Link Probability for Ad Hoc Mesh Networks in the Presence of Multiple Interferers

Andrew D. Harper
School of Electrical and Computer Engineering
Georgia Institute of Technology, Atlanta, GA 30332
Email: andrew.harper@gtri.gatech.edu

Robert J. Baxley
Georgia Tech Research Institute
Atlanta, Georgia
Email: bob.baxley@gtri.gatech.edu

***Abstract*—Previous works have addressed minimizing effects of interference in Ad Hoc Mesh Networks (AHMN). Maximizing interference is also of interest in military jamming applications. When AHMNs are used to facilitate remote detonation of explosives, continuous transmission may not be the goal. Rather, communication of a single message is sufficient to cause harm. For this purpose, it is useful to characterize the interference parameters, such as power and node density, in order to minimize the probability that any message can be communicated across the AHMN. In this paper we construct a model of randomly placed communication and interference nodes, and derive the closed-form probability of establishing an pairwise link within the network given the presence of multiple interferers. Though the expression for link probability is highly non-linear, we show that a binary Markov model accurately approximates the value. We use Monte-Carlo simulations to validate our analytical results, and give an example of how our simple analysis is a useful first step in designing an interference strategy.**

I. Introduction

The emergence of a number of affordable AHMN devices has broadened both availability and appeal of wireless mesh networking. As is often the case with wireless devices, it also introduced a new set of concerns about interference in shared bandwidths. Many AHMN devices offer sensors that facilitate gathering data from the environment of the sensor network. These devices are generally inexpensive, and operational straight out of the box, and are intended for varied applications such as monitoring the structural health of a bridge [1] or home-based health monitoring systems [2]. The versatility, availability, and user-friendliness of AHMN devices also introduces the possibility of their use for malicious purposes, such as remote explosive detonation. In such applications, the ability to interfere with the network transmission, and subsequently the ability of the network to withstand attempts at interference, are of great interest.

Recent works have addressed avoidance of interference from devices with similar hardware to that of the network, thereby limiting the possibilities of transmitted interference. In such cases, the AHMN may employ a variety of options to avoid transmission concurrent with the interferer in time or in frequency. However, interfering devices may not have similar constraints on bandwidth, waveform type, power output or range of transmission. The Universal Software Radio Peripheral (USRP) is one of a recent class of software defined radios (SDRs) that offer extremely flexible programming– allowing for wideband interference, specifically targeted waveforms, and more versatile output power. This flexibility enables a new class of adversarial interference governed primarily by minimizing link probability in the AHMN.

In this paper, we establish an analytical framework for predicting the probability that an in-network link exists in the presence of multiple interferers. Through analysis, we find the probability that a given pairwise link exists in an AHMN with randomly placed relay nodes. Then, by modeling the successive relay selections as a Markov process, successful message reception is indicated by the stationary distribution of the Markov process.

The organization of this paper is as follows: §2 discusses previous works that address the interference different contexts of wireless network communication. In §3, we define the model used in our analysis. In §4, we derive in-network link probabilities as a function of communication and interference transmission radii. We validate our model through Monte-Carlo simulations, and give an example of its use in §5. We finish in §6 with conclusions and possible directions for future work.

II. Background and Related Work

Device designers generally equip AHMN devices with a self-interference avoidance algorithm to prevent intra-network interference. Many devices with advanced programming support may have these algorithms disabled, allowing the possibility of using identical hardware to interfere with communication. Previous works have investigated interference that might be presented using 802.15.4 devices. Woods *et al.* [3] propose a sequence of jamming attacks and counter-jamming responses, where the communicator and jammer successively adapt to the actions of the other.

This research is illustrative of the constantly oscillating nature typical of a zero sum game– the attacking strategy is valid only until a defensive maneuver defeats it. They model interference in a point to point format with three nodes (sender, receiver and interferer), and quantify the performance experimentally by measuring the packet delivery ratio (PDR). The authors claim that their methods yield an 88% PDR, and that the interferer is left no option that will more effectively denigrate transmission. However, interference generated by a versatile SDR would not be so constrained in attacking strategy.

Other previous works have also addressed channel access issues. Stamatiou & Proakis [4] use an AHMN model similar to ours, and assess network throughput as a function of self-interference avoidance strategy. They examine the theoretical performance metrics for various multiple access (MA) scheme in avoiding self-interference in multiple-input multiple-output (MIMO) systems. Li *et al.* [5] also use a randomly placed network model similar to the one used in this paper, and investigate optimal jamming attacks in wireless sensor networks where the jamming parameters are controllable. Their work differs from ours in that it focuses on modeling the detection of interference, which in our model is unimportant. They also assume symmectrical links between communicating nodes, a simplification which cannot be adopted in studying directional communication. Khattab *et al.* [6] consider channel hopping to avoid interference, and evaluate the advantages of reactive (in response to detected jamming activity) versus random (without regard to channel activity) hopping. They find proactive hopping best for nodes with a single radio, and reactive best for nodes with multiple radios. However, wideband interference might alter these results.

Many previous works have considered the optimal physical layer interference strategies. Martin & McAdam [7] prove that for an average power constrained Gaussian noise interferer, pulsed interference performs optimally. They show that short pulses of higher-intensity interference are more effective per unit power than continuous lower-intensity interference in producing bit errors at the receiver. Optimal transmitter/interferer strategies have also been analyzed from information theoretic viewpoint for systems with various constraints. Wang and Giannakis [8] analyze a two-hop relay scenario. In the case of no fading, they show that the best strategy is to interfere with a linear combination of the transmitted signal and Gaussian noise. In a fading channel, though, they prove that a Gaussian noise interference strategy is optimal even with perfect knowledge of the transmitted signal. Kashyap *et al.* [9] consider interference on a MIMO Gaussian Rayleigh-fading channel, and show that in such systems knowledge of the transmitted signal does not increase effectiveness of interference.

The wide body of previous research has addressed both medium-access and physical layer point-to-point interference. However, models of analysis of physical layer interference from multiple sources are not as mature. We present a here simple model which has the potential for extension to more specific and complex applications in the future. Our model is unique in that we analyze the pairwise link probability and its effect of transmitting a single message, rather than assessing network throughput averaged over time. and use a Markov model to gage expected effectiveness. We consider a network of single-radio, single-input single-output nodes in the presence of multiple interferers, and assume an arbitrary interference strategy such that transmitted signals will be met with interference at all instances.

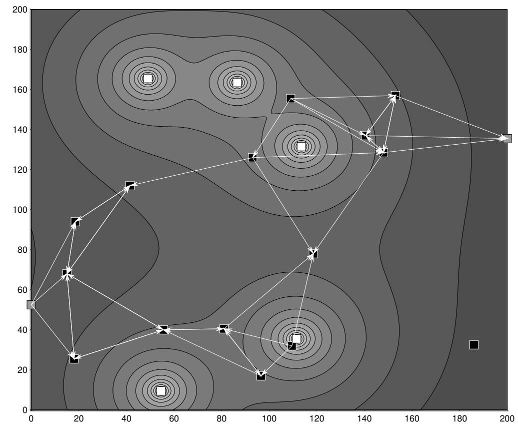

Fig. 1: Example network layout

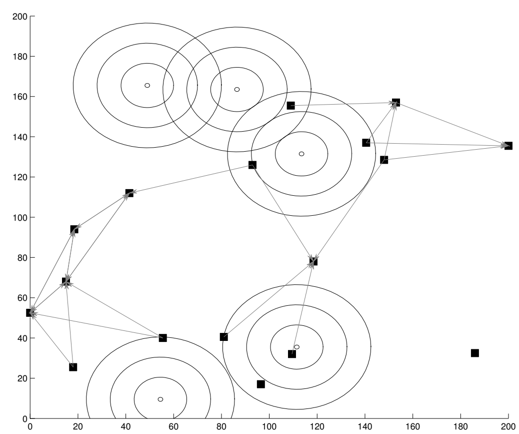

Fig. 2: Approximation network.

III. Model and Definitions

We are interested in the effects of non-cooperative interference on the performance of the network. Hence, we assume that a self-interference avoidance algorithm is implemented that makes the probability of self-interference negligible. As an example, to avoid multiple access interference within the network, 802.15.4 [10] uses carrier sense multiple access with collision avoidance (CSMA-CA) to sense channel activity before transmitting.

A. Physical Model

The transmission space S is modeled as a square of area $|S| = w^2$, populated with up to N communicating relay nodes indexed by $n \in \{1, \ldots, N\}$. The AHMN node coordinates are selected randomly from a uniform distribution across the space. A sending node c_s is positioned at random along the left edge of the space, and a receiving node c_r at random along the right edge. The goal of the mesh network nodes is to relay a single message from sender to receiver through K hops across the network. All AHMN nodes are assumed to have both sending and receiving capabilities, and are constrained to have identical power output. We denote the availability of a link from c_i to c_j as $c_i \rightarrow c_j$, and a reciprocal link as $c_i \leftrightarrow c_j$.

The transmission space is then populated with up to M interfering nodes indexed by $m \in \{1, \ldots, M\}$ whose goal it is to prevent the transmission of the message from c_s to c_r. The interference node coordinates are selected randomly from a uniform distribution across S. The case where interference from d_i prevents reception at c_i as $d_i \rightarrow c_i$, and lack of interference from d_i to c_i as $d_i \nrightarrow c_i$. Figures 1 and 2 show a graphic example of one possible rendering of the model. The sending node is located on the left edge of the image, and the receiving node on the right. Black squares with white borders represent AHMN nodes. Available links between nodes are shown as arrows. White squares with black borders represent interfering nodes. The grayscale contour shows the actual sum effect of all interfering nodes at various power levels, whereas the concentric circles show the interference power from individual nodes used as a simplification.

Note that, for any given realization, the existence of a reciprocal link between c_i and c_j cannot be assumed due to asymmetries in relation to interfering nodes. That is, in a symmetrical link network,

$$\begin{aligned}\Pr(c_i \rightarrow c_j|M=0) &= \Pr(c_i \leftarrow c_j|M=0)\\ &= \Pr(c_j \leftrightarrow c_i|M=0),\end{aligned}$$

but in general

$$\begin{aligned}\Pr(c_i \rightarrow c_j|M>0) &\neq \Pr(c_i \leftarrow c_j|M>0)\\ &\neq \Pr(c_i \leftrightarrow c_j|M>0).\end{aligned}$$

We assume the self-interference mitigation algorithm (e.g. 802.15.4 CSMA-CA) is effective in preventing packet collision within the communication AHMN, and that all interference arises from intentionally interfering nodes. MAC sublayer strategies (channel hopping, packet fragmentation, redundant encoding) for evading intentional interference are omitted, and we focus exclusively on the results of concurrent transmission of communicating nodes and interfering nodes. For simplicity we assume an isotropic radiation pattern and the standard free-space power decay model, as might be used to approximate a level outdoor environment, and note in advance that whether or not our analysis could be applied to a fading channel model remains an open question. Each communication node has an identical maximum radius of transmission r_{max} determined [11] by its power output through

$$r_{\text{max}} = \left(\frac{P_{\text{t,max}} G}{4\pi P_{\text{r,min}}}\right)^{\frac{1}{2}} \tag{1}$$

where G is an attenuation constant which accounts for non-ideal radiation and antenna reception. As an example, consider an IEEE 802.15.4 system where $P_{\text{t,max}} = 0$dBm is the maximum power transmission capability, and $P_{\text{r,min}} = -85$dBm is the minimum power reception necessary to establish a reliable link. The minimum and maximum power requirements are set according to IEEE 802.15.4 specifications, and $G = 1.5 \times 10^{-4}$ is defined to yield a maximum range of 60m.

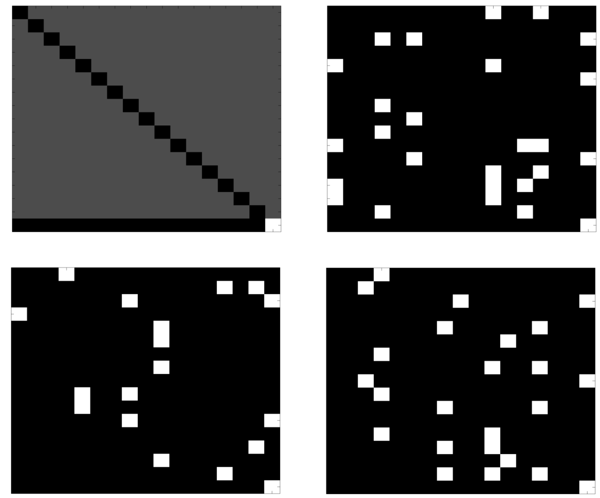

Fig. 3: Graphical representations of the Markov transition matrix. The top left image shows the ergodic $\mathbf{T}$ transition matrix, while the remaining three show different realizations of the $\tilde{\mathbf{T}}$ transition matrix.

B. Relay Model

The ultimate goal of this analysis is to determine whether a message can migrate across an AHMN of relays from a source node to a destination node, denoted by $c_1 \twoheadrightarrow c_N$. Thus we can determine whether the source and destination are connected through the relays by determining whether there exists any fully connected path through the relays that connect the source to the destination.

To model this, we assume that each relay broadcasts any received message to any relay in range. Subsequent relays do the same. In this way, all possible path are tested so that if a path through the relays between the source and destination exists, the message will be successfully received.

Analytically, this physical-link relay scheme can be modeled as a Markov process where the probability that the message is successfully received in time step $i+1$ by node $c_j^{(i+1)}$, when sent in time step i from node $c_k^{(i)}$ is conditionally independent of all previous hops given that c_k successfully received the message in time step i. That is,

$$\begin{aligned}&Pr(c_k^{(i)} \rightarrow c_j^{(i+1)}|c_k^{(i)}, c^{(i-1)}, ..., c^{(0)})\\ &\qquad = Pr(c_k^{(i)} \rightarrow c_j^{(i+1)}|c_k^{(i)})\\ &\qquad = Pr(c_k \rightarrow c_j|c_k)\\ &\qquad = [\mathbf{T}]_{k,j},\end{aligned} \tag{2}$$

where $\mathbf{T} \in \mathbb{R}^{N \times N}$ is the transition matrix.

Form here there are two ways to analyze the network throughput performance. The ergodic view of the network involves assuming that every link has a certain probability of success quantified by $Pr(c_k \rightarrow c_j|c_k)$ however small it might be. With this, the probability of successful transmission after K hops by is given by

$$Pr(c_1 \twoheadrightarrow c_N|K \text{ hops}) = [\mathbf{T}^K]_{1,N}. \tag{3}$$

An example $\mathbf{T}$ is shown in the top left of Fig. 3. In this graphical representation, rows represent sending AHMN nodes and columns represent receiving nodes at each time step. Each square thus shows the probability of the row node establishing a link with the column node, with black being zero probability and white being probability 1. The nodes are not allowed to transmit to themselves, so the matrix is black along the diagonal. The exception is the receiving node, which has a white square on its diagonal, signifying that it is an absorbing state. The gray values represent the estimated average probability of all other links. This model does not account for asymmetries in link probability due to the spatial arrangement of interfering nodes.

The alternative is to assume that the network is made up of connected relays and unconnected relays as illustrated in the top right and bottom two images of Fig. 3. Here, the model parameters explicitly determine the link availability for each realization. For a white square to appear in the matrix, denoting existence of a link from the row node to the column node, the column node must receive the minimum allowable legitimate signal power from the senders well as receive interference power below a threshold value. This view provides a better model of the effects of receiver saturation by an interferer. That is, at a certain level of interference power, the low-noise amplifier (LNA) present in any practical transmission system will saturate, making reception by the relay impossible regardless of the signal power.

In this case, the transition matrix $\tilde{\mathbf{T}}$ is a random variable that depends on the realization. The elements of $\tilde{\mathbf{T}}$ are normalized Bernoulli distributed with probability $Pr(c_k \rightarrow c_j|c_k)$. That is

$$\Pr([\tilde{\mathbf{T}}]_{k,j} \neq 0) = \Pr(c_k \rightarrow c_j|c_k) \tag{4}$$

and

$$\Pr([\tilde{\mathbf{T}}]_{k,j} = 0) = 1 - \Pr(c_k \rightarrow c_j|c_k). \tag{5}$$

In this case, the probability of successful transmission after K hops by is given by

$$\Pr(c_1 \twoheadrightarrow c_N|K \text{ hops}) = Pr([\mathbf{T}^K]_{1,N} \neq 0) \tag{6}$$

and the probability of successful transmission at any time is

$$\lim_{K\to\infty} \Pr(c_1 \twoheadrightarrow c_N|K \text{ hops}) = \Pr([\mathbf{T}^K]_{1,N} \neq 0). \tag{7}$$

IV. Link Probabilities

We now derive the probability of link within the AHMN in the presence of multiple interferers.

Theorem 1. *Let S be a square space with side length w. Given an arbitrary number of uniformly distributed communicating nodes c_i, $i \in \{1, 2, \ldots\}$ with maximum transmission radius $r_c < w$, the probability of link from the ith to the jth node in the absence of interference is*

$$Pr(c_i \leftrightarrow c_j|M = 0) = \left(\frac{r_c^4}{2w^4} - \frac{8r_c^3}{3w^3} + \frac{\pi r_c^2}{w^2}\right) \tag{8}$$

Proof: In a square space with side length a, the probability distribution $f_X(x)$ of length X between any two independently and uniformly selected points within the space has been shown [12] to be

$$f_X(x) = \frac{4x}{a^4}\left(\frac{\pi a^2}{2} - 2ax + \frac{x^2}{2}\right), 0 \leqslant x \leqslant a. \tag{9}$$

For the space S, we have $a = w$. We assume the typical output power constraint on AHMN nodes such that $r_c < w$, and thus the distribution is

$$f_X(x) = \frac{2x^3}{w^4} - \frac{8x^2}{w^3} + \frac{2\pi x}{w^2}, x \leqslant r_c < w. \tag{10}$$

The probability that the jth node is in range of the ith node then becomes

$$\begin{aligned}\Pr(c_i \leftrightarrow c_j|M = 0) &= \int_0^{r_c} f_X(x)dx \\ &= \frac{r_c^4}{2w^4} - \frac{8r_c^3}{3w^3} + \frac{\pi r_c^2}{w^2}.\end{aligned} \tag{11}$$

■

Using a similar analysis, we arrive at the probability of link from c_s to a node within S as

$$\Pr(c_s \rightarrow c_j|M = 0) = \frac{\pi r_c^2}{2w^2} - \frac{2r_c^3}{3w^3}. \tag{12}$$

Since c_s and c_r are independently and uniformly placed along sides of equal length, $\Pr(c_s \rightarrow c_i|M = 0) = \Pr(c_i \rightarrow c_r|M = 0)$. For the derivation of (12), we again refer to [12] and leave the proof as an exercise for the reader.

Theorem 2. *Let S be a square space with side length w. Given a finite number of uniformly distributed interfering nodes d_i, $i \in \{1, 2, \ldots, M\}$ with maximum transmission radius $r_d < w$, the probability of a point c being free from interference is*

$$Pr(d_1 \ldots d_m \nrightarrow c) = \left(1 - \frac{r_d^4}{2w^4} + \frac{8r_d^3}{3w^3} - \frac{\pi r_d^2}{w^2}\right)^M. \tag{13}$$

Proof: Following the same procedure as Theorem 1, we arrive at the probability that ith node d_i interferes with c as

$$\Pr(d_i \rightarrow c) = \frac{r_d^4}{2w^4} - \frac{8r_d^3}{3w^3} + \frac{\pi r_d^2}{w^2}, \tag{14}$$

and thus

$$\Pr(d_i \nrightarrow c) = 1 - \left(\frac{r_d^4}{2w^4} - \frac{8r_d^3}{3w^3} + \frac{\pi r_d^2}{w^2}\right). \tag{15}$$

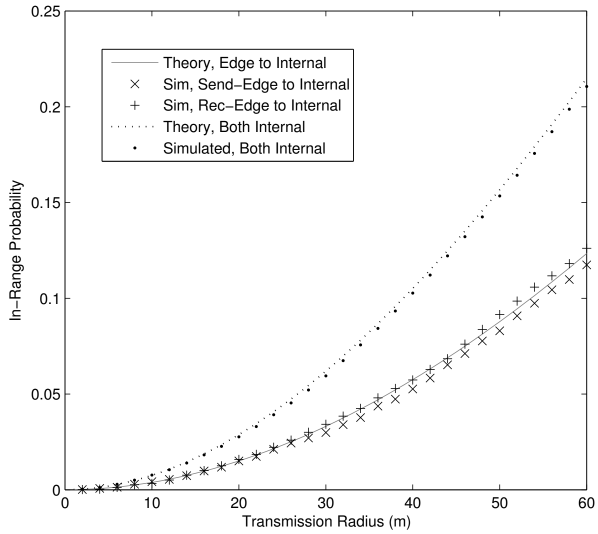

Fig. 4: Probability of link in the absence of interference.

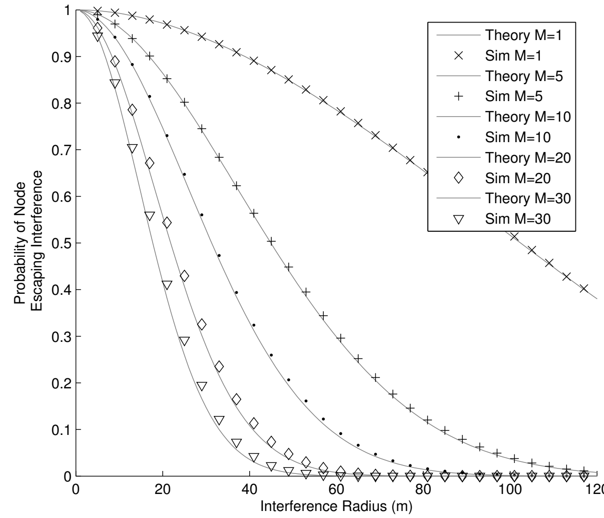

Fig. 5: Probability of escaping interference.

Since all interfering nodes are independent of one another, we have

$$\begin{aligned}\Pr(d_1 \dots d_m \nrightarrow c) &= \Pr\left(\bigcap_{m=1}^{M} d_m \nrightarrow c\right) \\ &= \prod_{i=1}^{M} \Pr(d_i \nrightarrow c) \\ &= \left(1 - \frac{r_d^4}{2w^4} + \frac{8r_d^3}{3w^3} - \frac{\pi r_d^2}{w^2}\right)^M .\end{aligned} \tag{16}$$

■

Theorem 3. *Let S be a square space with side length w. Given an arbitrary number of uniformly distributed communicating nodes c_i, $i \in \{1, 2, \dots\}$ with maximum transmission radius $r_c < w$, a finite number of uniformly distributed interfering nodes d_i, $i \in \{1, 2, \dots, M\}$ with maximum transmission radius $r_d < w$, the probability of link free from interference from the ith to the jth node is*

$$\begin{aligned}Pr(c_i \to c_j) &= \left(\frac{r_c^4}{2w^4} - \frac{8r_c^3}{3w^3} + \frac{\pi r_c^2}{w^2}\right) \\ &\quad \times \left(1 - \frac{r_d^4}{2w^4} + \frac{8r_d^3}{3w^3} - \frac{\pi r_d^2}{w^2}\right)^M .\end{aligned} \tag{17}$$

Proof: The proof follows from the combination of Theorems 3 and 4, and the independence of the communicating and interfering sensor networks. ■

V. Simulation

To verify Theorem 1, we performed a Monte-Carlo simulation of our AHMN for all transmission radii less than 60m, the maximum radius for an 802.15.4 network. The results are shown in Fig. 4. The top curve shows the theory and simulation comparison for the case where both communicating nodes are within S. The lower curves represent the theory and two simulations for when one node is within S and one is located on an edge, as is the case for c_s and c_r. The probability is lower for links with sending and receiving nodes, since their horizontal component is fixed and thus are out of range more nodes placed on the right side of S. The small offset in the simulated values may be due to quantizing S into a grid of points instead of a considering it a continuous space.

We verified Theorem 2 in a similar manner, and the results appear in Fig. 5. The probability of link decreases with each additional interfering node placed in S. However, as the space becomes more saturated, the placing additional interfering nodes begins to show diminishing returns. Despite the fact that the expression for link probability is highly non-linear, we see that the simple binary Markov transition matrix model is able to model the curves quite well when $K \to \infty$. While we note that the multi-hop link probability remains an open problem, we se here that with this simple analysis, interference parameters can be chosen to drive the pairwise link probability arbitrarily close to zero. We now follow with an example of how this modeling of AHMN might be useful in practice.

A. Example: Effects of Node Density and Spatial Arrangement

In designing a system to interfere with an AHMN, two central considerations are interfering node density and node layout. As an example scenario, consider a situation where the goal is to jam a AHMN with exactly M jammer nodes. To achieve the objective of maximum jamming efficiency, we must first determine how the jamming nodes should be spatially organized. We consider two options: place the jammers on a rectangular grid, or place the jammers randomly. The former placement is more intuitively appealing and does provide better performance for some values of M. In contrast, random jammer placement may be easier to deploy by, for

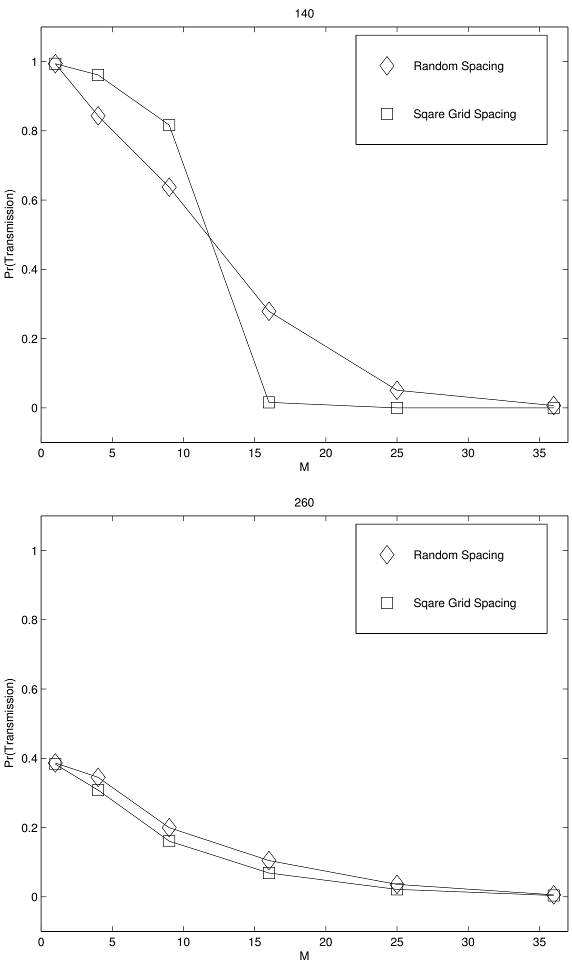

Fig. 6: Comparison of random and grid interferer performance for dense (top) and sparse (bottom) realizations.

instance, dropping the jammer node out of a plane.

We simulate this scenario, and keep the number of AHMN nodes constant as we vary the size of the space S and the number of interfering nodes M. Fig. 6 shows Monte-Carlo simulation results for two runs, each with $N = 15$ AHMN relay nodes. In the top figure, S has side length 140m, while in the bottom figure the length is increased to 260m.Two different interfering node layouts are tested: a randomly assigned layout, and a square grid layout. We assume the interferer has control of node placement, and thus can select the better arrangement once it is known. The graphs trace probability of transmission through the network as given in (7).

At low AHMN densities, the performance of the grid and random layouts are similar, and overall probability is reduced.This matches intuition, since in sparser networks the link probability is diminished, and a grid layout of interfering nodes is likely to cover a similar amount of territory as the random layout. As the densities are increased, however, we see the curves begin to differentiate. Now, there are regions where the random placement performs better than the grid layout, and vice versa. If the interferer is more constrained by number of nodes, a grid spacing will more effectively disrupt transmission. However, as interfering nodes increase, likelihood of transmission is depleted more quickly with a random arrangement.

VI. Conclusions

In this paper we present a closed-form expression for the probability of pairwise AHMN node link in the presence multiple interferes. We then show through Monte-Carlo simulation that a simple binary Markov model accurately approximates these link probabilities. We have also demonstrated an example application for how the model might be useful in AHMN network design. The models presented here are a first step in a novel approach to modeling AHMNs. Though this first model is somewhat simplistic, it nonetheless is able to account for asymmetry in pairwise link probability, and could be used to determine the interference parameters necessary to drive link probability arbitrarily low.

Future iterations could tailor the model to more specific needs and research areas. As a natural next step, the multi-hop probability could be derived and evaluated similarly. Other extensions might also include assessing the effects of additive noise, incorporating indoor or urban fading characteristics into the transmission model, and accounting for contour created by summation of interference signals.

References

[1] K. Chebrolu, B. Raman, N. Mishra, P. K. Valiveti, and R. Kumar, “Brimon: A sensor network system for railway bridge monitoring,” *MobiSys*, June 2008.

[2] C. Otto, A. Milenkovic, C. Sanders, and E. Jovanov, “System architecture of a wireless body area sensor network for ubiquitous health monitoring,” *Journal of Mobile Multimedia*, vol. 1, pp. 307–326, 2006.

[3] A. D. Wood, J. A. Stankovic, and G. Zhou, “Deejam: Defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks,” *Proc. of SECON ’07*, 2007.

[4] K. Stamatiou and J. G. Proakis, “Assessing the impact of physical layer techniques on ad hoc network performance,” *Physical Communication*, vol. 1, pp. 84–91, March 2008.

[5] M. Li, I. Koutsopoulos, and R. Poovendran, “Optimal jamming attacks and network devense policies in wireless sensor networks,” *IEEE International Conference on Computer Communications (INFOCOM)*, 2007.

[6] S. Khattab, D. Mosse, and R. Melhem, “Jamming mitigation in multi-radio wireless networks: Reactive or proactive?” *SecureComm*, September 2008.

[7] D. Martin and P. McAdam, “Convolutional code performance with optimal jamming,” *Conf. Rec. Int. Conf. Commun.*, vol. 4, pp. 4.3.1–4.3.7, 1980.

[8] T. Wang and G. B. Giannakis, “Mutual information jammer-relay games,” *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 2, pp. 290–303, June 2003.

[9] A. Kashyap, T. Basar, and R. Srikant, “Correlated jamming on mimo gaussian fading channels,” *IEEE Transactions on Information Theory*, vol. 50, no. 9, pp. 2119–2123, September 2004.

[10] “IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs),” *IEEE Std 802.15.4-2006*, 2006.

[11] B. Sklar, *Digital Communications Fundamentals and Applications*, 2nd ed. Prentice Hall PTR, 2000.

[12] A. Mathai, *Statistical Distributions and Models with Application, An Introduction to Geometrical Probability*. Gordon and Breach Science Publishers, 1999, vol. 1.