# Reliable Broadcast in Wireless Networks with Probabilistic Failures

*Technical Report (January 2007)*

Vartika Bhandari
Dept. of Computer Science, and
Coordinated Science Laboratory
University of Illinois at Urbana-Champaign
vbhandar@uiuc.edu

Nitin H. Vaidya
Dept. of Electrical and Computer Eng., and
Coordinated Science Laboratory
University of Illinois at Urbana-Champaign
nhv@uiuc.edu

**Abstract**

We consider the problem of reliable broadcast in a wireless network in which nodes are prone to failure. In the failure mode considered in this paper, each node can fail independently with probability $p$. Failures are permanent. The primary focus is on Byzantine failures, but we also handle crash-stop failures. We consider two network models: a regular grid, and a random network. For the grid network model, we establish necessary and sufficient conditions for the degree of each node as a function of the total number of nodes $n$ in the network, and the failure probability $p$, so as to ensure that reliable broadcast succeeds with probability 1, as $n \to \infty$. Our necessary and sufficient conditions for reliable broadcast with Byzantine failures indicate that failure probability should be less than $\frac{1}{2}$, and the *critical* node degree is $\Theta\left(d_{min} + \frac{\ln n}{\ln \frac{1}{2p} + \ln \frac{1}{2(1-p)}}\right)$ (where $d_{min}$ is the minimum node degree associated with a non-empty neighborhood, and is a small constant). For a random network we prove that, for failure probability less than $\frac{1}{2}$, the *critical* average degree for reliable broadcast is $\Theta(\ln n + \frac{\ln n}{\ln \frac{1}{2p} + \ln \frac{1}{2(1-p)}})$. Our necessary and sufficient conditions for crash-stop failures in a grid network yield a critical degree of $\Theta\left(d_{min} + \frac{\ln n}{\ln \frac{1}{p}}\right)$ for $p < 1$, and our results improve upon previously existing results for this model, when $p$ approaches 0. We also identify an interesting similarity in the structure of various known results in the literature pertaining to a set of related problems in the realm of connectivity and reliable broadcast.

## I. Introduction

Reliable broadcast in the presence of Byzantine and crash-stop failures has been extensively studied under different network and failure models. A reliable broadcast mechanism may be of significant utility in large-scale sensor network deployments. While the shared nature of the wireless medium is conducive to the broadcast operation, the unreliability of the wireless channel, and the possibility of collisions can make it a difficult problem to solve. As a first step towards addressing the issue, it is useful to focus on an idealized wireless channel. We consider the problem of reliable broadcast in a such an idealized wireless network. We primarily focus on Byzantine failures, but have also considered the case of crash-stop failures. The failures are permanent and are assumed to occur probabilistically, i.e.,

This report is a revised version of, and supercedes, an earlier report "Reliable Broadcast in a Wireless Grid Network with Probabilistic Failures", dated October 2005, and also includes some new and tighter results. Many of the results in this report will appear in a paper in IEEE INFOCOM 2007.

This research was supported in part by the NSF grant CNS 05-19817, and a Vodafone Graduate Fellowship.

Minor edits on May 5, 2007.

each node can fail independently with a certain probability $p$. However, once failure has happened, the faulty nodes can exhibit worst-case behavior. We present asymptotically tight bounds on the conditions under which reliable broadcast is achievable.

We show that when nodes exhibit Byzantine failures, reliable broadcast in a grid network of $n$ nodes requires that $p$ be less than half, and the *critical* node degree (defined in Section II) is $\Theta\left(d_{min}+\frac{\ln n}{\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)}}\right)$ for asymptotic achievability of reliable broadcast. This may alternatively be stated as $\Theta\left(d_{min}+\frac{\ln n}{D(Q_{\frac{1}{2}}||P)}\right)$ where $Q_{\frac{1}{2}}$ denotes the $Bernoulli(\frac{1}{2})$ distribution, $P$ denotes the $Bernoulli(p)$ distribution, and $D(Q||P)$ denotes the *relative entropy* (or Kullback-Leibler distance) between distributions $Q$ and $P$. We also prove that in a randomly deployed network with Byzantine failures, the critical average node degree for reliable broadcast is $\Theta(\ln n+\frac{\ln n}{\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)}})$(also expressible as $\Theta\left(\frac{\ln n}{\frac{1}{2}-p+\frac{1}{2}\ln\frac{1}{2(1-p)}}\right)$) when $p<\frac{1}{2}$.

We also consider the case of crash-stop failures in a grid network. For crash-stop failures, the problem of reliable broadcast is equivalent to connectivity. For this case, we have results showing that the critical node degree is $\Theta\left(d_{min}+\frac{\ln n}{\ln\frac{1}{p}}\right)$ with $p<1$, or alternatively stated, $\Theta\left(d_{min}+\frac{\ln n}{D(Q_1||P)}\right)$, where $Q_1$ is the $Bernoulli(1)$ distribution. Our results improve upon previous results proved in [1] when the failure probability $p$ approaches 0.

We also identify an interesting but intuitive similarity in the structure of results (previously known results, as well as the results derived in this paper) for a set of related problems pertaining to connectivity and reliable broadcast. This is discussed in Section XX.

## II. Notation and Terminology

We use the following asymptotic notation:

- $O(g(n))=\{f(n)|\exists c,N_o,\text{ such that } f(n)\leq cg(n) \text{ for } n>N_o\}$
- $o(g(n))=\{f(n)|\lim_{n\to\infty}\frac{f(n)}{g(n)}=0\}$
- $\omega(g(n))=\{f(n)|g(n)=o(f(n))\}$
- $\Omega(g(n))=\{f(n)|g(n)=O(f(n))\}$
- $\Theta(g(n))=\{f(n)|\exists c_1,c_2,N_o,\text{ such that } c_1g(n)\leq f(n)\leq c_2g(n) \text{ for } n>N_o\}$

We use $d$ to denote node degree, $r$ to denote transmission range, and $D$ to denote network diameter. The neighbor-set of a node $u$, including itself, is denoted by $nbd(u)$. The set of neighbors minus itself is termed as $nbd'(u)=nbd(u)-\{u\}$.

By *critical* transmission range for reliable broadcast, we imply a $r_{critical}$, such that

- For some constant $c_1>0$, reliable broadcast fails with some positive probability if $r<r_{critical}$
- For some constant $c_2>0$, reliable broadcast is achieved with probability 1 if $r\geq r_{critical}$

Thus:

- $r_{critical}$ is $\Omega(f(n,p)) \implies \exists c_1>0,$ such that $r\leq c_1f(n,p) \implies \lim_{n\to\infty}Pr[\text{reliable broadcast achievable}]<1$
- $r_{critical}$ is $O(f(n,p)) \implies \exists c_2>0,$ such that $r\geq c_2f(n,p) \implies \lim_{n\to\infty}Pr[\text{reliable broadcast achievable}]=1$
- $r_{critical}=\Theta(f(n,p))$ implies that $r_{critical}$ is $\Omega(f(n,p))$ and $O(f(n,p))$.

In a grid network, and under the considered distance metric (discussed in Section III), the node degree is exactly determined by specifying the transmission range. Hence, we can define the notion of *critical* degree $d_{critical}$ correponding to the transmission range $r_{critical}$. Thus:

- $d_{critical}=\Omega(g(n,p))\exists c_1>0,$ such that: $d\leq c_1g(n,p) \implies \lim_{n\to\infty}Pr[\text{reliable broadcast achievable}]<1$
  This yields a *necessary* condition. If $\lim_{n\to\infty}Pr[\text{reliable broadcast achievable}]=0$, it is a *strong* necessary condition.

- $d_{critical} = O(f(n,p)) \implies \exists c_2 > 0,$ such that: $d \geq c_2 f(n,p) \implies \lim_{n\to\infty} Pr[\text{reliable broadcast achievable}] = 1$ This yields a *sufficient* condition.
- $d_{critical}$ is $\Theta(f(n,p))$ implies that $d_{critical}$ is $\Omega(f(n,p))$ and $O(f(n,p))$

In a random network, the degrees of individual nodes can vary; however, it is possible to define a notion of *critical* average degree $d^{avg}_{critical}$, which is the average degree corresponding to the range $r_{critical}$. Then $d^{avg}_{critical}$ can be expressed in asymptotic notation, similar to $d_{critical}$ for a grid network.

## III. Problem Model

We consider a two network models, viz. a regular grid, where nodes are located on a two-dimensional square grid (each grid unit is a $1 \times 1$ square), and a random network, where node locations are i.i.d. over the deployment region. In both models, the network is assumed to be deployed over a $\sqrt{n}$ x $\sqrt{n}$ square region. The pre-failure topology (i.e., node locations) of the deployed network is assumed to be known by all nodes.

*Formal Definition of Reliable Broadcast:* Any node in the entire network can originate a broadcast message. In the Byzantine failure model, this source node may be faulty. Thus goal is to ensure that if the source is non-faulty, every non-faulty node in the network should correctly receive and determine the broadcast value; if the source is faulty, all non-faulty node should agree on some common value. In the crash-stop failure model, a message can only be originated by a non-faulty node (as faulty nodes cease to function), and the goal is to ensure that all non-faulty nodes receive this value.

If even one non-faulty node (in either model) fails to make a valid value determination, the broadcast is deemed to have failed. Reliable broadcast is said to fail in a given fault configuration, if it fails for at least one possible broadcast origin/source.

For a given broadcast instance, once an origin/source is designated, it is identified as $(0,0)$. All nodes can then be uniquely identified by their coordinate location $(x,y)$ w.r.t. this origin. In the grid network model, the node coordinates are always *integers*, while for random networks they are *real* numbers. All nodes have a common transmission radius $r(n,p)$. For grid networks, we assume that $r(n,p)$ is an integer, and for random networks it is allowed to be any real number. A message transmitted by a node $(x,y)$ is heard by all nodes within distance $r(n,p)$ from it (where distance is defined in terms of the particular metric under consideration). The set of these nodes is termed the neighborhood of $(x,y)$.

In this paper, we consider two distance metrics: $L_\infty$ and $L_2$. The $L_\infty$ metric is the metric induced by the $L_\infty$ norm [2], such that the distance between points $(x_1,y_1)$ and $(x_2,y_2)$ is given by $\max\{|x_1-x_2|,|y_1-y_2|\}$ in the this metric. Thus $nbd(a,b)$ comprises a square of side $2r$ with its centroid at $(a,b)$, and the degree of a node is $4r^2+4r$. In this metric, the minimum node degree $d_{min} = 8$ corresponding to $r = 1$. The $L_2$ metric is induced by the $L_2$ norm [2], and is the Euclidean distance metric. The $L_2$ distance between points $(x_1,y_1)$ and $(x_2,y_2)$ is given by $\sqrt{(x_1-x_2)^2+(y_1-y_2)^2}$, and $nbd(a,b)$ comprises nodes within a circle of radius $r$ centered at $(a,b)$. The $L_\infty$ metric enables more tractable analysis, from which necessary and sufficient conditions for the $L_2$ (Euclidean) metric proceed. In Section XI, we further elaborate on this.

A random failure mode is assumed, wherein each node can fail with probability $p$ independently of other nodes. Failures are permanent. We primarily focus on Byzantine failures. In the Byzantine failure mode, a faulty node can behave arbitrarily, in contrast to crash-stop failures, where a faulty node simply stops functioning. However, in our model, the Byzantine nodes cannot spoof addresses or cause collisions, i.e., the MAC layer is assumed fault-free, and the Byzantine faults reside only in higher layers of the protocol stack. [1]. We assume that the channel is perfectly

[1]A methodology to handle a bounded number of collisions and address-spoofing was proposed in [3] for a locally bounded fault model. It might be possible to adapt it to handle the random failure model. This requires further investigation.

reliable, and a local broadcast is correctly received by all neighbors. The same *reliable local broadcast* assumption underlies the results in [4] and [5] for a locally bounded adversarial fault model. Note that while the *occurrence* of the permanent failures is probabilistic, the failed Byzantine nodes can thereafter choose to behave in a worst-case manner (i.e. modulate the messages they send to cause most confusion to non-faulty nodes). The non-faulty nodes do not know which nodes have failed.

## IV. Some Useful Mathematical Results

We state some mathematical results that have been used in our proofs:

*FACT 1:* $\forall x \in [0,1] : \ln \frac{1}{1-x} \geq x$

*FACT 2:* If $|f(n)| \leq n^{\frac{1}{2}-\varepsilon} (0 < \varepsilon < \frac{1}{2})$:

$$\left(1 + \frac{f(n)}{n}\right)^n \leq e^{2f} \text{ for } n \geq 4$$

and

$$\lim_{n\to\infty} \left(1 + \frac{f(n)}{n}\right)^n = e^{(\lim_{n\to\infty} f(n))}$$

*Proof:* Let $f(n)$ be such that $|f(n)| \leq n^{\frac{1}{2}-\varepsilon}$, where $0 < \varepsilon < \frac{1}{2}$. Let $g(n) = (1 + \frac{f(n)}{n})^n$. Then:

$$\begin{aligned}
\ln g = n \ln(1 + \frac{f(n)}{n}) &= n\left(\frac{f(n)}{n} - \frac{1}{2}(\frac{f(n)}{n})^2 + \frac{1}{3}(\frac{f(n)}{n})^3 - ....\right)[6] \\
&= n\sum_{k=1}^{\infty}(-1)^{k-1}\frac{1}{k}(\frac{f(n)}{n})^k = f + \sum_{k=2}^{\infty}(-1)^{k-1}\frac{1}{k}(\frac{f(n)^k}{n^{k-1}}) \\
&\leq f(n) + f(n)\sum_{k=2}^{\infty}\frac{1}{k}(\frac{f(n)}{n})^{k-1} < f(n) + f(n)\sum_{k=2}^{\infty}(\frac{1}{\sqrt{n}})^{k-1} \\
&= f(n)\left(1 + \sum_{k=1}^{\infty}(\frac{1}{\sqrt{n}})^k\right) = f(n)\left(1 + \frac{1}{1-\frac{1}{\sqrt{n}}}\right) \\
&\leq 2f \text{ for } n \geq 4 \\
\therefore \left(1 + \frac{f(n)}{n}\right)^n &\leq e^{2f(n)} \text{ for } n \geq 4
\end{aligned}$$

$$\begin{aligned}
\ln g = n \ln(1 + \frac{f(n)}{n}) = n\left(\frac{f(n)}{n} - \frac{1}{2}(\frac{f(n)}{n})^2 + \frac{1}{3}(\frac{f(n)}{n})^3 - ....\right)[6] &= n\sum_{k=1}^{\infty}(-1)^{k-1}\frac{1}{k}(\frac{f(n)}{n})^k \\
= f(n) + \sum_{k=2}^{\infty}(-1)^{k-1}\frac{1}{k}(\frac{f(n)^k}{n^{k-1}}) \\
\lim_{n\to\infty} \ln g = \lim_{n\to\infty} f(n) + \sum_{k=2}^{\infty}(-1)^{k-1}\frac{1}{k}(\frac{f(n)^k}{n^{k-1}}) &= \lim_{n\to\infty} f(n) \\
\therefore \lim_{n\to\infty} g(n) = e^{(\lim_{n\to\infty} f(n))}
\end{aligned}$$

■

*FACT 3:* If $c > 0$ is a positive constant independent of $n$, and $b \geq 1$ is another positive constant independent of $n$, then $\exists n_o \in \mathcal{N}$ such that:
$1 - \frac{1}{(\ln n)^b} \leq \frac{1}{n^{\frac{c}{n}}}$ for $n > n_o$

*Proof:*

$$\because \frac{1}{1-\frac{1}{(\ln n)^b}} \geq e^{\frac{1}{(\ln n)^b}} \text{ (from Fact 1 )}$$

$$\therefore 1-\frac{1}{(\ln n)^b} \leq e^{-\frac{1}{(\ln n)^b}} = \frac{1}{e^{\frac{1}{(\ln n)^b}}} = \frac{1}{e^{\frac{\ln n}{(\ln n)^{(b+1)}}}}$$

$$= \frac{1}{n^{\frac{1}{(\ln n)^{(b+1)}}}} \leq \frac{1}{n^{\frac{c}{n}}} \text{ for large } n$$

$$\because \exists n_o \in \mathcal{N} \text{ s.t. } \frac{1}{(\ln n)^{(b+1)}} \geq \frac{c}{n}, \forall n > n_o$$

■

*LEMMA 1:* (Jogdeo & Samuels [7]) Given $X = Y_1 + Y_2 + ..., +Y_n$ where $\forall i, Y_i = Bernoulli(p_i)$, and $\sum p_i = np$, the median $m$ of the distribution is either $\lfloor np \rfloor or \lceil np \rceil$, i.e., $Pr[X \leq m] \geq \frac{1}{2}$ and $Pr[X \geq m] \geq \frac{1}{2}$.

*Corollary 1:* Given $X = Y_1 + Y_2 + ..., +Y_n$ where $\forall i, Y_i = Bernoulli(p)$, the median $m$ of the distribution is either $\lfloor np \rfloor or \lceil np \rceil$, i.e., $Pr[X \leq m] \geq \frac{1}{2}$ and $Pr[X \geq m] \geq \frac{1}{2}$.

*Proof:* The proof proceeds by setting $p_1 = p_2 = ... = p_n = p$ and applying Lemma 1. ■

*Corollary 2:* Given $X = Y_1 + Y_2 + ..., +Y_n$ where $n$ is even, and $\forall i, Y_i = Bernoulli(p)$ where $p \geq \frac{1}{2}$, the median $m$ of the distribution satisfies $m \geq \frac{n}{2}$.

*Proof:* We know that $m$ is either $\lfloor np \rfloor or \lceil np \rceil$. When $p = \frac{1}{2}$, $m = \frac{n}{2}$ (as $n$ is even). For $p > \frac{1}{2}$, $m \geq \lfloor np \rfloor \geq \lfloor \frac{n}{2} \rfloor = \frac{n}{2}$. ■

*LEMMA 2:* (Chernoff Bound) If $X = \sum_{i=1}^{n} X_i$, where each $X_i$ is independent and $Bernoulli(p_i)$, then for $0 < \beta < 1$:

$$Pr[X \leq (1-\beta)E[X]] \leq \exp(-\frac{\beta^2}{2}E[X]) \tag{1}$$

*LEMMA 3:* (Relative Entropy Form of Chernoff-Hoeffding Bound[8]) If $X = \sum_{i=1}^{n} X_i$, where each $X_i$ is $Bernoulli(p)$, then for $p \leq \beta \leq 1$:

$$Pr[X \geq \beta n] \leq e^{-n(\beta \ln \frac{\beta}{p} + (1-\beta) \ln \frac{1-\beta}{1-p})} \tag{2}$$

*LEMMA 4:* (Chernoff Bound [9]) Let $X_1, ..., X_n$ be independent Poisson trials, where $Pr[X_i = 1] = p_i$. Let $X = \sum_{i=1}^{n} X_i$. Then, for any $\beta > 0$:

$$Pr[X \geq (1+\beta)E[X]] < \left( \frac{e^{\beta}}{(1+\beta)^{(1+\beta)}} \right)^{E[X]} \tag{3}$$

*LEMMA 5:* (Chernoff Upper Tail Bound [9]) Let $X_1, ..., X_n$ be independent Poisson trials, where $Pr[X_i = 1] = p_i$. Let $X = \sum_{i=1}^{n} X_i$. Then, for $0 < \beta \leq 1$:

$$Pr[X \geq (1+\beta)E[X]] \leq \exp(-\frac{\beta^2}{3}E[X]) \tag{4}$$

*LEMMA 6:* [10] If $X_1$, $X_2$,..., $X_n$ are drawn i.i.d. from alphabet $\chi$ according to $Q(x)$, then probability of sequence $\mathbf{x}$ is given by:

$$Q^{(n)}(\mathbf{x}) = e^{-n(H(P_x) + D(P_{\mathbf{x}} || Q))} \tag{5}$$

where $H$ and $P$ denote the entropy and relative entropy functions (here considered w.r.t base $e$).

Also, for any distributions $P$ and $Q$, the size of type class $T(P)$ satisfies:

$$\frac{1}{(n+1)^{|\chi|}}e^{nH(P)} \leq |T(p)| \leq e^{nH(P)} \tag{6}$$

and, the probability of the type class $T(P)$ under $Q$ is governed by:

$$\frac{1}{(n+1)^{|\chi|}}e^{-n(D(P||Q))} \leq Q^{(n)}(T(p)) \leq e^{-n(D(P||Q))} \tag{7}$$

*LEMMA 7:* Suppose $S_1$ and $S_2$ are sets of Bernoulli random variables, such that $S_1 = \{I_1, I_1, ..., I_m\}$ and $S_2 = \{I_{k+1}, ..., I_{k+m}\}$, where $\forall i, I_i = Bernoulli(p)$. If $N_1 = \sum_{I_j \in S_1} I_j$ and $N_2 = \sum_{I_j \in S_2} I_j$ then:

$$Pr[N_2 < a | N_1 < a] \geq Pr[N_2 < a] \tag{8}$$

*Proof:* We know that $S_1 \cap S_2 = \{I_{k+1}, ..., I_m\}$. Let $M_1 = \sum_{I_j \in S_1 \cap S_2} I_j$, and let $T = \sum_{I_j \in (S_2 - S_1)} I_j$. Then $M_1 = N_1 - b$ where $b = \sum_{I_j \in (S_1 - S_2)} I_j \geq 0$. Thus $N_1 < a \Rightarrow M_1 < a - b < a$. Note that $Pr[M_1 < k | M_1 < a] = \frac{Pr[M_1 < k and M_1 < a]}{Pr[M_1 < a]} \geq Pr[M_1 < k]$.

$$Pr[N_2 < a | N_1 < a] \geq P[N_2 < a | M_1 < a] = \sum_{k=0}^{a-1} Pr[M_1 < k | M_1 < a] \cdot Pr[T = a - 1 - k] \tag{9}$$

$$\geq \sum_{k=0}^{a-1} Pr[M_1 < k] \cdot Pr[T = a - 1 - k] = Pr[N_2 < a] \tag{10}$$

■

*LEMMA 8:* For all $0 < x \leq \frac{1}{2}$:

$$\ln \frac{1}{1-x} + \ln \frac{1}{1+x} \geq x^2$$

*Proof:*

$$\ln \frac{1}{1-x} + \ln \frac{1}{1+x} = -(\ln(1-x) + \ln(1+x)) = -\left(\left(x - \frac{x^2}{2} + \frac{x^3}{3} - ....\right) + \left((-x) - \frac{(-x)^2}{2} + \frac{(-x)^3}{3} - ....\right)\right)$$
$$= 2\left(\frac{x^2}{2} + \frac{x^4}{4} + \frac{x^6}{6} + ...\right) \geq x^2 \tag{11}$$

■

*LEMMA 9:* (Vapnik-Chervonenkis Theorem) Let S be a set with finite VC dimension $VCdim(\mathcal{S})$. Let $\{X_i\}$ be i.i.d. random variables with distribution $P$. Then for $\varepsilon, \delta > 0$:

$$Pr\left(\sup_{D \in \mathcal{S}} \left|\frac{1}{N}\sum_{i=1}^{N} I_{X_i \in D} - P(D)\right| \leq \varepsilon\right) > 1 - \delta$$
$$\text{whenever } N > \max\left(\frac{8VCdim(\mathcal{S})}{\varepsilon}\log_2\frac{16e}{\varepsilon}, \frac{4}{\varepsilon}\log_2\frac{2}{\delta}\right)$$

*LEMMA 10:* Suppose we are given a region of area $n$, with $n$ nodes located uniformly at random. Consider all axis-parallel rectangles of area $a(n)$. If $a(n) \geq 100\alpha \log n, 1 \leq \alpha \leq \frac{n}{100 \log n}$, then each such rectangle has at least $100\alpha \ln n - 50 \log n$ nodes, with high probability.

*Proof:* We know that the set of axis-parallel rectangles has VC-dimension 4. In our construction, we have the set of all axis-parallel rectangles $\mathcal{S}$ of area $100\alpha \ln n$. Then considering the $n$ random variables $X_i$ denoting node positions, $Pr[X_i \in D(D \in \mathcal{S}] = \frac{100\alpha \ln n}{n}$. Then, from the VC-theorem (Lemma 9):

$$Pr\left(\sup_{D\in\mathcal{S}} \left|\frac{\text{No. of nodes in} D}{n} - \frac{100\alpha \ln n}{n}\right| \leq \varepsilon(n)\right) > 1-\delta(n)$$

$$\text{whenever } n > \max\left(\frac{32}{\varepsilon}\log_2\frac{16e}{\varepsilon}, \frac{4}{\varepsilon}\log_2\frac{2}{\delta}\right)$$

This is satisfied when $\varepsilon(n) = \delta(n) = \frac{50\ln n}{n}$. Thus, with probability at least $1 - \frac{50\ln n}{n}$, the population $Pop(D)$ of cell $D$ satisfies:

$$100\alpha \ln n - 50\ln n \leq Pop(D) \leq 100\alpha \ln n + 50\ln n \tag{12}$$

This completes the proof. ■

*FACT 4:* If we attempt to divide the $\sqrt{n}x\sqrt{n}$ grid into disjoint neighborhoods (as in Fig. 1), then the number of such disjoint neighborhoods that can be obtained is at least $\frac{\lfloor\sqrt{n}\rfloor}{(2r+1)^2} \geq \frac{(\sqrt{n}-1)^2}{4r^2+4r+1} \geq \frac{n}{8r^2}$ for large $n$. Observing that $d = 4r^2+4r$, the number of such disjoint neighborhoods obtainable is at least $\frac{\lfloor\sqrt{n}\rfloor}{(2r+1)^2} \geq \frac{(\sqrt{n}-1)^2}{4r^2+4r+1} \geq \frac{n}{2d}$ for large $n$

# Byzantine Failures

## V. Related Work

Reliable broadcast in radio networks has been studied in [11], [4], [5] and [12]. Crash-stop failures are considered in [11] for finite networks comprising nodes located in a regular grid pattern and algorithms are described for efficient broadcast to the part of the network that is reachable from the source. However this work does not attempt to quantify the number of faults that render some nodes unreachable. In [4], a locally bounded model is considered, where an adversary is free to place faults, as long as no neighborhood has more thasn $t$ faults. It was shown that for a network of nodes located on an infinite grid of unit squares and having transmission radius $r$, reliable broadcast is not achievable for $t \geq \lceil \frac{1}{2}r(2r+1)\rceil$ (in both $L_\infty$ and $L_2$ metrics). This was established as an *exact threshold* in $L_\infty$ by [5], and a protocol was described that achieved the threshold. An approximate threshold was also established for the $L_2$ metric (that is tight asymptotically, and corresponds to the same fraction of a neighborhood as in $L_\infty$). A sufficient condition for reliable broadcast in general graphs with a locally bounded adversarial model was described in [13], and a simpler protocol for the grid network case was also presented. In [14], further study of the locally bounded fault model has been undertaken on arbitrary graphs. Upper and lower bounds for achievability of reliable broadcast are presented based on graph-theoretic parameters, for arbitrary graphs. However, no exact thresholds are established. It is also shown that there exist certain graphs in which algorithms that work with knowledge of topology succeed in achieving reliable broadcast, while those that lack this knowledge fail to do so.

In closely related work, [12] considers the case of message-passing and radio networks with random transient failures. In our knowledge, the results in this paper are the first for radio networks exhibiting random but permanent Byzantine failures.

## VI. Notation and Terminology

We briefly describe here notation and terminology that shall be used in this paper. Nodes can be identified by their grid location i.e. $(x,y)$ denotes the node at $(x,y)$. The neighborhood of $(x,y)$ comprises all nodes within distance $r$

of $(x,y)$ and is denoted as $nbd(x,y)$. The degree of each node is referred to as $d$. In $L_\infty$ metric, $d = 4r^2 + 4r$, while the size of a neighborhood (including the neighborhood center) is $d+1 = 4r^2+4r+1$. Thus, the minimum degree is $d_{min} = 8$, corresponding to $r = 1$. The diameter of the network (in terms of distance, and not number of hops) is referred to as $D$. If $n$ is a perfect square, $D = \sqrt{n}$. The source of the broadcast may be deemed to be situated at $(0,0)$, without affecting generality of the results. In general, we allow any node of the network to be the source (with a corresponding shift of reference coordinates). For succint description, we define a term $pnbd(x,y)$ where $pnbd(x,y) = nbd(x-1,y) \cup nbd(x+1,y) \cup nbd(x,y-1) \cup nbd(x,y+1)$. Intuitively $pnbd(x,y)$ denotes the *perturbed neighborhood* of $(x,y)$, obtained by perturbing the center of the neighborhood to one of the nodes immediately adjacent to $(x,y)$ on the grid. Besides, we use $Bernoulli(p)$ to denote a Bernoulli random variable with parameter $p$.

## VII. Necessary Conditions for Reliable Broadcast

*THEOREM 1:* If a node $u \notin nbd(s)$ has at least half faulty neighbors, it can be made to commit to an erroneous value with probability at least $\frac{1}{2}$.

*Proof:* Assume that the message is drawn from $\{0,1\}$. A node $u$ which is not an immediate neighbor of the source must rely on messages received from its neighbors.

First, consider any function that takes as argument messages received from all neighbors and outputs one of 0 or 1. Then corresponding to each fault configuration $C_1$ with $t \geq \frac{d}{2}$ or more faults in $nbd'(u)$, there is another configuration $C_2$ with $t$ faults in $nbd'(u)$, such that all non-faulty nodes in $C_1$ are faulty in $C_2$, while the non-faulty nodes in $C_2$ were all faulty in $C_1$. Then, the faulty nodes can modulate their message-sending behavior so that $u$ is unable to distinguish between the case where the correct broadcast value was 0 and configuration was $C_1$ and the case when the correct value was 1 and the configuration was $C_2$ (recall that once failure has happened, the faulty nodes can exhibit worst-case behavior). Thus, there are two equally likely possibilities for a given set of received messages, and $u$ cannot expect to choose the correct one with a probability greater than half. If the message can have more than two possible vaues, it cannot increase the probability of correct choice.

Stated formally: suppose $\mathcal{S}_1 \subseteq nbd(u)$ is the set of faulty neighbors in $C_1$, and $\mathcal{S}_1^c = nbd'(u) - \mathcal{S}_1$ is its complement, i.e., the set of non-faulty neighbors. Then we know that $|\mathcal{S}_1| \geq \frac{|nbd'(u)|}{2} \geq \mathcal{S}_1^c|$. Consider a fault configuration $C_2$ in which the set of faulty neighbors is $\mathcal{S}_2 = \mathcal{S}_1^c \cup \mathcal{V}$ where $\mathcal{V} \subseteq \mathcal{S}_1$ is some subset of $\mathcal{S}_1$ that satisfies $|\mathcal{V}| = |\mathcal{S}_1| - |\mathcal{S}_1^c|$. It is easy to see that $|\mathcal{S}_1| = |\mathcal{S}_2|$. Consider the case where the correct value is 0, and configuration is $C_1$. Then all nodes in $\mathcal{S}_1$ can behave as though the value were 1, while the nodes in $\mathcal{S}_1^c$ will always act according to value 0. Now suppose the correct value is 1, and configuration is $\mathcal{C}_2$. Then the faulty nodes in $\mathcal{S}_1^c \subseteq \mathcal{S}_2$ behave as though the value were 0, while nodes in $\mathcal{V} = \mathcal{S}_2 - \mathcal{S}_1^c$ act as per the correct value 1. The non-faulty nodes in $\mathcal{S}_2^c$ always act as per value 1. From the viewpoint of node u, the two situations are indistinguishable.

Let us also consider the use of any function that takes as argument message values from a random subset of neighbors, and outputs one of 0 or 1 (since the faulty nodes are not known to the non-faulty node, this is the best it can do). We show that the output will be wrong with probability at least half. Consider a node $u$. Denote by $\mathcal{P}(nbd(u))$ the power set of $nbd(u)$, i.e., the set of all possible subsets of neighbors. Suppose, it is known to $u$ that half or more of its neighbors are faulty. Since failures are i.i.d., we obtain that:

$$Pr[v \in nbd(u) \text{ is faulty} | nbd(u) \text{ has half+ faults}] > \frac{1}{2} \tag{13}$$

Consider any set $S \in \mathcal{P}(nbd(u))$. Then $Pr[$ at least half nodes in S faulty$] \geq \frac{1}{2}$ (from Lemma 1). If this is so, then by the same argument as above, there are two configurations that are indistinguishable. Hence for any subset $S$, the probability of obtaining an erroneous value from $S$ is at least $\frac{1}{2}$. Applying a function iteratively to a sequence of

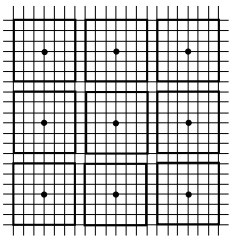

Fig. 1. Division of network into disjoint neighborhoods

different subsets would also not help, since half or more of the outcomes obtained will be incorrect, with probability at least half. ■

*THEOREM 2:* When failure probability $p$ satisfies $\frac{1}{2} \leq 1 - \frac{96}{n}$, and $\frac{n}{d} \to \infty$ (i.e., $d = o(n)$):

$$\lim_{n\to\infty} Pr[\text{ reliable broadcast fails}] > \eta > 0(\text{ for some positive constant } \eta \leq 1\ )$$

In particular, if $\frac{n(1-p)}{d} \to \infty$, then:

$$\lim_{n\to\infty} Pr[\text{ reliable broadcast fails}] = 1$$

When $1 - p = o(\frac{1}{n})$, all nodes are faulty w.h.p., and the broadcast issue is irrelevant.

*Proof:* Suppose we consider a particular node $j$ in the network. Then, if $j$ is non-faulty, but more than half of its neighbors are faulty, reliable broadcast fails with probability at least half. Given that there are $d$ neighbors, and each may fail independently with probability $p$, let $Y_j$ denote the number of failed neighbors of $j$. Then, $Y_j$ takes values from $0, 1, ..., d$, and $E[Y_j] \geq \frac{d}{2}$. Thus $\lfloor E[Y] \rfloor \geq \lfloor \frac{d}{2} \rfloor = \frac{d}{2}$ (since $d = 4r^2 + 4r$ is always even). Thus, $Pr[Y \geq \frac{d}{2}] \geq Pr[Y \geq \lfloor E[Y] \rfloor] \geq \frac{1}{2}$ (from Lemma 1). Let us call this probability $q$. When $p \leq 1 - \varepsilon$, we have $1 - p \geq \varepsilon > 0$. Thus:

$$Pr[\ j \text{ alive; at least half } nbd(j) \text{ faulty }] \geq (1-p)q \geq \frac{1-p}{2}$$

$\lim \frac{n(1-p)}{d} \geq 4$*:* Let us mark out a subset of nodes $j$ such that the neighborhoods of these nodes are all disjoint, as in Fig. 1. Then from Fact 4, the number of such nodes that we may obtain is at least $\frac{n}{2d}$ for large $n$.

Let $I_j$ be an indicator variable that takes value 1 if $j$ is non-faulty but has at least half faulty neighbors, and commits to the wrong value. Then $Pr[I_j = 1] \geq \frac{1-p}{2}$, and all $I_j$'s are independent.

Let $X$ be a random variable indicating the number of non-faulty nodes with at least half faulty neighbors that resultantly commit to the wrong value. Then $E[X] = \sum_j Pr[I_j = 1] \geq \frac{1-p}{2}(\frac{n}{2d}) = \frac{n(1-p)}{4d}$.

Thus setting $\beta = \frac{1}{2}$ in the Chernoff Bound in Lemma 2, when $E\frac{n(1-p)}{d} \to \infty, E[X] = \frac{n(1-p)}{4d} \to \infty$:

$$\lim_{n\to\infty} Pr[X > \frac{E[X]}{2}] > \lim_{n\to\infty} (1 - e^{-\frac{E[X]}{8}}) = 1$$

Thus, as $n \to \infty$, the number of non-faulty nodes isolated by half or more faulty neighbors, and which commit to the wrong value, will also tend to infinity with probability 1. When $\frac{n(1-p)}{d} \to \gamma \geq 4$:

$$\lim_{n\to\infty} Pr[X \geq 2] \geq Pr[X \geq \frac{E[X]}{2}] > \lim_{n\to\infty} (1 - e^{-\frac{E[X]}{8}}) = 1 - e^{-\frac{1}{4}} > 0$$

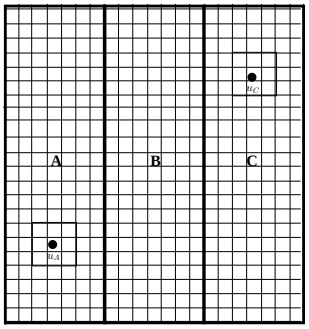


Fig. 2. Division of network area into three segments

$\lim \frac{n(1-p)}{d} < 4$, *but* $1-p \geq \frac{96}{n}$*:* This implies that $1-p < \frac{4d}{n} \implies p \geq \frac{3}{4} > \frac{1}{2}$ for large $n$ (since $\frac{n}{d} \to \infty$). Then the probability $q$ of having half or more faulty neighbors is at least half (from Lemma 1). Consider a partition of the network region into 3 segments A, B, and B, and C as in Fig. 2. Each segment has at least $\lfloor \sqrt{n} \rfloor \frac{\lfloor \sqrt{n} \rfloor}{3} \geq \frac{n}{6}$ nodes for large $n$. Let $p_A$ be the probability that segment A has at least one node $u_A$ that is non-faulty. Let $p_C$ and $u_C$ be the corresponding probability and node for segment C. If such $u_A$ and $u_C$ exist, and one of them (say $u_C$) has half or more faulty neighbors, then a broadcast from $u_A$ cannot be received by $u_C$, with any probability better than half (from Theorem 1).

Let $X_A$ be the total number of nodes in segment A that satisfy the desired property. Then $X_A = \sum_{j \in A} I'_j$, where $I'_j$ are i.i.d. Bernoulli(p) random variables denoting whether $j$ is faulty. Likewise, let $X_C$ be the corresponding random variable for segment C. Then, it can be easily verified that $E[X_A] \geq \frac{n(1-p)}{6}$. Similarly $E[X_C] \geq \frac{n(1-p)}{6}$. Then by setting $\beta = \frac{1}{2}$ in Lemma 2, it can be seen that:

$$Pr[X_A < 1] \leq Pr[X_A \leq \frac{n(1-p)}{12}] \leq Pr[X_A \leq \frac{E[X_A]}{2}] \leq e^{-\frac{E[X_A]}{8}} \leq e^{-\frac{n(1-p)}{48}} \tag{14}$$

If there exist such nodes, let us select from them an $u_A$.

$$Pr[X_C < 1] \leq Pr[X_C < \frac{n(1-p)}{24}] \leq Pr[X_C \leq \frac{E[X_C]}{2}] \leq e^{-\frac{E[X_C]}{8}} \leq e^{-\frac{n(1-p)}{48}} \tag{15}$$

If there exist such nodes, let us select from them an $u_C$.

Then by applying a union bound over the events that either one of $u_A, u_C$ does not exist, or $u_C$ does not have half or more faulty neighbors, it proceeds that:

$$Pr[\exists u_A, \exists u_C \text{ and } u_C \text{ has half or more faulty neighbors}] = p_b \geq 1 - e^{-\frac{n(1-p)}{48}} - e^{-\frac{n(1-p)}{48}} - q \tag{16}$$

$$\lim_{n \to \infty} p_b \geq 1 - \frac{1}{e^2} - \frac{1}{e^2} - \frac{1}{2} > 0 \tag{17}$$

Thus $u_C$ will make an erroneous decision about any messages broadcast by $u_A$ with probability at least half, and reliable broadcast will fail with a positive probability at least $\frac{p_b}{2} > 0$.

*a)* $1-p = o(\frac{1}{n})$ *:*

$$Pr[\text{All nodes faulty;broadcast issue moot}] = p^n \tag{18}$$

$$\geq (1-(1-p)))^n = (1-g(n))^n \text{ where } \frac{g(n)}{1/n} = ng(n) \to 0 \tag{19}$$

$$\lim_{n\to\infty} Pr[\text{All nodes faulty; broadcast issue moot}] \tag{20}$$

$$\geq \lim_{n\to\infty}(1-g(n)))^n = \lim_{n\to\infty}\left(1-\frac{ng(n)}{n})\right)^n \tag{21}$$

$$= e^{-\lim(ng(n))} = 1 \text{ from Fact 2} \tag{22}$$

■

*THEOREM 3:* When $p \leq \frac{1}{2} - \frac{1}{\ln n}$, and node degree $d \leq \frac{\ln n}{\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)}}$, reliable broadcast asymptotically fails with probability 1.

*Proof:* Any failure probability $p \leq \frac{1}{2} - \frac{1}{\ln n}$ can be expressed as $p = \frac{1}{2} - y$ for suitable $\frac{1}{\ln n} \leq y \leq \frac{1}{2}$. Thus:

$$\begin{aligned}\ln\frac{1}{2p} + \ln\frac{1}{2(1-p)} &= \ln\frac{1}{2(\frac{1}{2}-y)} + \ln\frac{1}{2(\frac{1}{2}+y)} = \ln\frac{1}{1-2y} + \ln\frac{1}{1+2y} \\ &\geq (2y)^2 = 4y^2 \geq \frac{4}{(\ln n)^2}(\text{ setting } x = 2y \text{ in Lemma 8 })\end{aligned} \tag{23}$$

Resultantly:

$$d \leq \frac{\ln n}{\frac{4}{(\ln n)^2}} = \frac{(\ln n)^3}{4} < (\ln n)^3 \tag{24}$$

$$\frac{\ln n}{2} + 6\ln\ln n \leq \ln n - 4\ln\ln n \text{ for large enough } n \tag{25}$$

Consider a particular node $j$ in the network. Then, if $j$ is non-faulty, but more than half of its neighbors are faulty, reliable broadcast fails with probability at least half (from Theorem 1). Given that there are $d$ neighbors, and each may fail independently with probability $p$, let $I_{jk}(1 \leq k \leq d)$ denote the indicator variable corresponding to neighbor $k$ of $j$ (enumerated in some order), such that $I_{jk} = 1$ if $k$ is faulty, and 0 otherwise. Then $Y_j = \sum I_{jk}$ denotes the number of failed neighbors of $j$. $Y$ takes values from $0, 1, ..., d$, and $E[Y] = pd$. $Pr[Y_j \geq \frac{d}{2}] = \sum_{i=\frac{d}{2}}^{d} \binom{d}{i} p^i (1-p)^{(d-i)}$. Let us simply consider the event $Y_j = \frac{d}{2}$. Then we can apply the lower bound from Lemma 6. The variables $I_{jk}(1 \leq k \leq d)$ are drawn from $\chi = \{0,1\}$ as per distribution $P = Bernoulli(p)$, and the distribution corresponding to $Y_j = \frac{d}{2}$ is $Bernoulli(\frac{1}{2})$ (we shall refer to this as $Q_{\frac{1}{2}}$). $|\chi| = 2$, and $\frac{1}{(d+1)|\chi|} = \frac{1}{(d+1)^2} > \frac{1}{\frac{3}{2}d^2} = \frac{2}{3}e^{-2\ln d}$ (since $d \geq 8$). Thus, we obtain:

$$\begin{aligned}Pr[Y_j \geq \frac{d}{2}] \geq Pr[Y_j = \frac{d}{2}] &\geq \frac{1}{(d+1)|\chi|} e^{-d(D(Q_{\frac{1}{2}}||P))} \\ = \frac{1}{(d+1)^2} e^{-d(D(Q_{\frac{1}{2}}||P))} &> \frac{2}{3} e^{-d(D(Q_{\frac{1}{2}}||P))-2\ln d} \\ > \frac{2}{3} e^{-(c\frac{\ln n}{\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)}})(\frac{1}{2}\ln\frac{1}{2p}+\frac{1}{2}\ln\frac{1}{2(1-p)})-6\ln\ln n} &\quad \text{from Eqn. (23)} \\ = \frac{2}{3} e^{-\frac{c}{2}\ln n - 6\ln\ln n} \geq \frac{2(\ln n)^4}{3n} &\quad \text{from Eqn. (25)}\end{aligned} \tag{26}$$

Let us call this probability $q$.

$$Pr[\ j \text{ non-faulty; at least half } nbd(j) \text{ faulty } ] \geq (1-p)q \tag{27}$$

$$> \frac{1}{2}\frac{2(\ln n)^4}{3n} = \frac{(\ln n)^4}{3n} \tag{28}$$

Let us mark out a subset of nodes $j$ such that the neighborhoods of these nodes are all disjoint, as in Fig. Fig. 1. Then, as noted earlier, the number of such nodes that we may obtain is $k \geq \frac{n}{2d}$ for large $n$. Let $I_j$ be an indicator

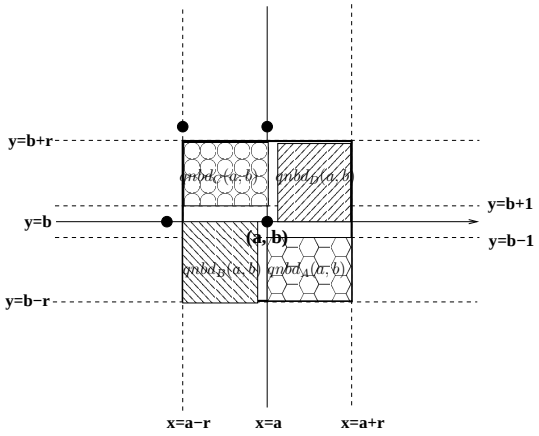


Fig. 3. Depiction of $qnbd_A$, $qnbd_B$, $qnbd_C$, $qnbd_D$

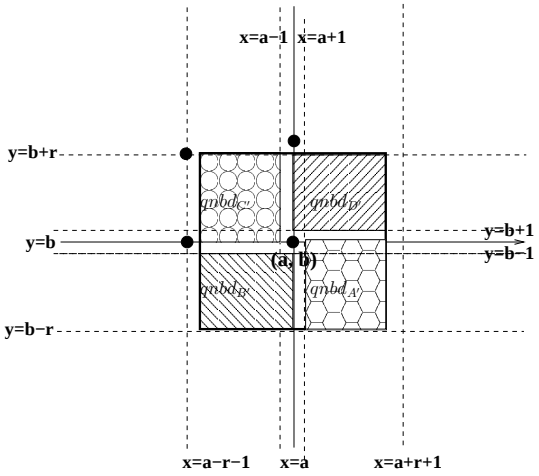


Fig. 4. Depiction of $qnbd_{A'}$, $qnbd_{B'}$, $qnbd_{C'}$, $qnbd_{D'}$

variable that takes value 1 if $j$ is non-faulty but has at least half faulty neighbors. Then $Pr[I_j = 1] = \frac{(\ln n)^4}{3n}$, and all $I_j$'s are independent. Let $I'_j$ be an indicator variable that takes value 1 if $j$ is non-faulty but commits to a wrong value. From Theorem 1, we know that if a non-faulty node has half or more faulty neighbors, it will commit to the wrong value with probability at least $\frac{1}{2}$. Thus $Pr[I'_j = 1] \geq \frac{1}{2} Pr[I_j = 1] \geq \frac{(\ln n)^4}{6n}$.

Let $X$ be a random variable indicating the number of non-faulty nodes with half or more faulty neighbors that commit to the wrong value. Then $X = \sum I'_j$, and $E[X] = \sum Pr[I'_j = 1] \geq \frac{(\ln n)^3}{6n} \left(\frac{n}{2d}\right) = \frac{(\ln n)^4}{12d} > \frac{\ln n}{12} \to \infty$ (as $d < (\ln n)^3$ from Eqn. (24)). Thus we can choose any $0 < \beta < 1$ (e.g. $\beta = \frac{1}{2}$) and apply the Chernoff bound in Lemma 2 to obtain:

$$\lim_{n\to\infty} Pr[X > (1-\beta)E[X]] > \lim_{n\to\infty} 1 - e^{-\frac{\beta^2 E[X]}{2}} = 1 \because E[X] \to \infty \tag{29}$$

Thus, as $n \to \infty$, the probability that some non-faulty node(s) fail to commit to the correct value tends towards 1:

$$\lim_{n\to\infty} Pr[\text{ reliable broadcast fails}] \to 1$$

■

## VIII. Sufficient Condition for Reliable Broadcast

We now present a sufficient condition for the asymptotic achievability of reliable broadcast.

*THEOREM 4:* When $p < \frac{1}{2}$, and node degree $d \geq \max\{d_{min}, 16\frac{\ln n}{\ln \frac{1}{p} + \ln \frac{1}{2(1-p)}}\} = \max\{d_{min}, 8\frac{\ln n}{D(Q_{\frac{1}{2}}||P)})\}$ (recall that $d_{min} = 8$ corresponding to $r = 1$), reliable broadcast is asymptotically achievable with probability 1.

Note that when $\ln \frac{1}{2p} + \ln \frac{1}{2(1-p)} \leq \frac{16 \ln n}{n}$, the degree exceeds total network size $n$, and thus the sufficient condition ceases to be relevant, merely indicating that having a single-hop network suffices for reliable broadcast (which is the trivial sufficient condition for the assumed radio network model). Thus the sufficient condition is of interest only so long as $\ln \frac{1}{2p} + \ln \frac{1}{2(1-p)} > \frac{16 \ln n}{n}$.

*a)* $p \leq o(\frac{1}{n})$*:* When the failure probability is so small as to fall in this range, the probability of even a single node failing approaches 0 asymptotically, and thus reliable broadcast is trivially ensured even with the minimum transmission range of 1. This may be seen thus:

$$Pr[\text{No failures;trivial broadcast}] = (1-p)^n \tag{30}$$

| Region | x-extent | y-extent |
|---|---|---|
| $qnbd_A(a,b)$ | $a \le x \le (a+r)$ | $(b-r) \le y \le (b-1)$ |
| $qnbd_B(a,b)$ | $(a-r) \le x \le (a-1)$ | $(b-r) \le y \le b$ |
| $qnbd_C(a,b)$ | $(a-r) \le x \le a$ | $(b+1) \le y \le (b+r)$ |
| $qnbd_D(a,b)$ | $(a+1) \le x \le (a+r)$ | $b \le y \le (b+r)$ |
| $qnbd_{A'}(a,b)$ | $(a+1) \le x \le (a+r)$ | $(b-r) \le y \le b$ |
| $qnbd_{B'}(a,b)$ | $(a-r) \le x \le a$ | $(b-r) \le y \le (b-1)$ |
| $qnbd_{C'}(a,b)$ | $(a-r) \le x \le (a-1)$ | $b \le y \le (b+r)$ |
| $qnbd_{D'}(a,b)$ | $a \le x \le (a+r)$ | $(b+1) \le y \le (b+r)$ |

TABLE I

SPATIAL EXTENTS OF QUARTER NEIGHBORHOODS

$$\lim_{n\to\infty} Pr[\text{No failures;trivial broadcast}] \ge \lim_{n\to\infty} (1-p)^n = e^{-\lim(np)} = 1 \text{ from Fact 2} \tag{31}$$

*b)* $p = \Omega(\frac{1}{n})$*:* We define a term called quarter-neighborhood of a node $(x,y)$, and denote it by $qnbd(x,y)$. We associate eight quarter-neighborhoods with each node: $qnbd_A$, $qnbd_B$, $qnbd_C$, $qnbd_D$, $qnbd_{A'}$, $qnbd_{B'}$, $qnbd_{C'}$, $qnbd_{D'}$. The quarter-neighborhoods for a node $(a,b)$ are depicted in Fig. 3 and 4, and their spatial extents are tabulated in Table I. Observe that $qnbd_B(a,b) = qnbd'_A(a-r-1,b)$, $qnbd_C(a,b) = qnbd_A(a-r,b+r+1)$, and $qnbd_D(a,b) = qnbd'_A(a,b+r+1)$. Similarly, $qnbd_{B'}(a,b) = qnbd_A(a-r-1,b)$, $qnbd_{C'}(a,b) = qnbd_{A'}(a-r-1,b+r)$, and $qnbd_{D'}(a,b) = qnbd_A(a,b+r+1)$ Thus if we simply consider $qnbd_A(u)$ and $qnbd_{A'}(u)\forall$ nodes $u$, we will have considered all quarter-neighborhoods, i.e. the number of distinct (but *not disjoint*) quarter-neighborhoods is $2n$. Henceforth, we shall sometimes use $Q(x,y)$ to refer to $qnbd_A(x,y)$, and $Q'(x,y)$ to refer to $qnbd_{A'}(x,y)$. The population of any $qnbd$ is $r(r+1)$, and since $d = 4r^2+4r = 4r(r+1)$, the $qnbd$ population = $\frac{d}{4}$. We now state and prove the following result which is crucial to proving our sufficient condition for reliable broadcast:

*THEOREM 5:* If $p < \frac{1}{2}$, $d \ge \max\{d_{min}, 16\frac{\ln n}{\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)}}\} = \max\{d_{min}, 8\frac{\ln n}{D(Q_{\frac{1}{2}}||P)})\}$, then:

$$\lim_{n\to\infty} Pr[\ \forall(x,y) \text{ less than } \frac{d}{8} \text{ faults in } Q(x,y) \text{ and } Q'(x,y)] \to 1$$

*Proof:* As shown above, the population of any $qnbd$ is $\frac{d}{4}$. Each node may fail independently with probability $p$.Let $Y_{(x,y)}$ be a random variable denoting the number of faulty nodes in $Q(x,y)$. Then $E[Y_{(x,y)}] = p\frac{d}{4}$. Using $\delta = \frac{1}{2p} - 1$, we may then apply the relative entropy form of the Chernoff bound (Lemma 3) to $Y_{(x,y)} = \sum_{j\in nbd(x,y)} I_j$. Note that $d \ge \max\{d_{min}, 16\frac{\ln n}{\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)}}\} \ge 16\frac{\ln n}{\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)}}$. Thus, we obtain:

$$Pr[Y_{(x,y)} \ge \frac{d}{8}] \le e^{-\frac{d}{4}(\frac{1}{2}\ln\frac{1}{2p}+\frac{1}{2}\ln\frac{1}{2(1-p)})} \tag{32}$$

$$\le e^{-(\frac{16\ln n}{4(\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)})})(\frac{1}{2}\ln\frac{1}{2p}+\frac{1}{2}\ln\frac{1}{2(1-p)})} \tag{33}$$

$$= e^{-2\ln n} = \frac{1}{n^2} \tag{34}$$

Similarly, setting $Y'_{(x,y)}$ be a random variable denoting the number of faulty nodes in $Q'(x,y)$, we obtain that:

$$Pr[Y'_{(x,y)} \ge \frac{d}{8}] \le \frac{1}{n^2} \tag{35}$$

The $Y_{(x,y)}$'s and $Y'_{(x,y)}$'s are not independent, as they are not all disjoint. However, it may be seen that where dependence exists, it is that of positive correlation (Lemma 7). Thus $Pr[Y_{(x',y')} < \frac{d}{8} | Y_{(x,y)} < \frac{d}{8}] \geq Pr[Y_{(x',y')} < \frac{d}{8}]$, and $Pr[Y_{(x',y')} < \frac{d}{8} | Y'_{(x,y)} < \frac{d}{8}] \geq Pr[Y_{(x',y')} < \frac{d}{8}]$. Similarly, we obtain that: $Pr[Y'_{(x',y')} < \frac{d}{8} | Y_{(x,y)} < \frac{d}{8}] \geq Pr[Y'_{(x',y')} < \frac{d}{8}]$, and $Pr[Y'_{(x',y')} < \frac{d}{8} | Y'_{(x,y)} < \frac{d}{8}] \geq Pr[Y'_{(x',y')} < \frac{d}{8}]$ Hence:

$$Pr[\forall (x,y), Y(x,y) < \frac{d}{8} \text{ and } Y'(x,y) < \frac{d}{8}] \tag{36}$$

$$\geq \prod Pr[Y_{(x',y')} < \frac{d}{8}] \prod Pr[Y'_{(x',y')} < \frac{d}{8}] \tag{37}$$

$$= \left(1 - \frac{1}{n^2}\right)^n \left(1 - \frac{1}{n^2}\right)^n \tag{38}$$

$$= \left(1 - \frac{1}{n^2}\right)^{2n} \tag{39}$$

$$\therefore \lim_{n \to \infty} Pr[\forall (x,y), Y(x,y) < \frac{d}{8} \text{ and } Y'(x,y) < \frac{d}{8}] \tag{40}$$

$$\geq \lim_{n \to \infty} \left(1 - \frac{1}{n^2}\right)^2 n = e^{-\lim(\frac{2}{n})} = 1 \text{ from Fact 2} \tag{41}$$

■

We now consider a simple broadcast protocol that is similar to the protocol described in [4] for the adversarial model:

- Initially, the source does a local broadcast of the message.
- Each neighbor $i$ of the source immediately commits to the the first value $v$ it heard from the source, and then locally broadcasts it once in a $COMMITTED(i,v)$ message.
- Hereafter, the following protocol is followed by each node $j \notin nbd(s)$:
  If $\frac{1}{2}r(r+1)+1 = \frac{d}{8}+1$ $COMMITTED(i,v)$ message are received for a certain value $v$, from neighbors $i$ all lying within a single *qnbd*, and not already committed to some value, commit to $v$, and locally broadcast a $COMMITTED(j,v)$ message.

*THEOREM 6: (Probabilistic Correctness)* The probability that a node shall commit to a wrong value by following the above protocol diminishes to 0 asymptotically.

*Proof:* If all $Q(x,y)$ and $Q'(x,y)$ have strictly less than $\frac{d}{8}$ faults, the correctness of the protocol proceeds as follows:

By the assumptions of *reliable local broadcast*, if $s$ sends exactly one message, fault-free nodes in $nbd(s)$ are guaranteed to receive it correctly. If $s$ is faulty and sends more than one version of the message, fault-free nodes in $nbd(s)$ receive both messages, and select the first one. Thus fault-free nodes in $nbd(s)$ are guaranteed to commit to the correct value.

The rest of the proof is by contradiction. Consider the first fault-free node, say $j$, that makes a wrong decision to commit to a value $v$. From our previous assertion, $j$ cannot be in $nbd(s)$, and thus followed protocol rules for nodes that are not $s$'s neighbors. This implies that $\frac{d}{8}+1$ of its neighbors within some *qnbd* must have broadcast a $COMMITTED$ message for $v$ (the $COMMITTED$ messages were directly heard, leaving no place for doubt). All of these nodes cannot be faulty, as no more than $\frac{d}{8}$ nodes in any *qnbd* are faulty. Thus there was at least one fault-free node that committed to $v$. Since $j$ is the first fault-free node to make a wrong decision, none of the fault-free nodes amongst the $\frac{d}{8}+1$ nodes could have made a wrong decision. Thus $v$ must indeed be the correct value.

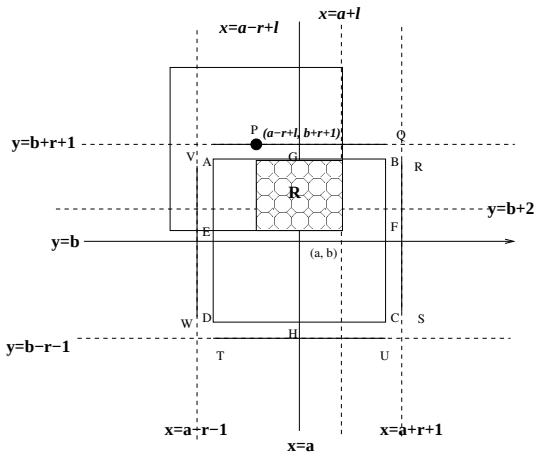


Fig. 5. Node at P has a *qnbd* in $nbd(a,b)$

We know that all $Qnbd(x,y)$ have less than $\frac{d}{8}$ faults with probability 1 asymptotically, and hence the protocol also functions correctly with probability 1 asymptotically. ■

*THEOREM 7: (Probabilistic Completeness)* Each node is eventually able to commit to the (probabilistically) correct value.

*Proof:*
The proof proceeds by induction.

*Base Case:*

All honest nodes in $nbd(0,0)$ are able to commit to the correct value. This follows trivially since they hear the origin directly, and we assume that address-spoofing is impossible.

*Inductive Hypothesis:*

If all honest neighbors of a node located at $(a,b)$ i.e. all honest nodes in $nbd(a,b)$ are able to commit to the correct value, then all honest nodes in $pnbd(a,b)$ are able to commit to the correct value.

*Proof of Inductive Hypothesis:*

We show that each node $P$ in $pnbd(a,b) - nbd(a,b)$ has one of $qnbd_A(P)$, $qnbd_B(P)$, $qnbd_C(P)$, $qnbd_D(P)$, $qnbd_{A'}(P)$, $qnbd_{B'}(P)$, $qnbd_{C'}(P)$, $qnbd_{D'}(P)$ fully contained in $nbd(a,b)$. Since no more than $\frac{d}{8}$ of the nodes in a *qnbd* are faulty with probability 1 (asymptotically), this guarantees that the node will become aware of $\frac{d}{8}+1$ nodes in $nbd(a,b)$ having committed to a (the correct) value, and will also commit to it. The situation is depicted in Fig. 5 for $P \in \{(a-r+l, b+r+1) | 1 \leq l \leq r\}$, for which $qnbd_A(P)$ lies in $nbd(a,b)$. For all other locations, a similar argument holds. ■

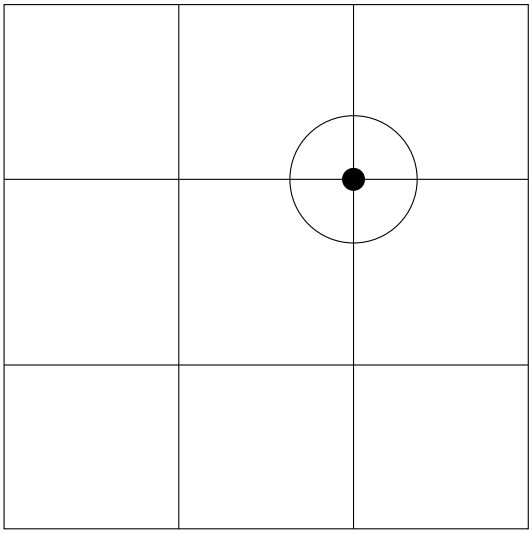

Fig. 6. Necessary Condition for Random Networks: cell $\mathcal{S}$

## IX. Necessary Condition for Random Networks

*THEOREM 8:* When failure probability $p \leq \frac{1}{2} - \sqrt{\frac{\ln n}{n^{\frac{1}{32}}}}$, and $r(n,p) \leq \frac{1}{2}\sqrt{\max\{\ln n, \frac{\ln n}{\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)}}\}}$:

$$Pr[\text{ reliable broadcast fails}] \to 1$$

*Proof:* We separately consider the following two cases:

$\ln n > \frac{\ln n}{\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)}}$*:* We know from the results of [15] that in a failure-free random network, $r(n) = \sqrt{\frac{\ln n}{\pi}}$ is necessary for connectivity (note that we are considering the network as being of area $n$ leading to a scaling of the result of [15]). When, $\ln n > \frac{\ln n}{\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)}}$, the condition in our theorem statement reduces to $r(n,p) \leq \frac{1}{2}\sqrt{\ln n} < \sqrt{\frac{\ln n}{\pi}}$. Thus, from the results of [15], the network is disconnected with some positive probability, and the necessary condition holds.

$\ln n \leq \frac{\ln n}{\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)}}$*:* As mentioned in the previous case, it is known from the results of [15], that even with $p = 0$, the *critical* transmission range is greater than $\frac{\sqrt{\log n}}{2}$. Consider a subdivision of the network into disjoint square cells of area $a(n) = 81r^2(n,p)$, where $\frac{\sqrt{\log n}}{2} \leq r(n,p) \leq \frac{1}{2}\sqrt{\frac{\ln n}{\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)}}}$.

Thus $\frac{81\ln n}{4} \leq a(n) \leq \frac{81\ln n}{4(\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)})}$.

*LEMMA 11:* Each cell contains at least $\frac{a(n)}{2}$ and at most $\frac{3a(n)}{2}$ nodes w.h.p.

*Proof:* Consider a particular cell $\mathcal{S}$. Denote by $X_i$ an indicator variable that is 1 if node $i$ lies in $\mathcal{S}$ and is 0 otherwise. Then $Pr[X_i = 1] = \frac{a(n)}{n}$, and the $X_i$'s are all i.i.d. Let, $X = \sum_{i=1}^{n} X_i$. Then $E[X] = a(n)$.

By applying the Chernoff bound from Lemma 2 (with $\beta = \frac{1}{2}$), it follows that:

$$Pr[X \leq \frac{a(n)}{2}] \leq \exp(-\frac{a(n)}{8}) \leq \exp(-\frac{81\ln n}{32}) = \frac{1}{n^{\frac{81}{32}}} \tag{42}$$

By applying the Chernoff bound from Lemma 5 (with $\beta = \frac{1}{2}$), it follows that:

$$Pr[X \geq \frac{3a(n)}{2}] \leq \exp(-\frac{a(n)}{12}) \leq \exp(-\frac{81\ln n}{48}) = \frac{1}{n^{\frac{81}{48}}} \tag{43}$$

Thus the cell population $n_s$ is least $\frac{a(n)}{2}$ and at most $\frac{3a(n)}{2}$ nodes with probability at least $1-\frac{1}{n^{\frac{81}{32}}}-\frac{1}{n^{\frac{81}{48}}} \geq 1-\frac{2}{n^{1.5}}$. Applying union bound over all $\frac{1}{a(n)} < n$ cells, this holds for all cells with probability at least $1-\frac{2}{\sqrt{n}}$. ■

*Event $\mathcal{E}_o$:* Denote by event $\mathcal{E}_o$, the event that $\frac{a(n)}{2} \leq n_s \leq \frac{3a(n)}{2}$, for all cells. Then $Pr[\neg\mathcal{E}_o] \leq \frac{2}{\sqrt{n}}$

Suppose $\mathcal{E}_o$ holds. Fixing $n_{s_i}$ for all cells $\mathcal{S}_i$ in the network, events occurring entirely within each cell may hereafter be treated as being independent.

Divide each such cell further into 9 square sub-cells of area $A(n) = \frac{a(n)}{9} = 9r^2(n)$ each. Note that $A(n) \leq \frac{9\ln n}{4(\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)})}$ and $A(n) \geq \frac{9}{4}\ln n$.

Consider a particular cell $\mathcal{S}$, and focus on the center sub-cell of this cell (call it $\mathcal{D}$). Then conditioned on the cell populations:

$$\begin{aligned} Pr[D \text{ has no non-faulty node } |N_s = n_s, \mathcal{E}_o] \leq (1-(1-p)\frac{A(n)}{a(n)})^{n_s} \leq (1-(1-p)\frac{A(n)}{a(n)})^{\frac{a(n)}{2}} \leq (1-\frac{A(n)}{2a(n)})^{\frac{a(n)}{2}} \\ \leq e^{-\frac{A(n)}{4}} \leq e^{-\frac{9\ln n}{16}}\frac{1}{n^{\frac{9}{16}}} \end{aligned} \tag{44}$$

*Event $\mathcal{E}_1$:* Denote by event $\mathcal{E}_1$, the event that in a given cell $\mathcal{S}$, the center sub-cell $\mathcal{D}$ has at least one non-faulty node. Then $Pr[\neg\mathcal{E}_1|\mathcal{E}_o] \leq \frac{1}{n^{\frac{9}{16}}}$.

Assuming there is at least one non-faulty node in $\mathcal{D}$, select one such node $j$. Consider its neighborhood, which is guaranteed to fall entirely within the cell S (Fig. 6). Also the area of the neighborhood is $A_1(n) = \pi r^2(n) \leq \frac{\pi\ln n}{4(\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)})} < \frac{\ln n}{\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)}}$. It is to be noted though that $A_1(n) = \pi r^2(n) \geq \frac{\pi\ln n}{4}$. Let $M$ be the number of nodes other than $j$ lying within this area (i.e., the number of neighbors of $j$). Thus $E[M|N_s = n_s, \mathcal{E}_o] = (n_s-1)\left(\frac{A_1(n)}{a(n)}\right) \leq n_s\left(\frac{A_1(n)}{a(n)}\right)$ and thus $\frac{A_1(n)}{2} - \frac{1}{a(n)} \leq (1-\varepsilon)\frac{A(n)}{2} \leq E[M|N_s = n_s, \mathcal{E}_o] \leq \frac{3A_1(n)}{2}$, for any arbitrarily small $\varepsilon$. Let us set $\varepsilon = (1-\frac{3}{\pi})$, to get that $E[M|N_s = n_s, \mathcal{E}_o] \geq \frac{3\ln n}{4}$. Then, setting $(1+\beta)E[M|N_s = n_s, \mathcal{E}_o] = 4A_1(n)$, we get $\beta \geq \frac{4A_1(n)}{E[M|N_s=n_s,\mathcal{E}_o]} - 1 \geq \frac{8}{3} - 1 = \frac{5}{3}$. Applying Lemma 4:

$$\begin{aligned} Pr[M \geq 4A_1(n)|N_s = n_s, \mathcal{E}_o] \leq Pr[M \geq \frac{8E[M|N_s = n_s, \mathcal{E}_o]}{3}] \leq \left(\frac{e^\beta}{(1+\beta)^{1+\beta}}\right)^{E[M|N_s=n_s,\mathcal{E}_o]} \\ \leq \left(\frac{e^{\frac{5}{3}}}{(\frac{8}{3})^{\frac{8}{3}}}\right)^{(1-\varepsilon)\frac{A_1(n)}{2}} \leq \left(\frac{1}{e^{\frac{8}{3}(3\ln 2-\ln 3)-\frac{5}{3}}}\right)^{\frac{3\ln n}{8}} < \left(\frac{1}{e^{\frac{2}{3}}}\right)^{\frac{3\ln n}{8}} = \frac{1}{n^{\frac{1}{4}}} \end{aligned} \tag{45}$$

*Event $\mathcal{E}_2$:* Denote by event $\mathcal{E}_2$, the event that in a given cell $\mathcal{S}$, the chosen non-faulty node (conditioned on such a node existing) in center sub-cell $\mathcal{D}$ has $m \leq 4A_1(n)$ neighbors. Then $Pr[\neg\mathcal{E}_2|\mathcal{E}_o \wedge \mathcal{E}_1] \leq \frac{1}{n^{\frac{1}{4}}}$.

Assuming that $M = m \leq 4A_1(n)$, let us now consider the probability that half or more of these neighbors of $j$ are faulty.

If $M = m = 0$, then automatically the node $j$ is isolated with probability 1. Thus, we only consider the case $M = m \geq 1$.

Given that there are $M = m$ neighbors, and each may fail independently with probability $p$, let $I_{jk}(1 \leq k \leq m)$ denote the indicator variable corresponding to neighbor $k$ of $j$ (enumerated in some order), such that $I_{jk} = 1$ if $k$ is faulty, and 0 otherwise. Then $Y_j = \sum I_{jk}$ denotes the number of failed neighbors of $j$. $Y$ takes values from $0, 1, ..., m$, and $E[Y] = pd$. $Pr[Y_j \geq \frac{m}{2}] = \sum_{i=\frac{m}{2}}^{m}\binom{m}{i}p^i(1-p)^{(m-i)}$. Let us simply consider the event $Y_j = \frac{m}{2}$. Then we can apply

the lower bound from Lemma 6. The variables $I_{jk}(1 \leq k \leq M)$ are drawn from $\chi = \{0,1\}$ as per distribution $P = Bernoulli(p)$, and the distribution corresponding to $Y_j = \frac{m}{2}$ is $Bernoulli(\frac{1}{2})$ (we shall refer to this as $Q_{\frac{1}{2}}$).

$|\chi| = 2$, and $\frac{1}{(m+1)^{|\chi|}} = \frac{1}{(m+1)^2} \geq \frac{1}{4m^2} = \frac{1}{4}e^{-2\ln m}$ (for all $m \geq 1$).

Note that $m \leq 4A_1(n) \leq \frac{4\ln n}{\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)}} \leq \frac{4\ln n}{4(\frac{1}{2}-p)^2} \leq n^{\frac{1}{32}}$ from Lemma 8.

Thus, we obtain:

$$\begin{aligned} q = Pr[Y_j \geq \frac{m}{2}] \geq Pr[Y_j = \frac{m}{2}] &\geq \frac{1}{(m+1)^{|\chi|}} e^{-m(D(Q_{\frac{1}{2}}||P))} \\ &= \frac{1}{(m+1)^2} e^{-m(D(Q_{\frac{1}{2}}||P))} = \frac{1}{4} e^{-m(D(Q_{\frac{1}{2}}||P))-2\ln m} \\ &> \frac{1}{4} e^{-(\frac{\ln n}{4(\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)})})(\frac{1}{2}\ln\frac{1}{2p}+\frac{1}{2}\ln\frac{1}{2(1-p)})-\frac{1}{16}\ln n} \\ &= \frac{1}{4} e^{-\frac{2}{16}\ln n-\frac{1}{16}\ln n} \geq \frac{1}{4n^{\frac{3}{16}}} \end{aligned}$$

Then, assuming that event $\mathcal{E}_o$ indeed held, the probability that one of events $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3$ did not occur can be bounded as follows:

$$\begin{aligned} Pr[\neg(\mathcal{E}_1 \wedge \mathcal{E}_2 \wedge \mathcal{E}_3)|\mathcal{E}_o] &\leq Pr[\neg\mathcal{E}_1|\mathcal{E}_o] + Pr[\mathcal{E}_1)]Pr[\mathcal{E}_2|\mathcal{E}_1 \wedge \mathcal{E}_o] \\ &\quad + Pr[\mathcal{E}_1 \wedge \mathcal{E}_2|\mathcal{E}_o]Pr[\neg\mathcal{E}_3|\mathcal{E}_o \wedge \mathcal{E}_1 \wedge \mathcal{E}_2)] \\ &\leq Pr[\mathcal{E}_1|\mathcal{E}_o] + Pr[\mathcal{E}_2|\mathcal{E}_o \wedge \mathcal{E}_1] + Pr[\mathcal{E}_3|\mathcal{E}_o \wedge \mathcal{E}_1 \wedge \mathcal{E}_2] \\ \leq \frac{1}{n^{\frac{9}{16}}} + \frac{1}{n^{\frac{1}{4}}} + (1 - \frac{1}{4n^{\frac{1}{4}}}) &= 1 - (\frac{1}{4n^{\frac{3}{16}}} - \frac{1}{n^{\frac{9}{16}}} - \frac{1}{n^{\frac{1}{4}}}) \leq 1 - \frac{1}{8n^{\frac{3}{16}}} \text{for large } n \end{aligned} \tag{46}$$

Thus, conditioned on $\mathcal{E}_o$, with probability at least $\frac{1}{8n^{\frac{3}{16}}}$, there is such a node $x$ which has half or more faulty neighbors. Denote by $I_j$, an indicator variable which is one if this event happens for a subsquare $i$. Then $\Pr[I_j = 1] \geq \frac{1}{8n^{\frac{3}{16}}}$. Recall again, that once we fixed all the cell populations $n_i$, the considered events in each subsquare are independent of each other.

The number $h$ of disjoint subsquares is at least $\left(\frac{\lfloor\sqrt{n}\rfloor}{9r(n)}\right)^2 \geq \frac{n}{2(\frac{81\ln n}{4\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)}})} = \frac{2n(\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)})}{81\ln n}$ for large $n$. From Lemma 8, we can thus see that $h \geq \frac{8n(\frac{1}{2}-p)^2}{81\ln n} \geq \frac{8n^{1-\frac{1}{32}}}{81} = \frac{8n^{\frac{31}{32}}}{81}$.

Let $I'_x$ be an indicator variable that takes value 1 if a node $j$ is non-faulty but commits to a wrong value. From 1, we know that if a non-faulty node has half or more faulty neighbors, it will commit to the wrong value with probability at least $\frac{1}{2}$. Thus $Pr[I'_x = 1|\mathcal{E}_o] \geq \frac{1}{2}Pr[I_j = 1|\mathcal{E}_o] \geq \frac{1}{16n^{\frac{3}{16}}}$.

Let $X$ be a random variable indicating the number of subsquares in which we were able to select a non-faulty node $x$, and which happened to have half or more faulty neighbors, and which commit to the wrong value.

Then $X = \sum I'_x$, and $E[X|\mathcal{E}_o] = \sum Pr[I'_j = 1|\mathcal{E}_o] \geq \frac{1}{16n^{\frac{3}{16}}}(h) = \frac{1}{16n^{\frac{3}{16}}}\frac{8n^{\frac{31}{32}}}{81} \geq \frac{n^{\frac{25}{32}}}{162}$. Also, since we are conditioning on subsquare populations, the indicator variables $I'_x$ are all independent.

Thus we can choose an appropriate constant $0 < \beta < 1$ (e.g., set $\beta = \frac{1}{2}$) and apply the Chernoff bound in Lemma 2 to obtain:

$$Pr[X < \frac{E[X]}{2}|\mathcal{E}_o] \leq e^{-\frac{E[X]}{8}} \leq e^{-\frac{n^{\frac{25}{32}}}{162(8)}}$$

Applying union bound over probability that $\mathcal{E}_o$ does not occur or that the above event does not hold, we obtain that with probability at least $1 - \frac{2}{\sqrt{n}} - e^{-\frac{n^{\frac{25}{32}}}{162(8)}} \to 1$, some non-faulty node commits to an incorrect value.

Thus:

$$\lim_{n\to\infty} Pr[\text{ reliable broadcast fails}] \to 1$$

■

*Corollary 3:* The critical average degree for reliable broadcast in a random network with Byzantine failure probability $p < \frac{1}{2}$, is expressible as $\Omega(\frac{\ln n}{\frac{1}{2}-p+\frac{1}{2}\ln\frac{1}{2(1-p)}})$ or $\Omega(\frac{\ln n}{(\frac{1}{2}-p)^2})$.

*Proof:* Note that when $p < \frac{1}{2}$: $\frac{1}{2} - p + \frac{1}{2}\ln\frac{1}{2(1-p)} = \Theta(\min\{1, \ln\frac{1}{2p} + \ln\frac{1}{2(1-p)}\})$. Similarly, $(\frac{1}{2} - p)^2 = \Theta(\min\{1, \ln\frac{1}{2p} + \ln\frac{1}{2(1-p)}\})$. In Theorem 8, we proved that $d_{critical} = \Omega(\max\{\ln n, \frac{\ln n}{\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)}}\}) = \Omega(\frac{\ln n}{\min\{1,\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)}\}})$. The result thus follows. ■

## X. Sufficient Condition for Random Networks

We obtain a sufficient condition for a network of $n$ randomly deployed nodes, based on the sufficient condition for the grid network model. To maintain consistency with the grid network formulation, we assume a toroidal region of area $\sqrt{n}$ x $\sqrt{n}$, with $n$ nodes located uniformly at random. The average degree of a node is the average number of the remaining $n-1$ nodes that fall within its neighborhood (recall we are using $L_\infty$ distance metric), i.e., $d_{avg}(n,p) = \frac{(n-1)(2r(n,p))^2}{n} \approx 4r^2(n,p)$ for large $n$.

*THEOREM 9:* When failure probability $p < \frac{1}{2}$, and $r(n,p) \geq \sqrt{\frac{100\ln n}{\frac{1}{2}-p+\frac{1}{2}\ln\frac{1}{2(1-p)}}}$, reliable broadcast is asymptotically achievable in the random network model with high probability.

*Proof:* At the outset, we make the observation that if $r(n,p) = \sqrt{n}$, all nodes are neighbors, and trivially broadcast is achievable. Thus this result is of interest only so long as $r(n,p) < \sqrt{n}$.

In light of Fact 2:

$$\begin{aligned} D(Q_{\frac{1}{2}}||p) &= \frac{1}{2}\ln\frac{1}{2p} + \frac{1}{2}\ln\frac{1}{2(1-p)} \\ \geq \frac{1}{2}(1-2p) + \frac{1}{2}\ln\frac{1}{2(1-p)} &= \frac{1}{2} - p + \frac{1}{2}\ln\frac{1}{2(1-p)} \end{aligned} \tag{47}$$

Also, since $p < \frac{1}{2}$:

$$0 < \frac{1}{2} - p + \frac{1}{2}\ln\frac{1}{2(1-p)} \leq \frac{1}{2}(1-\ln 2) < 1 \tag{48}$$

Similar to grid networks, we use a notion of quarter-neighborhoods. For a given broadcast instance, we again use relative coordinates by treating the source's coordinates as $(0,0)$. With some abuse of the grid network notation introduced in Section II, we can extend the notion of $nbd(x,y)$, to include all nodes within distance $r$ of point $(x,y)$ (regardless of whether or not there is a node at $(x,y)$), where $x$ and $y$ are real numbers. The notion of $pnd(x,y)$ is also similarly extended to all points $(x,y)$.

Note that in this model, a node's (or point's) coordinates are real numbers. We thus associate eight quarter-neighborhoods with each node, with spatial extents as in Table I, except that now $x$ and $y$ must be treated as real numbers. Also, now it is not possible to assert that there are only $2n$ distinct quarter-neighborhoods. Thus, all eight quarter-neighborhoods of a node must be treated as distinct[2], yielding $8n$ quarter-neighborhoods in all.

The quarter-neigborhoods are axis-parallel rectangles of area $r(n,p)(r(n,p)-1) \geq \frac{r^2(n,p)}{2}$ (for $r(n,p) \geq 2$). Then, if $4r^2(n,p) \geq \frac{400\ln n}{\frac{1}{2}-p+\frac{1}{2}\ln\frac{1}{2(1-p)}}$, then we can apply Lemma 10 for all axis-parallel rectangles of area $r(n,p)(r(n,p)-1) \geq$

[2]Note that distinct does not mean disjoint.

$\frac{50\ln n}{\frac{1}{2}-p+\frac{1}{2}\ln\frac{1}{2(1-p)}} \geq \frac{100\ln n}{1-\ln 2}$, to obtain that they all have at least $\frac{50\ln n}{\frac{1}{2}-p+\frac{1}{2}\ln\frac{1}{2(1-p)}} - 50\ln n > \frac{25\ln n}{\frac{1}{2}-p+\frac{1}{2}\ln\frac{1}{2(1-p)}} > \frac{50\ln n}{1-\ln 2}$ nodes, with probability at least $1-\frac{50\ln n}{n} \to 1$.

Thus all such rectangles are *non-empty*. Also:

$$\frac{25\ln n}{\frac{1}{2}-p+\frac{1}{2}\ln\frac{1}{2(1-p)}} \geq \frac{25\ln n}{D(Q_{\frac{1}{2}}||p)} > \frac{8\ln n}{D(Q_{\frac{1}{2}}||p)} \tag{49}$$

Hence all the quarter-neighborhoods have at least $\frac{8\ln n}{D(Q_{\frac{1}{2}}||p)}$ nodes (which is the quarter-neighborhood population in the grid network case). Then using a proof argument similar to Theorem 5, one can prove the following theorem:

*THEOREM 10:* If $p < \frac{1}{2}$, and $r(n,p) \geq \sqrt{\frac{100\ln n}{\frac{1}{2}-p+\frac{1}{2}\ln\frac{1}{2(1-p)}}}$, then

$$\lim_{n\to\infty} Pr[\text{ all } 8n \textit{ qnbds} \text{ have non-faulty majority}] \to 1$$

Thus, one can use a broadcast protocol similar to that for grid networks (a node commits to a value if it is received from half or more nodes in some quarter-neighborhood), and, for all broadcast sources, and instances, the correctness and completeness continue to hold, as follows:

*Correctness*: Relying on Theorem 10, we can apply a proof argument similar to Theorem 6.

*Completeness*: The proof uses the an inductive argument similar to the proof of Theorem 7, except that the terms $nbd(x,y), pnd(x,y)$ and quarter-neighborhood must be interpreted as per their re-definition in this section. In the base case, all neighbors of the source (which is at $(0,0)$) commit to the correct value trivially. In the inductive step, one can show that if all nodes in $nbd(x,y)$ (as per the re-defined notation) have comitted to the correct value, all nodes in $pnd(x,y) - nbd(x,y)$ have some *qnbd* contained in $nbd(x,y)$, and can thus commit to the value received from a majority of nodes in this *qnbd*. ■

Since the area within range of a node is $(2r)^2 \leq 4r^2$ (for the valid domain of $r$ values) in the $L_\infty$ metric, the result indicates that an average node degree $d_{avg}$ of $\frac{400\ln n}{\frac{1}{2}-p+\frac{1}{2}\ln\frac{1}{2(1-p)}}$ suffices for reliable broadcast. Hence the *critical* average node degree $d^{avg}_{critical}$ is $O(\frac{\ln n}{\frac{1}{2}-p+\frac{1}{2}\ln\frac{1}{2(1-p)}})$. [3]

*Corollary 4:* The critical average degree for reliable broadcast in a random network with Byzantine failure probability $p < \frac{1}{2}$ is $O(\max\{\ln n, \frac{\ln n}{\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)}}\})$ or $O(\frac{\ln n}{\min\{1,\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)}\}})$ or $O(\frac{\ln n}{(\frac{1}{2}-p)^2})$.

*Proof:* Note that when $p < \frac{1}{2}$: $\frac{1}{2}-p+\frac{1}{2}\ln\frac{1}{2(1-p)} = \Theta(\min\{1,\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)}\}) = \Theta((\frac{1}{2}-p)^2)$. In Theorem 9, we proved that $d_{critical} = O(\frac{\ln n}{\frac{1}{2}-p+\frac{1}{2}\ln\frac{1}{2(1-p)}})$. Thus, it follows that $d_{critical} = O(\frac{\ln n}{\min\{1,\ln\frac{1}{2p}+\ln\frac{1}{2(1-p)}\}}) = O(\frac{\ln n}{(\frac{1}{2}-p)^2})$. The result thus follows, ■

## XI. Conditions in Euclidean Metric

We show that our results derived for $L_\infty$ metric continue to hold for $L_2$ metric, with only the constants in the theta notation changing.

*LEMMA 12:* If reliable broadcast is achievable asymptotically in $L_\infty$ for all $r \geq r_{min}$, then it is achievable asymptotically in $L_2$ for all $r \geq r_{min}\sqrt{2}$.

*Proof:* The proof is by contradiction. Suppose that, for a given failure configuration, broadcast is asymptotically achievable in $L_\infty$ for all $r \geq r_{min}$ but is not asymptotically achievable for all $r \geq r_{min}\sqrt{2}$ in $L_2$. Observe that it is possible to circumscribe a $L_\infty$ neighborhood of range $r$ by a $L_2$ neighborhood of range $r\sqrt{2}$ (Fig. 7). Hence the non-faulty nodes in an $L_2$ network of transmission range $r\sqrt{2}$ can be made to simulate the operation of nodes in a

[3] A more intuitive way of viewing the result is that *critical* degree is $O(\max\{\ln n, \frac{\ln n}{D(Q_{\frac{1}{2}}||P)}\})$.

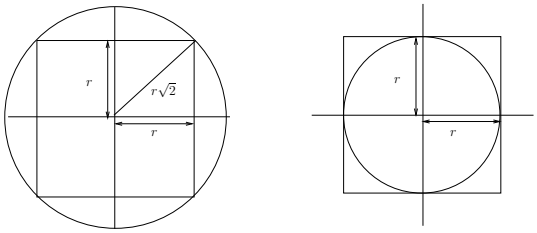


Fig. 7. Relationship between $L_\infty$ and $L_2$ neighborhoods

$L_\infty$ network with range $r$ (as the $L_\infty$ neighborhood is fully contained within the $L_2$ neighborhood). Also, given that this is a network of known topology, with no address spoofing allowed, the faulty nodes cannot gain any unfair advantage, by not simulating the the $L_\infty$ network. This implies that if broadcast is achievable in the $L_\infty$ network of range $r$ , so must it be in the $L_2$ network of range $r\sqrt{2}$. If there is some $r \geq r_{min}$ for which we can achieve broadcast in the $L_\infty$ network asymptotically, but not in the the $L_2$ network of range $r\sqrt{2}$, we obtain a contradiction, as achievability in the $L_\infty$ network would imply achievability in the $L_2$ network. ■

*LEMMA 13:* If reliable broadcast fails asymptotically in $L_\infty$ for all $r \leq r_{min}$, then it fails asymptotically in $L_2$ for all $r \leq r_{min}$.

*Proof:* The proof is by contradiction. Suppose that broadcast fails asymptotically in $L_\infty$ for range $r$, but does not fail in $L_2$ for range $r$. Observe that an $L_\infty$ neighborhood of transmission range $r$ circumscribes an $L_2$ neighborhood of range $r$ (Fig. 7). Thus, for any given failure configuration, if broadcast succeeds in the the $L_2$ network of range $r$, so can it in the $L_\infty$ network of radius $r$, as we could simply make the fault-free nodes in the $L_\infty$ network simulate the behavior of nodes in the $L_2$ network. Hence, if broadcast does not fail in the $L_2$ network of range $r \leq r_{min}$, it will not fail in the $L_\infty$ network of range $r \leq r_{min}$. This yields a contradiction. ■

### XII. Non-Toroidal Networks

We used the assumption that the network is toroidal to avoid edge effects. However, one can see that the results would continue to hold even if the network were spread over a non-toroidal rectilinear domain. The necessary condition would continue to hold, since the degree of nodes at the edges can be no more more than the degree of nodes towards the center, and if reliable broadcast is impossible even with the assumption of equal degree for all nodes, it must certainly be impossible when some nodes (those at the edges) have a smaller degree.

The sufficient condition continues to hold since the described protocol relies on information from quarter-neighborhoods, and it can be seen that even the nodes at the edges have at least one quarter-neighborhood within the network region.

## Crash-Stop Failures/Connectivity

### XIII. Related Work

Conditions for connectivity and coverage have been formulated in the context of different network models. In [15], it was proved that in a unit area network with uniformly distributed node placement, where nodes have a common transmission radius $r$, such that $\pi r^2 = \frac{(\log n + c(n))}{n}$, the network is asymptotically connected with probability one iff $c(n) \to \infty$. In [16], an alternate model was considered whereby randomly deployed nodes may modulate their transmission power (and hence range) to ensure that they have a certain number of neighbors. It was proved that each node must be connected to $\Theta(\log n)$ neighbors for asymptotic connectivity with probability one. Recently,

necessary and sufficient conditions for asymptotic connectivity in a network with low duty cycle sensors have been formulated in [17].

A grid network model was considered in [1] where nodes are located at grid locations on a square grid, but may fail independently. Nodes have a common transmission range $r$. The probability of not failing is specified as $p$, and it is shown that a sufficient condition for connectivity and coverage is that transmission range $r$ must be set to ensure that node degree is $c_1(\frac{\log n}{p})$ (for some constant $c_1$). It is also shown that a necessary condition for coverage (and hence for joint coverage and connetivity) is that node degree be at least $c_2(\frac{\log n}{p})$ (for another constant $c_2$. A fallacy in the above necessary condition was pointed out by [18], and a subsequent correction [19] by the authors of [1] presents examples illustrating that the necessary condition may fail to hold for certain subranges of $p$. The issue of coverage has been examined in detail in [18] for random, grid, and poisson deployments. However, the necessary and sufficient conditions formulated by them take a more complex form, and do not point to a single $f(n,p)$ such that a degree of $\Theta(f(n,p))$ is both necessary and sufficient for asymptotic coverage. Besides, the necessary condition is formulated for the specific case when $\lim_{n\to\infty} p \to 0$.

Our results for crash-stop failures are closely related to the results of [1]. However, we prove that, given a *failure* probability $p$, it is necessary and sufficient to have a degree of $\Theta(d_{min} + \frac{\log n}{\log \frac{1}{p}})$ for both connectivity and coverage. Expressed in the notation of [1], we stipulate a degree of $\Theta(\frac{\log n}{\log \frac{1}{1-p}})$. Our results diverge considerably from those of [1] when the failure probability becomes extremely small, and thus our necessary conditions would hold in a certain subdomain where that of [1] would not. However, there is a small sub-domain of $p$ in which our necessary conditions also cease to hold, as with the conditions of [1]. Besides, we work in the $L_\infty$ distance metric, and then map the results to $L_2$. This yields much simpler proofs. We also remark that our joint sufficient condition for connectivity and coverage is actually sufficient for 9-coverage and not merely 1-coverage (where $k$-coverage implies that each point is covered by at least $k$ non-faulty nodes). It is noteworthy that our results may be derived from analysis presented in [20] regarding the feasible rate in a sensor network, although no statement has been made in [20] in this regard.

## XIV. Notation and Terminology

We briefly describe here notation and terminology that shall be used in this paper. Nodes can identified by their grid location i.e. $(x,y)$ denotes the node at $(x,y)$. The neighborhood of $(x,y)$ comprises all nodes within distance $r$ of $(x,y)$ and is denoted as $nbd(x,y)$. The degree of each node is referred to as $d$. In $L_\infty$ metric, $d = 4r^2 + 4r$, while the size of a neighborhood (including the neighborhood center) is $d+1 = 4r^2+4r+1$. The diameter of the network (in terms of distance, and not number of hops) is referred to as $D$. If $n$ is a perfect square, $D = \sqrt{n}$.

## XV. Necessary Condition for Connectivity

*THEOREM 11:* When $p < 1 - \frac{1}{\ln n}$, if $r(n,p) < \max\{1, \frac{1}{4}\sqrt{\frac{\ln n}{\ln \frac{1}{p}}}\}$ (yielding node degree $d(n,p) < \max\{d_{min}, \frac{\ln n}{2\ln \frac{1}{p}}\}$):

$$\lim_{n\to\infty} Pr[\text{ disconnection}] = 1$$

*Proof:* It is obvious that the minimum transmission range required for connectivity is 1, yielding $d = d_{min} = 8$ (in $L_\infty$ metric), else the degree of all nodes is 0 (except in the case when all nodes are faulty, and connectivity becomes irrelevant). Thus, we only focus on the case where $\frac{1}{4}\sqrt{\frac{\ln n}{\ln \frac{1}{p}}} \geq 1$.

We show that the network is asymptotically disconnected with probability 1 if $r < \frac{1}{4}\sqrt{\frac{\ln n}{\ln \frac{1}{p}}}$, as long as $p \leq 1 - \frac{1}{\ln n}$.

It is evident that $r(n,p) \leq \max\{1, \frac{1}{4}\sqrt{\frac{\ln n}{\ln \frac{1}{p}}}\}$ yields a node degree $d(n,p) \leq \max\{d_{min}, \frac{\ln n}{2\ln \frac{1}{p}}\}$.

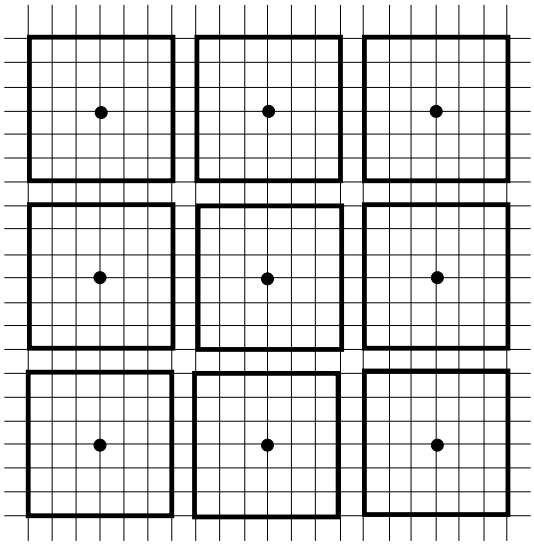

Fig. 8. Nodes having disjoint neighborhoods

*a)* $p \leq 1 - \frac{1}{\ln n}$*:* Consider a particular node $j$ in the network. Then, if $j$ is non-faulty, but all its neighbors are faulty, we have a potential disconnection event. Given that there are $d$ neighbors, and each may fail independently with probability $p$, the probability that $j$ does not fail, but all nodes in $nbd(j)$ fail, is $(1-p)p^d$.

Since $p \leq 1 - \frac{1}{\ln n}$, we obtain that $\frac{1}{1-p} \geq \ln n$.

$$\begin{aligned} Pr[\text{ A given node } j \text{ is alive, but isolated}] &\geq Pr[j \text{ is alive and all neighbors of } j \text{ are faulty }] \\ &= (1-p)p^d > \frac{1}{\ln n} p^{\frac{\ln n}{2\ln \frac{1}{p}}} = \frac{1}{\ln n}\frac{1}{\sqrt{n}} = \frac{1}{\sqrt{n}\ln n} \\ &\geq \frac{(\ln n)^3}{n} \text{for large } n, \text{ from our choice of } c \end{aligned} \tag{50}$$

Note the following:

$$d < \frac{\ln n}{2\ln \frac{1}{p}} \leq \frac{\ln n}{2(1-p)} \leq \frac{(\ln n)^2}{2}(\text{ from Fact 1}) \tag{51}$$

Let us mark out a subset of nodes $j$ such that the neighborhoods of these nodes are all disjoint, as in Fig. 8. Then, from Fact 4, the number of such nodes that we may obtain is at least $\frac{n}{2d}$ for large $n$.

Let $I_j$ be an indicator variable that takes value 1 if $j$ is alive but isolated. Then $Pr[I_j = 1] \geq \frac{(\ln n)^3}{n}$, and all $I_j$'s are i.i.d.

Let $X$ be a random variable denoting the number of nodes from the chosen set that are alive and isolated. Then $X = \sum I_j$, and $E[X] \geq \frac{(\ln n)^3}{n}\frac{n}{2d} \geq \frac{(\ln n)^3}{(\ln n)^2} = \ln n$. We can thus set $\beta = \frac{1}{2}$ in the Chernoff bound of Lemma 2, and obtain that:

$$Pr[X > \frac{\ln n}{2}] \geq 1 - e^{-\frac{\ln n}{8}} = 1 - \frac{1}{n^{\frac{1}{8}}} \tag{52}$$

Thus, for $p < 1 - \frac{1}{\ln n}$, $\lim_{n\to\infty} Pr[\text{ At least two alive nodes are isolated}] = 1$.

This result can actually be extended and shown to hold for a slightly larger range of $p$ values.

*b)* $1-p=o\left(\frac{1}{n}\right)$*:* When the failure probability becomes so high as to fall in this range, we obtain:

$$\lim_{n\to\infty} Pr[\text{ Any node is alive}] = 1-p^n = \lim_{n\to\infty} 1-(1-(1-p))^n = 1-e^{-\lim(n(1-p))} = e^0 = 0 \text{ from Fact 2} \quad (53)$$

Thus the issue of connectivity is irrelevant. ■

## XVI. Necessary Condition for Coverage

Since the connectivity condition proof is easily adaptable to also provide a necessary condition for coverage, we do so in this section. Recall that the network is considered covered if each point in the network region falls within range of at least one non-faulty node.

We now show that for the network to be asymptotically covered with probability approaching 1, it is necessary that the transmission range $r$ satisfy: $r \geq \max\{\frac{1}{2}, \Omega(\sqrt{\frac{\ln n}{\ln \frac{1}{p}}})\}$.

*THEOREM 12:* For $p < 1-\frac{1}{\ln n}$, for a suitable constant $0<c<1$, if $r(n,p) < \max\{\frac{1}{2}, \sqrt{c\frac{\ln n}{8\ln\frac{1}{p}}}\}$, for a suitable constant $c < \frac{8}{9}$, yielding $d < \frac{c\ln n}{\ln\frac{1}{p}}$ :

$$\lim_{n\to\infty} Pr[\text{Some point is not covered}] \to 1$$

*Proof:* Since the grid comprises unit squares, it is obvious that $r$ must be at least $\frac{1}{2}$, else some points between the lattice will not be covered. We handle two subranges of $p$ separately.

*a)* $p < 1-\frac{1}{\ln n}$*:* The proof relies on subdivision of the network into disjoint neighborhoods, as in Fig. 8. From Fact 4, the number of such neighborhoods obtained is at least $\frac{n}{2d}$ for large $n$.

If there exists at least one neighborhood with absolutely no nodes alive (neither the neighborhood center nor its neighbors), then the center of that neighborhood is not covered. Thus we seek to determine the probability of such an event.

We begin by choosing a constant $0<c<\frac{8}{9}$ such that $\frac{9}{8}c\ln n \leq \ln n - 3\ln\ln n$, for sufficiently large $n$. In general any constant $c \leq \frac{8}{9}-\varepsilon$ will satisfy this property for large $n$.

This also ensures that $\frac{1}{n^c} \geq \frac{1}{n^{\frac{9\ln n}{8}}} \geq \frac{(\ln n)^3}{n}$ for large $n$. Set $r \leq \sqrt{\frac{c\ln n}{8\ln\frac{1}{p}}}$. Then $d = 4r^2+4r \leq 8r^2 = \frac{c\ln n}{\ln\frac{1}{p}} \leq c(\ln n)^2 < (\ln n)^2$.

The neighborhood population is given by $d+1 = 4r^2+4r+1 \leq 4r^2+4r^2+r^2 = 9r^2$, for $n \geq 1$. Thus $d+1 \leq \frac{9c\ln n}{8\ln\frac{1}{p}}$

Let $I_j$ be an indicator variable that takes value 1 if there is no alive node in the neighborhood centered at node $j$, and value 0 otherwise.

Then $Pr[X_j = 1] = p^{d+1} \geq p^{\frac{9}{8}c\frac{\ln n}{\ln\frac{1}{p}}} = \frac{(\ln n)^3}{n}$ (from our choice of $c$).

Let $X = \sum I_j$ be a random variable indicating the number of neighborhoods with no alive node. Then $E[X] \geq \frac{(\ln n)^3}{n}\frac{n}{2d} \geq \frac{(\ln n)^3}{2d} \geq \frac{(\ln n)^3}{2(\ln n)^2} = \frac{\ln n}{2}$.

Application of the Chernoff bound from Lemma 2 with $\beta = \frac{1}{2}$ yields:

$$Pr[X \leq \frac{\ln n}{4}] \leq Pr[X \leq \frac{E[X]}{2}] \leq \exp(-\frac{E[X]}{8}) \to 0 \quad (54)$$

Thus there is some uncovered region with probability 1.

Hence $r \leq \sqrt{\frac{c\ln n}{8\ln\frac{1}{p}}} \implies$ some uncovered area.

Similar to the necessary condition for connectivity, observe that the proof can be extended to hold for a somewhat larger range of $p$ values, with suitable adjustment to the constant.

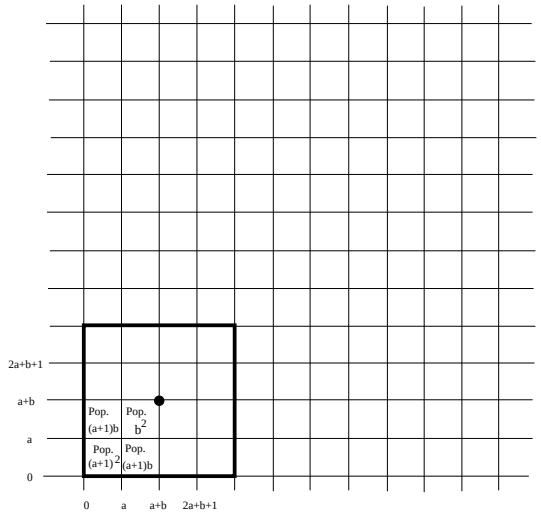


Fig. 9. Subdivision of network into cells

*b)* $1-p=o(\frac{1}{n})$*:* Thus $n(1-p)\to 0$. We obtain that $Pr[$ no nodes alive $]=p^n=(1-(1-p))^n$. As $n\to\infty$, the following holds:

$$\lim_{n\to\infty} Pr[\text{some point not covered}] \geq Pr[\text{no node alive}] \tag{55}$$

$$= \lim_{n\to\infty}(1-(1-p))^n = e^{-\lim(n(1-p))} = e^0 = 1 \text{ from Fact 2} \tag{56}$$

■

Thus the network is trivially not covered, regardless of transmission range.

## XVII. Sufficient Condition for Connectivity and Coverage

We now present a sufficient condition for the asymptotic existence of both connectivity and coverage. It is thus also a sufficient condition for each of them individually.

*THEOREM 13:* When $d \geq \max\{d_{min}, 32\frac{\ln n}{\ln\frac{1}{p}}\}$, the network is asymptotically connected and covered with probability 1.

*Proof:*

*a)* $p=o(\frac{1}{n})$*:* When the failure probability is so small as to fall in this range, the probability of even a single node failing approaches 0 asymptotically, and thus connectivity and coverage is trivially ensured even with the minimum transmission range of 1. This may be seen thus:

$$\lim_{n\to\infty} Pr[\text{No failures;full connectivity/coverage}] \geq \lim_{n\to\infty}(1-p)^n = e^{-\lim np} = e^0 = 1 \text{ from Fact 2} \tag{57}$$

*b)* $p=\Omega(\frac{1}{n})$*:* Consider the subdivision of the grid as depicted in Fig. 9, so that the resulting cells have x-extents (y-extents) 0 to $a$, $a+1$ to $a+b$, $a+b+1$ to $2a+b+1$, and so on. Here $a=\lfloor\frac{r}{2}\rfloor$ and $b=r-a=r-\lfloor\frac{r}{2}\rfloor$. Then, each node is within range of all other nodes in the cells adjoining its own. Thus it is obvious that if each square has at least one non-faulty node, there exists a connected backbone that covers all points, and hence all nodes. Thus all non-faulty nodes are connected to each other via this backbone. The dimensions of the cells thus

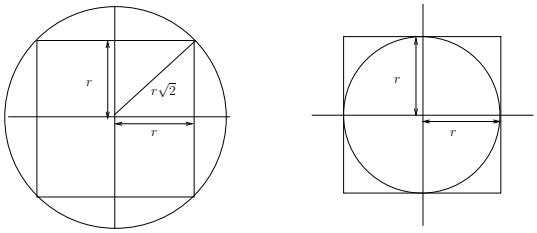


Fig. 10. Relationship between $L_\infty$ and $L_2$ neighborhoods

obtained can be $(a+1)^2$, $(a+1)b$ or $b^2$. Thus the population $k$ of any cell satisfies $k \geq \frac{r^2}{4}$, and the maximum possible number of cells $m \leq \frac{4n}{r^2}$. Then:

$$Pr[\text{ no node alive in a given cell }] = p^k \leq p^{\frac{r^2}{4}} \tag{58}$$

Let us choose $r \geq \sqrt{\frac{8\ln n}{\ln \frac{1}{p}}}$. Then:

$$Pr[\text{no node alive in a given cell}] \leq p^{\frac{r^2}{4}} \leq p^{\frac{2\ln n}{\ln \frac{1}{p}}} \tag{59}$$

$$= e^{-2\ln n} = \frac{1}{n^2} \tag{60}$$

The total number of cells $=\frac{4n}{r^2} \leq n$. Thus, by applying a union bound over all cells:

$$Pr[\text{at least 1 node alive in each cell}] \geq 1 - \frac{1}{n} \tag{61}$$

Since this condition ensures connectivity and coverage, we obtain that:

$$\lim_{n\to\infty} Pr[\text{network is connected and covered}] \to 1 \tag{62}$$

■

## XVIII. Conditions in Euclidean Metric

We show that our results derived for $L_\infty$ metric continue to hold for $L_2$ metric, with only the constants in the theta notation changing.

*LEMMA 14:* If the network is asymptotically connected (covered) in $L_\infty$ for all $r \geq r_{min}$, then the network is connected (covered) asymptotically in $L_2$ for all $r \geq r_{min}\sqrt{2}$.

*Proof:* The proof is by contradiction. Suppose that, for a given failure configuration, the network is asymptotically connected in $L_\infty$ for all $r \geq r_{min}$ but is not asymptotically connected for all $r \geq r_{min}\sqrt{2}$ in $L_2$. Observe that it is possible to circumscribe a $L_\infty$ neighborhood of range $r$ by a $L_2$ neighborhood of range $r\sqrt{2}$ (Fig. 10). Hence the nodes in an $L_2$ network of transmission range $r\sqrt{2}$ can be made to simulate the operation of nodes in a $L_\infty$ network with range $r$ (as the $L_\infty$ neigborhood is fully contained within the $L_2$ neighborhood). This implies that if the $L_\infty$ network of range $r$ is connected (covered), so must be the $L_2$ network of range $r\sqrt{2}$. If there is some $r \geq r_{min}$ for which the $L_\infty$ network of range $r$ is connected (covered) asymptotically, but the $L_2$ network of range $r\sqrt{2}$ is not, we obtain a contradiction, as connectedness (coverage) of the $L_\infty$ network would imply connectedness (coverage) of the $L_2$ network. ■

*LEMMA 15:* If the network is asymptotically disconnected (not covered) in $L_\infty$ for all $r \leq r_{min}$, then the network is disconnected (not covered) asymptotically in $L_2$ for all $r \leq r_{min}$.

*Proof:* The proof is by contradiction. Consider a failure configuration such that the network is asymptotically disconnected (not covered) in $L_\infty$ for range $r$, but is not disconnected (not covered) in $L_2$ for range $r$. Observe that an $L_\infty$ neighborhood of transmission range $r$ circumscribes an $L_2$ neighborhood of range $r$ (Fig. 10). Thus, for any given random failure configuration, if the $L_2$ network of range $r$ were connected (covered), so would be the $L_\infty$ network of radius $r$, as we could simply make the nodes in the $L_\infty$ network simulate the behavior of nodes in the $L_2$ network, and obtain connectedness (coverage). Hence, if the $L_2$ network of range $r \leq r_{min}$ is not asymptotically disconnected (not covered), the $L_\infty$ network of range $r \leq r_{min}$ must also not be disconnected (not covered). This yields a contradiction. ■

## XIX. Non-Toroidal Networks

We have made the assumption that the network is toroidal, so as to avoid edge effects. However, we can see that the degree of any node at the outermost edge is no more than $d$, and at least $\frac{d}{4}$ (where $d$ is the uniform degree that each node would have in the toroidal case). Thus, the necessary condition would continue to hold as is (since some nodes having a lesser degree can only increase the probability of disconnection). The construction used to prove the sufficient condition also continues to hold as is, since all full-cells in the tiling will have at least one active node each, and even if there are regions at the fringes left-over, they will still fall within range of some active node in the nearest full tile (due to the chosen dimensions of the cells). Thus, the results are not affected. A similar argument leads to the conclusion that the coverage results are not affected.

## XX. Discussion

An interesting observation is that the form of the results for Byzantine failures is very similar to the results for crash-stop failures/connectivity. For Byzantine failures, we have obtained that the critical node degree for grid networks is $\Theta(d_{min} + \frac{\ln n}{\ln \frac{1}{2p} + \ln \frac{1}{2(1-p)}})$, which may be re-stated as $\Theta(d_{min} + \frac{\ln n}{D(Q_{\frac{1}{2}}||P)})$ where $Q_{\frac{1}{2}}$ denotes the $Bernoulli(\frac{1}{2})$ distribution, $P$ denotes the $Bernoulli(p)$ distribution, and $D(Q||P)$ denotes the *relative entropy* (or Kullback-Leibler distance) between distributions $Q$ and $P$. Similarly, the node degree for crash-stop failures/connectivity is $\Theta(d_{min} + \frac{\ln n}{\ln \frac{1}{p}})$, and may be viewed as as $\Theta(d_{min} + \frac{\ln n}{\lim_{q \to 1} D(Q||P)})$, where $Q$ is the $Bernoulli(q)$ distribution, and $P$ is the $Bernoulli(p)$ distribution.

Recall that we derive the necessary condition from isolated failure events, and this is found to match the sufficient condition within a constant factor. Thus, possibly failure events involving isolated nodes not receiving correct broadcast may be the dominant failure events [4].

Focusing on these isolated failure events, the obtained expressions for node degree can be explained in the light of Sanov's Theorem [10]. As per Sanov's Theorem, the probability of occurrence of the event-set $\mathcal{E} =$ $\{$ half or more neighbors faulty$\}$ is dominated by the probability of the event in $\mathcal{E}$ closest in relative entropy to the governing fault distribution $P$. Since we are considering the regime $p < \frac{1}{2}$, the closest event is that of exactly half the neighbors faulty, corresponding to $Q_{\frac{1}{2}}$. In light of this, the critical degree expression for Byzantine failures is quite intuitive. One can similarly explain the crash-stop results.

The necessary and sufficient condition for connectivity in a sensor network where nodes sleep with probability $p$ was shown in [17] to be $\Theta(\frac{\ln(n(1-p))}{1-p})$ (when expressed in our notation) for the case of a randomly deployed network. This problem is equivalent to that of crash-stop failures in random networks. Our sufficient condition for

[4]Note that in [15], it was found that the primary disconnection events in non-faulty *random* networks are those involving single isolated nodes.

random networks with Byzantine failure probability $p < \frac{1}{2}$ is $O(\frac{\ln n}{\frac{1}{2}-p+\frac{1}{2}\ln\frac{1}{2(1-p)}})$. There is a similarity of form in the two results, and one may interpret the critical node degree as being $O(\max\{\ln n(1-p), \frac{\ln n(1-p)}{D(Q||P)}\})$ where $q = 1$ for the sleeping/crash-stop case in [17], and $q = \frac{1}{2}$ for the Byzantine failure case.

Also note that both our grid network and random network results (for Byzantine failure) have similar structural form, involving a minimum term required for connectivity without disruptive (Byzantine) behavior, and a second term required to ensure broadcast even in presence of failure.

Additionally, it is evident that the expressions for the grid network and random network diverge when $p \to 0$, but are otherwise within a constant factor of each other (for $p$ bounded away from 0). This difference is quite intuitive. In a grid network, as failure probability $p \to 0$, the network tends towards a deterministic topology, whereas in a random network, if failure or sleep probability $p \to 0$, the network can only tend towards a denser but still random network. Thus, at small values of $p$, a very small degree will suffice for a grid network, but may not for a random network. At larger $p$ values, the grid network exhibits increasing randomness and begins to resemble a network with random deployment. Thus, one may see that the two expressions are within a small range of each other when $p$ is large (given sufficiently large $n$), but diverge as $p \to 0$.

## XXI. Conclusions

We considered the problem of reliable broadcast in wireless networks with permanent probabilistic Byzantine failures, and obtained tight bounds for asymptotic achievability of broadcast in grid and random deployments. We also have results for crash-stop failure that are more accurate than earlier known results for this latter case.

## XXII. Acknowledgement

We acknowledge an anonymous reviewer of a prior manuscript version whose remarks suggesting the extensibility of our grid network sufficiency result to other network models motivated us to work out the sufficient condition for random networks described in Section X.

## References

[1] S. Shakkottai, R. Srikant, and N. Shroff, "Unreliable sensor grids: Coverage, connectivity, and diameter," in *Proc. of Infocom 2003*, 2003.

[2] E. Kreyszig, *Advanced Engineering Mathematics*, 7th ed. John Wiley & Sons, 1993.

[3] C.-Y. Koo, V. Bhandari, J. Katz, and N. H. Vaidya, "Reliable broadcast in radio networks: The bounded collision case," in *Proceedings of ACM PODC 2006*, 2006.

[4] C.-Y. Koo, "Broadcast in radio networks tolerating byzantine adversarial behavior," in *PODC '04: Proceedings of the twenty-third annual ACM symposium on Principles of distributed computing*. ACM Press, 2004, pp. 275–282.

[5] V. Bhandari and N. H. Vaidya, "On reliable broadcast in a radio network," in *PODC '05: Proceedings of the twenty-fourth annual ACM SIGACT-SIGOPS symposium on Principles of distributed computing*. ACM Press, 2005, pp. 138–147.

[6] G. B. Thomas, Jr. and R. L. Finney, *Calculus and Analytic Geometry*. Addison-Wesley Publishing Company, 1992.

[7] K. Jogdeo and S. M. Samuels, "Monotone convergence of binomial probabilities and a generalization of ramanujan's equation," *The Annals of Mathematical Statistics*, vol. 39, no. 4, pp. 1191–1195, August 1968.

[8] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *Journal of the American Statistical Association*, vol. 58, no. 301, pp. 13–30, Mar. 1963.

[9] M. Mitzenmacher and E. Upfal, *Probability and computing*. Cambridge University Press, 2005.

[10] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Wiley & Sons, Inc., 1991.

[11] E. Kranakis, D. Krizanc, and A. Pelc, "Fault-tolerant broadcasting in radio networks," *J. Algorithms*, vol. 39, no. 1, pp. 47–67, 2001.

[12] A. Pelc and D. Peleg, "Feasibility and complexity of broadcasting with random transmission failures," in *PODC '05: Proceedings of the twenty-fourth annual ACM SIGACT-SIGOPS symposium on Principles of distributed computing*, 2005, pp. 334–341.

[13] V. Bhandari and N. H. Vaidya, "On reliable broadcast in a radio network: A simplified characterization," Technical Report, CSL, UIUC, May 2005.

[14] A. Pelc and D. Peleg, "Broadcasting with locally bounded byzantine faults," *Information Processing Letters*, vol. 93, no. 3, pp. 109–115, Feb 2005.

[15] P. Gupta and P. R. Kumar, "Critical power for asymptotic connectivity in wireless networks," in *Stochastic Analysis, Control, Optimization and Applications: A Volume in Honor of W.H. Fleming*, W. M. McEneany, G. Yin, and Q. Zhang, Eds. Boston: Birkhauser, 1998, pp. 547–566.

[16] F. Xue and P. R. Kumar, "The number of neighbors needed for connectivity of wireless networks," *Wirel. Netw.*, vol. 10, no. 2, pp. 169–181, 2004.

[17] D. Kim, C. Hsin, and M. Liu, "Asymptotic connectivity of low duty-cycled wireless sensor networks," in *Proc. MILCOM*, 2005.

[18] S. Kumar, T. H. Lai, and J. Balogh, "On k-coverage in a mostly sleeping sensor network," in *MobiCom '04: Proceedings of the 10th annual international conference on Mobile computing and networking*. New York, NY, USA: ACM Press, 2004, pp. 144–158.

[19] S. Shakkottai, R. Srikant, and N. Shroff, "Correction to unreliable sensor grids: Coverage, connectivity, and diameter," Personal Communication, 2005.

[20] X. Liu and R. Srikant, "An information-theoretic view of connectivity in wireless sensor networks," in *the first IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON)*. Santa Clara, CA: IEEE, Oct. 4-7 2004.