

JAMMING DUST: A LOW-POWER DISTRIBUTED JAMMER NETWORK

Hong Huang, Nihal Ahmed and Santhosh Pulluru1
Klipsch School of Electrical and Computer Engineering
New Mexico State University
Las Cruces, NM 88003

ABSTRACT

In this paper, leveraging recent advancement in MEMS and NANO technology, we introduce a new type of denial of service attack to wireless networks: low power, distributed jammer network (DJN). Jamming attack on wireless networks was traditionally treated from the perspective of individual jammers. We advocate an approach from a networked perspective, and using this networked approach we show that some interesting results can be obtained. In the paper, we demonstrate that DJN can cause a phase transition in the performance of the target network. We employ Percolation Theory to explain such phase transition, analyzing the impact of DJN on the connectivity of the target network, and providing lower and upper bounds for percolation of the target network to occur in the presence of DJN. We also provide scaling relationship of the node intensity and the number of jammers with power constraints.

1. INTRODUCTION

Radio technology has evolved a great deal since its invention in the late nineteenth century. One aspect of this evolution is the form factor, which undergoes a transition from vacuum tube radio, transistor radio, micro sensor radio, to future’s nanotube radio, as shown in Figure 1. Such technological advancement can bring radical changes in how we design and use radio devices. In this paper we introduce an example of such new designs: *Distributed jammer network* (DJN). A DJN is composed of a large number of tiny, low-power jammers, which are distributed inside a target network and emit radio energy to disrupt its communications. Recent advancement in MEMS and NANO technology [24][25] makes it possible to make jammers sufficiently small that a DJN can take the form of a dust suspending in the air, thus the name *Jamming Dust* (a takeoff from “Smart Dust” composed of micro sensors [26]). Miniaturization of jammers should be less challenging than that of wireless sensors since jammers just emit noise signal without requiring complex modulation, filtering and other signal processing functions. Therefore, new miniature devices such as nanotube radio may find their first application in jamming dust.

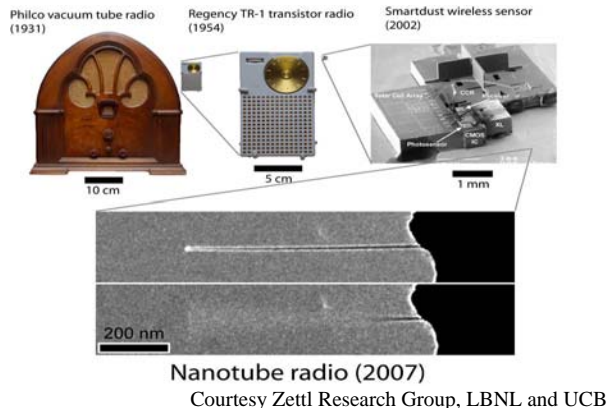


Figure 1: Evolution of radio technology.

DJN, in a sense, forms a mirror-image to distributed wireless network (DWN), e.g. distributed sensor network (DSN), for DWN communicates information, whereas DJN disrupts such communications. The *importance* of DJN can be seen in the following application scenarios.

Military/security applications: DJN can be deployed to form a low-power (possibly air-born) jamming dust that are more attractive than traditionally high-power jammers because of its low deployment profile (the naked eye can not see the nanotube radios) and its much reduced effect on self-interference. The importance of such self-interference-free jamming has been demonstrated in the second Iraq war as reported in *Washington Post* [29]. Future warfare will increasingly depend on radio signal for command and control, weapons guidance, GPS navigation, etc. DJN can play an important role in future net-centric warfare.

Civilian applications: DJN can have many civilian usages as well. Although owning or using jammers is illegal in USA, and is tantamount to property theft (the property being the government owned frequency); it is legal and put into sensible use in some other countries [27]. For example, in France, jammers are used in restaurants or theaters to silence obnoxious cell phone users. In Italy, jammers are used in exam rooms to frustrate potential cheaters. In Mexico, jammers are deployed in churches to prevent disruption of sacred services. In such cases, deploying a low-power DJN instead of high-power ones is clearly preferable due to

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE 2010	2. REPORT TYPE	3. DATES COVERED 00-00-2010 to 00-00-2010	
4. TITLE AND SUBTITLE Jamming Dust: A Low-Power Distributed Jammer Network		5a. CONTRACT NUMBER	
		5b. GRANT NUMBER	
		5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)		5d. PROJECT NUMBER	
		5e. TASK NUMBER	
		5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) New Mexico State University, Klipsch School of Electrical and Computer Engineering, Las Cruces, NM, 88003		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)	
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited			
13. SUPPLEMENTARY NOTES To be presented at The 27th Army Science Conference (ASC), sponsored by the Assistant Secretary of the Army (Acquisition, Logistics and Technology), will be held at the JW Marriott Grande Lakes, Orlando, Florida, November 29 - December 2, 2010.			
14. ABSTRACT In this paper, leveraging recent advancement in MEMS and NANO technology, we introduce a new type of denial of service attack to wireless networks: low power, distributed jammer network (DJN). Jamming attack on wireless networks was traditionally treated from the perspective of individual jammers. We advocate an approach from a networked perspective, and using this networked approach we show that some interesting results can be obtained. In the paper, we demonstrate that DJN can cause a phase transition in the performance of the target network. We employ Percolation Theory to explain such phase transition, analyzing the impact of DJN on the connectivity of the target network, and providing lower and upper bounds for percolation of the target network to occur in the presence of DJN. We also provide scaling relationship of the node intensity and the number of jammers with power constraints.			
15. SUBJECT TERMS			
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified	
			18. NUMBER OF PAGES 8
			19a. NAME OF RESPONSIBLE PERSON

health concerns. In fact in today’s world of wireless device proliferation (cell phone, WiFi, WiMax, and Bluetooth devices, wireless game console, sensor networks, etc.), DJN can spontaneously form in the crowded ISM bands since devices speaking different MAC protocols are essentially jammers to one another within the same frequency band. This kind of jamming may already become a reality as indicated by the reported incident of possible Xbox game console interfering with WiFi [28].

DJN is different from traditional jammers [1] used by the military, which are typically located outside the target network and cause inference by beaming high-power radio signal over long distance using directional antenna. DJN is also different from the kind of in-network jamming studied recently, which uses jammers of similar size as DWN devices whereas DJN can use much smaller, lower-power devices than DWN nodes. More importantly, existing works on jamming are mostly from the perspective of individual jammers. DARPA realized the importance of DJN in future battlefields and founded the WolfPack program [16], which is essentially a high-power, large-node version of DJN but of which not much technical detail is available in the public. Despite DJN’s importance, not much work on the subject has emerged in the research community. This paper intends to advocate *studying jamming from a network perspective*, rather than from the perspective of individual jammers. That is, we ask the question: What is the impact of *a network of jammers*. A large number of jammers have a network effect which can not be fully accounted by that of individual jammers. The network approach is conducive to broaden the problem scope considerably and increases the likelihood of obtaining important/interesting results.

The *advantages* of DJN are reminiscent of those of DSN. First, DJN is robust because it is composed of a large number of devices with ample redundancy. Second, DJN nodes emit low power, which is advantageous because of health, self-interference concerns. Third, DJN is hard to detect because of nodes’ small size (the naked eye can not even see a nanotube radio) and low power emission. Forth, DJN provides extended coverage with high energy efficiency. In Section 4, we will show that using the same total amount of power, a DJN of n nodes covers an effective area $n^{1-2/\alpha}$ times larger than that of a single jammer, where α is the path loss exponent with a typical value of 4. So the typical power efficiency gain of DJN is $n^{1/2}$, which is unbounded as n goes to infinity.

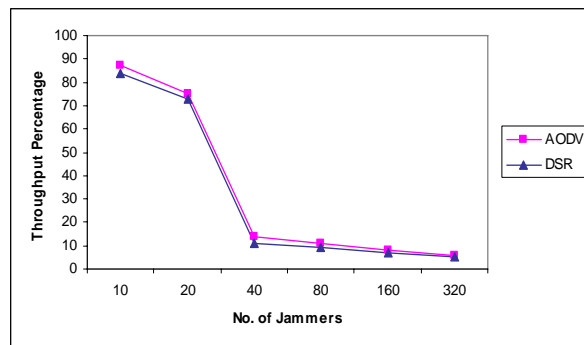


Figure 2: The jamming performance as a function of number of jammers

To provide empirical evidence and to test the hypothesis that DJN provides superior performance to traditional jammers, we show some simulation results in Figure 2. The simulation is performed using Qualnet [30], with the following setup: The target network (DWN) has 100 nodes deployed in an area of 1000 by 1000 meters, with half of the nodes having CBR UDP sessions with the other half of the nodes. The MAC protocol used is IEEE802.11, and two routing protocols are used: AODV and DSR. We start by deploying 10 jammers with the same transmitting power as the target device (15 dbm). Then we increase the number of jammers while reducing jamming power, holding the total power consumed by the jammers constant. The performance metric is the ratio of DWN throughput with jamming versus that without jamming. From Figure 2, we can see a *phase transition* occurring at roughly 20 jammers, where throughput ratio drops precipitously. Given that the total power consumption is constant, the benefit of using a large number of low-power jammers (i.e., DJN) is evident.

The *contributions* of the paper are the following: 1) We identify an effective jamming approach: DJN consisting of large number of low-power jammers that have important military and civilian applications. 2) We report a phase transition of jamming performance. We explain the phase transition by using Percolation Theory. We derive bounds on critical conditions, which is practically useful in selecting DJN parameters to force the phase transition to occur. 3) We provide a scaling analysis of the node intensity and the number of jammers with power constraints.

Much previous work on jamming focuses on the physical layer [1]. Recently, papers on jamming in wireless networks, especially wireless sensor network due to its vulnerability from field deployment, began to appear [2-15]. The fundamental difference between our work and existing work is that we consider the problem

from the perspective of a network of jammers, instead of that of individual jammers as typical with previous work.

The paper is organized as the following: In Section 2, we first state our assumptions, and then describe the modeling of network connectivity in the absence of DJN using Percolation Theory. In Section 3, we explain the phase transition in DWN performance caused by DJN by the method of Percolation Theory. We provide a scaling analysis of DJN parameters in Section 4. We conclude in Section 5.

2 ASSUMPTIONS AND PERCOLATION OF DWN IN THE ABSENCE OF DJN

In the following, we make the following *assumptions*. We assume that DWN and DJN are deployed in a 2-D surface, with the radio energy spreading out in the 3-D space; and that radio antenna of both DWN and DJN are omnidirectional. We assume node deployment in DJN and DWN are uniformly random, forming Poisson point processes [19], which is justifiable for applications such as jamming dust in battlefields or among random crowds. We assume no knowledge about the DWN device type and network protocols, which is true in adversarial scenarios where the enemy device type or the enemy identity itself can hardly to be known a priori, e.g., in terrorist attacks. In addition, DWN packets can be encrypted to reveal as little information as possible. Thus methods [4][5][15] that take advantage of the knowledge about network protocol are not applicable here.

As for *jamming mechanism*, we assume jammers in DJN are reactive jammers, which are among the most effective jamming methods [9]. A reactive jammer senses a wide frequency range and jams the channel on which it detects radio activity. Recent advancement in software defined radio and UWB radio provides technology to make such jammers. The jammer has two parameters: period P and duty cycle D . That is: after sensing a busy channel, a jammer becomes active in D percentage of time in a period of P seconds after which the jammer restarts sensing again. Since the slot time represents an elementary transmission unit, P can be chosen to be on the same order of magnitude of a slot time in DWN, which is roughly $20 \mu\text{s}$ in IEEE 802.11 and 802.15. Since jamming stops once the channel is sensed to be idle, such reactive jammer automatically adapts to DWN packet size: large DWN packet size causes the jammer jamming for a longer duration whereas small DWN packet size causes the jammer jamming for a shorter duration, but both with constant duty cycle D . D should be selected to be no less than the redundancy provided by the DWN error-correcting code; so that the intensity of jamming is

just enough to ensure that every DWN packet is destroyed without wasting unnecessary energy. In typical military applications, $D = 30\%$ is considered adequate [1]. Jammer parameter selections, of course, should depend on the particular application in question, and here we assume we can make adequate selections. If DWN does not use error-correcting code, the jammer jams for one slot time, ignores the ensuing period of busy channel (letting the current damaged packet to finish), and begins to jam the channel again when the channel returns busy after an idle period (e.g., inter-frame time in IEEE802.11). Such jamming can achieve very high jamming gain, i.e., expending a small amount of jamming energy to waste a large amount of DWN transmission energy.

We assume that transmission powers of both DWN and DJN radios are adaptable up to their respective maximum transmitting powers. If the maximum transmitting powers of DWN and DJN nodes are the same, we consider a DWN receiver is jammed if there exists a DJN jammer that is closer to the receiver than the DWN transmitter. For in such case the jammer can always adapt its power to overpower the transmitter however the transmitter adapts its own power. If the transmitting powers of DWN and DJN nodes are different, we properly scale the distances, details of which will be given later.

Next we describe stochastic modeling of DWN/DJN. We assume that average numbers of nodes per unit area in DWN and DJN are λ_1 and λ_2 , respectively, and the maximum radio range in DWN is r_1 (corresponding to its maximum transmission power). A suitable stochastic model for describing connectivity in DWN is the *Poisson Boolean model* $B(\lambda_1, r_1)$ [19], defined below.

DEFINITION 1. In a Poisson Boolean model $B(\lambda_1, r_1)$, nodes are distributed in a 2-D space R^2 according to a Poisson point process with intensity λ_1 , which is the average number of nodes per unit area. Specifically, the probability that there are k nodes in an area A is given by:

$$P(N_A = k) = e^{-\lambda_1 A} \frac{(\lambda_1 A)^k}{k!} \quad (1)$$

Two nodes are considered being connected if the distance between them is no larger than the maximum radio range r_1 .

We can visualize that balls of radius $r_1/2$, whose centers corresponds to node locations, are scattered in space, and an edge is formed if two balls touch each other. The sets of nodes and edges in DWN, V_1 and E_1 , constitute a graph $G_1(V_1, E_1)$. Connected components of G_1 are called clusters. Clusters can be finite or infinite in the infinite 2-D space. The network is composed of a

number of clusters, which by definition have no connection between them (an isolated node is considered as a one-node cluster). *The key question relevant to network connectivity* is whether there exists an infinite cluster, so called a giant cluster that includes a large proportion of nodes in the network. We will address this question later in the section.

DJN is described by a Jamming process $J(\lambda_2, \beta)$, defined below.

DEFINITION 2. A Jamming process $J(\lambda_2, \beta)$ consists of a Poisson point process of jammer intensity λ_2 with a parameter β defined as such that a DWN receiver is considered jammed if a jammer is within a distance of $\beta\nu$, where ν is the distance between the transmitter and receiver in DWN.

The parameter β is designed to allow flexibility to allow devices in DJN and DWN to have different transmitting power levels. The presence of DJN causes some links between nodes of DWN to break. We require bi-directional links for DWN. Thus, if a jammer is within a distance $\beta\nu$ to either of the two DWN nodes that had a link before, the link is now considered to be broken.

Now let us consider percolation of DWN in the absence of DJN. Consider a DWN described by a Poisson Boolean process $B(\lambda_1, r_1)$ in a infinite 2-D space, and randomly select a node. We can set the origin of the coordinate system at this node without loss of generality because $B(\lambda_1, r_1)$ has translational invariance. Let $C_1(0)$ be the cluster that the origin is connected to, the size of which, $|C_1(0)|$, is a parameter of interest. If $|C_1(0)|$ is 1, the origin is isolated. If $|C_1(0)|$ is finite, the origin has poor connectivity (since the total number of nodes is infinite). If $|C_1(0)|$ is infinite, the origin has reasonably good connectivity. We can parameterize the network connectivity by the *percolation* probability $\theta_1(\lambda_1)$, which is defined as probability that $|C_1(0)|$ is infinite at a given λ_1 . According to the theory of continuum percolation [19], there is a critical intensity $\lambda_{1,c}$, such that,

$$\theta(\lambda_1) \begin{cases} = 0 & \text{if } \lambda_1 < \lambda_{1,c} \\ > 0 & \text{if } \lambda_1 > \lambda_{1,c} \end{cases} \quad (2)$$

And

$$P(\exists C_1 : |C_1| = \infty) \begin{cases} = 0 & \text{if } \lambda_1 < \lambda_{1,c} \\ = 1 & \text{if } \lambda_1 > \lambda_{1,c} \end{cases} \quad (3)$$

In other words, the network behaves in two regimes: *Sub-critical regime* where $\lambda_1 < \lambda_{1,c}$, all the clusters are finite almost surely, i.e., nodes in the network are essentially isolated. *Super-critical regime* where $\lambda_1 > \lambda_{1,c}$,

there exists a infinite cluster almost surely, i.e., nodes in the network are reasonably well connected.

At the critical point where $\lambda_1 = \lambda_{1,c}$, there exists no infinite cluster almost surely in a 2-D space, i.e., it belongs to the sub-critical regime, which is not always true in other dimensions. There is no known analytical expression for $\lambda_{1,c}$, whose approximate value can be obtained by numerical simulation.

In a number of previous works [20][21], continuum percolation has been applied to study the connectivity of wireless networks with the assumption that the network is considered connected if it is in the super-critical regime.

3. PERCOLATION OF DWN IN THE PRESENCE OF DJN

Now let us consider DWN in the presence of DJN, in other words, a joint process of $B(\lambda_1, r_1)$ and $J(\lambda_2, \beta)$. We argue that the occurrence of percolation in DWN implies a *phase transition* in network performance since the network goes from a disconnected state to a connected one. For jamming, we are interested in the reverse direction of the transition, but in the following we describe it in the manner of the forward direction (from the disconnected state to the connected state) in accordance to the standard treatment of percolation theory. *The key questions* we consider here are: 1) whether percolation in DWN still occurs in the presence of DJN; and 2) if yes, how the percolation of DWN is impacted by the presence of DJN. The answer to the first question is affirmative as long as certain condition on $J(\lambda_2, \beta)$ is satisfied. The answer to the second question is that the presence of DJN pushes up the value of $\lambda_{1,c}$, making it more difficult for DWN to percolate. To obtain those answers, we adopt a constructive approach similar to the Penrose's approach [19], and not only provide the existence proof but also bounds on the critical intensity. Our results are summarized in Proposition 1 below.

PROPOSITION 1. In the joint $B(\lambda_1, r_1)$ and $J(\lambda_2, \beta)$ process, the sufficient condition for percolation to occur is given by:

$$\lambda_2 \beta^2 r_1^2 \leq 0.548 \quad (5)$$

The precise meaning for percolation to occur is: there exists a critical intensity $\lambda_{1,c} > 0$, above which the probability of the existence of infinite cluster is strictly positive,

PROOF. We proceed by deriving lower and upper bounds on $\lambda_{1,c}$. Lower bound tells us the necessary condition in terms of DJN parameters for percolation to

occur. Upper bound tells us the sufficient condition for percolation to occur, i.e., equation (5).

LOWER BOUND. We first provide an overview: In Penrose's approach, the $B(\lambda_I, r_I)$ process is linked to a suitable branching process. Due to the translational invariance of $B(\lambda_I, r_I)$, we need only to study the behavior of the origin. In the branching process, origin is the root and it gives birth to children, which in turn give birth to their own children. A parent is said to have a child if the distance between parent and child is within radio range r_I , with proper accounting for the overlap between parent and children. Percolation occurs when the offspring of the branching process is infinite. Detailed analysis is as follows.

In $B(\lambda_I, r_I)$, let x_k indicate a point of k th generation. Let $S(x_k, r_I)$ be a ball centered at x_k with a radius r_I . Consider the children of a point of k th generation, x_k , which is located at a distance u away from its own parent at $(k-1)$ th generation, x_{k-1} . These children of $(k+1)$ th generation are located in the following region:

$$A_{k+1}^B = \{S(x_k, r_I) \setminus S(x_{k-1}, r_I)\} \cap \{y : |y - x_k| \leq r\}$$

Referring to Figure 3, let $g^B(v/u)$ be the length of the curve given by:

$$\{S(x_k, r_I) \setminus S(x_{k-1}, r_I)\} \cap \{y : |y - x_k| = v\}$$

Straightforward trigonometry gives:

$$g^B(v|u) = \begin{cases} 2v \cos^{-1} \left(\frac{r_I^2 - u^2 - v^2}{2uv} \right) & \text{if } r_I - u < v < r_I \\ 0 & \text{if } 0 < v < r_I - u \end{cases} \quad (6)$$

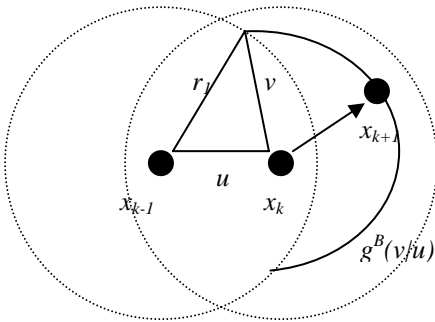


Figure 3: Illustration for computing $g^B(v/u)$

According to the definition of the $B(\lambda_I, r_I)$ process, the expected number of children of x_k is given by:

$$N_{k+1}^B = \lambda_1 A_{k+1}^B = \lambda_1 \int_0^{r_I} g^B(v|u) dv$$

Now consider the joint $B(\lambda_I, r_I)$ and $J(\lambda_2, \beta)$ process. In such process a children can communicate with its parent only if no jammer is located within βv distance of the parent, and vice versa. So we require that no jammer exists in the region $S(x_k, \beta v) \cap S(x_{k+1}, \beta v)$, which we call the effective jamming area A_j , and this area can be computed as:

$$\pi(\beta v)^2 + \int_0^v g^B(w|v) dw \equiv \gamma(\beta v)^2 \equiv A_j$$

In the above γ is a constant reflecting the geometry of jamming area. We can obtain approximate value of γ through numerical integration, which gives: $\gamma \approx 5.055$. So the probability that there is no jammer in A_j is:

$$e^{-\lambda_2 A_j} = e^{-\lambda_2 \gamma \beta^2 v^2}$$

Now let us define a new version of $g^B(v/u)$ that counts only the length free of jamming in A_j :

$$g(v|u) = e^{-\lambda_2 \gamma \beta^2 v^2} g^B(v|u) \quad (7)$$

Because $B(\lambda_I, r_I)$ and $J(\lambda_2, \beta)$ are independent processes, the expected number of children of x_k in the joint process, with the effect of jamming accounted by (7), is given by:

$$N_{k+1} = \lambda_1 A_{k+1} = \lambda_1 \int_0^{r_I} g(v|u) dv$$

In the same manner, the expected number of grand children of x_k is given by:

$$N_{k+2} = \lambda_1 \int_0^{r_I} \left(\lambda_1 \int_0^{r_I} g(v|w) dv \right) g(w|u) dw$$

Let us define:

$$g_1(v|u) = \int_0^{r_I} g(v|w) g(w|u) dw$$

Then we have:

$$N_{k+2} = \lambda_1^2 \int_0^{r_I} g_1(v|u) dv$$

Now let us define recursively:

$$g_n(v|u) = \int_0^{r_1} g_{n-1}(v|w)g(w|u)dw$$

Then the expected number of n th generation offspring from an ancestor which has a distance u from its own parent is given by:

$$N_n^u = \lambda_1^n \int_0^{r_1} g_n(v|u)dv$$

We can recast the above equation in the form of Hilbert-Schmidt operators [23]. Let us define:

$$T_f(u) = \int_0^{r_1} f(u)g(v|u)dv \quad (8)$$

Then we have:

$$N_n^u = \lambda_1^n T_1^n(u)$$

And the total number of offspring from an ancestor which has a distance u from its own parent is given by:

$$N^u = \sum_{n=1}^{\infty} N_n^u = \sum_{n=1}^{\infty} \lambda_1^n T_1^n(u) \quad (9)$$

The above sum is guaranteed to converge if λ_1 is smaller than $|T_1|^{-1}$, where $|T_1|$ is the operator norm of T_1 , which in our case is equal to α , the largest eigenvalue of T_1 (details see [34][19]). So $\lambda_{1,c}$ is lower-bounded by α^{-1} , which can be computed through Monte-Carlo simulation. The results from numerical simulation is reported in Figure 5, where we plot the lower bound of $\lambda_{1,c}$ (indicated as $LB(\mu)$) as function of $\mu \equiv \lambda_2 \gamma \beta^2$, with $\lambda_1 = 2$ to conform with the results in [19]. Recall that γ is a constant with an approximate value of 5.055.

UPPER BOUND. To obtain upper bound, we link the joint $B(\lambda_1, r_1)$ and $J(\lambda_2, \beta)$ process to site percolation in a triangular lattice with edge length of $r_1/2$. Each site is defined as the “flower” centered at a vertex of the lattice. The flower is bounded by six circular arcs, each centered at a midpoint of one of six edges adjacent to the vertex and having a radius of $r_1/2$. A site is called occupied if there exists a point from $B(\lambda_1, r_1)$ in the associated flower. Because of the geometric construction, if two adjacent flowers are occupied by two points in $B(\lambda_1, r_1)$, then the distance between the two points is no more than r_1 . Therefore, in the absence of DJN, occurrence of site

percolation in the triangle lattice translates into percolation in $B(\lambda_1, r_1)$. For percolation in a triangle lattice to occur, the site occupancy probability must be no less than a critical value p_c (equal to 0.5 in 2-D lattice). In $B(\lambda_1, r_1)$, the site (flower) occupancy probability p_f can be computed as:

$$p_f = 1 - e^{-\lambda_1 A_f} \quad (10)$$

where A_f is the area of flower and is approximately $0.206 r_1^2$.

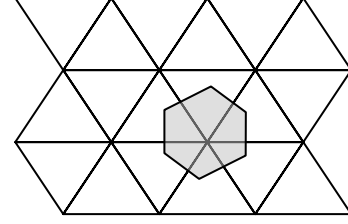


Figure 4: Illustration of the linkage to the site percolation in triangular lattice for computing the upper bound on critical intensity $\lambda_{1,c}$. The “flower” is the shaded area.

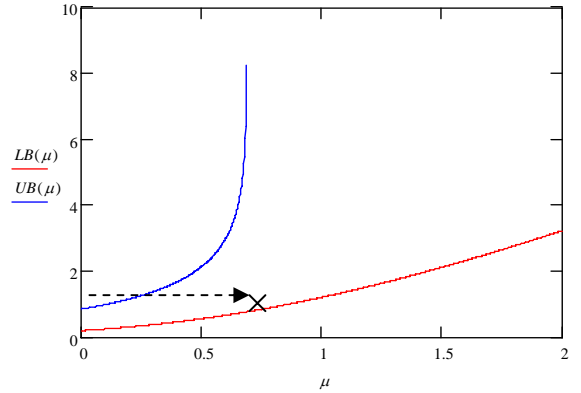


Figure 5: Lower and upper bounds, $LB(\mu)$ and $UB(\mu)$, on critical intensity $\lambda_{1,c}$ as a function of $\mu \equiv \lambda_2 \gamma \beta^2$, the arrow indicating the movement toward phase transition point indicated by the cross.

Now let us take jamming into account. In the joint $B(\lambda_1, r_1)$ and $J(\lambda_2, \beta)$ process, two nodes, x_1 and x_2 , separated by a distance v , can communicate with each other only if no jammer is located within βv distance of each other. This is guaranteed if no jammer exists in the region $A_j = S(x_{1,f}, \beta r_1) \cap S(x_{2,f}, \beta r_1)$, where $x_{1,f}$ and $x_{2,f}$ are the centers of flowers associated with x_1 and x_2 and $S(x, r)$ is a ball centered at x with a radius r . A_j can be obtained by simple numerical integration, with an approximate

value of $1.264 \beta^2 r_l^2$. The probability p_j of no jammers in A_j is given by:

$$p_j = e^{-\lambda_2 A_j} \quad (11)$$

In the joint $B(\lambda_l, r_l)$ and $J(\lambda_2, \beta)$ process, the probability that a site is occupied is $p_f p_j$ since it requires two events: 1) the site is occupied in DWN (with probability p_f); and 2) the site is not jammed by DJN (with probability p_j). Percolation occurs if the site occupation probability is no less than the critical site occupation probability, i.e.,

$$p_f p_j = \left(1 - e^{-\lambda_l A_f}\right) e^{-\lambda_2 A_j} \geq p_c = 0.5$$

Or

$$\lambda_l \leq -\frac{\ln\left(1 - 0.5 e^{\lambda_2 A_j}\right)}{A_f} \approx -\frac{\ln\left(1 - 0.5 e^{1.264 \lambda_2 \beta^2 r_l^2}\right)}{0.206 r_l^2} \quad (12)$$

The results from numerical simulation is again reported in Figure 5, where we plot the upper bound of $\lambda_{l,c}$ (indicated as $UB(\mu)$) as function of $\mu \equiv \lambda_2 \beta^2$, again with $\lambda_l = 2$ to conform with results in [19]. Recall that γ is a constant with an approximate value of 5.055.

The upper bound abruptly ends around $\mu = 0.7$, at which point p_j becomes larger than p_c , i.e., the probability of the flower being jammed is greater than the critical site occupation probability. On the other hand, percolation can be guaranteed (upper bound exists) as long as we have:

$$p_j \approx e^{1.264 \lambda_2 \beta^2 r_l^2} \leq p_c = 0.5 \quad (13)$$

It is straightforward to invert equation (13) to obtain equation (5). Existence of upper bound guarantees the occurrence of percolation at a λ_l somewhere below the upper bound. The termination of the upper bound curve around $\mu = 0.7$ in Figure 5 is not an indication that percolation in DWN can not occur beyond this point, but rather is an artifact of the method used. Q.E.D.

It is clear from Figure 5 that the effect of DJN is to push up the both lower and upper bounds for critical intensity of DWN. Also the effect of DJN is exerted in terms of the collective factor $\mu \equiv \lambda_2 \beta^2$ ($\mu=0$ corresponding to the absence of DJN). The sufficient condition for percolation in DWN to occur, i.e., Equation (5), also solely depends on the collective factor $\lambda_2 \beta^2 r_l^2$. This should not be surprising since $\lambda_2 \beta^2 r_l^2$ is proportional

to the number of jammers within the radio range of DWN (r_l is set to be 2 in Figure 5).

Looking from another angle, given a connected DWN with such λ_l that percolation occurs, one can always increase λ_2 and/or β so that the joint state of DWN and DJN will go under the lower bound, as shown by the arrow in Figure 5. Recall that the lower bound provides the necessary condition for percolation to occur, going under the lower bound forces the DWN become disconnected, and accordingly causing a phase transition in DWN performance.

Given the results we have derived, we are now ready to explain the phase transition shown in Figure 2. Scaling the distance unit so that the radio range is 2, we can find the operating point (λ_l, μ) through straightforward calculation once λ_2 is given. The phase transition occurs around $\lambda_2 = 0.2$, giving the operating point at $(\lambda_l, \mu) = (1, 0.707)$, shown in the Figure 2 as the point where the arrow points to. Thus phase transition occurs when the presence of DJN moves the operating point from $(1, 0)$ in the absence of jammers, where the network lies in the super-critical regime to the point $(1, 0.707)$ where the lies in the sub-critical regime, i.e., the network transitions from connected to disconnected.

4. SCALING BEHAVIOR OF PERCOLATION IN DWN IN PRESENCE OF DJN

In this section, consider the scaling behavior with respect to the node intensity and the number of jammers in the DJN with power constraints. Suppose the transmission powers of DWN and DJN devices are P_l, P_2 , respectively. We assume a standard path loss model for both DWN and DJN radios:

$$P_r = \frac{P_t}{r^\alpha}$$

In the above P_t, P_r are transmitting and received powers, respectively, and r is the distance between transmitter and receiver. We have omitted a constant antenna gain coefficient because it is irrelevant to the analysis of scaling behavior here.

Definition 2 implies that a transmitter in DWN and a jammer in DJN, at distances v and βv to a receiver in DWN, respectively, should have the same received power at the receiver, i.e.,

$$\frac{P_l}{v^\alpha} = \frac{P_2}{(\beta v)^\alpha} \quad \text{or} \quad \beta = \left(\frac{P_2}{P_l}\right)^{\frac{1}{\alpha}} \quad (14)$$

An important question to ask is: how to maximize the impact of DJN given the constraint of fixed power consumption per unit area in DJN, i.e., $\lambda_2 P_2$. We know

from the last section that DJN's impact on DWN is in terms of the collective $\lambda_2 \beta^2 r_1^2$, which using equation (14) can be written as:

$$\lambda_2 \beta^2 r_1^2 = \lambda_2 \left(\frac{r_1^\alpha P_2}{P_1} \right)^{\frac{2}{\alpha}} = \lambda_2^{1-\frac{2}{\alpha}} \left(\frac{1}{P_{1,r}} \right)^{\frac{2}{\alpha}} (\lambda_2 P_2)^{\frac{2}{\alpha}} \quad (15)$$

In the above, the last term is constant due to power constraint, $P_{1,r}$ ($=P_1/r_1^\alpha$) is minimum received power in DWN corresponding to the radio range, which again can be assumed as a constant. Therefore we can make the following statement based on equation (16).

PROPOSITION 3. Under the unit area power consumption constraint on DJN, the impact of DJN on DWN scales as $\lambda_2^{1-2/\alpha}$.

In typical radio environments, α is close to 4, so to maximize DJN impact under the unit area power constraint, the optimal strategy is to deploy lots of low power jammers rather than a few high power jammers.

5. CONCLUSION

In this paper, motivated by the advancement in radio technology, we introduce a new type of jamming—DJN, which is composed of a large number of tiny, low-power jammers. We demonstrated that DJN can cause a phase transition in target network performance even when the total jamming power is held constant. We explained the phase transition using Percolation Theory, and analyzed scaling behavior of node intensity and number of nodes in DJN. We believe approaching the problem of jamming in wireless networks from a network perspective can broaden the research scope significantly and can bring out some interesting results otherwise unattainable by focusing on individual jammers. As for future work, we think the interplay between DJN and DWN makes for intriguing problems, which cut across network layers: device placement, topology control, power control, medium access, routing, and data transport. Investigating those problems can result in deeper understanding of not only DJN but DWN as well. We believe a lot more interesting results can be obtained from this approach and are currently working in this direction.

ACKNOWLEDGMENTS

This work was supported by the ARL AHPCRC consortium under the grant W911NF-07-2-0027.

REFERENCES

[1] C. Schleher. *Electronic Warfare in the Information Age*. MA: Artech House, 1999.

[2] R. Mallik, R. Scholtz, and G. Papavassilopoulos. Analysis of an on-off jamming situation as a dynamic game. *IEEE Trans. Commun.*, vol. 48, no. 8, pp. 1360-1373, Aug. 2000.

[3] A. D. Wood and J. A. Stankovic. Denial of service in sensor networks. *IEEE Computer*, vol. 35, no. 10, pp. 54-62, 2002.

[4] R. Negi and A. Perrig. Jamming analysis of MAC protocols. *Carnegie Mellon Technical Memo*, 2003.

[5] J. Bellardo and S. Savage. 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In *Proc. of the USENIX Security Symposium*, pages 15-28, 2003.

[6] A. Wood, J. Stankovic, and S. Son. JAM: A jammed-area mapping service for sensor networks. In *Proc. of IEEE Real-Time Systems Symposium*, pages 286-297, 2003.

[7] G. Noubir and G. Lin. Low-power DoS attacks in data wireless LANs and countermeasures. *SIGMOBILE Mob. Comput. Commun. Rev.*, 7(3):29-30, 2003.

[8] J. M. McCune, E. Shi, A. Perrig and M. K. Reiter. Detection of denial-of-message attacks on sensor network broadcasts. In *Proc. IEEE Symposium on Security and Privacy*, 2005.

[9] W. Xu et al. The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. In *Proc. of ACM Int'l. Symp. Mobile Ad Hoc Net. and Comp.*, 2005, pp. 46-57.

[10] W. Xu, T. Wood, W. Trappe, and Y. Zhang. Channel surfing and spatial retreats: defenses against wireless denial of service. In *Proc. of ACM workshop on Wireless Security*, pages 80-89, 2004.

[11] M. Li, I. Koutsopoulos, and R. Poovendran. Optimal jamming attacks and network defense policies in wireless sensor networks. In *Proc. of IEEE Infocom*, May 2007.

[12] Anthony D. Wood, John A. Stankovic, and Gang Zhou. DEEJAM: defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks. In *Proc. of ACM SECON*, 2007.

[13] M. Cagalj, S. Capkun, J.-P. Hubaux. Wormhole-based anti-jamming techniques in sensor networks. *IEEE Trans. on Mobile Computing*, vol. 6, no. 1, pp. 100-114, Jan. 2007.

[14] Jerry T. Chiang and Yih-Chun Hu. Cross-layer jamming detection and mitigation in wireless broadcast networks. In *Proc. of ACM MobiCom* pages 346-349, New York, NY, USA, 2007.

[15] X. Liu, R. Rajaraman, G. Noubir, B. Thapa, C. King and E. Bayraktaroglu. On the Performance of IEEE 802.11 under Jamming. In *Proc. of IEEE Infocom*, April 2008.

[16] <http://www.darpa.mil/STO/strategic/wolfpack.html>

[17] G. R. Grimmett, *Percolation*. Springer, 1999.

[18] E. N. Gilbert. Random plane networks. *SIAM J.*, vol. 9, pp. 533-543, 1961.

[19] R. Meester and R. Roy. *Continuum percolation*. Cambridge University Press, 1996.

[20] T. K. Philips, S. S. Panwar, and A. N. Tantawi. Connectivity properties of a packet radio network model. *IEEE Trans. Inform. Theory*, vol. 35, pp. 1044-1047, Sept. 1989.

[21] O. Dousse, P. Thiran, and M. Hasler. Connectivity in ad-hoc and hybrid networks. In *Proc. IEEE Infocom*, New York, June 2002.

[22] L. Booth, J. Bruck, M. Franceschetti, and R. Meester. Continuum percolation and the geometry of wireless networks. *Annals of Applied Probability*, vol. 13, no. 2, pp. 722-731, 2003.

[23] N. Dunford and J.T. Schwartz, *Linear Operators*, Wiley-Interscience, New York.

[24] B. Otis, Y.H. Chee, R. Lu, N.M. Pletcher, J.M. Rabaey. An Ultra-Low Power MEMS-Based Two-Channel Transceiver for Wireless Sensor Networks. In *Proc. of IEEE Symp. VLSI Circuits*, June 2004.

[25] J. Weldon, K. Jensen, and A. Zettl. Nanomechanical radio transmitter. *Phys. Stat. Sol. (b)* 245 (10), 2323-2325. 2008.

[26] J. M. Kahn, R. H. Katz and K. S. J. Pister. Mobile Networking for Smart Dust. In *Proc. of MobiCom 99*, Seattle, WA, August 17-19, 1999.

[27] <http://news.bbc.co.uk/1/hi/magazine/3738652.stm>

[28] <http://games.slashdot.org/article.pl?sid=07/12/17/1514217>

[29] http://www.washingtonpost.com/wp-dyn/content/article/2007/10/02/AR2007100202366_pf.html

[30] <http://www.scalable-networks.com/>