Examining Reliability of Wireless Multihop Network Routing with Linear Systems

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

In this study, we present a control theoretic technique to model routing in wireless multihop networks. 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. The usefulness of this approach lies in the fact that it can help obtain bounds on reliability of end-to-end packet transmissions. We compare this approach with the reliability achieved by some of the widely used routing techniques in multihop networks.

Categories and Subject Descriptors

C.4 [**Performance of Systems**]: Reliability, availability, and serviceability

Keywords

Multihop networks, reliability, stochastic dynamic systems

1. INTRODUCTION

Wireless multihop networks consist of wireless nodes where data transmission typically spans over multiple nodes or hops. Security of wireless networks can be studied in two broad categories, namely, security of data and correctness of routing. We focus on the latter and study *reliability* of routing in wireless multihop networks using theoretical methods. Reliability is a mission-specific metric evaluating the probability that a packet gets delivered with a given deadline. It can be considered to be a combination of availability and dependability, both of which are metrics related to the security of a system.

In this study, we investigate characteristics of wireless network routing, and present a stochastic dynamic model to represent such a system. The performance indicator used in our system is that of a network's ability to reliably deliver packets in a failure-prone network. 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. We compare predicted reliability values from our system with established routing approaches in multihop networks, such as OLSR and AODV.

This work is funded by the National Security Agency.

HotSoS '14, Apr 08-09 2014, Raleigh, NC, USA
ACM 978-1-4503-2907-1/14/04.
http://dx.doi.org/10.1145/2600176.2600195

2. THE MODEL: MULTIHOP NETWORK AS A DYNAMICAL SYSTEM

We model multihop wireless networks as a dynamical system, consisting of a state, a control input, and a transition model 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.

From the above model, if $\mathcal{U}(x_t)$ is defined 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

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

2.1 Modeling Wireless Link States

Wireless links are prone to the random uncertainty of the medium and we model this characteristic with various probabilistic models.

2.1.1 *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:

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

2.1.2 *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 $\mathbb{P}^m = \begin{bmatrix} \alpha & 1-\alpha \\ 1-\beta & \beta \end{bmatrix}$. Then,

$$T_q(\overline{q}_{t+1} \mid \overline{q}_t) = \prod_{m=1}^{M} \mathbb{P}^m\left(q_t^m, q_{t+1}^m\right) \tag{3}$$

3. 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 2. Each node determines its forwarding strategy when it receives a packet by querying the pre-computed oracle, till the packet reaches the destination.

We use reachability techniques applied to Def. 1 to determine with what probability packets will reach some goal node, denoted *end*. We 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 [1], 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.

$$RA_{start}^{\tilde{\pi},T}(\tilde{\mathcal{N}}, end) = \mathbb{E}\left[\sum_{t=1}^{T}\left(\prod_{i=0}^{t-1}\mathbf{1}_{\tilde{\mathcal{N}}}(x_i)\right)\mathbf{1}_{end}(x_t)\right] \tag{4}$$

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 mapping the current state to a routing decision, $\pi_t(n_t, \overline{q}_t) = u_t$. Eq. (4) 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 find an upper bound on the reachability probability (4) 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, (4) must be evaluated according to the optimal policy $\tilde{\pi}^*$. Both problems can be jointly solved using a dynamic programming formulation. The following recursion, modified from [1], is iterated backwards in time starting at T and ending at 0.

$$V_T^*(n, \overline{q}) = \mathbf{1}_{end}(n) \tag{5}$$

$$V_t^*(n, \overline{q}) = \max_{u \in \mathcal{U}(n,\overline{q})} \Bigg\{ \mathbf{1}_{end}(n) + \sum_{\overline{q}_{t+1} \in \{0,1\}^M} V_{t+1}^*(\tilde{\pi}_t^*(n, \overline{q}), \overline{q}_{t+1}) T_q(\overline{q}_{t+1} \mid \overline{q}) \Bigg\} \tag{6}$$

Equation (5) is evaluated first for all $(n, \overline{q}) \in \mathcal{N} \times \{0,1\}^M$, to get the so-called "value function" at time T, and then for all $t = T-1, \ldots, 0$, the value function (6) is calculated recursively for every $(n, \overline{q})$, finally producing $V_0(n, \overline{q})$, where $V_0(start, \overline{q}_0) = RA_{start}^{\tilde{\pi}^*,T}(\mathcal{N}, end)$. The value function $V_t(n_t, \overline{q}_t)$ 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.

4. NUMERICAL EXPERIMENTS

The system presented in Section 3 can predict the reliability of a packet transmission, given the independent availability values or Markov transition probabilities of the links in the network. 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. Predicted reliability from our model was based on both stationary link probabilities and Markov link probabilities. Simulations in OPNET were carried out using the wireless network deployment tool with uniform random node placement. We used the *wlan_wkstn_adv* node model for ad hoc nodes to run simulations with standard implementations of AODV and OLSR. Wireless link failures were simulated using the radio module in OPNET.

5. CONCLUSIONS

In this research, we presented a theoretical technique to model a wireless multihop network as a stochastic dynamical system. This model allowed us to apply 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 compared prediction from our approach to applications in real network scenarios. We also compared our model to existing routing protocols such OLSR and AODV. Results show that our model predicts the optimal reliability values, and successfully bounds reliability of standard routing protocols. Although this approach can be computationally expensive to apply as a routing protocol for large networks, it can be a useful tool to analyze the maximum achievable reliability in a given network.

6. REFERENCES

[1] S. Summers and J. Lygeros. Verification of discrete time stochastic hybrid systems: A stochastic reach-avoid decision problem. *Automatica*, 46(12):1951–1961, 2010.