On Topology and Resilience of Large-Scale Cognitive Radio Networks Under Generic Failures

Lei Sun, *Student Member, IEEE*, Wenye Wang, *Senior Member, IEEE*, and Zhuo Lu, *Member, IEEE*

***Abstract*—It has been demonstrated that in wireless networks, *blackholes*, which are typically generated by isolated node failures, and augmented by failure correlations, can easily result in devastating impact on network performance. In order to address this issue, we focus on the topology of Cognitive Radio Networks (CRNs) because of their phenomenal benefits in improving spectrum efficiency through opportunistic communications. Particularly, we first define two metrics, namely the *failure occurrence probability* p and *failure connection function* $g(\cdot)$, to characterize node failures and their spreading properties, respectively. Then we prove that each blackhole is exponentially bounded based on percolation theory. By mapping failure spreading using a branching process, we further derive an upper bound on the expected size of blackholes. With the observations from our analysis, we are able to find a sufficient condition for a resilient CRN in the presence of blackholes through analysis and simulations.**

***Index Terms*—Resilience, cognitive radio networks, topology, generic failures.**

I. Introduction

WIRELESS communication has experienced an explosive growth in the past few decades, which imposes a significant demand for the already-crowded radio spectrum. However, a recent report by the Federal Communications Commission (FCC) indicated that over 90% of the licensed spectrum remains idle at a given time and location [2]. This observation immediately incurs considerable attentions [3]–[7] to Cognitive Radio Networks (CRNs), which show great potential for improving spectrum usage efficiency by permitting secondary networks to coexist with licensed primary networks. On one hand, many efforts have been devoted to understanding the performance limits of CRNs, including maximum capacity, minimum delay and connectivity [1], [8]–[13]. These works have presented a very good understanding of the potential of CRNs for a variety of applications in theory. On the other hand, the properties and dynamics of *global topology*, which plays an important role in designing fundamental networking functionalities, such as point-to-point routing and scheduling algorithms, has never been well studied. The lack of knowledge about network topology greatly hinders the practical deployment of CRNs, which motivates the study on topological features of CRNs in this paper.

Topology of wireless networks changes frequently due to different factors (e.g., node mobility, failures) and in this paper, we focus on topological transmutation by studying *Blackholes* due to node failures. Such unavoidable faults can be brought out by malfunctions of electrical devices, energy depletion, natural disasters (fire, river overflow, earthquake, etc) or adversarial attacks (a bomb explosion for example). Communications may be disabled by jamming, traffic congestion or energy depletion. In addition, causal relations often exist among failures, i.e., some failures happen as a result of other earlier failures. One example of such correlated failures is traffic overloading and energy depletion [14], that is, when a node fails to deliver packets, the incoming and outgoing traffic is redistributed to the neighboring nodes. Some neighbors may work under heavy traffic loads, resulting in early energy depletion and node failures. Such correlation among failures and cascading effects lead to *Blackholes* (i.e., components of failed nodes, see formal definition in Section II) in the network, where information cannot be transmitted or forwarded.

Understanding the properties of Blackholes in the CRNs, or in particular, investigating structure and size of *Blackholes*, is of great importance in the design of basic networking operations. For example, a number of networking protocols exploit geometric intuitions for simple and scalable data delivery, such as geographical greedy forwarding [15], [16]. These algorithms based on local greedy advances may not work properly in the presence of *Blackholes*, where routing messages will be lost. Backup and restoration methods, such as face routing on a planar subgraph, can help packets get out of Blackholes, but also create high traffic on hole boundaries and eventually undermine network lifetime [15], [16]. In addition, a number of routing schemes address explicitly the importance of topological properties and propose routing with virtual coordinates that are adaptive to the intrinsic geometric features [17]. However, constructing these virtual coordinate systems requires the identification of topological features, especially Blackholes first in order to proceed routing.

Therefore, *Blackholes* have been extensively explored in wireless networks [18]–[20]. For example, Fang *et al.* [18] studied the difficulties imposed by *Blackholes* on geographic routing and proposed a distributed algorithm to build a path bypassing such holes. Wang *et al.* [19] focused on topology discovery and presented an algorithm to identify Blackholes.

Manuscript received June 28, 2014; revised September 30, 2014 and December 25, 2014; accepted February 11, 2015. Date of publication February 20, 2015; date of current version June 6, 2015. This work is supported by the NSF Award CNS 0546289, NSF Career Award and Defense Threat Reduction Agency (DTRA) Award HDTRA1-08-1-0024. Part of the work was presented at the 32th IEEE International Conference on Computer Communications, April 2013. The associate editor coordinating the review of this paper and approving it for publication was D. Niyato.

The authors are with the Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27606 USA (e-mail: leisun2@ncsu.edu; wwang@ncsu.edu; zlu3@ncsu.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2015.2404919

The spatial features of the holes and their impact on data preservation have been investigated in [20]. These results significantly improve our understanding of the disadvantageous impact of Blackholes on network performance.

Meanwhile, it is evident that all of these studies presume a few interesting but more fundamental questions. First, what is the driving force in the formation of Blackholes and how large are these holes? *Failure correlation* [20], [21] has been recognized as one of the most important factors for the occurrence of Blackholes and Xu *et al.* [21] further studied how an initial failure may incur a *giant hole* spanning over the entire network. Given its detrimental consequences, the occurrence of *giant hole* needs to be avoided in the initial network design [21] such that node failures can result in many *finite* holes in the network. However, how to quantify the *finite* size of these holes has not been discussed. Moreover, existing works [18]–[20] are focused on locating and bypassing these holes in the network. But a fundamental question is whether we can always find alternative routes to bypass all holes. If such routes do not exist, routing protocols may not be a good solution, which is a fundamental issue in multihop networks. Particularly, the ability of wireless networks to maintain global communication in the face of these Blackholes is a central concern for these routing protocols. And a network may be considered to be resilient if the largest connected component of operational nodes are distributed to the whole network and alternative routes bypassing dysfunctional nodes always exist in a resilient network. Therefore, network resilience is a premise for the applications of the existing solutions.

In this paper, we aim to provide insightful understanding of the above questions. In particular, we first study the process of how an initial failure "explodes" to a Blackhole and present theoretical analysis to quantify the scope of Blackholes. Using combinatorial arguments, we prove that the distribution of Blackhole size decays exponentially and we further provide an upper bound on the expected size of Blackholes by mapping failure spreading to a branching process. Then we investigate network resilience in the presence of Blackholes. A network is said to be *resilient* to node failures when there exists a large connected component of "surviving" (not failed) nodes spanning over the entire network. We have identified a sufficient condition for a resilient CRN against Blackholes by using techniques in *percolation theory* [22].

Our contributions to the understanding of topological resilience are as follows:

- We investigate the formation of Blackholes due to explosive spreading of random failures, and prove that each Blackhole is exponentially bounded and provide an upper bound on its expected size.
- We identify a sufficient condition when a CRN is resilient to blackholes, which can be used as a prerequisite for the blackhole locating and bypassing algorithms in the existing works [18]–[20].

Although we only addressed topological features and resilience of CRNs, questions presented in this paper are important yet remain unanswered in general multihop networks (e.g., wireless sensor networks and wireless *ad hoc* networks). Letting spatial density of primary users $\lambda_p = 0$, our results can be extended to other wireless multihop networks, which serves a timely complement to existing studies on restoration algorithms and protocols [18]–[20].

The rest of this paper is organized as follows. In Section II, we introduce network models and formulate the problem. In Section III, we present our main results about Blackhole size and network resilience, along with discussions of applications of our observations. We provide detailed proofs for our analytical results about size of Blackholes and network resilience in Sections IV and V, respectively. In Section VI, we use simulations to explain and validate our analysis, followed by the conclusions in Section VII.

II. System Models and Problem Formulation

In this section, we first present a brief description of preliminaries, then describe the network models, basic assumptions and notations, and formulate the problem last.

A. Preliminary

Before introducing network models, we need a brief introduction of common models and tools used to study wireless networks for clarification. A *continuum graph* consisting of nodes $\mathcal{X}$ placed in space $\mathbb{R}^2$, with edges added to connect pairs of nodes which are close to each other, can be used to model wireless networks [21], [23]–[26]. Rather than any specific positions, nodes $\mathcal{X}$ are usually assumed to be a Poisson point process for the following reasons. First, precise configuration of points may not be known. In addition, Poisson point process represents an average case. Some properties of graphs are unfeasible to compute for large graphs, and understanding their average behavior may be a useful alternative to exact computation. For example, given a Poisson point process $\mathcal{X} \subset \mathbb{R}^2$, the graph, denoted by $\mathcal{G}(\mathcal{X}, r)$, with vertex set $\mathcal{X}$ and edges connecting those pairs $\{x_1, x_2\} \in \mathcal{X}$ with $\|x_1 - x_2\| \leq r$, is called *Boolean model* and has been used in [23] to represent a large wireless network. If edge between x_1 and x_2 is added with probability $g(\|x_1 - x_2\|)$, the resulted graph $\mathcal{G}(\mathcal{X}, r, g)$ is called *random connection model* and has been used in [21] to study failure spreading.

Recently, *Percolation theory*, especially continuum percolation, has been widely used to study the coverage, connectivity, capacity and resilience of large-scale wireless networks [14], [21], [23]–[26]. A percolation process resides in a random geometric graph, where nodes or links are randomly designated as either "active" or "inactive". When the graph structure resides in continuous space, the resulting model is described by continuum model [14], [22]. A major focus of continuum percolation theory is the random geometric graph induced by a Poisson point process with density λ. A fundamental result for continuum percolation concerns a phase transition effect whereby the macroscopic behavior of the system is very different for densities below and above some critical value λ_c. For $\lambda > \lambda_c$, there exists a *giant component* containing an infinite number of points with positive probability; otherwise any component in the graph is finite.

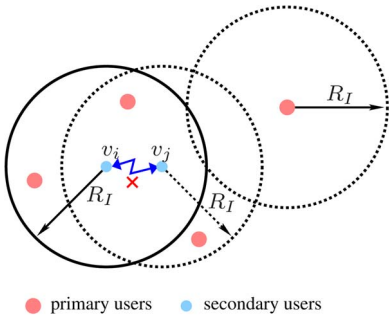

Fig. 1. *Primary-secondary* interference.

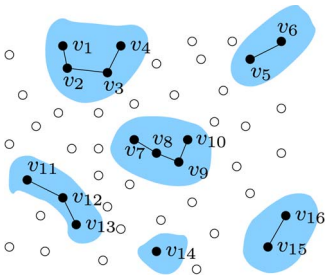

Fig. 2. An example of Blackholes.

B. Network and Failure Models

In this paper, we consider a large CRN consisting of n secondary users $\{v_1, \ldots, v_n\}$, which are modeled by a *random geometric graph* $\mathcal{G}(\mathcal{H}_\lambda, r)$, where $\mathcal{H}_\lambda = \{x_1, \ldots, x_n\}$ denotes the node set and r denotes the node transmission radius. In this model, $x_1, \ldots, x_n$ denote the random locations of secondary users and they are independently and identically distributed (i.i.d) in a region $\Omega = [0, \sqrt{\frac{n}{\lambda}}]^2$ for some constant λ. By definition, $\mathcal{H}_\lambda$ is a Poisson Point process with density λ as $n \to \infty$ [27]. The secondary users are assumed to share a set of m channels $\{ch_1, \ldots, ch_m\}$ with coexisting primary users. Particularly, we assume that for any $1 \le k \le m$, an overlay network of primary users with spatial density λ_{pk} are transmitting with channel ch_k, and $\lambda_{pk} = \lambda_p$ for any k for simplicity. A synchronized slotted structure has been adopted to model the dynamics of the primary traffic, which has been used in [24] to study the connectivity of a large single-channel CRN. Particularly, time is slotted into units and at any time slot, primary users transmitting on any channel ch_k are assumed to be uniformly and independently distributed in Ω, and such distribution is i.i.d across slots.

1) Interference Models: In CRNs, there are two types of interference for information dissemination among secondary users: *secondary-secondary* and *primary-secondary* interference. The former interference can be characterized by the well-known *protocol model* [28]. Particularly, without interference from primary users, a successful transmission from a secondary user v_i to v_j is achievable if $\|x_i - x_j\| \le r$ and for any other simultaneously transmitting node on the same channel v_l, $\|x_l - x_j\| \ge (1 + \Delta)r$, where r is the transmission radius of secondary users, and Δ models the guard zone around v_j in which any simultaneous transmission on the same channel causes collision at v_j. For the latter interference, denote R_I as the interference range of primary users. And as shown in Fig. 1, the secondary users v_i is permitted to use channel ch_k to transmit to some other secondary user v_j only when there are no primary users on ch_k in the neighborhood, i.e., $\|x_i(t) - u(t)\| > R_I$ for any primary user u transmitting with ch_k, where $u(t)$ is the position of u at time t.

2) Failure Model and "Explosion": In wireless networks, nodes fail unavoidably due to adversary attacks, natural hazards, resource depletion, etc. Node failures are often not independent and causal relations exist among these failures, i.e., some failures happen as a result of other earlier failures. Traffic overloading and energy depletion [14] is an example as a result of failures spreading. Because of failure correlation, each initial failure will "explode" and impact a component of nodes in the neighborhood. An illustration of such process is shown in Fig. 2. In this example, random failures initially occur at nodes v_1, v_5, v_8, v_{12}, v_{14} and v_{15}. As a result of the failure on v_1, node v_2 fails subsequently and spreads the failure further away to nodes v_3 and v_4. Similarly, nodes v_6, v_7, v_9, v_9, v_{10}, v_{11}, v_{13}, and v_{16} fail subsequently due to random failures on v_5, v_8, and v_{12}. In Physics, a Blackhole is a region of spacetime from which nothing, not even light, can escape [29]. Likewise, in a wireless network, any information (e.g., routing packets) transmitting to components of failed nodes will be absorbed (lost). This similarity motivates us call a component of failed nodes incurred by a particular initial failure (see the shaded area in Fig. 2) a *Blackhole* for convenience.

The above example shows that the formation of Blackholes consists of the occurrence of initial failures and explosion of these failures. Thus we introduce the following models:

- Random failure model: each node is either *surviving* or *failed* independently and a node may fail with probability p (*failure occurrence probability*). This model describes the initial occurrence of node failures.
- Failure explosion: We define *failure connection function* $g(\cdot)$ to model the likelihood of failure propagation from v_i to v_j. If $\|x_i - x_j\| < r$, failure spreads from v_i to v_j with a probability $g(\|x_i - x_j\|)$ that depends on their distance but not their respective locations. If v_j is beyond the transmission radius of v_i, failure cannot spread from v_i to v_j directly.

In this paper, we assume that $g(\cdot) \equiv \tau$, which is called *failure connection probability* and $r = 1$ by default, if there is no specific explanation. Thus failure spreading among secondary users can be represented as a random connection model $\mathcal{G}(\mathcal{H}_\lambda, 1, \tau)$.

Remark 1: These two models are not new. Particularly, *random failure model* has been used in [23] to study topology transition of wireless networks because of independent node failures (without considering failure spreading) and *failure connection function* has been used in [21] to determine whether an initial failure will spread to the entire network. However, as discussed above, the occurrence of random failures and their subsequent explosion are inseparable, and we are interested in this paper how these two processes together result in Blackholes in the network.

C. Problem Formulation

In order to understand the impact of Blackholes on network implementation (e.g., routing), we first focus on a particular hole, initiated by a failure on a node, say v_1, *w.l.o.g*, and denoted by $\mathcal{O}_{v_1}$. Existing results on *random connection model* [22] shows that there exists some critical value ζ on node density λ, such that if $\lambda > \zeta$, $\mathcal{O}_{v_1}$ may spread to the entire network with some positive probability; and if $\lambda < \zeta$, $\mathcal{O}_{v_1}$ is finite. Given the devastating consequence of large-scale failure spreading, previous work in [21] provided bounds on ζ, which helps network designers to operate network at $\lambda < \zeta$, making network be resilient to cascading failures. In this paper, we are interested in when $\lambda < \zeta$, how large $\mathcal{O}_{v_1}$ is.

Definition 1: (**BHG** problem): For a CRN which is resilient to large-scale failure spreading (i.e., $\lambda < \zeta$), how large does a Blackhole grow (i.e., how many failure nodes are in a Blackhole)?

Definition 2: (Blackholes Resilient, **BHR**): Given the existence of Blackholes, a CRN is said to be BHR if a *giant component* of surviving nodes, spanning over the entire network, exists.

A network may be said to be resilient if the remaining network is functional even after many node and link failures. For example, if a wireless sensor network still manages to collect information from a constant fraction of the sensors even after a substantial number of node and link failures, then the network is resilient. BHR property makes a CRN maintain global communication capability in the presence of Blackholes, i.e., information can bypass Blackholes and be disseminated to the entire network through the giant component, and thus a CRN with BHR property is considered to be resilient in this paper. And the BHR property provides a theoretical foundation to the existing studies on locating and bypassing Blackholes [18]–[20]. Next, we will formally define BHR problem.

BHR property makes a CRN maintain global communication capability in the presence of Blackholes, i.e., information can bypass Blackholes and be disseminated to the entire network through the giant component. And BHR property provides theoretical foundation to the existing studies on locating and bypassing Blackholes [18]–[20]. Next, we will formally define BHR problem.

Definition 3: (**BHR** problem). For a large CRN which is assumed to be initially connected (percolated), given node failures characterized by random failure model and failure explosion model, determine the condition under which the network is BHR.

III. Results and Applications

In this section, we present our main results concerning BHG and BHR problems. We find that the size of Blackholes is exponentially bounded and provide an upper bound on their expected size. Based on the understanding of size of Blackholes, we further identify a sufficient condition for a resilient CRN. In addition, we further discuss potential applications of our theoretical analysis.

A. Main Results

We summarize our main results as follows. First, following theorems solve the BHG problem.

Theorem 1: **Exponential decay of** $|\mathcal{O}_{v_1}|$. When Blackhole $\mathcal{O}_{v_1}$ is not percolated, there exists some $\epsilon > 0$ such that

$$\mathbb{P}\left(|\mathcal{O}_{v_1}| \geq N\right) \leq e^{-N\epsilon} \text{ for all } N \text{ sufficiently large.} \quad (1)$$

Remark 2: Theorem 1 shows that when a failure cannot spread to the entire network, the number of nodes that may be infected by this failure is exponentially bounded. Exponential distribution is not enough to show how large Blackhole $\mathcal{O}_{v_1}$ is, since the expected value $E(|\mathcal{O}_{v_1}|)$ of $|\mathcal{O}_{v_1}|$ is unidentified, i.e., the parameter ϵ in Eq. (1) is unknown. We provide $E(|\mathcal{O}_{v_1}|)$ in the next theorem.

Theorem 2: When Blackhole $\mathcal{O}_{v_1}$ is not percolated, its expected size is upper bounded by

$$\beta = E\left(|\mathcal{O}_{v_1}|\right) \leq \frac{1.43\pi\lambda^2\tau^2}{1 - 1.43\lambda\tau} + 1, \quad (2)$$

where λ is spatial density of secondary users and τ is failure connection probability.

Remark 3: Theorem 2 indicates that the expected Blackhole size grows as failure connection probability τ increases, which corresponds to our intuition that the Blackhole is large when nodes are prone to be infected by their neighbors. Eq. (2) further implies that $1 - 1.43\lambda\tau > 0$ is necessary to guarantee that Blackhole $\mathcal{O}_{v_1}$ is not percolated.

Theorems 1 and 2 study distribution and expected size of Blackhole $\mathcal{O}_{v_1}$. In particular, Eqs. (1) and (2) tells us that the size of Blackhole is expontentlaly distributed with a bounded mean. We note that our failure models (see Section II-B) do not take primary users into account, because reasons incurring failure correlation (e.g., due to traffic overloading and energy depletion) are usually independent of primary users. In fact, our failure models are similar to those used in general wireless networks [21], [23]. This implies that our results concerning Blackhole size can be directly applied to general wireless networks. In previous work [21], Xu *et al.* prove a value ζ such that when node density $\lambda > \zeta$, a failure is percolated, and it is not percolated otherwise. And our results further illustrate the size of nodes infected by a failure when $\lambda < \zeta$, which is an important and necessary complement to the existing work.

The next theorem answers the BHR problem, providing a sufficient condition for a resilient CRN in the presence of Blackholes.

Theorem 3: Given a CRN where each secondary node fails with probability p according failure models defined in Section II-B, it is BHR if $p < 1 - \frac{\Lambda e^{\beta}}{1 - e^{-\beta} + \Lambda}$, where

$$\Lambda = \sqrt{\frac{p_c^{\square}}{\left(1 - e^{\lambda d_l^2}\right)^2 \left(1 - (1 - e^{-\lambda_p \alpha})^m\right)}}, \quad (3)$$

$d_l = \frac{r}{\sqrt{5}}$, $\alpha = (d_l + 2R_I)(2d_l + 2R_I)$ and $p_c^{\square}$ is given in the Appendix.

Remark 4: BHR problem is not only important in CRNs, it also remains unanswered in general wireless networks. Setting

spatial density of primary users $\lambda_p = 0$, Theorem 3 also provides BHR condition for a general wireless network.

B. Applications

Besides the theoretical importance of our findings, our results can be used practically not only in the initial deployment, but also as a theoretical foundation in evaluating protocol designs. Here are some examples.

- In the initial deployment, an appropriate value for spatial density λ of wireless nodes can be decided to guarantee that any random failure can only spread within a predefined area, if failure connection probability τ is known.
- There are many routing protocols [18]–[20] proposed to identify a path to bypass Blackholes through the entire network. However, when the network is not BHR, such path does not exist and thus these protocols will not work properly and waste network energy. Our result concerning BHR can be used as a prerequisite in determining whether adopt these routing protocols, or as a benchmark in evaluating the efficiency of these protocols.
- In wireless networks, node failures affect the communication connectivity and in turn impair network functionality. As mentioned in [30], redeploying additional nodes is necessary to replace failed nodes so that a connected network topology can be maintained. Let T_i $(1 \le i \le n)$ denote the lifetime of node v_i before it is failed. Given survival function $S(t) \triangleq \mathbb{P}(T_i > t)$ (thus failure occurrence probability $p = 1 - S(t)$), our results provide network designers a guideline on the optimal time that the redeployment of additional nodes should be carried out.

IV. How Large is a Blackhole?

In this section, we demonstrate how to obtain the results concerning size of Blackhole $\mathcal{O}_{v_1}$ given in Section III. Specifically, we investigate how many nodes will be infected by occurrence of failure on v_1. We first study the distribution of $|\mathcal{O}_{v_1}|$.

A. The Distribution of $|\mathcal{O}_{v_1}|$

Using *percolation theory*, Xu *et al.* [21] determine the condition under which $\mathcal{O}_{v_1}$ may be percolated to the entire network. However, when $\mathcal{O}_{v_1}$ is not percolated, how large $|\mathcal{O}_{v_1}|$ is, remains unknown. To study distribution of $|\mathcal{O}_{v_1}|$, our approach takes following procedures. We first map failure spreading process defined on continuous plane onto a discrete lattice, whose edges are declared *open* if certain properties are met (*closed* otherwise). In the discrete lattice, we then investigate the size of components consisting of open edges using combinatorial arguments. With a careful definition on the open edge in the lattice, a relation between the size of Blackholes and size of components of open edges can be derived. Finally, we obtain the distribution of Blackhole size $|\mathcal{O}_{v_1}|$ in Theorem 1. The detailed proof is presented as follows.

Proof of Theorem 1: When studying topology of continuum graph, an useful technique is the discretization of the graph on $\mathbb{R}^2$ into lattice on integer space $\mathbb{Z}^2$, since topological properties of the latter are easier to be analyzed [31]. One of the technical uses of such a discretization lies in the availability of combinatorial arguments for enumerating the sets in $\mathcal{Z}^2$. To proceed, we shall require a variety of notations. A set $A \subset \mathbb{Z}^2$ is said to be *symmetric* if $-x \in A$ for all $x \in A$. Vertices $x, y \in A$ are said to be *A-adjacent*$(x \sim_A y)$ if and only if $y - x \in A$. A subset $S \subset \mathbb{Z}^2$ is *A-connected* if it induces a subgraph with adjacency relation $\sim_A$. The following lemma, which says that the number of *A-connected* subsets of $\mathbb{Z}^2$ of size N containing the origin grows at most exponentially, is helpful.

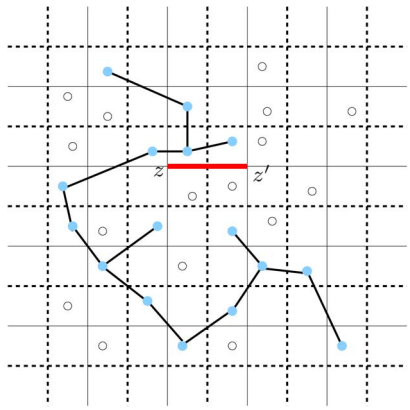

Fig. 3. An illustration of mapping from continuum graph to discrete lattice.

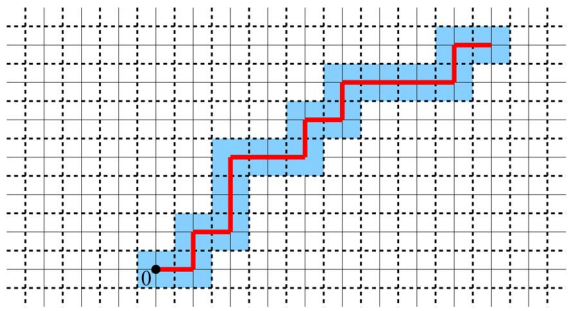

Fig. 4. An example of open path and the union of its associated boxes.

Lemma 4: (**Peierls argument**, see page 178 in [27]) Let A be a finite symmetric subset of $\mathbb{Z}^2$ with $|A|$ elements. The number of *A-connected* subsets of $\mathbb{Z}^2$ containing the origin, of cardinality N, is at most $2^{|A|N}$.

In this paper, we consider a discrete lattice $\mathcal{L} = d_l \times \mathbb{Z}^2$ with side length d_l. The coordinates of the vertices of $\mathcal{L}$ are $(d_l \times i, d_l \times j)$ for $(i, j) \in \mathbb{Z}^2$. Adjacency is defined by $A = \{z \in \mathcal{L} : \|z\|_1 = d_l\}$ where $\|\cdot\|_1$ denotes 1-norm distance, i.e., an edge connects $x, y \in \mathcal{L}$ only when $\|x - y\|_1 = d_l$ (see solid lines in Figs. 3 and 4). For any $z \in \mathcal{L}$, we construct a box B_z of size d_l centered at $d_l \times z$ (see the dash lines in the Figs. 3 and 4). As Fig. 3 shows (for figures in this paper, solid dots and circles denote failed and surviving nodes respectively), failure spreading, represented by random geometric graph $G(\mathcal{H}_\lambda, r, \tau)$ (i.e., graph consisting of failed nodes and edges connecting them), induces a realization of the bond percolation on $\mathcal{L}$ by setting an arbitrary bond $zz' \in \mathcal{L}$ to be *open* if there exists an edge $uv \in G(\mathcal{H}_\lambda, r, \tau)$ such that $u \in B_z$ and $v \in B_{z'}$. That is, given one or more failed nodes in B_z, at least one failed node connects to some some nodes in $B_{z'}$. And an example of *open*

bond zz' is shown in Fig. 3. Let $C(v_1)$ denote the cluster of open bonds and $|C(v_1)|$ denote its size. It is obviously true that if $|\mathcal{O}_{v_1}| < \infty$, then $|C(v_1)| < \infty$, and vice versa. The mapping between the cluster of failed nodes and the cluster of open bonds allows us to find $|C(v_1)|$ and thus use it to study $|\mathcal{O}_{v_1}|$.

Particularly, when $\mathcal{O}_{v_1}$ is not percolated, $C(v_1)$ is not percolated. *Bond percolation* on discrete lattice (see Theorem 6.75 in [31]) shows that if $C(v_1)$ is not percolated, then there exist constants $\mu > 0$, $n_0 > 0$ such that

$$\mathbb{P}\left(|C(v_1)| \geq N\right) \leq e^{-\mu N}, \quad N \geq n_0. \tag{4}$$

By Peirels argument (Lemma 4), there is a constant γ such that, for all N, the number of open paths of $\mathcal{L}$ of cardinality N containing the origin is at most γ^N. If $|C(v_1)| < N$ and $|\mathcal{O}_{v_1}| > KN + 1$, then for at least one of these open paths, the union of associated boxes B_z contains at least KN nodes of $\mathcal{H}_\lambda$ (an example of such path and its associated boxes are shown in Fig. 4 as the bold line and shaded area). Therefore, we have

$$\mathbb{P}\left[\{|C(v_1)| < N\}\{|\mathcal{O}_{v_1}| > KN + 1\}\right] \leq \gamma^N \mathbb{P}\left[Po\left(N\lambda d_l^2\right) \geq KN\right], \tag{5}$$

where $Po(\cdot)$ denotes Poisson distribution. To continue, we need the following lemma (see (1.12) in [27]).

Lemma 5: Let $Po(\lambda)$ be a Poisson random variable with density λ. If $K > e^2\lambda$, then

$$\mathbb{P}\left[Po(\lambda) \geq K\right] \leq e^{-\left(\frac{K}{2}\right)log\left(\frac{K}{\lambda}\right)}. \tag{6}$$

Letting $K \geq e^2 d_l^2 \lambda$ and putting Eq. (6) into Eq. (5), we have

$$\mathbb{P}\left[\{|C(v_1)| < N\}\{|\mathcal{O}_{v_1}| > KN+1\}\right] \leq \gamma^N e^{-\left(\frac{KN}{2}\right)log\left(\frac{K}{d_l^2\lambda}\right)}. \tag{7}$$

If we take K sufficiently large, we see from Eqs. (4) and (7) that $\mathbb{P}(|\mathcal{O}_{v_1}| > KN + 1)$ decays exponentially in N, so that Eq. (1) follows. ■

After proving exponential distribution of Blackhole $\mathcal{O}_{v_1}$, we next study its expected size.

B. The Expected Value of $|\mathcal{O}_{v_1}|$

In this subsection, we investigate the expected number of nodes in Blackhole $\mathcal{O}_{v_1}$ and prove the upper bound Eq. (2) given in Theorem 2. Specifically, we model failure spreading in CRNs as a branching process [32]. By studying the number of offspring in this branching process, we obtain our result. The detailed proof is given as follows.

Proof of Theorem 2: Denote our network with a graph $G(\mathcal{H}_\lambda, 1, \tau)$. Let $x_1, x_2, \ldots$ be the points of the Poisson process $\mathcal{H}_\lambda$ and assume that a failure initially occurs to x_1 (thus x_1 is initial member of the 0-th generation of the branching process, as shown in Fig. 5). The children of x_1 in this branching process are points which can be infected by x_1 directly. According to failure spreading model in Section II-B, each point of $\mathcal{H}_\lambda$ which lies in the ball $\mathcal{B}(x_1, 1) = \{y \in \mathbb{R}^2 : \|y - x_1\| \leq 1\}$ (see the big circle in Fig. 5) may be a child of x_1 with probability τ. If we take another Poisson process X_1 with density $\lambda \cdot \tau$, independent of $\mathcal{H}_\lambda$ and let $x_{1,1}, \ldots, x_{1,n_1}$ be all the points of X_1 which lie in the ball $\mathcal{B}(x_1, 1)$, the children of x_1 in the branching process are equivalent to these points $x_{1,1}, \ldots, x_{1,n_1}$ by *thinning theorem* [22].

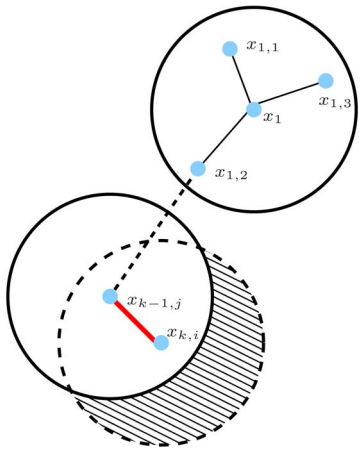

Fig. 5. An illustration of the branching process for the failure spreading.

Let $x_{k,1}, x_{k,2}, \ldots, x_{k,n_k}$ be the members of the k-th generation of the branching process. To obtain the children of $x_{k,i}$, we consider a Poisson point process $X_{k+1,i}$ of density $\lambda \cdot \tau$ on $\mathbb{R}^2$, where $X_{k+1,i}$ is independent of all the processes described as yet. The children of $x_{k,i}$ are those points of the process $X_{k+1,i}$ which fall in the region $\mathcal{B}(x_{k,i}, 1) \setminus \mathcal{B}(x_{k-1,j}, 1)$ (see the shaded area in Fig. 5), where $x_{k-1,j}$ is the parent of $x_{k,i}$. The *type* of a child is defined as the distance between this child and its parent. For example, the type of $x_{k,i}$ is defined $\|x_{k-1,j} - x_{k,i}\| \in (0, 1)$ (e.g., the length of the solid line in Fig. 5). Clearly, the distribution of the number and types of children of $x_{k,i}$ depend only on $x_{k,i}$ and its type. Indeed, the distribution of the number of children of $x_{k,i}$ whose types lie in (a, b), $0 \leq a < b \leq 1$ depends only on the area of the region $(\mathcal{B}(x_{k,i}, 1) \setminus \mathcal{B}(x_{k-1,j}, 1)) \cap \{y : \|y - x_{k,i}\| \in (a, b)\}$, and this area depends on $x_{k-1,j}$ only through the distance $\|x_{k-1,j} - x_{k,i}\|$, which is precisely the type of $x_{k,i}$. Also, the distribution of the number and types of children of an individual $x_{k,i}$ does not depend on its generation k.

Given that $x_{k,i}$ is of type h, i.e., $\|x_{k,i} - x_{k-1,j}\| = h$, let $f(w|h)$ be the length of the curve given by $(\mathcal{B}(x_{k,i}, 1) \setminus \mathcal{B}(x_{k-1,j}, 1)) \cap \{y : \|y - x_{k,i}\| = w\}$. A precise expression for $f(w|h)$ follows from an elementary trigonometric calculation, which yields

$$f(w|h) = \begin{cases} 2w\cos^{-1}\frac{1-h^2-w^2}{2hw} & \text{if } 1-h < w < 1 \\ 0 & \text{if } 0 < w \leq 1-h. \end{cases}$$

Recalling our earlier discussion on the independence properties of the offspring distribution, we easily see that the expected number of children whose types lie in (a, b) of an individual whose type is h is given by $\int_a^b \lambda\tau f(w|h)dw$. Moreover, given that an individual is of type h, the expected total number of grandchildren of this individual whose types lie in (a, b) is given by

$$\int_0^1 \left(\int_a^b \lambda^2\tau^2 f(w|t)dw\right) f(t|h)dt. \tag{8}$$

In other words, if we let

$$f_1(w|h) = \int_0^1 f(w|t)f(t|h)dt,$$

the integral in (8) reduces to

$$\lambda^2\tau^2 \int_a^b f_1(w|h)dw.$$

Thus defining recursively,

$$f_i(w|h) = \int_0^1 f_{i-1}(w|t)f(t|h)dt,$$

we easily see that the expected number of members of the n-th generation having types in (a, b) coming from a particular individual of type h as an ancestor n generations previously is given by

$$\lambda^i\tau^i \int_a^b f_i(w|h)dw.$$

Hence the expected total number of individuals in the branching process if we start off with an individual of type h is

$$\sum_{i=1}^{\infty} \lambda^i\tau^i \int_0^1 f_i(w|h)dw. \tag{9}$$

The node density λ is small enough to make Eq. (9) converge by the assumption that failure is not percolated. To estimate Eq. (9), we define

$$T(h) = \int_0^1 f(w|h)dw.$$

It is easy to see that

$$\int_0^1 f_i(w|h)dw = T^i(h).$$

Thus Eq. (9) reduces to

$$\sum_{i=1}^{\infty} \lambda^i\tau^i T^i(h). \tag{10}$$

By using Hilbert-Schmidt operator and standard numerical methods of calculating eigenvalues (see page 87 of [22]), we can show that $T(h) < 1.43$. Thus Eq. (9) reduces to

$$\sum_{i=1}^{\infty} \lambda^i\tau^i T^i(h) \leq \sum_{i=1}^{\infty} \lambda^i\tau^i 1.43 = \frac{1.43\lambda\tau}{1 - 1.43\lambda\tau}. \tag{11}$$

Come back to the 0-generation node x_1. By *thinning theorem* [22], the expected number of children of x_1 is $\pi\lambda\tau$. Note that the expected total number of individuals starting of any child $x_{1,j}$ of x_1 is upper bounded by Eq. (11), thus the expected number of nodes in each hole is upper bounded by Eq. (2). This completes the proof. ■

Now we have proved distribution and expected size of Blackhole $\mathcal{O}_{v_1}$ given in Theorems 1 and 2, which solve the BHG problem. Next, we formally solve the BHR problem defined in Section II-C, i.e., given exponentially distributed Blackholes, does there exist a giant component of surviving nodes spanning over the entire network?

V. Is a Large CRN Blackhole Resilient?

In this section, we study the macroscopic structure of a large CRN in the face of Blackholes and formally prove the sufficient condition for a BHR network addressed in Theorem 3. As mentioned in Section II-A, *percolation theory* [22] is a useful tool to investigate topology of wireless networks. For example, by using *percolation theory*, Sun *et al.* [25] study the *connectivity* of a large CRN without failures, and identify a critical density λ_c, above which (i.e., node density $\lambda > \lambda_c$) there exists a giant component of nodes. Xu *et al.* [21] prove a value ζ such that when node density $\lambda < \zeta$, a failure can only spread among a finite number of nodes. In this paper, we are interested in the scenario that $\lambda_c < \lambda < \zeta$. That is, the CRN is percolated initially. As time goes on, random failures may occur and each failure may infect a *finite* number of neighboring nodes, i.e., a sequence of *Blackholes* may appear. An interesting question is that in the event of Blackholes, whether the network remains percolated, or the giant component breaks into many small components. Next, we aim at answering this question.

A. Challenges and Differences With Earlier Work

As mentioned earlier, node failures and their impact on network topology have been studied in [21], [23]. Particularly, under a subtle assumption of no failure correlations, Xing *et al.* [23] provide a condition for a percolated network when random failures may occur independently. On the other hand, Xu *et al.* [21] focus on a particular failure and study the condition when this failure may spread to the entire network due to failure correlations. Note that existing results in *percolation theory* [22], [27] are based on the fundamental assumption that the nodes are distributed as a Poisson point process. *Thinning theorem* [22], [27] ensures that nodes after failures in [21] and [23] are still distributed as Poisson point process and hence existing results can be applied directly. For example in [23], nodes are initially distributed as a Poisson point process with spatial density λ and each node may fail *independently* with probability p. By *Thinning theorem*, the resulted network of surviving nodes is a Poisson point process with density $\lambda(1-p)$. *Percolation theory* [22], [27] states that a Poisson distributed network is percolated when node density is above some critical value ϕ, and therefore a condition for network percolation in [23] is $\lambda(1-p) > \phi$.

In contrast to these two extreme scenarios investigated in [21], [23], we studied a generic scenario that initially, random failures may occur independently, and then each failure may explode and incur an exponentially bounded Blackhole. Therefore, *Thinning theorem* [22], [27], which requires independent failures, cannot be used here and obviously surviving nodes are *no longer* distributed as a Poisson point process. This indicates that existing results in percolation theory cannot be used to solve *BHR* problem directly. Fortunately, reference [22] (Page 181) shows that *percolation phenomenon* (see Section II-A) happens not only in the *Poisson* point process, but in any **stationary** point process. The occurrence of Blackholes does not change

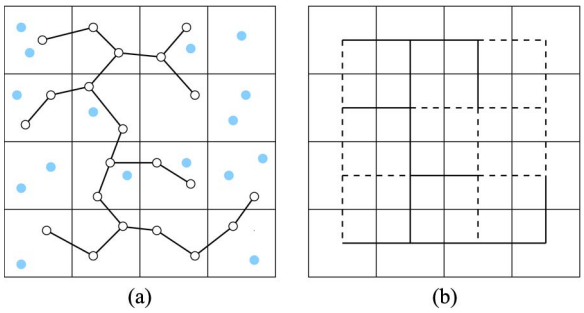

Fig. 6. Mapping from continuous to discrete percolation. (a) continuous; (b) discrete.

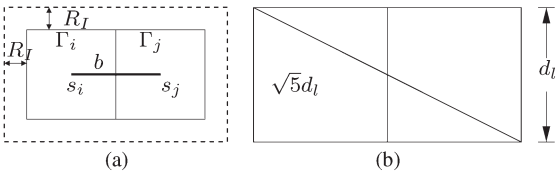

Fig. 7. Illustration of events and cell size. (a) Events; (b) Determination of cell size.

the *stationary* property of the original Poisson point process, which motivates us to use some fundamental proof techniques in *percolation theory* to study the BHR problem.

B. Sufficient Condition for a Resilient CRN

In this section, we determine the BHR condition provided in Theorem 3 by using the technique of *continuous-to-discrete* percolation mapping. Specifically, we divide the network area into many small square cells and thus the graph consisting of surviving nodes and their connections now appear on the background of these cells, as illustrated in Fig. 6(a). The size of components of surviving nodes is studied via bond percolation on a discrete grid, as shown in Fig. 6(b). In particular, to obtain this discrete grid, we represent a cell in Fig. 6(a) by a site located at the center of this cell and two neighboring sites are connected by a bond, which represents the neighborhood between the two corresponding cells. We choose the size of each cell small enough such that given two arbitrary locations in two neighboring cells, one in each, their distance is at most r (r is the transmission range of secondary users defined in Section II-B). This small cell size guarantees that a secondary node is able to communicate with every node in the neighboring cell. Two nodes are separated farthest as shown in Fig. 7(b), in which their distance is $d_l\sqrt{5}$ and d_l is side length of the cell. Letting $d_l\sqrt{5} = r$, we obtain $d_l = \frac{r}{\sqrt{5}}$. To proceed, we need the following notations for a given bond $b = s_i s_j$.

- Event A_{s_i}: At least one surviving secondary node lies in the cell Γ_i associated with site s_i (see Fig. 7(a)).
- Event $C_{s_i s_j}$: The rectangle Rec_b associated with bond b is defined as the union of two squares associated with s_i and s_j respectively (e.g., see the solid rectangle in Fig. 7(a)). Particularly, denote d_l as the length of the square (see Fig. 7(b)), and (X_{s_i}, Y_{s_i}) and (X_{s_j}, Y_{s_j}) as coordinates of sites s_i and s_j respectively. Then $Rec_b \triangleq [X_{s_i} - \frac{d_l}{2}, X_{s_i} + \frac{3d_l}{2}] \times [Y_{s_i} - \frac{d_l}{2}, Y_{s_j} + \frac{d_l}{2}]$. The extended rectangle is defined as $RecE_b \triangleq [X_{s_i} - \frac{d_l}{2} - R_I, X_{s_i} + \frac{3d_l}{2} + R_I] \times [Y_{s_i} - \frac{d_l}{2} - R_I, Y_{s_i} + \frac{d_l}{2} + R_I]$ (see the dash rectangle in Fig. 7(a)), where R_I is the interference range of primary users. We define event $C_{s_i s_j}$ as the set of outcomes for which the following condition is satisfied: there exists at least one channel ch_k such that no primary users using ch_k lie in $RecE_b$.

Note that event $C_{s_i s_j}$ guarantees that for some channel ch_k, the distance between primary users using ch_k and any locations within Rec_b is larger than the interference range of primary users R_I, which indicates that ch_k can be used by any secondary users in Rec_b. We next define a bond $s_i s_j$ to be open when events A_{s_i}, A_{s_j} and $C_{s_i s_j}$ occur simultaneously. Particularly, let $\mathbb{P}_o$ be the probability that any bond is open. Then we have $\mathbb{P}_o = \mathbb{P}(A_{s_i} \cap A_{s_j} \cap C_{s_i s_j})$. By this definition, an open bond $s_i s_j$ implies that surviving nodes exist in Γ_i and Γ_j respectively, and some channel can be used by these nodes. This is equivalent to saying that an open bond $s_i s_j$ implies an communication link across Γ_i and Γ_j. By this mapping, bond percolation on the discrete lattice ensures percolation of CRN. Therefore, we next investigate bond percolation condition for the discrete grid, which is sufficient for a BHR network.

In Section IV, we have shown that the number of failed nodes in each Blackhole $\mathcal{O}_{v_1}$ is upper bounded by $\Upsilon \sim Exp(-\beta)$, where the expected size β of $\mathcal{O}_{v_1}$ is given in Eq. (2). That is, any node v_i may be infected by at most $\Upsilon - 1$ nodes. Thus let $\mathbb{P}_l$ denote the probability that a node v_i is surviving (not failed) and we have

$$\begin{aligned}\mathbb{P}_l &= \sum_{\iota=1}^{\infty} \mathbb{P}(v_i \text{ is surviving} | \Upsilon = \iota)\mathbb{P}(\Upsilon = \iota) \\ &= \sum_{\iota=1}^{\infty} (1-p)^{\iota} \left(\mathbb{P}(\Upsilon \geq \iota) - \mathbb{P}(\Upsilon \geq \iota + 1)\right) \\ &= \sum_{\iota=1}^{\infty} (1-p)^{\iota}(1 - e^{-\beta})e^{-\beta\iota} \\ &= \frac{(1-e^{-\beta})(1-p)e^{-\beta}}{1-(1-p)e^{-\beta}}. \end{aligned} \tag{12}$$

And

$$\mathbb{P}\left(A_{s_i}\right) \geq \mathbb{P}_l \left(1 - e^{\lambda d_l^2}\right). \tag{13}$$

And by the assumption that primary users on any channel ch_k are distributed as a Poisson point process with density λ_p, we have

$$\mathbb{P}\left(C_{s_i s_j}\right) = 1 - \left(1 - e^{-\lambda_p \alpha}\right)^m, \tag{14}$$

where $\alpha = (d_l + 2R_I)(2d_l + 2R_I)$ denotes the area of $RecE_b$ (as illustrated in Fig. 7(a)).

To obtain $\mathbb{P}_o = \mathbb{P}(A_{s_i} \cap A_{s_j} \cap C_{s_i s_j})$, another challenge is that A_{s_i} and A_{s_j} are not independent. To continue, we need introduce the following concept and inequality.

Definition 4: For two geometric random graphs $\mathcal{G}$ and $\mathcal{G}'$, a partial ordering $\preceq$ is defined as $\mathcal{G} \preceq \mathcal{G}'$ if and only if $\mathcal{G}'$ can be induced from $\mathcal{G}$ by adding more (Poisson) points. Then an event

E is said to be increasing (decreasing) if $\forall \mathcal{G} \preceq \mathcal{G}'$, $1_E(\mathcal{G}) \leq 1_E(\mathcal{G}')(1_E(\mathcal{G}) \geq 1_E(\mathcal{G}'))$, where 1_E is the indicator function of event E.

Lemma 6: (KFG's inequality [22]) If two events E_1 and E_2 are both increasing or decreasing, then

$$\mathbb{P}(E_1 \cap E_2) \geq \mathbb{P}(E_1)\mathbb{P}(E_2).$$

By our definition, the more points in Γ_i, the more likely A_{s_i} occurs. Thus A_{s_i} is increasing. Therefore, we have

$$\begin{aligned}\mathbb{P}_o &= \mathbb{P}(A_{s_i} \cap A_{s_j} \cap C_{s_i s_j}) \\ &= \mathbb{P}\left(A_{s_i} \cap A_{s_j}\right) \mathbb{P}\left(C_{s_i s_j}\right) \geq \mathbb{P}\left(A_{s_i}\right) \mathbb{P}\left(A_{s_j}\right) \mathbb{P}\left(C_{s_i s_j}\right) \\ &\geq \mathbb{P}_l^2 \left(1 - e^{\lambda d_l^2}\right)^2 \left(1 - \left(1 - e^{-\lambda_p \alpha}\right)^m\right). \end{aligned} \tag{15}$$

Finally, by using the percolation condition in square lattice, we can achieve the sufficient BHR condition given in Theorem 3.

Proof of Theorem 3: As analyzed above, by careful definition of *open* bond in the square lattice, bond percolation on the mapped lattice guarantees the BHR property of CRN. In the Appendix, we derived a probability $p_c^{\square}$ such that if bond is open with probability $\mathbb{P}_o > p_c^{\square}$, the square lattice is percolated, which further indicates a BHR CRN. Plugging Eq. (15) and solving

$$\mathbb{P}_l^2 \left(1 - e^{\lambda d_l^2}\right)^2 \left(1 - \left(1 - e^{-\lambda_p \alpha}\right)^m\right) > p_c^{\square}, \tag{16}$$

we arrive at

$$\mathbb{P}_l > \Lambda, \tag{17}$$

where Λ is given in Eq. (3). Then substituting Eq. (12) into Eq. (17), we have

$$1 - p > \frac{\Lambda e^{\beta}}{1 - e^{-\beta} + \Lambda}, \tag{18}$$

which indicates that $p < 1 - \frac{\Lambda e^{\beta}}{1 - e^{-\beta} + \Lambda}$ is sufficient for a BHR CRN. This completes the proof. ■

VI. Simulations

In this section, we have performed a series of simulations in MATLAB to explain and demonstrate the occurrence of Blackholes, and validate our theoretical analysis. In the simulation, secondary users are distributed independently and uniformly with density λ. Time is slotted into units, and at each time slot, primary users on any channel are distributed as a Poisson point process with density λ_p. The transmission range r of secondary users and interference range R_I of primary users are set as $r = 50$ (meters) and $R_I = 80$ (meters) respectively.

We consider a CRN deployed within area $[0, 1000]^2$ (meters) with $m = 4$ channels, $\lambda = 0.0008(per\ meter^2)$ and $\lambda_p = 0.00001(per\ meter^2)$. To study Blackholes, we first investigate the occurrence of random failures (according to the random failure model in Section II-B). Assume that each secondary node fails independently with probability $p = 0.1$, as shown in

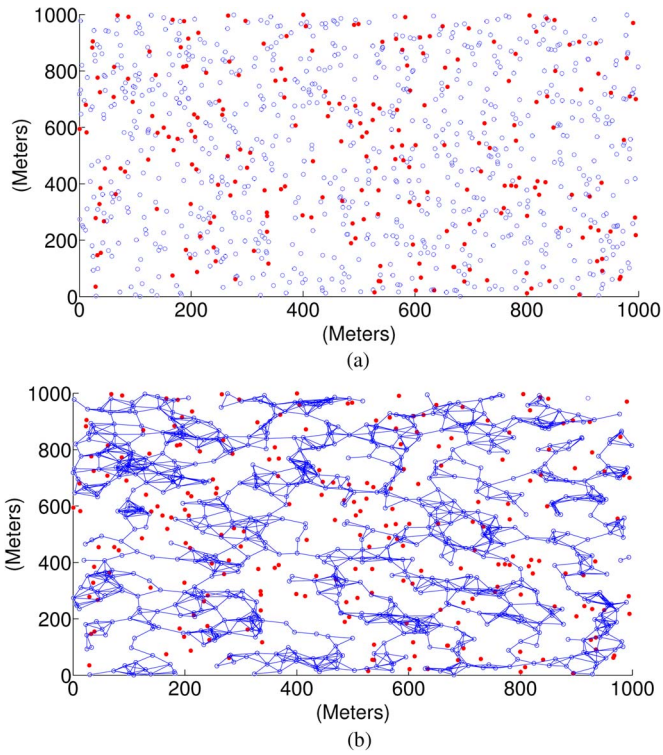

Fig. 8. Network percolation in the event of random failures. (a) Random failures. (b) A percolated CRN in the event of random failures.

Fig. 8(a) (in Figs. 8–11, solid dots and circles represent failed and surviving nodes respectively, a line connecting two failed (surviving) nodes denotes a failure connection (communication link), and the positions of primary users are not shown in the figures for simplicity). Ignoring failure correlation, the condition of whether a network is percolated in the event of such independent failures has been studied in [23]. An example of a percolated CRN in the face of independent failures has been shown in Fig. 8(b). On the other hand, to understand the failure correlation, we simulate the scenario studied in [21]. Specifically, a particular failure occurs initially, as shown in Fig. 9(a) (see the solid dot in square area). This failure may infect its neighbors, according to the failure explosion model defined in Section II-B, and similarly, infected neighbors may further impact more nodes. Xu *et al.* [21] determine when this failure will spread to the entire network and an example of such failure percolation has been shown in Fig. 9(b).

In contrast, we will study the random failures and then their explosion subsequently. In particular, random failures may occur initially according to the random failure model, as shown in Fig. 8(a). Each random failure then explodes according to the failure explosion model. By using the results in [21], we can set network parameters to ensure that each failure will not spread to the entire network. Therefore, each failure only infects a finite number of nodes and thus a sequence of Blackholes occur (see the components of solid dots in Figs. 10(a) and 11(a), and two examples of Blackholes have been circled in Fig. 10(a)). The size of Blackholes depends on the *failure connection probability* τ in the failure explosion model (Blackhole size increases as τ increases, as shown in Eq. (2)). And Blackholes in Figs. 10 and 11 are incurred by setting $\tau = 0.2$ and 0.3

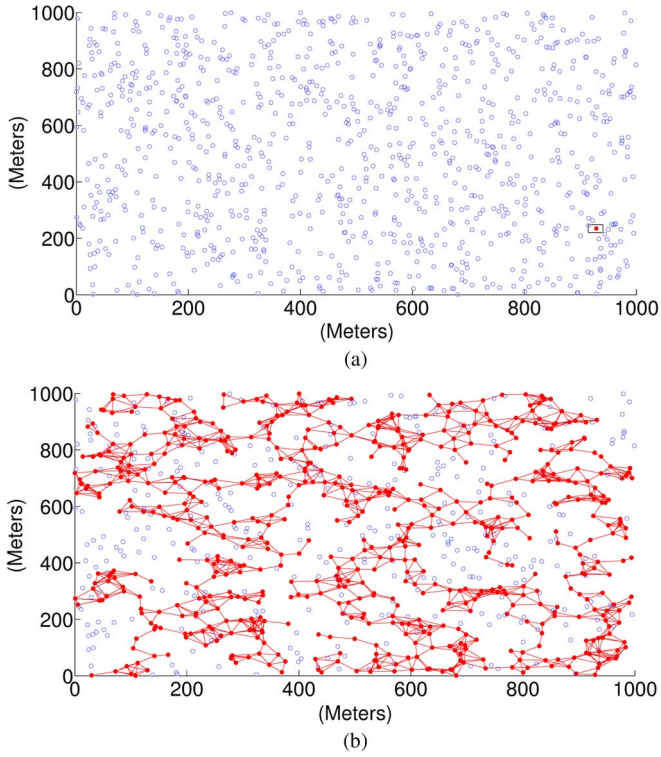

Fig. 9. An initial failure explodes to the entire network. (a) An initial failure. (b) Failure percolation.

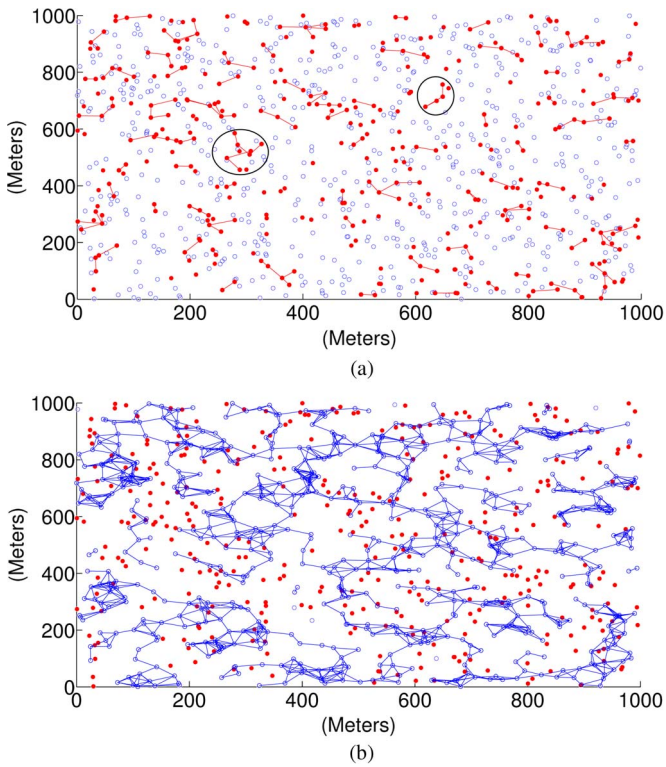

Fig. 10. Network is percolated in the event of small Blackholes. (a) Small Blackholes. (b) Network percolation in the face of Blackholes.

respectively. When Blackholes are small, CRN is percolated (see the giant component of surviving nodes in Fig. 10(b)). As Blackholes grow, this giant component may disappear and CRN is not percolated, as shown in Fig. 11(b). This motivates our

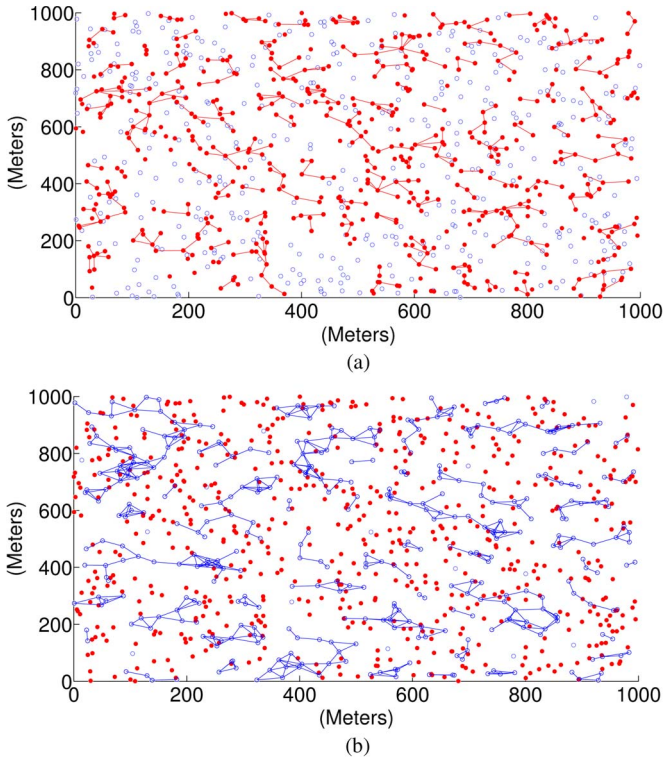

Fig. 11. Network is not percolated in the face of large Blackholes. (a) Large Blackholes. (b) Non-percolation in the face of Blackholes.

study on the size of Blackholes (BHG problem) and determine when the network is percolated in the presence of Blackholes (BHR problem).

To study the size of Blackholes $\mathcal{O}_{v_1}$, we run the simulation with $\lambda = 0.0008$ and $\lambda_p = 0.00001$ within $[0, 1000]^2$ 1000 times independently for variant failure connection probability τ. The probability $\mathbb{P}(|\mathcal{O}_{v_1}| = N)$ is calculated by the frequency of the occurrence of Blackholes with size N. Using this method, the complementary distributions (CCDF) of $\mathcal{O}_{v_1}$ under $\tau = 0.2$, 0.25, 0.3 have been calculated and shown in Fig. 12 on a semi-log scale. As illustrated in Fig. 12, CCDFs under different τ are approximately linearly under semi-log scale, which validates our analysis in Theorem 1 that the size of Blackholes $\mathcal{O}_{v_1}$ decays exponentially. In addition, Fig. 12 further shows that the CCDF of $\mathcal{O}_{v_1}$ decreases, which indicates the expected size of Blackholes $E(|\mathcal{O}_{v_1}|)$ decreases, as failure connection probability τ decreases. This corresponds to our result about expected size of Blackholes in Theorem 2.

The major objective of this paper is to build analytical models for failure spreading and investigate the stochastic properties of Blackholes, and derive theoretical conditions for resilience to these Blackholes in closed-form. Therefore, in the simulations, we focus on illustrating the spreading of failures, the formation of Blackholes, the existence of "percolation phenomenon" in the face of the Blackholes and more importantly verifying the stochastic results (e.g., the exponential tail of Blackholes verified in Fig. 12). Note that the exact value of critical density cannot be derived in the closed form even for the fundamental *Boolean model* [27], given the random positions of nodes. Therefore, we focus simulations on verifying such stochastic properties of the Backholes rather than trying to find the exact

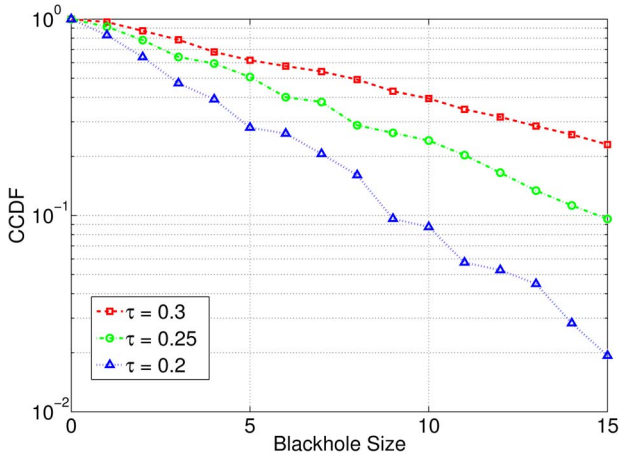

Fig. 12. CCDF of Blackhole size $\mathcal{O}_{v_1}$ under different *failure connection probability* τ (see Section II-B) on a semi-log scale.

value of the Backhole size. We will focus on obtaining more accurate quantitative values via both analysis and simulations in the future work.

VII. Conclusion

In this paper we have studied the topology and resilience of large CRNs in the presence of node failures. When there exist causal relations, a single failure may initiate a component of related failures, and thus random failures may trigger a sequence of Blackholes in the network. In order to understand network topology in the face of Blackholes, two metrics, *failure occurrence probability* p and *failure connection function* $g(\cdot)$ are defined to characterize the occurrence of random failures and their spreading to neighbors, based on which we prove that when a Blackhole cannot spread to the entire network, it is exponentially bounded. By mapping failure spreading to a branching process, we derive an upper bound on the expected size of Blackholes. After studying Blackhole size, we then investigate network resilience. A network is said to be resilient to Blackholes if there exists a giant component of surviving nodes spanning through the entire network. By coupling with a continuum percolation process on the random geometric graph, we further obtain a sufficient condition for a resilient CRN to a sequence of Blackholes. We finally confirm correctness of our theoretical results by simulations. It is worthy of pointing out that although our results concerning Blackhole size and resilience are derived for CRNs, nevertheless, by setting spatial density of primary users $\lambda_p = 0$, these results can also be applied practically in general wireless networks. For instance, Fang *et al.* [18] described a distributed algorithm to build routes around Blackholes in wireless sensor networks, and our results can be used to determine the feasibility of such routes, and thus validate this algorithm.

Appendix

A. Calculation of Critical Probability $p_c^{\square}$

Let $p_c^{\square}$ be the bond percolation probability of the square lattice mapped from CRN (see Fig. 6(b)). It was proved in [31] that

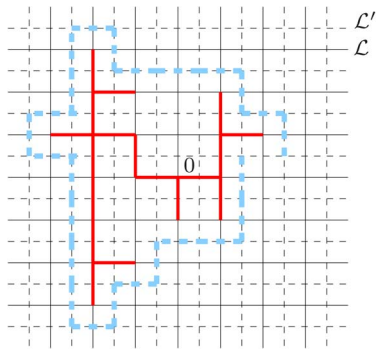

Fig. 13. A finite open cluster at the origin, surrounded by a closed circuit in the dual lattice.

bond percolation probability in square lattice is $\frac{1}{2}$. In discrete percolation theory, the open or closed state of every edge (or vertex) is independent from others. In our discrete lattice mapping, the state of an edge depends on, however, how primary and secondary nodes are distributed around this edge, which implies that adjacent edges are not independent. Therefore, we cannot directly use the result in discrete percolation theory and we need to find out alternative percolation conditions for our mapping. Our method is based on the following observation.

Consider square lattice and its dual $\mathcal{L}$ and $\mathcal{L}'$ (see Fig. 13). The construction of $\mathcal{L}'$ is as follows: let each vertex of $\mathcal{L}'$ be located at the center of a square of $\mathcal{L}$. Let each edge of $\mathcal{L}'$ be open if and only if it crosses an open edge of $\mathcal{L}$, and closed otherwise. Now a key observation is that if the origin belongs to an infinite open edge cluster in $\mathcal{L}$, for which the event is denoted by $E_{\mathcal{L}}$, then there cannot exist a closed circuit (a circuit consisting of closed edges) surrounding the origin in $\mathcal{L}'$, for which the event is denoted by $E_{\mathcal{L}'}$, and vice versa (see page 17 in [31]). This is illustrated in Fig. 13. To proceed, we further need the following lemma.

Lemma 7: Given a lattice $\mathcal{L}$ containing the origin 0 and its dual $\mathcal{L}'$, let $\sigma(z)$ be the number of paths with length z in $\mathcal{L}$ (i.e., comprising z edges) that start at 0, and $\rho(z)$ be the number of circuits in $\mathcal{L}'$ with length z and containing 0 in their interiors, then $\sigma(z) \leq 4 \cdot 3^{z-1}$ and $\rho(z) \leq 2 \cdot (z-2) \cdot 3^{z-2}$.

Proof: See Lemma 3 in [23]. ■

Let $\mathcal{C}_z$ be a circuit of the lattice $\mathcal{L}'$ with length z containing the origin in its interior, then $\mathbb{P}(\mathcal{C}_z \text{ is closed}) = \mathbb{P}(\text{all } z \text{ edges are closed})$. Based on the open edge definition described in Section V-B, edges a and b are independent if their distance is larger than $\max\{R_I, d_l\}$ (the distance between two edges is defined as the minimum distance between any two points on edges a and b). This implies that an independent subset of edges among z edges of $\mathcal{C}_z$ can be obtained by selecting an edge in every $\lceil \frac{2R_I}{d_l} + 1 \rceil$ edges. Thus at least $\kappa = \lfloor \frac{z}{\lceil 2R_I/d_l + 1 \rceil} \rfloor$ have independent states among z edges of $\mathcal{C}_z$. Let q be the probability of any edge being closed, i.e., $q = 1 - p_c^{\square}$, then for any $\mathcal{C}_z$, $\mathbb{P}(\mathcal{C}_z \text{ is closed})$ is upper bounded by q^{κ}. Thus the probability that there exists a closed circuit surrounding the origin in $\mathcal{L}'$ is,

$$\sum_{\mathcal{C}_z, \forall z} \mathbb{P}(\mathcal{C}_z \text{ is closed}) \leq \sum_{z=4}^{\infty} q^{\kappa} \rho(z). \tag{19}$$

Therefore, $\sum_{z=4}^{\infty} q^{\kappa}\rho(z) < 1$ indicates that the probability of no closed circuit surrounding the origin in $\mathcal{L}'$ is strictly greater than 0, which provides a lower bound of $p_c^{\square}$. For example, if $R_I < \frac{d_I}{2}$, $\kappa = \lfloor \frac{z}{2} \rfloor$ and thus

$$\sum_{\mathcal{C}_z, \forall z} \mathbb{P}(\mathcal{C}_z \text{ is closed}) \leq \sum_{z=4}^{\infty} q^{\lfloor \frac{z}{2} \rfloor} \rho(z) = \frac{4(9q)^2}{9(1-9q)^2}.$$

When $q < \frac{1}{15}$, $\frac{4(9q)^2}{9(1-9q)^2} < 1$ and thus the lattice is percolated, which implies $p_c^{\square} > \frac{14}{15}$.

REFERENCES

[1] L. Sun and W. Wang, "Understanding blackholes in large-scale cognitive radio networks under generic failures," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 728–736.

[2] "Spectrum policy task force report," Washington, DC, USA, FCC 02-155, Nov. 2002.

[3] L. Ding *et al.*, "All-spectrum cognitive networking through joint distributed channelization and routing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 11, pp. 5394–5405, Nov. 2013.

[4] N. Tadayon and S. Aissa, "Modeling and analysis of cognitive radio based IEEE 802.22 wireless regional area networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 9, pp. 4363–4375, Sep. 2013.

[5] N. Mahmood, F. Yilmaz, G. Oien, and M.-S. Alouini, "On hybrid cooperation in underlay cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 9, pp. 4422–4433, Sep. 2013.

[6] A. Arafa, K. Seddik, A. Sultan, T. ElBatt, and A. El-Sherif, "A feedback-soft sensing-based access scheme for cognitive radio networks," *IEEE Trans. Wireless Communications*, vol. 12, no. 7, pp. 3226–3237, Jul. 2013.

[7] Q. Wu, G. Ding, J. Wang, and Y.-D. Yao, "Spatial-temporal opportunity detection for spectrum-heterogeneous cognitive radio networks: Two-dimensional sensing," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 516–526, Feb. 2013.

[8] S. Gong, P. Wang, and J. Huang, "Robust performance of spectrum sensing in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 2217–2227, May 2013.

[9] S. Kumar, N. Shende, C. R. Murthy, and A. Ayyagari, "Throughput analysis of primary and secondary networks in a shared IEEE 802.11 system," *IEEE Trans. Wireless Commun.*, vol. 12, no. 3, pp. 1006–1017, Mar. 2013.

[10] A. Rao, H. Ma, M.-S. Alouini, and Y. Chen, "Impact of primary user traffic on adaptive transmission for cognitive radio with partial relay selection," *IEEE Trans. Wireless Commun.*, vol. 12, no. 3, pp. 1162–1172, Mar. 2013.

[11] W. Yin, P. Ren, Q. Du, and Y. Wang, "Delay and throughput oriented continuous spectrum sensing schemes in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 6, pp. 2148–2159, Jun. 2012.

[12] H. Zhang, Z. Zhang, and H. Dai, "On the capacity region of cognitive multiple access over white space channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 11, pp. 2517–2527, Sep. 2013.

[13] R. Subramanian, I. Land, and L. K. Rasmussen, "Asymptotic throughput and throughput-delay scaling in wireless networks: The impact of error propagation," *IEEE Trans. Wireless Commun.*, vol. 13, no. 4, pp. 1974–1987, Apr. 2014.

[14] Z. Kong and E. M. Yeh, "A distributed energy management algorithm for large-scale wireless sensor networks," in *Proc. ACM MOBIHOC*, May 2007, pp. 209–218.

[15] B. Karp and H. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in *Proc. ACM MOBICOM*, Aug. 2000, pp. 243–254.

[16] P. Bose, P. Morin, I. Stojmenovin, and J. Urrutia, "Routing with guaranteed delivery in Ad Hoc wireless networks," *Wireless Netw.*, vol. 7, no. 6, pp. 609–616, Nov. 2001.

[17] J. Bruck, J. Gao, and A. Jiang, "Map: Media axis based geometric routing in sensor networks," in *Proc. ACM MOBICOM*, Aug. 2005, pp. 88–102.

[18] Q. Fang, J. Gao, and L. J. Guibas, "Locating and bypassing routing holes in sensor networks," in *Proc. IEEE INFOCOM*, Mar. 2004, pp. 2458–2468.

[19] Y. Wang, J. Gao, and J. S. Mitchell, "Boundary recognition in sensor networks by topological methods," in *Proc. ACM MOBICOM*, Sep. 2006, pp. 122–133.

[20] N. H. Azimi, H. Gupta, X. Hou, and J. Gao, "Data preservation under spatial failures in sensor networks," in *Proc. ACM MOBIHOC*, Sep. 2010, pp. 171–180.

[21] Y. Xu and W. Wang, "Characterizing the spread of correlated failures in large wireless networks," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[22] R. Meester and R. Roy, *Continuum Percolation*. New York, NY, USA: Cambridge Univ. Press, 1996.

[23] F. Xing and W. Wang, "On the critical phase transition time of wireless multi-hop networks with random failures," in *Proc. ACM MOBICOM*, Sep. 2008, pp. 175–186.

[24] W. Ren, Q. Zhao, and A. Swami, "On the connectivity and multihop delay of Ad Hoc cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 805–818, Apr. 2011.

[25] L. Sun and W. Wang, "Understanding the tempo-spatial limits of information dissemination in multi-channel cognitive radio networks," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 1278–1286.

[26] L. Sun and W. Wang, "On latency distribution and scaling: From finite to large cognitive radio networks under general mobility," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 1287–1295.

[27] M. Penrose, *Random Geometric Graphs*. London, U.K.: Oxford Univ. Press, 2003.

[28] P. Gupta and P. R. Kumar, "The capacity of wireless networks," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 388–404, Mar. 2007.

[29] P. Davies, "Thermodynamics of black holes," *Rep. Progr. Phys.*, vol. 41, pp. 1313–1355, Jun. 1978.

[30] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Comput. Netw.*, vol. 38, no. 4, pp. 393–422, Mar. 2002.

[31] G. Grimmett, *Percolation,* 2nd ed. New York, NY, USA: Springer-Verlag, 1999.

[32] S. M. Ross, *Stochastic Processes*. Hoboken, NJ, USA: Wiley, 1983.

Lei Sun received the M.S degree in electrical engineering from Zhejiang University, Hangzhou China in 2005, the M.S. degree in statistics from Stephen F. Austin State University in 2007, and the Ph.D. degree in electrical and computer engineering from North Carolina State University in 2012. His research interests include mobility modeling and management, networking topology and performance analysis, networking resilience and security, vehicular communications as well as cognitive radio networks.

Wenye Wang (SM'08) received the M.S. degree in electrical engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 1991 and the M.S. and Ph.D. degrees in electrical and computer engineering from Georgia Institute of Technology, Atlanta, GA, USA, in 1999 and 2002, respectively. She is currently a Full Professor with the Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC, USA. Her research interests are in the broad areas of wireless communications and networking, including mobility modeling and management, radio resource management, cognitive radio networks and opportunistic wireless communications, vehicular communications, and security and applications of wireless communications in the emerging smart grids. Dr. Wang was elevated to IEEE Senior Member in 2008. She was a recipient of the NSF CAREER Award in 2006.

Zhuo Lu received the B.S and M.S. degrees from Xidian University in 2002 and 2005, respectively, and the Ph.D. degree from North Carolina State University in 2013. He is an Assistant Professor at the Department of Computer Science, University of Memphis. He currently leads the Cyber, Security, and Analytics (CSA) Lab, University of Memphis. He was a Research Scientist at Intelligent Automation Inc., Rockville, MD, USA, from 2013 to 2014. His research interests include cyber security, moving target defense, mobile computing, cyber-physical systems, information forensics and data analytics.