic events as in the aftermath of a large-scale attack.

In Sec. II, we outline our theoretical approach to the blind-spot problem. In Sec. III, we derive analytic formulas for critical occupying probability for different types of networks and provide numerical confirmation. Conclusions and discussions are presented in Sec. IV.

II. THEORETICAL APPROACH TO BLIND SPOTS

Because of power limitation, physically a sensor can communicate with sensors within a certain range only. On average, it is convenient to introduce a communication radius r_c to model this effect: there can be a link between any pair of sensors (nodes) only if their distance is smaller than r_c. Topologically, sensors can be regarded as being distributed in a *two-dimensional* region. A sensor network can be defined naturally based on these considerations. This construction is motivated by the observation that sensor networks arising in a variety of practical situations[1] can be regarded as being effectively embedded in a two-dimensional space. The blind-spot dynamics in "two-dimensional" sensor networks is the focus of this paper.

From the standpoint of theoretical analysis, there is an important advantage associated with sensor networks embedded in a space of dimension greater than 1. That is, the probability for multinode blind spot is typically much smaller than that for single-node blind spot. This is so because a multi-node region has a larger perimeter and more neighboring nodes than any single node in the network. In order to isolate such a region, all its neighboring nodes need to be disabled at the same time, the probability of which is in general much smaller than that for a single isolated node. As a result, multinode blind spots can be neglected. In fact, this approximation makes analytic derivations of the scaling laws associated with the critical behavior of the blind spots feasible for a number of network connecting topologies. As we will show in this paper, direct numerical simulations of the blind-spot dynamics generate results that are in excellent agreement with the theoretical predictions, providing further justification to the approximation.

A. On-off processes

The process of battery drainage and replacement is equivalent to an on-off process, which can be modelled statistically. For a large network, in the long term the on-off process, which is highly dynamic, can be treated in the framework of percolation theory. Let n_{on} denote the number of on-nodes and n_{off} be the number of off-nodes, which satisfy $n_{\mathrm{on}}+n_{\mathrm{off}}=N$. At each time step, there is a finite probability π_1 for an on-node to be off, due to the battery drainage or sensor failure. Likewise, every off-node has probability π_2 to be turned on, due to recharge, repair, or sensor replacement, etc. We have

$$\Delta n_{\text{on}} = - n_{\text{on}}\pi_1 + n_{\text{off}}\pi_2 .$$

In the continuous-time limit, this becomes

$$\frac{dn_{\text{on}}}{dt} = - n_{\text{on}}\pi_1 + n_{\text{off}}\pi_2 . \tag{1}$$

Using $n_{\text{on}}+n_{\text{off}}=N$ and the initial condition $n_{\text{on}}(0)=N$, Eq. (1) can be solved explicitly as

$$n_{\text{on}}(t) = \frac{N}{\pi_1+\pi_2}[\pi_2 + \pi_1 e^{-(\pi_1+\pi_2)t}]. \tag{2}$$

Letting $q=n_{\text{on}}/N$, where q is the occupying probability in the language of percolation, we obtain

$$q(t) = \frac{1}{\pi_1+\pi_2}[\pi_2 + \pi_1 e^{-(\pi_1+\pi_2)t}]. \tag{3}$$

As $t \rightarrow \infty$, we have $q(t) \rightarrow \pi_2/(\pi_1+\pi_2)$. In this way, the on-off dynamical process is completely equivalent to a percolation problem. Given a sensor network, solutions to the on-off problem can be obtained by solving the corresponding percolating dynamics. For example, suppose a network has a percolation threshold q_{th}. For $q > q_{\text{th}}$, there exists a spanning cluster and the network is globally connected and functional, while it is disintegrated and loses its global function for $q < q_{\text{th}}$. The threshold q_{th} in general depends on network details such as its size and degree distribution. Say we have determined the threshold q_{th}. Given a particular value of π_1 (which usually depends on the sensors), it is necessary to adjust π_2 (through sensor recharging or replacement) to guarantee $\pi_2/(\pi_1+\pi_2) \geq q_{\text{th}}$. That is, the network integrity can be maintained by increasing π_2 to minimize the likelihood of losing a spanning cluster.

A special case is $\pi_2=0$, where sensor batteries are never replaced. We have

$$q(t) = e^{-\pi_1 t} \equiv e^{-t/\tau}, \tag{4}$$

where $\tau = 1/\pi_1$ is the characteristic average lifetime of sensor battery.

B. Blind spots

In sensor networks, coverage plays a critical role for fielding monitoring and information collecting. An intimately related issue is the blind spot, where a blind spot is a node or a cluster of several connected nodes isolated from other parts of the network. This boils down to the occurrence of blind spots.

To analyze the occurrence and the number of blind spots, we consider single-node blind spots. A node having k neighbors is isolated if it is on but all its neighbors are off. The probability of this event is qp^k, where $p=1-q$ is the probability that a node is off. Let N be the network size and $P(k)$ be the degree distribution.[16] On average, $NP(k)$ nodes have k neighbors. The total number of single-node blind spots is $n_1 = \Sigma_k qp^k NP(k)$. Similarly, the probability for multinode, say, m-node blind spot is proportional to $q^m p^{k_1+\cdots+k_m-2l_i}$ for a given configuration that the m nodes have l_i internal links. For a networks with homogeneous connections and average degree $\langle k\rangle$, there are $N\langle k\rangle/2$ edges, and we have

$$l_i = [m(m-1)]/[N(N-1)]N\langle k\rangle/2 \approx m(m-1)\langle k\rangle/(2N).$$

Thus, the probability of m-node blind spot is approximately proportional to $q^m p^{m\langle k\rangle[1-(m-1)/N]} \approx q^m p^{m\langle k\rangle}$, where $1 < m \ll N$. Near the critical point where blind spots begin to appear, $p \ll 1$, the probabilities of various multi-node blind spots are negligible.

From a physical point of view, blind spots are single nodes or small clusters of nodes left out of a percolating process. At the percolation threshold where a spanning cluster forms, the remaining clusters can have various sizes that follow a power-law distribution. As q is increased further, the size distribution of the remaining clusters becomes exponential and most of them have small size. At the critical point where the last remaining cluster merges into the spanning cluster, the remainder will consist mostly of single, isolated nodes. Thus, near the critical point, it is reasonable to focus on single-node blind spots. We emphasize that this consideration applies to networks embedded in space of dimension higher than 1 only. For networks embedded in one dimension, multinode blind spots are as likely as single-node blind spots.[17] For instance, for a one-dimensional regular lattice, we have $k_1+\cdots+k_m-2l_i=2$, which is independent of the value of m.

Under the single-node blind spot approximation, the number of blind spots is given by

$$n_s \approx n_1 = \sum_k qp^k NP(k). \tag{5}$$

We see that n_s/N depends only on the degree distribution. For a given degree distribution, there is a scaling law such that $n_s = Nf(q)$. Furthermore, Eq. (5) does not depend on the detailed construction of the network. That is, for a network with certain degree distribution, regardless of the ways that it is generated (e.g., by randomly picking up a pair of nodes and connecting them, by some preferential-attachment rule, or by connecting nearest spatial neighbors), it will have the same function $f(q)$ and the same scaling laws near the critical point q_c. This may be interesting, considering that the percolation threshold is sensitive to fine details such as the degree correlation,[18,19] the degree of clustering,[20] ways of embedding into a Euclidean space,[21,22] etc.

To determine the critical point q_c, we note that for a given network size N, blind spots can practically occur if $\langle n_s\rangle > 1$, while they are unlikely for $\langle n_s\rangle < 1$, where $\langle n_s\rangle$ is the ensemble-averaged value of n_s. Thus, we can conveniently choose $n_s=1$ to be the criterion for determining q_c, which can be solved as a function of network size N and some network parameter μ characterizing the degree distribution: $q_c = q_c(N, \boldsymbol{\mu})$. Knowing q_c, by solving Eq. (3) with $q=q_c$, we can determine the critical time t_c when the first blind spot occurs, provided that the network undergoes an on-off process.

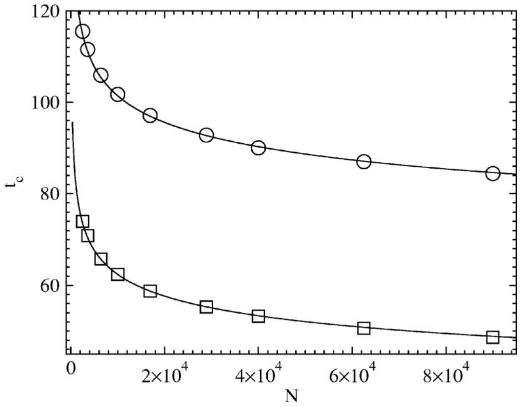

FIG. 1. Critical time t_c vs the network size N for lattice networks. Data points are numerical results for $m=12$ (squares) and $m=20$ (circles). The parameters are $\pi_1=0.01$, $\pi_2=0$, and $\tau=100$. Each data point is averaged over 10^4 realizations. Curves are from Eq. (8) with $c'=1.01$.

III. SOLUTIONS TO BLIND-SPOT PROBLEM FOR DIFFERENT NETWORK TOPOLOGIES

A. Regular sensor networks

Imagine that a sensor network is built up according to the geometry of a regular lattice, where the distances between any nearest neighboring pairs of sensors are constant. The degree distribution is thus a delta function $P(k)=1$ if $k=m$ and 0 otherwise, where m is the number of nearest neighbors. The number of blind spots is

$$n_s = Nqp^m. \tag{6}$$

As the probability p goes to zero, n_s/N also approaches zero. For a given network of size N, there exists a p_c such that $n_s<1$ for $p<p_c$. Setting $n_s=c$, we have

$$n_s = Nq_c p_c^m = c.$$

As q_c is varied, the change of n_s is dominated by the factor $p_c^m=(1-q_c)^m$. We can thus treat q_c as a constant and obtain

$$p_c = \left(\frac{Nq_c}{c}\right)^{-1/m} \approx c' N^{-1/m}, \tag{7}$$

where c' is a constant. To obtain the scaling law for t_c, we substitute $q_c=1-p_c$ into Eq. (3) and note $q(t_c)=q_c$. This yields

$$t_c = -\tau \ln q_c = -\tau \ln(1 - c' N^{-1/m}). \tag{8}$$

For $m=4$, this result reduces to the previous one obtained in Ref. 9.

For a given network, starting with all nodes on, in simulation the on-off process can be applied and the critical time t_c at which the first blind spot arises can be measured. Figure 1 shows the behavior of the critical time of two regular sensor networks, where the decrease of t_c as N goes large can be seen. The data points are from numerical computation and the curves are from theory. Both agree well.

B. Random sensor networks

In this case, nodes are distributed randomly within a region S. Two nodes are connected if their distance is less than the responding distance r_c. Thus, node i is connected with all its neighbors that are located in a circle of radius r_c centered at i. We call it the *connecting circle*. The degree distribution can be obtained as follows. For a given node i, the $N-1$ other nodes in the network are distributed randomly in S. One can thus imagine randomly dropping particles over an area S and ask the probability for a particle to fall in the connecting circle of i. This is basically a point process and the probability is given by the Poisson distribution

$$P(k) = \frac{e^{-k_a} k_a^k}{k!},$$

with parameter

$$k_a = (N-1)\pi r_c^2/S \approx N\pi r_c^2/S.$$

The average degree is $\langle k\rangle=\Sigma_k P(k)k=k_a$; thus, $P(k)=e^{-\langle k\rangle}\langle k\rangle^k/k!$. Substituting the distribution into Eq. (5), we obtain

$$n_s = \sum_k qp^k N e^{-\langle k\rangle}\frac{\langle k\rangle^k}{k!} = Nqe^{-\langle k\rangle}e^{p\langle k\rangle} = Nqe^{-q\langle k\rangle}. \tag{9}$$

When p approaches 0, n_s decays exponentially to $Ne^{-\langle k\rangle}$. For a given value of $\langle k\rangle$, when the network size N is large enough, e.g., larger than $e^{\langle k\rangle}$, blind spots will occur for arbitrary small probability p that a node is turned off. This comes from the fact that for the Poisson degree distribution, the probability that a node has no connection is $P(0)=e^{-\langle k\rangle}$. For $N>1/P(0)$, even if all nodes are on, there still exist blind spots; i.e., those with no neighbors by the way of network construction. This property illustrates that, for random placement of sensors, blind spots are almost certain, particularly when the number of sensors is large. However, when N is not so large as compared with $e^{\langle k\rangle}$, whether blind spots can arise depends on the value of q.

Assuming $N<e^{\langle k\rangle}$, we now obtain the scaling laws for q_c and t_c. Setting $n_s=c$, we have

$$n_s = Nq_c e^{-q_c\langle k\rangle} = c.$$

Since q_c varies much more slowly than $e^{-q_c\langle k\rangle}$, the main dependence of q_c upon N comes from the latter term. We can write the solution as

$$q_c = \frac{1}{\langle k\rangle}\ln\left(\frac{Nq_c}{c}\right).$$

Neglecting the slow variation of q_c and absorbing it into c, i.e., $c'=c/q_c$, we obtain

$$q_c = \frac{1}{\langle k\rangle}\ln(N/c'). \tag{10}$$

From Eq. (3) with $q(t_c)=q_c$, we can find the scaling law for t_c:

$$t_c = \tau[\ln\langle k\rangle - \ln\ln(N/c')]. \tag{11}$$

Compare to Eq. (8) for regular networks, the critical time for random sensor networks decreases much faster as N increases.

To construct a numerical model for random sensor networks, we can fix r_c and S (N is proportional to S). The

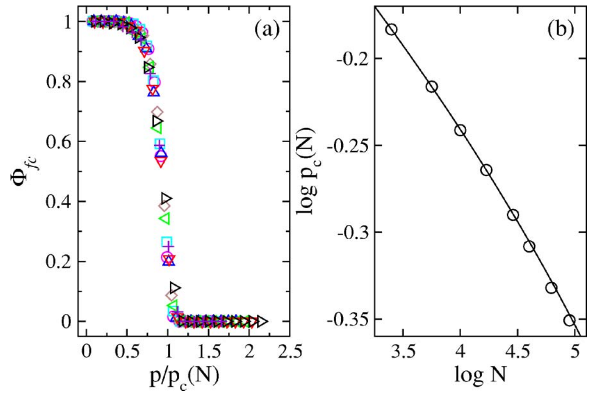

FIG. 2. (Color online) For random sensor networks with $\langle k\rangle=20$, (a) universal behavior in the probability Φ_{fc} of full network connection vs the normalized occupying probability $p/p_c(N)$ for eight different network sizes: 2500, 5625, 10 000, 16 900, 28 900, 40 000, 62 500, and 90 000, where each data point is the result of ensemble average of 1000 networks, and (b) $\log_{10} p_c(N)$ vs $\log_{10} N$. The solid curve in (b) is calculated from the theory [Eq. (9)] by setting $n_s=1$.

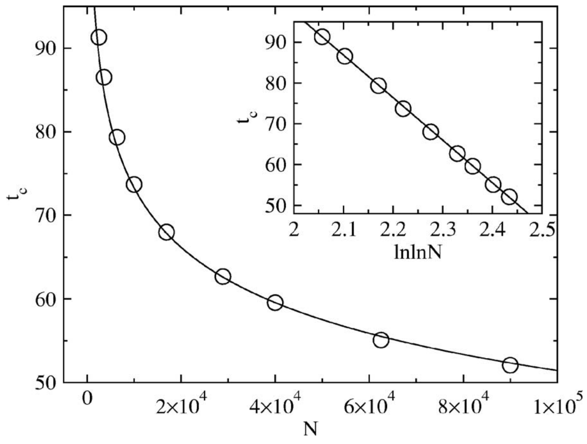

FIG. 3. Critical time t_c vs network size N of random sensor network with $\langle k\rangle\approx 20$. Data points are obtained from the numerical simulations with parameters $\pi_1=0.01$ and $\pi_2=0$ ($\tau=100$). Each data point is averaged over 10^4 realizations. The solid curve is from Eq. (11) with $c'=0.8$. Inset: t_c vs $\ln\ln N$. The straight line is only a guide to the eye.

average degree is $\langle k\rangle=N\pi r_c^2/S$, which is independent of N. For convenience, periodic boundary conditions can be assumed.

Since the critical point p_c (or q_c) depends on the network size, we focus on the scaling relation $p_c(N)$. The probability that the network formed by all on-nodes under a given occupying probability is fully connected depends on N as $f[p/p_c(N)]$, where $f(x)$ may have a universal form for given degree distribution. Having numerically determined $f[p/p_c(N)]$ for a set of N values, we can adjust the parameter $p_c(N)$ so that all the f-curves overlap with each other completely. This way the relation $p_c(N)$ can be obtained. Figure 2(a) shows the dependence of $f[p/p_c(N)]$ on $p/p_c(N)$ for a set of random sensor networks with different sizes, which indeed exhibits a universal form after proper adjustment of $p_c(N)$. The scaling relation $p_c(N)$ is shown in Fig. 2(b), where symbols are the data of $p_c(N)$ obtained from Fig. 2(a), and the line is from the theoretical distribution Eq. (9) by setting $n_s=1$. Both are normalized so that their values for $N=2500$ are unity. Theory and numerical simulations agree quite well.

Figure 3 shows that the critical time t_c decreases as the network size is increased. The solid curve is the theoretical prediction from Eq. (11). There is again a good agreement between numerics and theory.

C. Mixed sensor networks

A mixed network is not strictly a regular lattice, nor is it completely random. Such a network can be constructed by using the Gaussian degree distribution:

$$P(k)=\frac{1}{\sqrt{2\pi\sigma^2}}\exp\left[-\frac{(k-\langle k\rangle)^2}{2\sigma^2}\right],$$

for $k\geq 0$, where $\langle k\rangle$ is the average degree, σ^2 is the variance, which is assumed to be small compared with $\langle k\rangle$ so that the summation of $P(k)$ from $-\infty$ to 0 in the normalization can be disregarded. Note that when σ^2 approaches to 0, the Gaussian distribution limits to delta function $P(k)\to\delta(k-\langle k\rangle)$; thus, the network approaches regular network. While if σ^2 approaches $\langle k\rangle$, the Gaussian distribution approaches to the Poisson distribution, and the network is effectively a random sensor network. Substituting $P(k)$ into Eq. (5), we have

$$\begin{aligned}n_s&=\sum_{k=0}^{\infty}Nqp^k\frac{1}{\sqrt{2\pi\sigma^2}}e^{-(k-\langle k\rangle)^2/2\sigma^2}\\&=Nqp^{\langle k\rangle}\frac{1}{\sqrt{2\pi\sigma^2}}\sum_{k=0}^{\infty}p^{k-\langle k\rangle}e^{-(k-\langle k\rangle)^2/2\sigma^2}\\&=Nqp^{\langle k\rangle}\frac{1}{\sqrt{2\pi\sigma^2}}\sum_{k=0}^{\infty}e^{(\ln p)(k-\langle k\rangle)}e^{-(k-\langle k\rangle)^2/2\sigma^2}\\&=Nqp^{\langle k\rangle}e^{\sigma^2(\ln p)^2/2}\frac{1}{\sqrt{2\pi\sigma^2}}\sum_{k=0}^{\infty}e^{-(k-\langle k\rangle-\sigma^2\ln p)^2/2\sigma^2}.\end{aligned}\quad(12)$$

If the variance σ^2 is small compared with the new mean $\langle k\rangle+\sigma^2\ln(p)$, the summation in Eq. (12) can be approximated by a standard Gaussian integral. We obtain

$$n_s=Nqp^{\langle k\rangle}e^{\sigma^2(\ln p)^2/2}.\quad(13)$$

Notice that as σ^2 goes to zero, this equation reduces to Eq. (6). If σ^2 is nonzero but small as compared with the average degree, the scaling laws for q_c and t_c can be obtained, as follows.

First, setting $n_s=c$ yields

$$n_s=Nq_cp_c^{\langle k\rangle}e^{\sigma^2(\ln p_c)^2/2}=c.$$

Taking the logarithm of both sides, we have

$$\frac{\sigma^2(\ln p_c)^2}{2}+\langle k\rangle\ln p_c+\ln(Nq_c/c)=0.$$

Absorbing q_c into c', i.e., $c'=c/q_c$, we have

$$\ln p_c=-\frac{1}{\sigma^2}\left(\langle k\rangle-\sqrt{\langle k\rangle^2-2\sigma^2\ln(N/c')}\right)$$

or

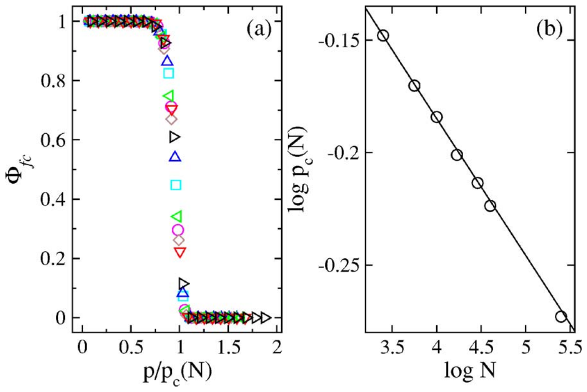

FIG. 4. (Color online) For a mixed network with Gaussian degree distribution, $\langle k\rangle=20$, $\sigma^2=4$, (a) the probability Φ_{fc} of full connection vs the normalized occupying probability $p/p_c(N)$ for seven different network sizes: 2500, 5625, 10 000, 16 900, 28 900, 40 000, and 250 000, where each data point is the result of ensemble average of 1000 network realizations, and (b) $\log_{10} p_c(N)$ vs $\log_{10} N$. The solid line in (b) is from theory [Eq. (13)].

$$p_c = \exp\left[-\frac{1}{\sigma^2}\left(\langle k\rangle - \sqrt{\langle k\rangle^2 - 2\sigma^2 \ln(N/c')}\right)\right]. \qquad (14)$$

From Eq. (3) with $q(t_c)=q_c=1-p_c$, the scaling law for t_c becomes

$$t_c = -\tau \ln q_c = -\tau \ln\left[1 - e^{(-1/\sigma^2)\left(\langle k\rangle - \sqrt{\langle k\rangle^2 - 2\sigma^2 \ln(N/c')}\right)}\right]. \qquad (15)$$

When σ^2 approaches 0, employing Taylor expansion, Eqs. (14) and (15) will reduce to Eqs. (7) and (8) respectively, by noting that $\langle k\rangle=m$.

Figure 4 shows the scaling of p_c for mixed networks with Gaussian degree distribution, where we observe a good agreement between the theoretical formula (14) and numerical computations. Figure 5 shows the dependence of t_c on N. There is also a good agreement between the numerics and the formula (15).

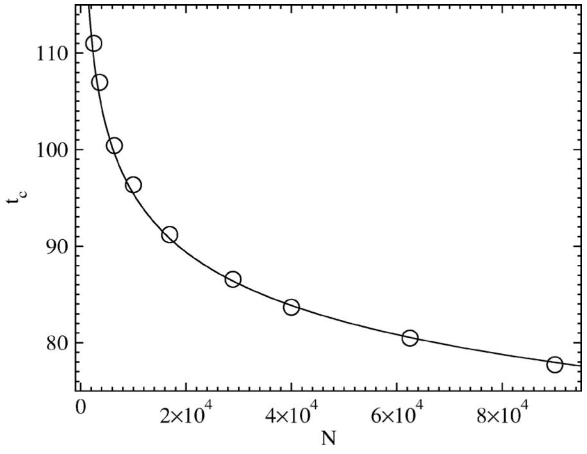

FIG. 5. Critical time t_c vs size N for mixed networks having Gaussian degree distribution with parameters $\langle k\rangle\approx 20$ and $\sigma^2=4$. Data points are numerical results with simulation parameters $\pi_1=0.01$, $\pi_2=0$, and $\tau=100$. Each data point is averaged over 10^4 realizations. The solid curve is from the theoretical formula Eq. (15) with $c'=1.24$.

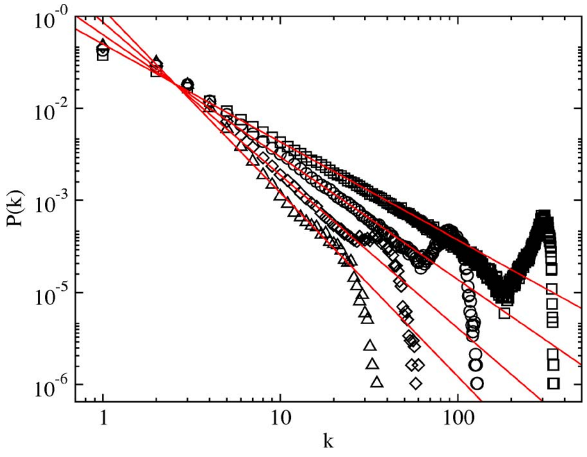

FIG. 6. Degree distribution of sensor networks on a two-dimensional disk. $\alpha=1.25$, 1.0, 0.8, 2/3 for squares, circles: diamonds, and triangles, respectively. The ratio of the connecting radius of a sensor r_c and the radius of the disk R is 0.01. The number of sensors is $N=10^4$. Each data point is averaged over 100 realizations. The lines are power-law distribution with exponent $\lambda=2/\alpha$, which are $\lambda=1.6$, 2.0, 2.5, and 3.0 from up to down.

D. Scale-free sensor networks

The three types of sensor networks discussed so far all are homogeneous networks in the sense that the sensors are distributed uniformly in space. While homogeneous networks allow for analytic treatment in terms of the scaling laws, in reality nonuniform or locally preferred distribution of sensors, e.g., hybrid sensor networks,[23,24] are also of interest. For example, hierarchical sensor network can consist of a large number of cheap sensors and a few more powerful gateways which could naturally lead to heterogeneous degree distributions. Heterogeneous networks such as scale-free networks would naturally fit in such a situation. This can be further argued by considering the degree distribution. Say the density ρ of sensors is not uniform, but depends on r in a polar-coordinate system: $\rho=\rho(r)$. If $\rho(r)$ has the form of $\rho(r)\sim r^{-\alpha}$, then the degree distribution of the sensor network in the limiting case will be scale free: $P(k)\sim k^{-\lambda}$, where $\lambda=D/\alpha$, D is the spatial dimension.

To show this, suppose the connecting radius r_c of a sensor is much smaller than the characteristic scale of the system. A sensor located at r will on average have $k(r)=\rho(r)V_c\sim\rho(r)\sim r^{-\alpha}$ neighboring sensors, where V_c is the volume of the D-dimensional sphere of radius r_c. We thus have $r\sim k^{-1/\alpha}$. The number of sensors in a spherical shell of radius r and width Δr is $n(r)\sim\rho(r)r^{D-1}\Delta r\sim r^{-\alpha}r^{D-1}\Delta r$. From the relation between r and k, we have $\Delta r\sim k^{-1/\alpha-1}\Delta k$. If we set $\Delta k=1$, the shell is such that the sensors in it have on average the same degree. The quantity $n(r)$ thus becomes

$$n[k(r)] \sim k k^{-(D-1)/\alpha} k^{-1/\alpha-1} = k^{-D/\alpha}.$$

After normalization, the degree distribution becomes $P(k)\sim k^{-D/\alpha}$. In the situation in which the physical space in which the sensors are distributed is two-dimensional, we have $\lambda=2/\alpha$.

Numerical support for the scale-free nature of heterogeneously distributed sensor networks is shown in Fig. 6, where the degree distributions of several sensor networks

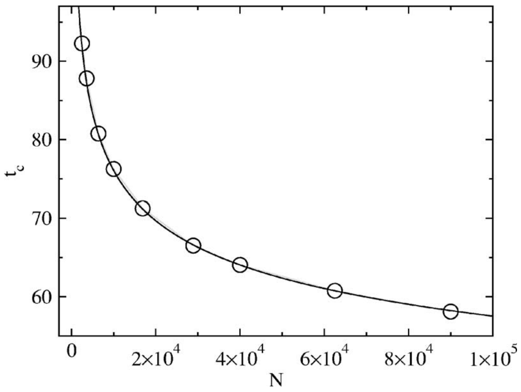

FIG. 7. Critical time t_c vs size N for scale-free networks with parameters $\lambda=3.5$ and $m=12$. Data points are simulation results with parameters $\pi_1=0.01$, $\pi_2=0$, and $\tau=100$. Each data point is averaged over 10^4 realizations. The solid curve is the numeric solution from the theory with $c'=0.65$.

located in a two-dimensional disk (symbols) are plotted, together with theoretical results. We observe a power-law behavior in the degree distribution and the exponent agrees well with the theory.

In a strict sense, the degree distribution can be written as $P(k)=k^{-\lambda}/(\sum_{k=m}^{\infty}k^{-\lambda})$ for $k\geq m$, where m is the minimum degree. Substituting the degree distribution into Eq. (5) yields[10]

$$n_s = Nqp^m\frac{\sum_{k=0}^{\infty}[p^k/(k+m)^{\lambda})}{\sum_{k=m}^{\infty}k^{-\lambda}}. \tag{16}$$

As p goes to zero, n_s/N also approaches zero, meaning that scale-free sensor networks may be resilient to blind spots, as compared with, say, random networks. The critical value q_c can be obtained numerically from Eq. (16) by setting $n_s(q_c)=c'$, where $c'\approx 1$ is a constant. The critical time t_c can be obtained from q_c as $t_c=-\tau\ln q_c$. Figure 7 shows the dependence of t_c on the network size for scale-free networks. The theory and the numerical simulation agree well.

IV. DISCUSSION

In conclusion, we have studied the critical behavior of the occurrence of blind spots in sensor networks. In such networks, at any time a sensor may be off due to battery drainage or may be turned back on if it is recharged. We have proposed a simple model to describe this on-off process. We have shown that, in the long-time limit, the dynamical on-off process is equivalent to a static percolation model and have then studied the occurrence of blind spots in four classes of topologically distinct networks: regular, random, mixed, and scale free. Scaling relations for the critical parameters p_c and t_c with the network size N have been obtained. Our result for t_c is reduced to the known result of Franceshetti *et al.*[9] under the same condition. The scaling relations for different types of networks can be significantly different; i.e., from power-law form to logarithmic. For realistic applications, the type of the network should be identified carefully in order to apply the scaling relations. Since our analysis depends only on degree distribution, it can be applied to other realistic networks such as the wireless cellular network, the Internet, or the transportation network, where the issue of blind spots may be of concern. For example, in wireless cellular networks, the likelihood that the network is totally disintegrated, i.e., the disappearance of a global spanning cluster, is small. Users of the network are more concerned with whether they can get access to the network (e.g., to receive and make phone calls). This is also determined by the occurrence of blind spots.

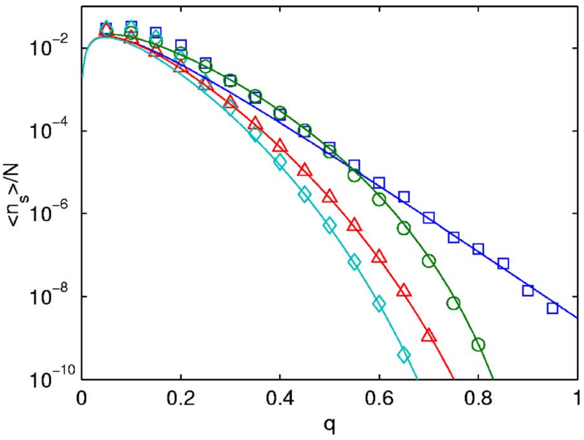

FIG. 8. (Color online) Comparison of the number of blind spots for the four classes of networks. Squares: random sensor network; circles: scale-free network with $\lambda=3.5$; triangles: mixed network with $\sigma^2=4$; diamonds: regular network. $N=10^4$ and $\langle k\rangle=20$ for all networks. Each data point is the average of 10^6 random realizations. Curves are from theory.

For the purpose of comparison, we have shown in Fig. 8 the number of blind spots n_s versus the occupying probability q for the four classes of networks considered in this paper, where $N=10^4$ is identical for all networks. We observe that for a fixed value of q, n_s is the smallest for the regular network, indicating that it is relatively more resilient to blind spots. Figure 9 compares the critical time t_c that the blind spots begin to occur in the circumstance of the dynamical on-off processes for the four types of networks with various network sizes. We observe that the random sensor network has the smallest t_c; thus it is most susceptible to having blind

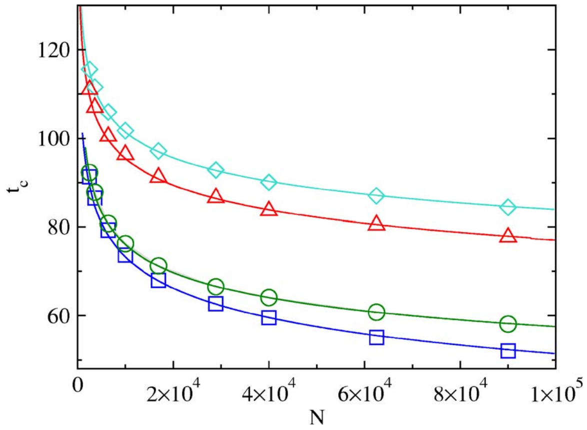

FIG. 9. (Color online) Comparison of the critical time t_c when blind spots begin to occur for the four classes of networks. Squares: random sensor network; circles: scale-free network with $\lambda=3.5$; triangles: mixed network with $\sigma^2=4$; diamonds: regular network. $N=10^4$ and $\langle k\rangle=20$ for all networks. $\pi_1=0.01$, $\pi_2=0$, and $\tau=100$. Each data point is the average of 10^4 random realizations. Curves are from theory.

spots. For example, take $N=90\,000$, blind spots occur at 50 time steps for the random sensor network, while for the regular network, it takes 85 time steps for the first blind spots to occur. Although in reality it is not always possible to have regular sensor networks due to practical restrictions (e.g., time-varying link conditions), our result provides a criterion for minimizing the occurrence of blind spots: try to make the network as regular as possible.

In an event-driven sensor network, total disintegration of the network is highly unlikely; i.e., whether there is a spanning cluster may not be a pressing issue (e.g., for intrusion detection). What one is concerned with most is whether individual nodes with information can get access to the network; i.e., the occurrence of blind spots. Since blind spots are more probable in networks that are more susceptible to percolation,[10] this may present a significant challenge to the design of secure and reliable networks: to make the network robust against attacks or random failures, it is necessary to reduce the percolation threshold, but the network may be unreliable from the standpoint of individual users because of the relatively higher likelihood of blind spots.

ACKNOWLEDGMENT

This work was supported by NSF under Grant No. ITR-0312131, by AFOSR under Grant Nos. FA9550-06-1-0024 and FA9550-07-1-0045, and by ONR under Grant No. N00014-05-1-0636.

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, IEEE Commun. Mag. **40**, 102 (2002).

[2] R. B. Owen and A. A. Zozulya, Opt. Eng. **39**, 2187 (2000).

[3] E. S. Biagioni and K. W. Bridges, Int. J. High Perform. Comput. Appl. **16**, 315 (2002).

[4] S. T. Vohra, F. Bucholtz, G. M. Nau, K. J. Ewing, and I. D. Aggarwal, Appl. Spectrosc. **50**, 985 (1996).

[5] S. Kamijo, Y. Matsushita, K. Ikeuchi, and M. Sakauchi, IEEE Trans. Intell. Transp. Syst. **1**, 108 (2000).

[6] E. A. Johannessen, L. Wang, L. Cui, T.-B. Tang, M. Ahmadian, A. Astaras, S. W. J. Reid, P. S. Yam, A. F. Murray, B. W. Flynn, S. P. Beaumont, D. R. S. Cumming, and J. M. Cooper, IEEE Trans. Biomed. Eng. **51**, 525 (2004).

[7] C. I. Merzbachery, A. D. Kersey, and E. J. Friebele, Smart Mater. Struct. **5**, 196 (1996).

[8] K. Kar, A. Krishnamurthy, and N. Jaggi, IEEE/ACM Trans. Netw. **14**, 15 (2006).

[9] M. Franceshetti and R. Meester, IEEE/ACM Trans. Netw. **14**, 2831 (2006).

[10] L. Huang, Y.-C. Lai, K. Park, and J. Zhang, Phys. Rev. E **73**, 066131 (2006).

[11] G. Grimmett, *Percolation* (Springer, New York, 1999).

[12] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, Phys. Rev. Lett. **85**, 4626 (2000); **86**, 3682 (2001).

[13] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, Phys. Rev. Lett. **85**, 5468 (2000).

[14] H. Hinrichsen, Adv. Phys. **49**, 815 (2000).

[15] G. Paul, S. Sreenivasan, and H. E. Stanley, Phys. Rev. E **72**, 056130 (2005); G. Paul, S. Sreenivasan, S. Havlin, and H. E. Stanley, Physica A **370**, 854 (2006).

[16] R. Albert and A.-L. Barabási, Rev. Mod. Phys. **74**, 47 (2002).

[17] One may also conceive some particular networks, say, in a two-dimensional space for which multinode blind spots are more likely than single-node blind spots. For example, think of N clusters, each of three fully interconnected nodes, each of which also is connected with a single edge to a common center, which is a single node. There are no blind spots as long as the center node is on, but all three-node clusters will be blind spots as soon as the central node goes off. Our point is that such specially constructed networks can be regarded effectively as a one-dimensional network. The one-dimensional feature is caused by nothing but the center node itself: if it is off, all clusters are disconnected, similar to what happens in a one-dimensional lattice when an arbitrary node is removed, disconnecting the subnetworks on both sides of the node. In fact, we conjecture that any network for which multinode blind spots can occur as often as single-node blind spots would be equivalent to a one-dimensional network.

[18] M. E. J. Newman, Phys. Rev. Lett. **89**, 208701 (2002).

[19] A. Vazquez and Y. Moreno, Phys. Rev. E **67**, 015101(R) (2003).

[20] E. Volz, Phys. Rev. E **70**, 056115 (2004).

[21] C. P. Warren, L. M. Sander, and I. M. Sokolov, Phys. Rev. E **66**, 056105 (2002).

[22] L. Huang, L. Yang, and K. Yang, Europhys. Lett. **72**, 144 (2005).

[23] B. Liu, Z. Liu, and D. Towsley, INFOCOM 2003: IEEE 22nd Annual Joint Conference of the IEEE Computer and Communications Societies, 2003, Vol. 2, pp. 1543.

[24] G. Sharma and R. Mazumdar, Proceedings of the 6th ACM International Symposium on Mobile ad hoc Networking and Computing, Urbana-Champaign, IL, 2005, p. 366.