# On Connectivity in Ad Hoc Networks under Jamming Using Directional Antennas and Mobility

Guevara Noubir

College of Computer and Information Science
Northeastern University
Boston, MA 02118, USA

noubir@ccs.neu.edu

**Abstract.** In this paper we investigate the problem of maintaining connectivity under jamming in multihop ad hoc wireless networks. Connectivity is measured using a connectivity index, which indicates the probability that there exists a path between two nodes. We first show that connectivity can be drastically reduced with a relatively small number of jammers. We show that using sectored antennas can maintain connectivity in the presence of a significantly higher number of jammers at the expense of higher average number of hops. Finally, we show that mobility allows further resiliency to jamming.

## 1 Introduction

Wireless communication is exposed to various denials of service attacks at all protocol layers. Robustness of wireless multihop ad hoc networks is essential to various applications both in the military context and in future commercial applications. Jamming is the most traditional technique to prevent wireless communication. Jamming can be malicious, aiming at preventing wireless communication in an area, but can also be due to non-interoperability of wireless standards. In a military context adversaries intentionally jam the communication channel to prevent nodes from correctly receiving data packets. In [1] we have shown that for a single hop omni-directional communication of *data packets*, an adversary can easily break the wireless link at a very low energy cost. Jammers do not need to be large high power transmission devices, they can be composed of a set of small low cost "cyber-mines" randomly spread over the area of jamming interest to the adversary. Non-malicious jamming can occur in both military and commercial communication. For example the 2.4GHz Industrial, Scientific and Medical band is crowded by multiple non-interoperable standards (e.g., IEEE802.11, Bluetooth, cordless phones in the US) and the 5GHz frequency band will also be used by various non-compatible standards (e.g., IEEE802.11, Hiperlan II). The presence of non-compatible communication leads to interference that can have the same effect as jamming. Multihop ad hoc networks have the advantage of being able to use multiple paths to maintain connectivity. In this paper, we show that, under jamming, the connectivity can drop drastically. However, the use of sectored antennas can significantly improve connectivity. In the past, sectored antennas were only used at

fixed base-stations of access points. But the advent of compact sectored antennas will make their integration feasible for mobile devices. For example, Antenova [2] already sells 5 and 16-sectored antennas of small dimensions (5cm x 15cm). Some new PDAs such as the Wanda from Texas Instruments [3] already integrate 4 antennas to allow co-existence of Bluetooth, IEEE802.11, and GPRS (General Packet Radio Service). This integration trend will continue specially for high frequencies bands because the antenna size is usually directly related to the signal wavelength. Directionality will also be provided using smart antennas' beam forming techniques or MIMO (Multiple Input Multiple Output) technology.

Connectivity of ad hoc networks has been extensively studied and various results were obtained [4-7]. Previous research has mainly addressed the problem of determining the optimal transmission range or nodes degree to maintain connectivity. More recent studies used percolation theory [8-10] both in a 0-1 connectivity model and in interference based connectivity model. Analysis based on percolation theory proved to be a powerful tool in exhibiting phase transition behavior for connectivity. In [11], it was shown that when the number of nodes goes to infinity the minimum range for achieving k-connectivity (existence of $k$ disjoint paths) is the same as the minimum range for each node having $k$ neighbors. Some recent studies addressed the modeling issues related to links failures [12] by looking at the graph minimum cut. In addition to physical layer jamming several DoS techniques can be applied at higher protocol layers of systems such as IEEE802.11 (e.g., by forcing the backoff window to remain at its maximum) or Bluetooth MAC (e.g., by destroying some control packet), routing (e.g., by injecting erroneous or destroying control routing packets), and transport protocols (e.g., by forcing TCP multiplicative decrease to keep the congestion window small) [13-20]. However to the best of our knowledge no work has been done in investigating the use of directional antennas and mobility in maintaining connectivity.

In Section 2, we present the problem of jamming in multihop ad hoc networks, describe traditional jamming and anti-jamming techniques, and introduce the connectivity measures that we will be using to evaluate our techniques. In Section 3, we analyze the network connectivity under jamming when using omni-directional antennas. In Section 4, we show how sectored antennas can increase the tolerance of the network connectivity to a higher number of jammers. In Section 5, we show how mobility can further increase the network connectivity.

## Notation:

| | |
|---|---|
| $N$: the number of communicating nodes | $R$: nodes communication range |
| $NJ$: the number of jamming nodes | $JR$: range of jamming |

## 2 Problem of jamming and connectivity in ad hoc networks

### 2.1 Jamming principles

Traditional jamming techniques address the energy cost of jamming a single symbol/bit in a communication. The jamming capability of a single symbol is a function of the jammer power, the transmitter power, the antennas gains (from jammer to receiver, receiver to jammer, transmitter to receiver, and receiver to transmitter), the communication receiver bandwidth, the jamming transmitter bandwidth, the range between the transmitter and receiver, the range between the jammer and receiver, the jammer signal loss, and the communication signal loss [21]. Classical jamming consists in injecting an interfering signal that submerges the signal at the receiver. Several interfering waveforms can be used such as noise modulated FM, noise bursts, or continuous wave (CW) tone. The jammer can also play-back a previously recorded signal. Resistance to jamming is traditionally achieved by tuning various parameters such as transmission power, directional antennas, and receiver communication bandwidth. In the next paragraph, we describe one of the most common and efficient bit-level anti-jamming techniques; namely *spread spectrum.*

Traditionally, jamming strength is measured through the jamming-to-signal ratio defined as follows [21]:

$$\frac{J}{S} = \frac{P_j G_{jr} G_{rj} R_{tr}^2 L_r B_r}{P_t G_{tr} G_{rt} R_{jr}^2 L_j B_j}$$

| | |
|---|---|
| $P_j$: jammer power | $P_t$: transmitter power |
| $G_{jr}$: antenna gain from jammer to receiver | $G_{tr}$: antenna gain from transmitter to receiver |
| $G_{rj}$: antenna gain from receiver to jammer | $G_{rt}$: antenna gain from receiver to transmitter |
| $R_{tr}$: distance from transmitter to receiver | $R_{jr}$: distance from jammer to receiver |
| $L_r$: communication signal loss | $L_j$: jammer signal loss |
| $B_r$: communications receiver bandwidth | $B_j$: jamming transmitter bandwidth |

Protection against jamming in wireless communication is usually achieved by reducing the jamming to signal ratio. The obvious technique to reduce the jamming-to-signal ratio is based on increasing the transmission power level. However, this technique is not very efficient and is usually used as a last solution. The most commonly used anti-jamming technique is *spread spectrum* [22]; it relies on reducing $B_r/B_j$. These techniques force the jammer to spend much more energy than the sender. This is achieved by forcing the adversary to jam over a larger frequency bandwidth than the effective receiver/communication bandwidth. The typical value of the spread spectrum processing gain in military communication is between 20 dB and 30 dB. Spread spectrum technology uses a pseudorandom sequence to spread a signal over a much larger frequency band than what is required for its transmission. Correlating the received signal with the pseudorandom sequence carries out the dispreading

operation. There are two main spread spectrum techniques, namely: the direct sequence technique and frequency hopping. If the pseudorandom sequence is unknown to the jammer, then the spreading operation achieves a processing gain *G* in the signal-to-jamming ratio. To successfully jam a communication the adversary would have to compensate this processing gain by increasing its transmission power. As will be explained in the next paragraph, spread spectrum in not sufficient to fully protect jammers. In this paper we consider the reduction of the antenna gain from the jammer to the receiver and use it in the context of multihop communication.

One has to note that reducing the jamming-to-signal ratio does not necessarily lead to complete resiliency to jamming. This is due to other vulnerabilities introduced by higher protocol layers. In [1], we have shown that it is easy to jam existing wireless data networks at a very low energy cost. We have shown that the jamming cost for IP over IEEE802.11 can be as low as $10^{-4}$ the cost of the communication. This is done by destroying a chosen very small fraction of the data packet to make the CRC wrong. An adversary can therefore deploy a set of low-cost *cyber-mines* that can passively detect packets (or some packets such as routing control packets) and destroy them. These cyber-mines can therefore last for long period of times. They not only can prevent communication but also might be used to force communication through paths where more powerful nodes intercept the traffic. We have shown that using a cryptographic interleaver with error correction codes can reduce the problem of jamming into resiliency to noise over a binary symmetric channel (BSC). Therefore, the capacity bound under jamming is given by Shannon's theorem as the channel entropy. The achieved result allows providing much better resiliency to jamming specially compared to existing WLAN standards such as IEEE802.11 and bluetooth.

In this paper, we will investigate the impact of the antenna gain factors to reduce the jamming-to-signal ratio and its impact on connectivity in multihop ad hoc networks. We propose to reduce the jammer to receiver antenna gain factor in the jamming to signal ratio. A simple approach to achieve this is by using sectored antennas, which results in isolating the jammers. The limitation of this technique is that complete isolation is not possible for example when the jammer and transmitter happen to be on the same sector of the receiver. Therefore, the use of multipath is helpful because there might be another receiver that cannot be jammed for the same transmitter. In practice the jamming range can be bigger or smaller than the communication range depending on the transmitter's power, jammer's power, spreading factor, etc. In our simulation we make the assumption that the jamming range is equal to communication range. Our results can be extended to the power controlled jamming range case. Our connectivity analysis considers an arbitrary jamming and communication range. However, a more careful analysis has to be applied to investigate energy efficient jamming/anti-jamming strategies.

### 2.2 Connectivity

A graph is said to be connected if there exists at least one path between any two nodes. Since jamming results in a directed graph, characterizing the level of

connectivity of such a graph that is not connected is more difficult. Intuitively we characterize the level of connectivity of a graph by the average number of nodes that can be reached from any node of the graph. This can be measured using a function similar to the gamma index of the transitive closure of the connectivity graph. We first define a link that is not jammed. Then we define the connectivity index.

**Definition 1:** Let $R$ be the communication range of the nodes, $JS$ be the set of jammers, and $JR$ be the jammer range. A link from node $A$ to node $B$ is said to be non-jammed if and only if:

$$d(A,B) < R \wedge \forall J \in JS : d(J,B) > JR$$

$d(A, B)$ denotes the Euclidian distance between the locations of node $A$ and node $B$. We will later generalize this definition to the case of directional antennas. It is worth noting that links are not symmetric.

**Definition 2:** Let $G = (V, E)$ be the directed connectivity graph of a multihop ad hoc network after removing jammed links. Let $G'=(V, E')$ be the transitive closure of $G$. The connectivity index of $G$ is defined as: $\frac{|E'|}{|V|^2}$.

A connected graph has connectivity index 1, since its transitive closure is a clique. A graph partitioned into two equal size connected graphs has a connectivity index of 0.5. Therefore the connectivity index drops quickly with partitions and from a practical perspective maintaining a connectivity of 0.9 can be seen as a good result.

## 3 Jamming omni-directional communication

In this section we assume that the nodes communicate using omni-directional antennas. Therefore, a node will not be able to receive any data if it is within range of at least one jammer. However, this does not necessarily prevent the jammed node from transmitting to a non-jammed node, therefore creating an asymmetric network. We consider two cases, first when a large number of jammers are randomly spread over a large area $A$. In the second case we investigate the minimum number of jammers required to jam the whole area $A$.

### 3.1 Randomly located jammers

Let us assume that both the communicating nodes and the jammers are randomly distributed over a large area $A >> \pi R^2$. The nodes are distributed according to a homogeneous spatial Poisson process of density (intensity) $\lambda$ (which corresponds to $N/A$). Similarly the jamming nodes distribution intensity is $\mu$ ($NJ/A$). Such a scenario corresponds to a completely unplanned dissemination of jammers and communicating nodes. This also implies that if there were $N$ nodes in any given region, their location would be independently, uniformly distributed over the region.

**Proposition 1:** The probability that the network is disconnected is lower bounded by the following formula: $1-(1-e^{-\lambda\pi R^2})^N e^{-\mu\pi JR^2 N}$.

**Proof:**

$$\begin{aligned}\Pr[\text{G is disconnected}] &\geq 1-\Pr[\text{node is connected}]^N \\ &\geq 1-\Pr[\text{other node within range} \wedge \text{no jammer within range}]^N \\ &\geq 1-(1-e^{-\lambda\pi R^2})^N e^{-\mu\pi JR^2 N}\end{aligned}$$

For the case of *non-jammed* communication, Penrose [11] has shown that in the limit when *N* grows to infinity, the range that leads to a connected network is the same as the range that leads to each node having one neighbor. The result is in fact more general and applies *k*-connectivity in geometric graphs. It is not obvious how this result can be generalized to the case of a geometric graph where some links are failing due the presence of a jammer. If this result could be extended to the presence of jammers, the proposition would provide a tight bound.

Another connectivity metric that one might consider is the probability of all the nodes being disconnected.

**Proposition 2:** The probability that all nodes are disconnected is given by: $[1-e^{-\mu\pi RJ^2}(1-e^{-\lambda\pi R^2})]^N$.

Proof: A node is disconnected if it does not have any neighbouring node within it's communication range or if there exists a jammer within it's jamming range. Since the location of jammers is independent of location of the node, the probability of a node being disconnected is: $1-e^{-\mu\pi RJ^2}(1-e^{-\lambda\pi R^2})$. Assuming that the nodes are independently disconnected leads to the proof.

The probability that the network becomes disconnected is very high in the presence of even few jammers. This probability quickly increases to one as a function of the number of nodes. The reason is that there will necessarily be some communicating nodes within range of a jammer. Therefore the connectivity index we have introduced is a better measure, because it gives the probability that any two nodes can communicate. Figure 1, shows the increase in the probability of all nodes being disconnected (from **Proposition 2**) as a function of the number of jammers, for *N*=400 in an area of 2000x2000, and with a communication/jamming range of 200. The figure indicates that all the nodes are with very high probability disconnected when the number of jammers exceeds 100. It also indicates a relatively sharp phase transition around 50 jamming nodes. This is confirmed by the simulation from Figure 4, which shows that the connectivity index drops quickly as a function of the number of jammers (consider only the curve for 1-sectored antennas). This result is not surprising because it is expected that a large number of jammers (e.g., 100) would lead a completely communication denied area. Our goal is a better characterizing of the connectivity under jamming using the connectivity index we have defined earlier.

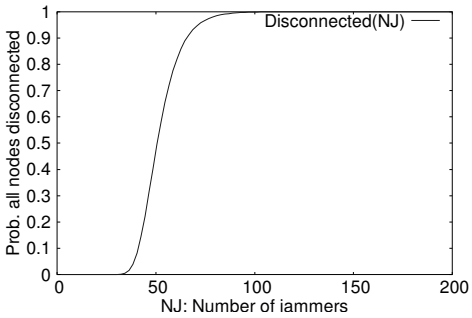


**Figure 1. Probability that all nodes are disconnected as a function of the number of jammers.**

### 3.2 Optimally placed jammers

If the adversary can choose the location of the jammers than the minimum number of jammers is given by the following theorem and their location is shown in Figure 5. This is in fact similar to the problem of area converage in cellular systems.

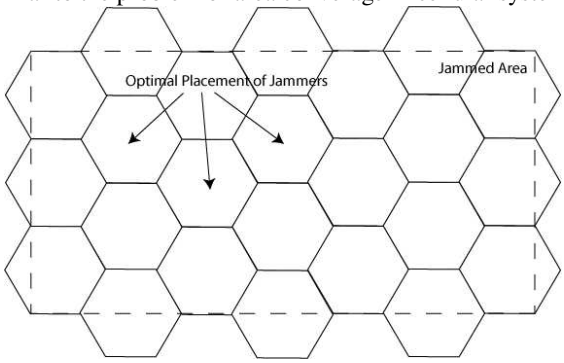


**Figure 2. Against omnidirectional communication, the optimal placement of antennas is at the centre of hexagonal cells.**

**Theorem 1**: Given a jamming range *JR,* the minimum number of jammers to cover an area *A* is

$$\text{(on the limit)}\ \frac{2A}{3\sqrt{3}JR^2}.$$

**Proof:** This is a direct result from [23], where it is proven that the best covering of a plane with congruent circles is obtained with the hexagonal lattice covering.

In the case of an area of 2000x2000, Theorem 1 indicates that 39 jammers can prevent all communication when the jamming range is 200. This is to be contrasted with the simulation results for randomly located jammers. One first conclusion is that not being able to control the location of the jammers drastically limits the adversary capability to prevent communication.

## 4 Maintain connectivity using sectored antennas

In this section, we show that the use of sectored antennas can provide significant resiliency to jammers. A sectored antenna is a set of directional antennas that can cover all directions but can isolate the sectors. Usually sectored antennas are used to improve energy efficiency by only radiating in the sector where the receiver is located. They also reduce the network interference level because they do not radiate on unnecessary sectors. We take advantage of the symmetry property of antennas. A sectored antenna can also be used to receive on a single sector therefore ignoring all interference/jamming coming from the sectors where the transmitter is not located.

**Definition 3:** Let $R$ be the communication range of the nodes, $JS$ be the set of jammers, and $JR$ be the jamming range. A link between two nodes $A$, $B$ is said to be non-jammed if and only:

$$d(A,B) < R \wedge \forall J \in JS : [d(J,B) > JR \vee Sector(A,B) \neq Sector(J,B)]$$

Where $Sector(X, Y)$ denotes the sector used to transmit from $X$ to $Y$.

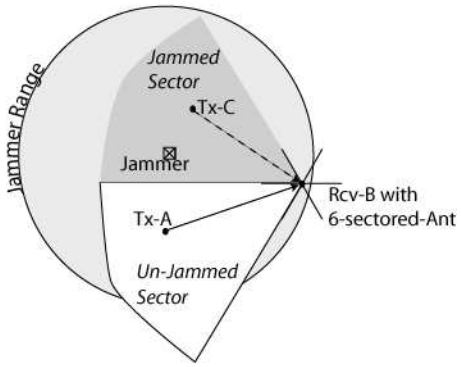


**Figure 3. Node *B* uses a 6-sectored antenna. The jammer can only prevent the communication from *C* to *B* and not from *A* to *B*.**

As a first step, in the evaluation of the connectivity, we assume that the sectors direction is fixed. As a next step, we will investigate generalization to randomly oriented antennas and steerable antennas.

### 4.1 Randomly placed jammers against sectored antennas

We have simulated the impact of randomly located jammers on the connectivity index when the communicating nodes use sectored antennas.

To evaluate the connectivity gain achieved by sectored antennas, we compare the number of jammers that lead to the same connectivity index for 1, 3, 6, and 12 sectors antennas. The simulation area is 2000x2000 and 1000x1000, the number of nodes is 400 and 200, and communication/jamming range is 200. Note that the 1000x1000 has node density twice that of area 2000x2000. For a connectivity index of 0.7, a 12

sectored antenna communication can resist to at least twice the number of jammers leading to a connectivity index of 0.7 for a 6 sectored antenna. This observation is valid for all values of connectivity index. The simulation seems to indicate that using *k*-sectored antennas will lead to resiliency to a factor of *k* more randomly located jammers. However, were not able to provide a theoretical proof for this simulation result.

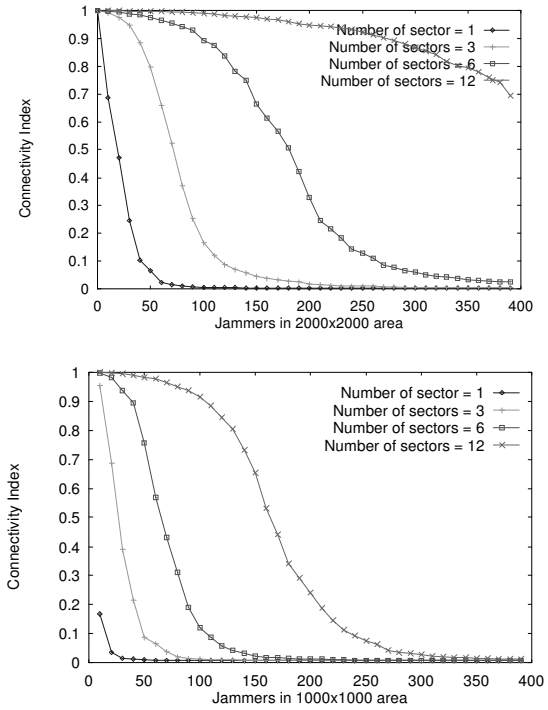


**Figure 4. Connectivity as a function of the number of jammers. The number of communicating nodes is 400 (200) and simulated over an area of 2000x2000 $m^2$ (1000x1000 $m^2$).**

## 4.2 Optimally placed jammers against sectored antennas

In this section we analyze the number of jammers required to prevent all communication within and area *A* when communication nodes use sectored antennas. We compare this number to the number of jammers required to jam omni-directional antennas.

### 4.3 3-sectored antennas

We provide an upper bound on the number of jammers needed to prevent, all communication in an area, between nodes equipped with 3-sectored antenna. The plane is tessellated into equilateral triangles. The jammers are located at the middle of the triangles sides. The sides length is such that for the given jamming range (*JR*), the jammers centered at points *z, t, x,* and *y* satisfy the following property: all circles defined by the jamming limit and centered at *z, t, x,* and *y* intersect at the gravity center *G* of triangle (*A, B, C*) (See Figure 5). By considering all area cases it can be shown that any mobile node will be within reach of at least one jammer on each of its sectors.

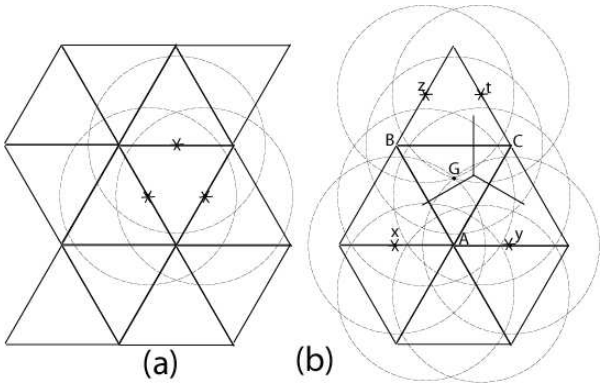


**Figure 5. Jammers placement to jam mobiles equiped with 3-sectored antennas.**

**Lemma 1:** For the circles centered in *x, y, z, t* (and of radius *JR*) to intersect at the gravity center of triangle (*A, B, C*), the triangle sides has to be equal to $\sqrt{\frac{12}{7}}JR$.

**Proof:** This can be analytically shown by placing point *A* at location (0, 0). Therefore the location of points $y = (d/2, 0)$, $G = (0, d/\sqrt{3})$, and $t = (d/4, 3\sqrt{3}d/4)$. Hence

$$\text{distance}(y, G) = JR$$

$$\sqrt{\frac{7}{12}}d = JR$$

It can also be easily shown that distance(*y*, *G*) = distance(*x*, *G*) = distance(*z*, *G*) = distance(*t*, *G*).

**Theorem 2:** To prevent all communication, between nodes equipped with 3-sectored antennas, within an area *A*, the adversary need at most 3.5 more jammers in comparison with jamming omni-directional antennas.

**Proof:** Placing jammers according to Lemma 1 covers all sectors of all nodes. The number of jammers needed is equal to the number of triangles. The number of triangles in a large area *A* is equal to:

$$\text{Number of triangles} = \text{surface}(A)/\text{surface}(triangle) = \frac{4A}{\sqrt{3}d^2} = \frac{7A}{3\sqrt{3}JR^2} \quad \text{[From Lemma 1]}$$

From Theorem 1, we know that $\frac{2A}{3\sqrt{3JR^2}}$ is the minimum number of jammers needed to prevent all communication between nodes using omni-directional antennas within and area $A$. Therefore, the ratio of number jammers needed against 3-sectored antennas versus omni-directional antennas is at most: $\frac{7A}{3\sqrt{3}JR^2} / \frac{2A}{3\sqrt{3}JR^2} = 3.5$.

### 4.4 4-sectored antennas

Using the same approach as for 3-sectored antennas, and by positioning jammers on the corners of squares of side $JR/\sqrt{2}$. The required number jammers is $A/2JR^2$. Therefore, 4-sectored antennas would require at most $\frac{2A}{JR^2} / \frac{2A}{3\sqrt{3}JR^2} = 3\sqrt{3}$.

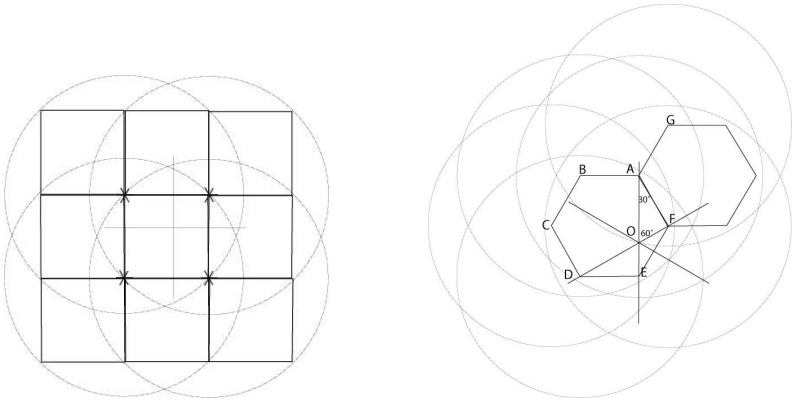


**Figure 6. Jammers location for complete denial of communication against nodes equipped with 4-sectored antennas and 6-sectored antennas.**

### 4.5 6-sectored antennas

In the case of a 6-sectored antennas, we place the jammers on the vertices of hexagonal cells (*A, B, C, D, E, F*) as shown in Figure 6. The jamming radius has to be such that the jammer located on point *G* can reach point *O*. The reason for this is to have any point to be covered on all its sectors anywhere within the cell. Using the

same approach as 3 and 4-sectored antennas we can conclude that the hexagons sides have to be equal to $JR\sqrt{\frac{3}{13}}$. The number of jammers is $\frac{52A}{9\sqrt{3}JR^2}$. The gain compared to omni-directional antennas is at most: $\frac{52A}{9\sqrt{3}JR^2} / \frac{2A}{3\sqrt{3}JR^2} = \frac{26}{3}$.

| | **Omni-directional** | **3-sectors** | **4-sectors** | **6-sectors** |
|---|---|---|---|---|
| **Required num jammers** | $\frac{2A}{3\sqrt{3}JR^2}$ | $\frac{7A}{3\sqrt{3}JR^2}$ | $\frac{2A}{JR^2}$ | $\frac{52A}{9\sqrt{3}JR^2}$ |
| **Ratio to omni-directional** | 1 | 3.5 | $3\sqrt{3}$ | 26/3 |

**Figure 7. Required number of jammers and the ratio to the required number of jammers against omni-directional communication as a function of the jammed area and jamming range.**

We can observe that the gain of multi-sector antennas against optimally placed jammers can be bounded by a value close to the number of sectors. An interesting result would be to derive a general bound on the gain obtained by using *N*-sector antenna.

## 5 Mobility improves connectivity under jamming

In this section we investigate how the concept of time-space routing helps against jamming. Here, nodes can buffer a packet until it can forward it to an intermediate node. We are interested in the connectivity of a mobile ad hoc network, under jamming. If the area is not fully jammed, then it is still possible for some nodes to communicate when they are out of the range of the jammers. Two nodes $N_1$ and $N_k$ are connected if there exists a path $N_1$, $N_2$, $N_3$, … $N_k$ and time instants $t_1 < t_2 < \ldots < t_{k-1}$ such that link $N_i$-$N_{i+1}$ is valid at instant $t_i$. A full path between two nodes might not exist at a single instant but for each link in the path there should be an instant of time when it is valid. It is natural to expect that mobility will increase the chances of nodes to communicate. If the nodes are moving randomly within an area they will eventually pass through an unjammed area and therefore be able to communicate. In [24] it was already shown that mobility increases capacity of ad hoc networks. We study the connectivity improvement under jamming. Designing a routing protocol that can exploit mobility under jamming using sectored antennas is an important question that we plan to address in the future. As a first step in the analysis, we have simulated a random-walk mobility where the nodes at each step select a random direction and destination within a mobility range. The number of nodes is 400, the jamming nodes vary within 100-400. The simulation area is 2000x2000. At each step the destination is randomly uniformly selected within the disc of radius *R*/10 centered at the current position, which corresponds to a maximum speed of 20m/s. Figure 8 shows a substantial increase in connectivity when combining sectored antennas and mobility. Mobility expands the minimum connectivity achieved by sectored antennas. Although

the combination of directivity and mobility increases the connectivity, existing routing and transport protocols are not designed to make use of it. The applications assumptions have also to be reassessed to operate in such environments.

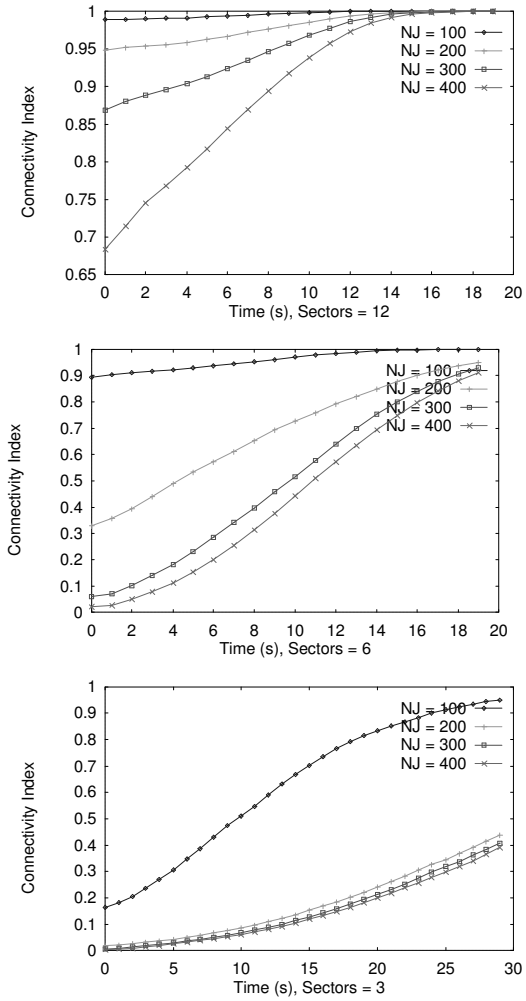


**Figure 8. Connectivity index when combining sectored antennas and mobility.**

## 6 Conclusions and Future Research

In this paper, we have investigated the problem of jamming multihop communication in an ad hoc network. We have shown that even a small number of jammers can drastically reduce the network connectivity when the nodes communicate using omni-

directional antennas. We also showed that a combination of directional antennas and mobility provide significant improvement of connectivity. We investigated both the case where the jammers can be optimally placed by the adversary, and when they are randomly located within an area. Two important problems remain open. First, is there a lower bound on the connectivity gain achieved by a *k*-sectored antennas versus omni-directional antennas. Second, existing routing and transport protocols were mainly designed for symmetric or wired networks and would perform poorly in a jammed environment. Therefore, the question on how to design efficient time-space routing protocols and transport protocols that use mobility and take into account the application requirements and temporarily jammed links or areas.

## 7 References


1. Guevara Noubir and Guolong Lin. "*Low Power DoS Attacks in Data Wireless LANs and Countermeasures*". in *Proceedings of Poster: ACM MobiHoc*. 2003. Annapolis, MD: ACM Press.
2. Antenova Ltd. 2003. http://www.antenova.com/.
3. Texas Instruments Inc. 2003. www.ti.com/wanda.
4. Hideaki Takagi and L. Kleinrock, "*Optimal Transmission Ranges for Randomly Distributed Packet Radio Terminals*". IEEE Transactions on Communications, 1984. **32**(3): p. 246-255.
5. Christian Bettstetter. "*On the Minimum Node Degree and Connectivity of a Wireless Multihop Network*". in *Proceedings of MobiHoc*. 2002. Lausanne, Switzerland: ACM Press.
6. Miguel Sanchez, Pietro Manzoni, and Z.J. Haas. "*Determination of critical transmission range in ad-hoc networks*". in *Proceedings of Multiaccess Mobility and Teletraffic for Wireless Communications Workshop*. 1999.
7. Imrich Chlamtac and A. Farago, "*A New Approach to the Design and Analysis of Peer-to-Peer Mobile Networks*". ACM/Baltzer Wireless Networks, 1999. **5**(8).
8. Olivier Dousse, Francois Baccelli, and P. Thiran. "*Impact of Interferences on Connectivity in Ad Hoc Networks*". in *Proceedings of IEEE Infocom*. 2003.
9. P. Santi and D.M. Blough. "*An Evaluation of Connectivity in Mobile Wireless Ad Hoc Networks*". in *Proceedings of IEEE DSN*. 2002.
10. P. Gupta and P.R. Kumar, "*Critical Power for Asymptotic Connectivity in Wireless Networks*". Stochastic Analysis, Control, Optimization and Applications: A Volume in Honor of W. H. Fleming, ed. W. M. McEneany, G. Yin, and Q. Zhang. 1998: Birkhauser.
11. Mathew D. Penrose, "*On k-Connectivity for a Geomtric Random Graph*". Random Structures and Algorithms. **15**(2): p. 145-164.
12. Andras Farago. "*Graph Theoretic Analysis of Ad Hoc Network Vulnerability*". in *Proceedings of WiOpt: Modeling and Optimization in Mobile Ad Hoc and Wireless Networks*. 2003.

13. Yih-Chun Hu, Adrian Perrig, and D.B. Johnson. "*Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks*". in *Proceedings of ACM Mobicom*. 2002. Atlanta, GA.
14. P. Papadimitratos and Z.J. Haas, *Securing Mobile Ad Hoc Networks*, in *Handbook of Ad Hoc Wireless Networks*, M. Ilyas, Editor. 2002, CRC Press.
15. Pradeep Kyasanur and N. Vaidya, "*Detection and Handling of MAC Layer Misbehavior in Wireless Networks*". August 2002, UIUC.
16. Bridget Dahill, et al., "*A Secure Routing Protocol for Ad Hoc Networks*". 2001, Electrical Engineering and Computer Science, University of Michigan.UM-CS-2001-037,
17. Jean-Pierre Hubaux, Levente Buttyan, and S. Capkun. "*The Quest for Security in Mobile Ad Hoc Networks.*" in *Proceedings of MobiHoc'01*. 2001: ACM Press.
18. Sergio Marti, et al. "*Mitigating Routing Misbehavior in Mobile Ad Hoc Networks*". in *Proceedings of Sixth Annual IEEE/ACM International Conference on Mobile Computing and Networking (MobiCom 2000)*. 2000: ACM Press.
19. Frank Stajano and R. Anderson. "*The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks.*" in *Proceedings of Security Protocols, 7th International Workshop*. 1999: Lecture Notes in Computer Science, Springer Verlag.
20. Lidong Zhou and Z.J. Haas, "*Securing Ad Hoc Networks*". IEEE Networks Magazine, 1999. **13**(6).
21. Curtis D. Schleher, "*Electronic Warfare in the Information Age*". 1999, Norwood, Artech House.
22. Bernard Sklar, "*Digital Communications, Fundamentals and Applications*". 2001: Prentice-Hall.
23. Richard Kershner, "*The Number of Circles Covering a Set*". American Journal of Mathematics, 1939. **61**(3): p. 665-671.
24. Mathias Grossglauser and D. Tse. "*Mobility Increases the Capacity of Ad Hoc Wireless Networks*". in *Proceedings of IEEE Infocom*. 2001.