Using Linear System Reliability to Obtain Theoretical Understanding of Wireless Routing

Trisha Biswas†, Kendra Lesser‡, Rudra Dutta†, Meeko Oishi‡
†North Carolina State University {tbiswas, rdutta}@ncsu.edu
‡University of New Mexico {lesser, oishi}@unm.edu

***Abstract*—Wireless multihop networks have a wide variety of applications, due to their rapid deployment times and minimal configuration requirements. Transmissions in wireless networks may require performance guarantees, which can be achieved by using advanced routing strategies. We examine one such performance metric, namely reliability, or packet delivery ratio in a failure-prone wireless network. We use control theoretic methods to obtain an understanding of routing in wireless multihop networks. In particular, we model ad hoc wireless networks as stochastic dynamical systems where, as a base case, a centralized controller pre-computes optimal paths to the destination. This technique can be used to obtain the highest achievable reliability for a given transmission. We compare this approach with the reliability achieved by some of the widely used routing techniques in multihop networks. We also propose extensions to the base case that can be more applicable to practical scenarios. Results show that our approach can be used to theoretically characterize reliability of end-to-end transmissions in wireless networks.**

I. Introduction

Wireless multihop networks are well suited for strategic applications where little or no infrastructure is available beforehand, and networks can be deployed rapidly with minimal configuration requirements. Such networks are decentralized, i.e. each node participates in routing by forwarding data to other nodes. The decision of which nodes forward data is made dynamically on the basis of network connectivity and the routing strategy. Network connectivity depends on density of nodes, transmission power of nodes as well as the wireless links formed, which are prone to failures due to the inherent nature of the medium. The routing strategy depends on requirements of the network, such as minimizing hops using shortest paths, increasing network lifetime by saving power, reducing interference using diverse paths, avoiding malicious nodes such as jammers, and increasing reliability of end-to-end transmissions.

In this study, we investigate the characteristics of ad hoc wireless network routing and present a stochastic dynamical model to represent such a system. A stochastic dynamical system is a dynamical system subjected to the effects of noise. Our goal is to study and model routing in wireless networks in order to obtain an understanding of the performance of routing. In particular, we would like to come up with reachability-based predictors of theoretical bounds on network performance as opposed to experimental analysis using simulations. The approach we use is to model networks using hybrid control theory [1] to characterize them in terms of fundamental theory. The performance indicator used in our system is that of a network's ability to reliably deliver packets in a failure-prone network. In this context, reliability is a mission-specific metric evaluating the probability that a packet gets delivered with a given deadline. We use reachability analysis to compute bounds on the probability of a data packet reaching the destination within a given time.

Our system consists of a centralized controller, which we call an "oracle," that computes optimal paths to the destination. As an idealized base case of the system, the oracle knows steady state availability of all links in the network as well as the up/down state of the links at the start of packet transmission. The links themselves are independent of each other, and their states vary either independently or follow a two-state Markov process. It is worth noting that such an "oracle" can easily be implemented in a controller-based architecture as in OpenFlow [2].

To verify the paths computed by the centralized "oracle" in our system we run simulations of networks with link failures and use the pre-computed paths. We compare the packet delivery ratio obtained from these simulations with the value predicted by the "oracle". The usefulness of this approach lies in the fact that it can help obtain bounds on reliability of end-to-end packet transmissions and to compare with existing routing protocols. To that end, we compare predicted reliability values from our system with well established routing approaches in multihop networks, such as Optimized Link State Routing (OLSR) and Ad-hoc On-demand Distance Vector routing (AODV).

Our contributions in this paper are as follows:

- Present a stochastic dynamical model to represent wireless multihop networks
- Present different ways to model wireless link states in a discrete-time system
- Show how reachability analysis can be used to predict bounds on wireless routing performance
- Experimentally validate predictions of the "oracle" in our system with simulations of existing routing approaches

II. Related Work

Routing protocols in wireless multihop networks have been studied extensively [3], [4]. Many of these techniques take into account the failure prone nature of wireless networks

This work was funded by the National Security Agency.

and carry out redundant routing to increase the reliability of end-to-end transmissions [5]–[7]. In this paper, we study the feasibility of using a control theoretic approach to model wireless multihop networks. We also provide a means of applying the concept of reachability analysis [8] to wireless multihop networks, in order to provide reliability guarantees for end-to-end transmissions. In contrast to other performance studies of wireless routing [4], [9], our approach is theoretical and not based on network simulations.

In the past, TCP congestion control and traffic flows have been modeled using hybrid control theory [1]. The dynamic behavior of routing algorithms has been studied in Low et al. [10]. Linear programming formulations [11] have been used to compute optimal routing strategies to maximize the lifetime of wireless sensor networks. The goal of our dynamic programming formulation is to obtain the maximum achievable reliability for a given transmission, using a novel technique to model wireless networks as stochastic dynamical systems.

III. The Model: Multihop Network as a Stochastic Dynamical System

In this section, we present a theoretical model for wireless multihop networks. We first present a stochastic dynamical model for such networks in III-A and then present various ways of modeling link states in the network in III-B.

A. Model for Wireless Multihop Networks

We model a wireless multihop network as a dynamical system consisting of a state (x_t), a control input (u_t), and a transition model (τ) that determines how the state evolves over time. Additionally, in order to capture random link failures, the transition model is defined as stochastic and incorporates randomness into the state transitions. We therefore define the discrete time multihop network model as follows.

Definition 1. *Multihop Network Model*

1) $\mathcal{N} = \{1, 2, \ldots, N\}$ *is a finite set of nodes.*
2) $\mathcal{M} = 1, \ldots, M$ *is a finite set of* M *links between nodes.*
3) $n_t \in \mathcal{N}$ *is the node location of a packet in the network at time* t*.*
4) $\overline{q}_t \in \{0, 1\}^M$ *is the state of all links in the network at time* t*, where the* m^{th} *entry of* q *equals 1 if link* m *is up, and 0 if it is down.*
5) $x_t = (n_t, \overline{q}_t) \in \mathcal{X}$ *is the full state of the system at time* t*, with* $\mathcal{X} = \mathcal{N} \times \{0, 1\}^M$*.*
6) $u_t \in \mathcal{U}(x_t)$ *is the routing decision for time* t*, telling the node* n_t *where to send the packet given current link condition* $\overline{q}_t$*.*
7) $\tau : \mathcal{X} \times \mathcal{X} \times \mathcal{U} \to [0, 1]$ *is a discrete stochastic transition kernel assigning a probability distribution to* x_{t+1} *given* x_t *and* u_t*.*

We are given a network with a set of N nodes labeled from 1 to N, and a set of links between those nodes labeled from 1 to M. By assigning the value 1 to any link that is currently up, and the value 0 to any link that is currently down, the variable $q_t^m \in \{0, 1\}$ can represent the availability of link m at time t. The vector $\overline{q}_t = [q_t^1, \ldots, q_t^M]^T \in \{0, 1\}^M$ then represents the state of every link (assuming M total links) in the network at time t. Further, letting $\mathcal{N} = \{1, 2, \ldots, N\}$ be the set of all possible nodes, $n_t \in \mathcal{N}$ can represent the node a packet is being held in at time t. The full state x_t combines n_t with $\overline{q}_t$ so that $x_t = (n_t, \overline{q}_t)$ and $\mathcal{X} = \mathcal{N} \times \{0, 1\}^M$.

The control input u_t is defined as the node the packet is sent to between times t and $t + 1$ according to some routing strategy, so that $u_t \in \mathcal{U}(x_t) \subseteq \mathcal{N}$. The set $\mathcal{U}(x_t)$ contains all potential nodes the packet can be sent to, given it is currently at node n_t and the links are in state $\overline{q}_t$.

Finally, we define the stochastic transition function τ. If $\mathcal{U}(x_t)$ is defined as above, so that u_t can only be selected from feasible forwarding nodes, and assuming that once a forwarding command is issued it is carried out with probability 1, then $\mathbb{P}[n_{t+1} = i \mid x_t, u_t = i] = 1$. If we further assume that the state of the links is governed by a discrete stochastic transition kernel $T_q(\overline{q}_{t+1} \mid \overline{q}_t)$ so that the link state probabilities may be affected by previous link states, but not by the packet location or routing policy, then

$$\tau(x_{t+1} \mid x_t, u_t) = \mathbf{1}_{u_t}(n_{t+1}) T_q(\overline{q}_{t+1} \mid \overline{q}_t) \tag{1}$$

The discrete stochastic transition kernel $T_q(\overline{q}_{t+1} \mid \overline{q}_t)$ depends on the wireless link model described in Section III-B.

B. Model for Wireless Link States

We now describe some variations of modeling wireless link states that we will use in the subsequent analysis, ranging from how T_q is defined to what information is available at each node. We model link failures in wireless networks by assigning probability values to each link. By considering these different variations, we will have the tools to develop theoretical network performance results using an array of routing policies, to compare the performance of basic routing policies when different types of information are available, and to produce bounds on packet delivery probabilities. Although we intend to look at several variations of this model to reflect varying levels of stochasticity and information available to the controller when picking forwarding nodes (see Section VII), we now focus on two approaches to model wireless links.

1) Independent Links, Stationary Probabilities: Here we assume that the state of each link is independent of the state of all other links, and also independent of its past state, so that T_q simplifies to:

$$\begin{aligned} T_q(\overline{q}_{t+1} \mid \overline{q}_t) &= \prod_{m=1}^{M} \mathbb{P}\left[q_{t+1}^m \mid q_t^m\right] \\ &= \prod_{m=1}^{M} \mathbb{P}\left[q_{t+1}^m\right]. \end{aligned} \tag{2}$$

2) Independent Links, Markov Probabilities: Here we again assume that the state of each link is independent of all other links, but that its probability follows the Markov property, and is determined by a transition matrix $\mathbb{P}^m$:

$$\mathbb{P}^m = \begin{bmatrix} \alpha & 1 - \alpha \\ 1 - \beta & \beta \end{bmatrix} \tag{3}$$

so that $\mathbb{P}^m(0,0) = \alpha$ is the probability of the link m being down, given it was down at the previous time step, $\mathbb{P}^m(0,1) = 1-\alpha$ is the probability of link m going up given it was down at the last time step, etc. Then

$$T_q(\overline{q}_{t+1} \mid \overline{q}_t) = \prod_{m=1}^{M} \mathbb{P}^m \left(q_t^m, q_{t+1}^m\right) \tag{4}$$

IV. The System: Reachability Analysis for Network Performance

Our general system consists of a centralized controller, or oracle that generates routing strategies based on knowledge of the current state of all links in the network (up or down), as well as network and link information available from the model in Section III. Each node determines its forwarding strategy when it receives a packet by querying the pre-computed oracle, until the packet reaches the destination. In this section, we describe the technique of reachability analysis used by the oracle to pre-compute optimal paths to the destination.

The concept of reachability can be applied to any dynamical system in order to determine whether the state of the system is able to remain within some desired set of states, reach a desired state or set of states, or both, all within a given time horizon. For stochastic dynamical systems with some level of uncertainty, stochastic reachability extends that concept to provide the *probability* of the state of the system reaching or maintaining a desired set of states [8].

We can therefore use reachability techniques applied to Def. 1 to determine with what probability packets will reach some goal node, denoted end. We can also define a set of nodes $\tilde{\mathcal{N}} \subseteq \mathcal{N}$ that packets should be restricted to being sent to if nodes outside of this set are known to be unreliable or compromised by a malicious attacker, for instance. Using a formulation presented in Summers et al. [12], the probability that a packet starting from node $start$ reaches end no later than time T, while avoiding nodes outside of $\tilde{\mathcal{N}}$ can be represented as follows.

$$RA_{start}^{\tilde{\pi},T}(\tilde{\mathcal{N}}, end) = \mathbb{E}\left[\sum_{t=1}^{T}\left(\prod_{i=0}^{t-1}\mathbf{1}_{\tilde{\mathcal{N}}}(x_i)\right)\mathbf{1}_{end}(x_t)\right] \tag{5}$$

The notation $\tilde{\pi}$ denotes a specific routing policy that tells nodes where to send the packet based on the current state of all links. Specifically, $\tilde{\pi}$ is a sequence of functions $(\pi_0, \ldots, \pi_{T-1})$ mapping the current state to a routing decision, $\pi_t(n_t, \overline{q}_t) = u_t$. Eq. (5) can be related back to a probability by recalling that $\mathbb{P}[x \in K] = \mathbb{E}[\mathbf{1}_K(x)]$, where $\mathbb{E}$ is the expected value and K is some set, and $\mathbf{1}_K(x)$ is the indicator function defined as $\mathbf{1}_K(x) = 1$ if $x \in K$ and 0 otherwise.

We focus only on reaching an intended goal node, and do not consider a set $\tilde{\mathcal{N}}$ of nodes to avoid (so $\tilde{\mathcal{N}} = \mathcal{N}$). We also want to find an upper bound to the reachability probability (5) in order to determine the highest achievable reliability for packet transmission. The problem is twofold. First, the optimal routing policy $\tilde{\pi}^*$ must be calculated that delivers packets to end with highest probability. Second, (5) must be evaluated according to the optimal policy $\tilde{\pi}^*$.

Both problems can be jointly solved using dynamic programming (for an overview of dynamic programming, see [13]). The so-called "value function" at time t, $V_t(n_t, \overline{q}_t)$ tells us the following: at time t, and given that the packet is currently at node n_t and links are currently up and down according to $\overline{q}_t$, what is the probability that the state reaches the desired node end before time limit T is reached. The following recursion, modified from Summers et al. [12], is iterated backwards in time starting at T and ending at 0.

$$V_T^*(n, \overline{q}) = \mathbf{1}_{end}(n) \tag{6}$$

$$V_t^*(n, \overline{q}) = \max_{u \in \mathcal{U}(n,\overline{q})} \Bigg\{ \mathbf{1}_{end}(n) + \sum_{\overline{q}_{t+1} \in \{0,1\}^M} V_{t+1}^*(\tilde{\pi}_t^*(n, \overline{q}), \overline{q}_{t+1}) T_q(\overline{q}_{t+1} \mid \overline{q}) \Bigg\} \tag{7}$$

Equation (6) is evaluated first for all $(n, \overline{q}) \in \mathcal{N} \times \{0,1\}^M$, to get the value function at time T, and then for all $t = T-1, \ldots, 0$, the value function (7) is calculated recursively for every $(n, \overline{q})$, finally producing $V_0(n, \overline{q})$, where $V_0(start, \overline{q}_0) = RA_{start}^{\tilde{\pi}^*,T}(\mathcal{N}, end)$.

When the link probabilities are assumed to be independent and stationary, as in (2), Equation (7) reduces to

$$V_t(n, \overline{q}) = \mathbf{1}_{end}(n) + \sum_{\overline{q}_{t+1} \in \{0,1\}^M} V_{t+1}(u_t, \overline{q}_{t+1}) \mathbb{P}\left[\overline{q}_{t+1}\right] \tag{8}$$

The optimal routing policy is defined at each time step by

$$\tilde{\pi}_t^*(n, \overline{q}) = u_t = \arg\max_{u \in \mathcal{U}(n,\overline{q})} V_t^*(n, \overline{q}). \tag{9}$$

From a networking perspective, T can be considered the deadline or *time to live (TTL)* for a given packet transmission. If the TTL value is a finite number, we solve equation (7) exactly T times. If the deadline to reach the destination is unlimited, then we compute the value function recursively until it converges. A potentially infinite deadline can be used to identify reliable transmissions when the packet needs to be delivered regardless of the time taken for delivery, due to failures in the network.

V. Numerical Experiments

A. Experiment Set-up

The system presented in Section IV can predict the reliability of a packet transmission, given the independent availability values of the links in the network. This computation is done by the "oracle" that knows the probabilities of each link being available in the steady state. The "oracle" also stores the computed paths to the destination to achieve the predicted reliability. To verify the paths computed by the "oracle", we simulate networks with intermittent link failures. We also compare the predicted reliability of different transmissions with OPNET simulations of existing routing protocols.

In order to represent practical wireless networks and failure scenarios, we propose to use two metrics for a given source-destination pair, namely, deadline and ambient noise. Deadline signifies the time limit by which the packet must get delivered or T from the system in Section IV. Ambient noise or background noise is a major cause of packet drops in wireless mesh networks. As the noise in the network increases the quality of the links decrease, until the point when the link fails all or most of the time. While ambient noise is not represented directly in our model, we consider this to be an inherent property of the input network to our system and it is represented in the link probability values described in Section III. By varying the deadline and ambient noise in the network, we compare predictions of our system with various simulations.

We carry out our experiments with stationary as well as Markov link probabilities. For both cases we compare the oracle's predicted values with simulations. Simulations are of two kinds. First, we simulate the application of paths computed by the oracle, to compare reliability predicted by the oracle with achieved results based on applications of it. Simulations of our system are carried out with networks deployed using either a uniform random distribution or a 2D Poisson distribution. Nodes in the network have pre-set range and fading models implemented to account for multipath fading. We apply the oracle's pre-computed paths to a sequence of likely events of links failing at different time instances. In other words, the routing policy for nodes in these simulations is the oracle's pre-computed paths. We simulate multiple such scenarios and present the aggregated results of packet delivery ratios. These values would indicate the reliability achieved by different paths from the source to destination.

Simulations in OPNET are carried out using the wireless network deployment tool with uniform random node placement. We use the *wlan_wkstn_adv* node model for ad hoc nodes and run simulations with standard implementations of AODV and OLSR. Wireless link failures are simulated using the radio module in OPNET. We set appropriate fading parameters and ambient noise to simulate link failures. Each set of 1000 simulations with a fixed source-destination pair and a network deployment results in a single data point. We compute the packet delivery ratio for a source-destination pair based on the number of packets that were received by the destination.

The output from our system is in the form of a vector of predicted reliability values, one for each combination of link states for links incident on the source node. We present these values in the form of best, average and worst case reliability computed by the oracle. The best case reliability is achieved when all the incident links of the source are up. For the average and worst case reliabilities, we compute the average and minimum reliability values from the system, excluding the case when all the incident edges of the source have failed. This definition of the best, average and worst case reliability values from the system is used consistently in all the comparative plots.

B. Using Stationary Link Probabilities

We compare our system with stationary probabilities to OPNET simulations of wireless networks with existing routing protocols. In order to achieve a fair comparison between OPNET simulations and our system, we provide the network generated by OPNET to our system. Stationary link failure probabilities are computed by studying the links on OPNET. Steady state link availability for a certain ambient noise value was obtained from OPNET by making each node broadcast a stream of packets. One-hop neighbors compute the packet delivery ratio based on how many of the sent packets were received, in order to compute the success probability of the link.

Given this network generated by OPNET, and computed link failure probabilities, we use our system to get the oracle's pre-computed paths. We compare the reliability of the paths computed by the oracle with OPNET simulations of existing routing protocols. Figure 1 shows a sample 38 node network used for OPNET simulations and comparisons with the model. The network has 38 nodes spread over a region of 6 km^2 and the nodes transmit with a power of 200 milliwatts.

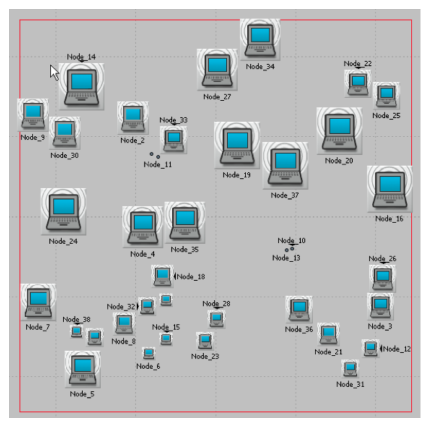

Fig. 1. **Sample 38 node network generated by OPNET, using random node placement**

C. Using Markov Link Probabilities

To carry out comparisons between OPNET simulations and the oracle for Markov links, we use an OPNET generated network of 8 nodes, and provide the topology information to our system. We obtain link transition matrices from OPNET by the following method: generate a stream of packets between each node pair in the network. For each packet received, a node looks up the state of the link in the previous time step, which it maintains. Based on the previous state it increases the appropriate count of received packets (down to up or up to up), and also accounts for all the missing packets in between this time step and last time it received a packet. At the end of the simulation, each link's transition probability matrix values are obtained by normalizing the values along each of the two rows of the matrix shown in (3).

Using Markov transition probabilities creates computational challenges, in that we have to evaluate (7) for all possible states x_t, and for each x_t and u_t we will need to evaluate $\tau(x_{t+1} \mid x_t, u_t)$. To reduce the number of computations, we use stationary probabilities to generate link state probabilities for links more than two hops away from the current node. All comparisons of the oracle's pre-computed paths include this approximation. In addition, due to the large number of computations, we present initial comparative results for the Markov case, with fairly small networks. Improving this technique so that it can be applied to larger networks is part of our ongoing work.

VI. Evaluations and Results

A. Stationary Link Probabilities

1) Visualizing computed paths: We observe the reliability of paths computed by the oracle using stationary link availabilities (as in III-B1). We vary the deadline value as well as the ambient noise, to note the difference in reliability. For this visualization, we used a randomly generated network of 20 nodes. It was observed that there were paths of lengths 5 hops and above between a randomly picked source-destination pair. We varied the deadline and the ambient noise. As expected, we observed that increasing the noise and decreasing the deadline both reduce the probability of successful transmission, until the reliability drops to 0.

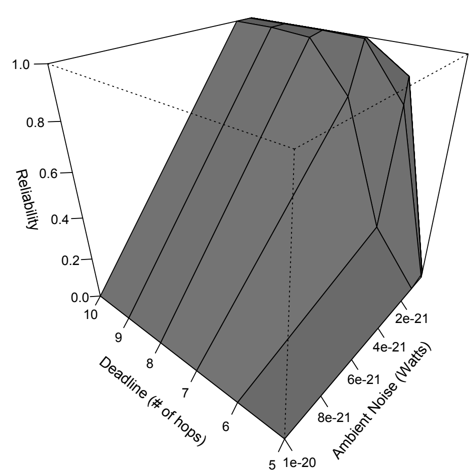

Fig. 2. **Varying deadline and ambient noise for a 20 node network for oracle's pre-computed paths**

2) Simulations of variant III-B1: We compare reliability predicted by the oracle, to reliability achieved from applications of the paths in real network scenarios. Since the pre-computed paths give the next hop information from any node, given any combination of incident edge states, we are able to apply these paths when specific links in the network are made to fail. Reliability values from the system are based on incident link states from the starting time step. We ran 1000 simulations for each ambient noise value, and the result of each was aggregated to get the overall packet delivery ratio. Comparisons show that the reliabilities computed by the oracle are indeed achievable (Fig. 3). Note that the reliability for both the oracle and simulations drop to zero as the noise is increased because the network becomes disconnected if the noise becomes too large.

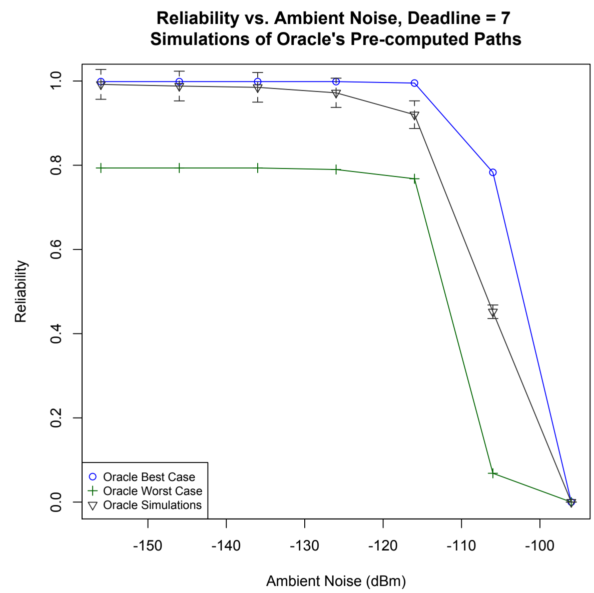

Fig. 3. **Comparison between pre-computed paths and simulations of the network for stationary probabilities**

3) Comparisons to existing routing protocols: For comparisons with existing routing protocols, we ran OPNET simulations with OLSR and AODV routing. We obtained network topologies and stationary link probabilities from OPNET and provided these as inputs to our system. From the OPNET simulation runs, we observed that the length of the paths from a randomly picked source and destination varied between 5 and 8. We thus calculated the reliability values from our system when setting the deadline to 5, 6, 7, and 8. Due to limited space, a subset of these comparative plots for deadline values 6 and 7 are shown in figures 4, 5.

In each of the cases, we observed that our approach performs better than AODV and OLSR. Specifically the best case predictions of the oracle always have higher values than what was achieved by either OLSR or AODV. It is interesting to note that for shorter path lengths (such as 6), there is a significant variation between the best and worst case estimate. In such cases, the performance of the routing algorithm would depend heavily on specific network scenarios, i.e. for an "unlucky" combination of link failures, the reliability could be much lower that the best case, irrespective of the routing approach.

We also observed that for lower deadline values, AODV performed poorly, but performed better than OLSR for higher deadline values. As a general observation, we found that packet delivery ratios in AODV were high, but the paths computed by the algorithm were usually longer than the ones from OLSR. Our technique can be useful to benchmark exiting routing protocols. Using this approach, one can observe specifics of routing protocols, such as packet delivery ratio under specific deadlines, to infer the performance of a routing protocol under those conditions. The oracle in our system also provides the best case achievable delivery ratio for each condition. This in turn can be used to design more robust routing protocols.

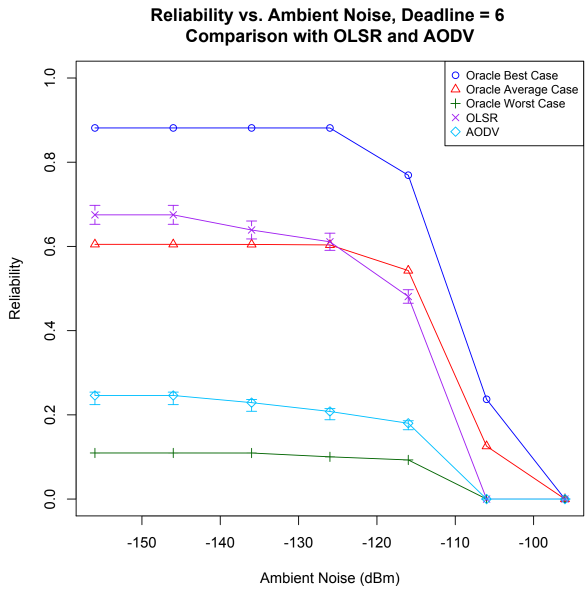

Fig. 4. **Comparison between pre-computed paths from the model and OPNET simulations; Deadline = 6**

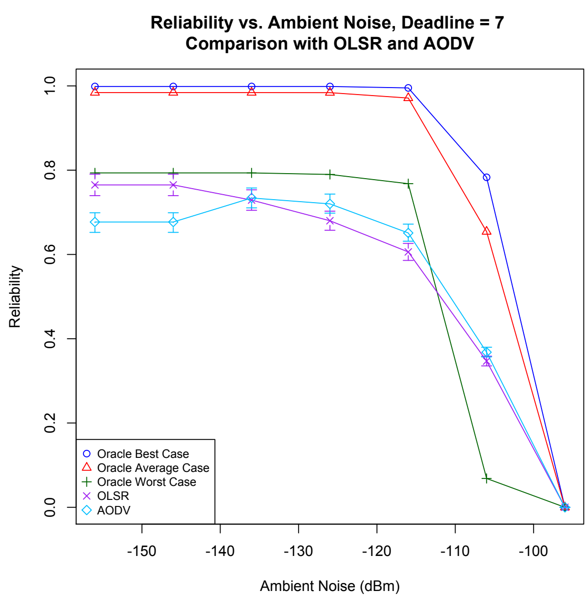

Fig. 5. **Comparison between pre-computed paths from the model and OPNET simulations; Deadline = 7**

B. Markov Link Probabilities

1) Simulations of variant III-B2: In this case, our system pre-computes paths to the destination using Markov probabilities. A link's state at time t, thus depends on its state at the previous time instant. We then simulate networks, where these pre-computed paths are used to obtain packet delivery ratios. Each value of the simulation run shown in Figure 6 was obtained from 1000 runs with the same source-destination pair. Since the Markov variation is more computationally expensive, we were not able to run the pre-computation for very large networks. For the limited sized networks, it can be seen that the computed best reliability values are always higher than the ones achieved from simulations.

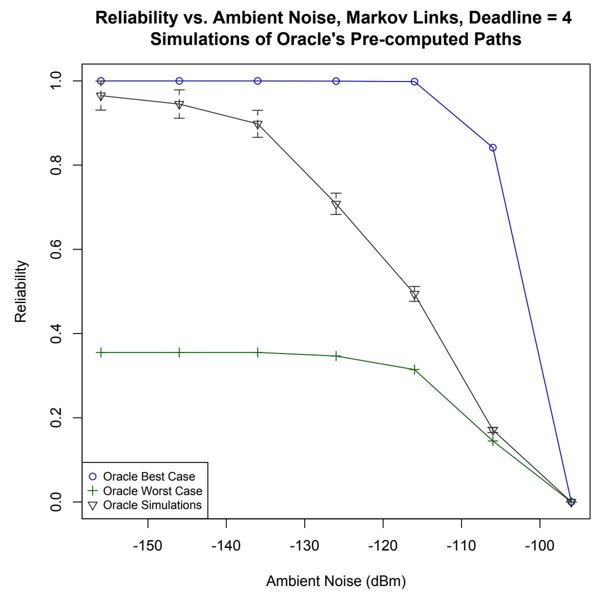

Fig. 6. **Comparison between pre-computed paths and simulations of the network for Markov probabilities**

2) Comparisons to existing routing protocols: We compared the predicted realibility from the oracle with OPNET simulations of OLSR and AODV, in networks with Markov links. An 8-node network with a randomly selected source destination pair was used for this comparison. From OPNET simulations, it was observed that most of the paths were of length 4 for the cases where the packet was delivered to the destination. We thus set the deadline to be 4 in our system, and discarded all paths from the OPNET simulations that used paths of other lengths. Figure 7 shows that both AODV and OLSR perform better than the average predicted value from our model for the fairly small network of eight nodes. In this case, it is again observed that there is a significant difference between the predicted best and worst case reliability values.

VII. Extensions and Future Work

Although the oracle's computation in our current model provides optimal reliability paths, we would like to consider several extensions to the model in order to a) better reflect the

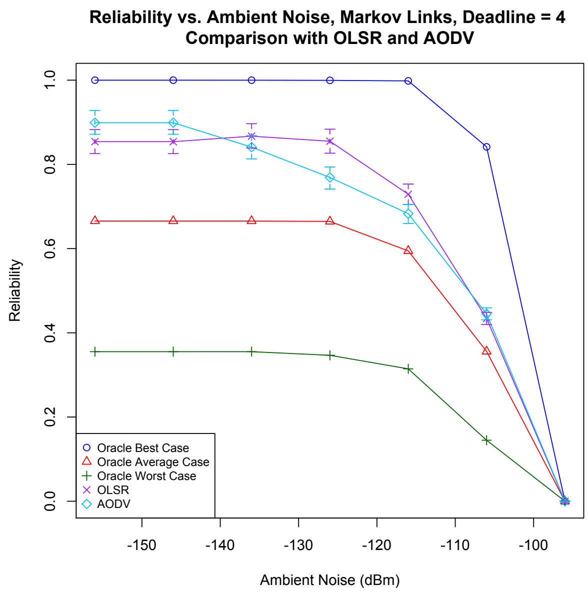

Fig. 7. **Comparison between pre-computed paths from the model with Markov links and OPNET simulations; Deadline = 4**

information available when routing choices are made, and b) more accurately represent the stochastic nature of link failures. We believe the assumption that the oracle always has updated link state information for the entire network may not represent practical networks, and thus we would like to propose three variations to defining links in our model:

- *Limited Node Information*: In this case, the link transition probabilities are Markov, but each node makes forwarding decisions based on limited knowledge of the network. Each link is assumed to have a stationary distribution ν^m, which will be the case for some simple conditions on $\mathbb{P}^m$, and all nodes are aware of the stationary distribution of each link.
- *Delayed Node Information*: Next consider the case where each node again has limited information about the state of the network, but now in the form of delayed information. We preserve the assumption that the state of direct links (to 1-hop neighboring nodes) is known at the current time, but all other link states are not current, and their delay is correlated to their distance from the current node. The state at time t is defined as $x_t = (n_t, \tilde{q}_t(n_t))$, where $\tilde{q}_t(n_t)$ includes the most current information available to node n_t on each link state.
- *Correlated Link States*: Link probabilities are always considered independent of one another in the model we present. Consider the case where nodes located nearby in a spatial region affect one another. Then each link would depend on the state of other links close to it. This variant could be especially useful in modeling jammers that affect geographically correlated links.

VIII. Conclusions

In this paper, we present a theoretical technique to model a wireless multihop network as a stochastic dynamical system. This model allows the application of reachability techniques to evaluate maximum packet delivery probabilities using a dynamic programming solution. Using this tool, we are able to compute paths to the destination, solely based on link availability values (either stationary probability or Markov transition probability). We compare prediction from our approach to applications in real network scenarios with existing routing protocols such OLSR and AODV. The oracle in our system predicts the optimal reliability values. We observe that for shorter path lengths there is a marked difference in the predicted best and worst case scenarios. Thus, even with a good routing algorithm, the achieved reliability could turn out to be much lower than the average case for a given sequence of link failures. Although this approach can be computationally expensive to apply as a routing protocol for large networks, it is a useful tool to analyze the maximum achievable reliability in a given network, and thus obtain a theoretical understanding of wireless routing.

References

[1] J. Lee, S. Bohacek, J. Hespanha, and K. Obraczka, "Modeling communication networks with hybrid systems," *Networking, IEEE/ACM Transactions on*, vol. 15, no. 3, pp. 630–643, 2007.

[2] "ONF. Software-Defined Networking: the new norm for networks," https://www.opennetworking.org.

[3] E. M. Royer and C.-K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," *Personal Communications, IEEE*, vol. 6, no. 2, pp. 46–55, 1999.

[4] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," in *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*. ACM, 1998, pp. 85–97.

[5] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 5, no. 4, pp. 11–25, 2001.

[6] T. Biswas and R. Dutta, "Spatially diffuse pathsets for robust routing in ad hoc networks," in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*. IEEE, 2011, pp. 1–6.

[7] U. Patel, T. Biswas, and R. Dutta, "A routing approach to jamming mitigation in wireless multihop networks," in *Local & Metropolitan Area Networks (LANMAN), 2011 18th IEEE Workshop on*. IEEE, 2011, pp. 1–6.

[8] A. Abate, M. Prandini, J. Lygeros, and S. Sastry, "Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems," *Automatica*, vol. 44, no. 11, pp. 2724–2734, 2008.

[9] Z. Ye, S. V. Krishnamurthy, and S. K. Tripathi, "A framework for reliable routing in mobile ad hoc networks," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 1. IEEE, 2003, pp. 270–280.

[10] S. Low and P. Varaiya, "Stability of a class of dynamic routing protocols (igrp)," in *INFOCOM'93. Proceedings. Twelfth Annual Joint Conference of the IEEE Computer and Communications Societies. Networking: Foundation for the Future, IEEE*. IEEE, 1993, pp. 610–616.

[11] R. Madan and S. Lall, "Distributed algorithms for maximum lifetime routing in wireless sensor networks," *Wireless Communications, IEEE Transactions on*, vol. 5, no. 8, pp. 2185–2193, 2006.

[12] S. Summers and J. Lygeros, "Verification of discrete time stochastic hybrid systems: A stochastic reach-avoid decision problem," *Automatica*, vol. 46, no. 12, pp. 1951–1961, 2010.

[13] D. P. Bertsekas, *Dynamic Programming and Optimal Control*. Athena Scientific, 2005, vol. 1.