On the reliability of WiFi multihop backhaul connections for rural areas

Zainab Zaidi
zzaidi@ieee.org

Abstract—In this paper, reliability of WiFi multihop backhaul connections, in terms of probability of successful packet delivery, is analyzed in detail. The major issue in providing a cost-effective rural broadband network is to connect the remote sites to the existing network and with each other over distances of tens or hundreds of miles. There has been a lot of research activity around long distance WiFi links. These links require high-gain directional antennas and very expensive tall towers to maintain LoS (Line-of-Sight). In this paper, we evaluated, using empirical models, the idea of using multiple hop connections in linear topology, also termed as multihop chains, for rural backhaul. Reliability of WiFi chains is evaluated in adverse conditions of radio propagation and in the presence of node failures. This analysis shows promising potential of cost-effective WiFi chain networks as backhauls with reasonable reliability. Considerable improvement in reliability and robustness can be achieved by providing some redundancy in network topology. Networks with redundant nodes can tolerate larger separation between adjacent nodes, thus reducing the overall deployment cost.

I. INTRODUCTION

In developing regions of the world, WiFi technology is not an alternative, rather the only solution to provide connectivity mainly due to economic constraints. Wire-line technologies, such as, cable, DSL, dialup are too expensive for remote areas merely because of sparse and low density population. WiFi, i.e., 802.11 technology, offers a cost-effective alternative. According to a study, a WiFi deployed node could be more then 2-3 order of magnitude cheaper than cellular and WiMax nodes [1]. Satellite communication, though offers best rural coverage, is also very expensive to use. The cost of 1Mbps connectivity in Africa exceeds $3000/month [2]. There are several initiatives around the globe to bring the remote communities closer to the rest of the world but most of the efforts are still in experimental phases. Some notable efforts are listed in Table I. All of these initiatives were started within the last decade and almost all use WiFi or some variant of WiFi to provide connectivity. The networks were mainly deployed to provide broadband access to rural communities besides providing e-health, remote learning, e-governance services, etc.

On the other hand, unavailability of maintenance personal, harsh climate, hostile environment, frequent power breakdowns, etc. pose serious questions about the practicality and survivability of WiFi based solutions. Also, WiFi is not designed to transfer data over very long distances and form backhaul links, which are very common in remote rural settings. The classic solution for increasing reliability of WiFi multihop networks by providing multiple paths trough the mesh is also not realizable in such operational settings. DakNet [6] provides another solution to cover longer distances in an inexpensive manner by means of mechanical backhauls, such as, WiFi transceivers mounted on buses or trucks, but it prohibits the use of real-time applications, such as, VoIP and interactive video which are termed as killer apps for rural broadband [1].

There has been a lot of research activity around long distance WiFi links as shown in Table I. The record to-date is 6 Mbps link over 384 km in Venezuela. These links require LoS (Line-of-Sight) for sufficient signal-strength otherwise signal attenuation in 2.4-5 GHz range is too high beyond a few hundred meters [1]. In order to provide LoS, significant infrastructure in terms of antenna towers is required [1]. Tall towers are one or two orders of magnitude costlier than the radio equipment [1]. The use of high-gain directional antennas also increases the cost considerably. High altitude sites are preferred for long-distance WiFi links to reduce the cost of towers but these sites are usually difficult to access.

In this paper, we evaluate the idea of using multihop linear chain network instead of a single link to cover large distances. Such networks can be deployed along the existing roads, making them easily accessible and can utilize the available utility poles and resources further reducing the cost. The major concerns with such solution are:

- Every node in a wireless multihop chain can be thought of as a single point of failure.
- WiFi throughput is shown to decrease at a better than linear rate inversely proportional to the number of hops away from the gateway in a multihop network limiting the network size per gateway [3].

The present paper is only concerned with the first point. We have simulated node failures and unreliability of wireless medium through empirical propagation models and estimated upper bound on probability of packet delivery over a distance when packet can be delivered via any possible path, i.e., two neighboring nodes can also by-pass an intermediate node and connect with probably a weaker link. Such redundant connections can increase reliability of WiFi chains in wake of node failures. Reliability of the network can also be improved by using redundant nodes along the chain. Such ideas of backoff...
nodes are also briefly discussed in [1]. This study is the first step towards a more comprehensive feasibility study of WiFi multihop backhauls which will include the effects of specific routing and MAC protocols, environmental/terrain factors and other design issues, such as, bandwidth and capacity, security, availability/non-availability of alternative power sources, and more detailed performance measures, i.e., throughput and delay. The present paper shows that by taking certain measures at the deployment stage, reliability of chain networks can be considerably improved and multihop WiFi chain can provide a low cost alternative to long-distance WiFi links.

II. PRELIMINARIES

A. RELIABILITY OF A WIRELESS LINK

The fundamental element of our analysis is the probability of successful packet delivery over a wireless link considering the effects of radio propagation environment. The rural radio propagation environment can be closely represented by free-space models and it is sufficient to consider LoS models only. Moreover, these wireless chains in rural settings will most probably be operating in low external interference regions and RTS/CTS type mechanisms will take care of hidden node issue and collisions could be reduced to a minimal level.

Most of the empirical path loss models [7] are useful for cellular network settings. These models are evaluated and adjusted for Wireless LAN (WLAN) frequencies [8]. In this paper, we used empirical Okumura-Hata (OH) model for free space path loss [7] with suitable parameters and compared it with a specific outdoor path loss model for 2.4 GHz [8]. Both models yield similar results as discussed later. The basic propagation model with shadowing noise is as follows [7]:

\[ P_r(d)_{(dBm)} = EIRP_{(dBm)} + 10 \log_{10}(G_r)_{(dB)} - L_p(d)_{(dB)} + \epsilon(d), \]  

where \( P_r(d) \) (in dBm) is the received power in dBm at a distance \( d \) from the transmitter, \( EIRP_{(dBm)} \) is the Effective Isotropically Radiated Power in dBm, \( G_r \) is the receiver antenna gain, \( L_p(d)_{(dB)} \) is the path loss at distance \( d \) in dB, and \( \epsilon(d) \) is the log-normal shadowing noise with standard deviation \( \sigma_\epsilon \). In this analysis, \( EIRP_{(dBm)} \) is taken as 36 dBm for 2.4 GHz which is the maximum allowable point-to-point values from FCC (Federal Communications Commission), USA. It is reasonable to assume that the antennas used for transmission will also be used for reception of signals and the maximum allowable transmitter antenna gains from FCC can be used as the values of \( 10 \log_{10}(G_r)_{(dB)} \), i.e., 6 for 2.4 GHz. Typical value for \( \sigma_\epsilon \) for free space is 8 dB [7]. According to Okumura-Hata (OH) model, path loss \( L_p(d)_{(dB)} \) in (1) for free space is as follows [7]:

\[ L_p(d)_{(dB)} = A + B \log_{10}(d) - D, \]

where \( d \) is the distance of receiver from the transmitter in km, \( A = 69.55 + 26.16 \log_{10}(f_c) - 13.82 \log_{10}(h) - a(h), \)

\( B = 44.9 - 5.55 \log_{10}(h) \), and \( D = 40.94 + 4.78 \log_{10}(f_c)^2 - 18.33 \log_{10}(f_c). \) Here \( a(h) = [1.1 \log_{10}(f_c) - 0.7]h - [1.56 \log_{10}(f_c) - 0.8], h \) is the height of the wireless nodes from ground in m, and \( f_c \) is the carrier frequency in MHz. According to the specific model described in [8], the path loss \( L_p(d)_{(dB)} \) is given as:

\[ L_p(d)_{(dB)} = 40 \log_{10}(d) + 20 \log_{10}(f_c) - 40 \log_{10}(h), \]

where \( d \) is distance between nodes in m, \( f_c \) is carrier frequency in GHz, and \( h \) is the height of nodes from ground. For simplification in analysis, we assume that all of the nodes in multihop chain are erected at the same height and are located at equal distances. If receiver sensitivity is \( P_r^{Th} \), probability of successful delivery \( p(d) \) of a message over a link \( d \) m long, termed as link probability in this paper, is given as

\[ p(d) = \Pr(P_r(d) \geq P_r^{Th}) = Q \left( \frac{P_r^{Th} - EIRP - 10 \log_{10}(G_r) + L_p(d)}{\sigma_\epsilon} \right), \]

where \( P_r(d) \) is given in (1) and \( Q(x) = \int_x^\infty e^{-\frac{t^2}{2}} dt. \)

B. NODE FAILURE MODEL

It is difficult to predict typical equipment failure rate. The likelihood of mechanical parts’ failure, in general, increases with usage. In this paper, a generic model is presented to represent the condition of inoperativeness of nodes which could result from a number of causes, e.g., power failures, intentional or unintentional human intervention, environmental factors, accidental damages, software/hardware malfunctions, etc., besides failure of mechanical parts.

We have considered two types of situations for node failure. The first simpler model assumes iid node failures with probability \( p_f \). The value of \( p_f = 10^{-5} \) is selected for most of our experiments. It might be reasonable to assume independence of failure from one node to another when it is caused by malfunctions or human intervention, but failures due to power breakdown or climate affects a considerably larger region instead of a single node. In order to model such failure, three new variable are defined: 1) \( p_c \): probability that a given node failure is due to a regional failure, 2) \( d_c \): range of a regional failure, 3) \( p_{fr} \): probability of failure for nodes within the range of regional failure. A value of 20 km is selected for our experiment which is high enough for a massive power breakdown and weather related havoc and will help us in stress-testing the chain topologies. \( p_{fr} \) is selected to be 0.99 just to cater for the lucky instances when a node might be working in a disaster situation and \( p_c \) is arbitrarily selected to be 0.5.

III. CHAIN TOPOLOGIES AND RELIABILITY UPPER BOUNDS

Different topologies for multihop network, used in this study, are shown in Fig. 1. A simple chain is the most common configuration of placing one node after another. A trivial setting of putting two chains together instead of one, called a double chain, is also used to benchmark the improvement in reliability. The third configuration of chain multihop network in Fig. 1 is termed as a rhombus chain where every other node has a redundant peer node. The redundancy should help in improving the reliability comparing
to a simple chain. The fourth topology is called a hybrid chain and redundant peer is provided to every \( m \)th node. Not all possible links are shown in Fig. 1. In this section, we define the upper bound on reliability of a WiFi chain when a packet can be delivered through any of the possible paths. Since a close form expression for the probability of the union of all possible events of packet delivery is not trivial, we have estimated the probabilities via simulation. The simulations are verified though for different test cases.

### A. Simple Chain

To calculate reliability upper bound for a simple chain, we assume that node \( n \) can receive packets from node \( n-1 \) along with packets from nodes \( n-2, n-3, \ldots \) over possibly weaker links as shown by the arcs in Fig. 1. The probability of successful delivery of a message at node \( n \) from all the previous nodes, \( P(n) \), of a simple chain with equidistant nodes \( d \) \( m \) apart from each other is given as

\[
P(n) = (1 - p_f) \sum_{i=1}^{n} \left[ p_i \prod_{j=1}^{i-1} (1 - p_j) \right]
\]  

(5)

where \( p_f \) is the probability of a node failure and \( p_i = p(id)P(n-i) \), where \( p(d) \) is calculated from (4). In this section, all nodes are assumed to have iid failures and each link is considered to be independent. The situation of failures affecting a larger region is discussed later in the analysis section. The closed form expression of (5) is not trivial and we resort to simulate it. For validation of the simulation, we derived \( P(n) \) for two test cases only: (1) when only \( n-1 \) is allowed to forward the data to \( n \), (2) when \( n-1 \) and \( n-2 \) are allowed to forward packets to \( n \). For the first case, expression (5) reduces to

\[
P(n) = (1 - p_f)p(d)P(n-1),
\]  

(6)

\[
P(0) = [(1 - p_f)p(d)]^n.
\]  

(7)

\( P(0) \) is considered to be 1 in this study. For case (2), the derivation of \( P(n) \) is non-trivial. The probability that node \( n \)

As shown in Fig. 2, our simulations matches perfectly with the analytical calculations of \( P(n) \) for the above mentioned two cases. The distance between the nodes is varied as shown in Fig. 2, but the total distance spanned by the chain remains 1000 km in all cases. Number of nodes \( n \) are different for each internodal distance. Typical values of propagation model parameters for \( f_c = 2.4 \) GHz, as given in Section II-A, are used for Fig. 2. Antenna height is selected to be 9 m, the height of a utility pole, and the probability of node failure \( p_f \) is selected to be \( 10^{-3} \). \( P(n) \) calculated from Okumura-Hata model is slightly larger than that calculated from 2.4 GHz specific model, (3), as shown in the figure. However, both models yield similar trends. The right most curves in Fig. 2, shows the probability \( P(n) \) when simulation is extended for general case of receiving all possible signals.

Interestingly, consideration of redundant paths from node \( n-2 \) to node \( n \) brings significant improvement in the chain network reliability. When only a single path is considered along the chain, reducing the distance between the nodes has two effects:1) improving received signal strength and 2) increasing the number of nodes for the fixed distance and hence increasing the network vulnerability in wake of equipment failure. The two phenomena are responsible for the convex shape of the curve. The vulnerability caused by node failures can be addressed to a reasonable extent by consideration of redundant paths as shown by our results in Fig. 2. The general case of receiving messages from any of the previous nodes is shown by the right most curves which are representing the reliability upper bound of a simple chain network.

### B. Double Chain

The double chain configuration, as shown in Fig. 1, should give the best reliability performance, for same link separation, among the topologies considered in this study. It is assumed that both chains consist of same number of equidistant nodes \( d \) \( m \) apart from each other and the distance between each
\[ P(n) = (1 - p_f) \sum_{i=1}^{2} p_i \prod_{j=1}^{i-1} (1 - p_j) \]

\[ = \begin{cases} 
C_2^{n/2} + (d)(1 - p_f)^2 \left( C_2^{n/2 - 1} - C_2^{n/2 - 1} \right), & n \text{ is even;} \\
\frac{d}{2} - p(d) + (p(d))^3 \left( C_2^{n/2 - 1} - C_2^{n/2 - 1} \right) + \\
\frac{d}{2} - p(d)(2d)(1 - p_f)^2 \left( (1 - p(d))^3 \right) C_2^{n/2 - 1} - \frac{p(d)(2d)(1 - p_f)^2 \left( 1 - C_2^{n/2 - 1} \right) C_2^{n/2 - 1}}, & n \text{ is odd.}
\end{cases} \]

where

\[ C_1 = p(2d)(1 - p_f)(1 - C_2^0(1 - p_f)) + C_2, C_2 = p(d)(1 - p_f)^2 + p(2d)(1 - p_f) - p(d)^2 p(2d)(1 - p_f)^2, \text{ and} \]

\[ C_3 = (1 - (1 - p(d))(1 - p(2d))). \]

redundant pair of nodes is \( d_c \). \( d_c = 1 \) m is sufficient for independent and uncorrelated links in both chains. It is important to note that a double chain is only analyzed to benchmark the performance of different topologies and, although, the reliability of the double chain would be better than a simple chain but additional contention in the medium would result in extra latency and reduced capacity. In this case, the probability of successful packet delivery at node \( n \), \( P(n) \), of either of the chains, from all the previous nodes is

\[ P(n) = (1 - p_f) \sum_{i=1}^{n} [p_i + p_i^* (1 - p_i)] \times \prod_{j=1}^{i-1} \left( (1 - p_j)(1 - p_j^*) \right) \]

where \( p_i = p(id)P(n - i) \) and \( p_i^* = p(d_c)P(n - i^*) \), where \( d_c = \sqrt{d_2^2 + (id)^2} \) and \( n^* \) refers to the node \( n \) of the other chain. Also, perfect links are assumed between peer nodes.

C. Rhombus Chain

A rhombus chain in Fig. 1 refers to the topology where every other node has a redundant peer. It is assumed that the distance between the peer nodes is \( d_c \) and there is perfect link between them. In this study, \( d_c = 1 \) m. In this case, the probability of successful delivery of a message at node \( n \), where \( n = 1, 3, 5, \cdots \), from all the previous nodes is

\[ P(n^u) = (1 - p_f) \sum_{i=1}^{n} p_i \prod_{j=1}^{i-2} (1 - p_j) + \left[ \sum_{i=2}^{n} \left[ p_{i,uu} + p_{i,uu}(1 - p_{i,uu}) \right] \prod_{j=1,3}^{i-1} (1 - p_{i,uu}) \right] \times \prod_{j=2,4}^{i-2} (1 - p_{j,uu})(1 - p_{j,uu}) \]

where \( p_{i,uu} = p(d_{ai})P(n - i) \), \( d_{ai} = \sqrt{(d_2^2 + (id)^2)} \), \( p_{i,lu} = p(d_{bi})P(n - i^l) \), \( d_{bi} = \sqrt{(d_2^2 + (id)^2)} \), \( p_{i,uu} = p(id)P(n - i^u) \), \( n^u \) refers to upper node, and \( n^l \) refers to lower node at the \( n^{th} \) position of a rhombus chain as shown in Fig. 1. Similarly,

\[ P(n') = (1 - p_f) \sum_{i=1,3,5}^{n} p_i \prod_{j=1}^{i-2} (1 - p_{j,cl}) + \left[ \sum_{i=2,4}^{n} \left[ p_{i,cl} + p_{i,ul}(1 - p_{i,ul}) \right] \prod_{j=1,3}^{i-1} (1 - p_{i,ul}) \right] \times \prod_{j=2,4}^{i-2} (1 - p_{j,ul})(1 - p_{j,ul}) \]

where \( p_{i,cl} = p(d_{ai})P(n - i) \), \( p_{i,ul} = p(id)P(n - i^l) \) and \( p_{i,ul} = p(d_{bi})P(n - i^u) \). \( P(n) \) for \( n = 2, 4, 6, \cdots \) is given as

\[ P(n) = (1 - p_f) \sum_{i=2}^{n} p_i \prod_{j=1}^{i-2} (1 - p_j) + \left[ \sum_{i=2,4}^{n} \left[ p_{i,uc} + p_{i,lc}(1 - p_{i,lc}) \right] \prod_{j=1,3}^{i-1} (1 - p_{i,lc}) \right] \times \prod_{j=2,4}^{i-2} (1 - p_{j,uc})(1 - p_{j,lc}) \]

where \( p_{j,uc} = p(d_{ai})P(n - i^u) \) and \( p_{j,lc} = p(d_{ai})P(n - i^l) \)

D. Hybrid Chain

The fourth topology in Fig. 1 is called a hybrid chain and a redundant peer is provided to every \( m^{th} \) node. The first node with a redundant peer is \( m - 1 \). Double and rhombus chains are special instances of hybrid chain with \( m = 1 \) and \( m = 2 \) respectively. The distance between the peer nodes is assumed to be \( d_c = 1 \) m and perfect links are assumed between them. In this case, \( P(n) \) at node \( n = jm - 1 \), where \( j = 1, 2, \cdots \), from all the previous nodes is given in (14), where \( p_{i,uu}, p_{i,ul}, p_{i,uu}, p_{i,uu}, \cdots \), are defined in the previous section, \( j = 1, 2, \cdots < (n + 1)/m \), \( n^u \) refers to upper node, and \( n^l \) refers to lower node at the \( n^{th} \) position. Similarly, for \( n^l \), \( P(n) \) is given in (15) and for the rest of the nodes, \( P(n) \) is given in (16).
height is assumed to be

The estimated probability $P(n)$ of double, rhombus, and hybrid chains, with different values of $m$, are compared with $P(n)$ of a simple chain in Fig. 3. In this simulation, a distance of 1000 km is assumed to be spanned by $n$ nodes. The number of nodes $n$ changes as the distance between the nodes is varied. Okumura-Hata model is used to calculate link probabilities with typical parameter values listed in Section II-A. Antenna height is assumed to be 9 m. $p_f$ is selected as $10^{-3}$.

It is clear from Fig. 3 that a double chain has much better reliability than a simple chain and a rhombus chain exhibits similar reliability performance as a double chain as every other node has a redundant peer. The values $m = 1$ and $m = 2$ are only used to validate the simulations of hybrid chain with that of double and rhombus chain. It is clear from Fig. 3 that with $m = 1$, a hybrid chain becomes a double chain and with $m = 2$, it becomes a rhombus chain. The reliability performance of a hybrid chain is better than a simple chain and it improves as we increase the redundant pairs. It is, however, interesting to see that the improvement in reliability is not always linearly proportional to number of redundant nodes. We should keep in mind that this study is using empirical propagation models only and reliable very long links might not be possible in practical scenarios. Testbed experiments are needed to re-calibrate the propagation model and probability simulations.

### IV. ANALYSIS OF CHAIN TOPOLOGIES

**Fig. 3. $P(n)$ vs. distance between nodes.**

The estimated probability $P(n)$ of double, rhombus, and hybrid chains, with different values of $m$, are compared with $P(n)$ of a simple chain in Fig. 3. In this simulation, a distance of 1000 km is assumed to be spanned by $n$ nodes. The number of nodes $n$ changes as the distance between the nodes is varied. Okumura-Hata model is used to calculate link probabilities with typical parameter values listed in Section II-A. Antenna height is assumed to be 9 m. $p_f$ is selected as $10^{-3}$.

It is clear from Fig. 3 that a double chain has much better reliability than a simple chain and a rhombus chain exhibits similar reliability performance as a double chain as every other node has a redundant peer. The values $m = 1$ and $m = 2$ are only used to validate the simulations of hybrid chain with that of double and rhombus chain. It is clear from Fig. 3 that with $m = 1$, a hybrid chain becomes a double chain and with $m = 2$, it becomes a rhombus chain. The reliability performance of a hybrid chain is better than a simple chain and it improves as we increase the redundant pairs. It is, however, interesting to see that the improvement in reliability is not always linearly proportional to number of redundant nodes. We should keep in mind that this study is using empirical propagation models only and reliable very long links might not be possible in practical scenarios. Testbed experiments are needed to re-calibrate the propagation model and probability simulations.

### A. Number of nodes

**Fig. 4. $P(n)$ vs. number of nodes.**

Number of nodes are linearly proportional to the network deployment/maintenance cost. More nodes, in general, mean higher cost. Reliability or $P(n)$, from the experiment of Fig. 3, is plotted against number of nodes in Fig. 4. We are interested in the region where changing $n$ changes $P(n)$. Once $P(n)$ is unity, adding more nodes does not bring any benefit. For this experiment, $P(n) \geq 90\%$ is possible when $n$ is 182 for the simple chain, 150 for the double chain, 130 for the rhombus chain, and 141 and 147 for the hybrid chain with $m = 5$ and $m = 10$ respectively. Larger separation between the nodes degrades received signal strength but redundancy of nodes
provides robustness against equipment failure improving the overall reliability of the network while reducing the cost.

Although, it is not fair to compare our theoretical results with the practical deployments but just to get an idea about the cost per transmitted bit per meter in both cases, we assume that the radio equipment costs $50 per node and each 9 m pole costs $100 [1]. If existing utility poles are used for the deployment, then pole cost can be taken out from the estimate. We also assume additional $50 per node for alternate supply of power, such as small solar panel to power up the WiFi node. The best case shown in Fig. 4, i.e., 130 nodes of rhombus chain yielding almost 100% reliability over 1000 km will cost $26,000 or $13,000 using existing poles. With 802.11g nodes, the maximum data rate can be 54 Mbps. The actual throughput of the multihop chain is affected by the specific MAC and routing protocols but the upper bound remains 1/3 of the maximum data rate, which is 18 Mbps in case of multihop chain using 802.11g nodes. The lower bound for cost per Mb per km in this case is $1.44 or $0.72 when existing poles are used. Whereas if long-distance WiFi technology is used, the cost for each node could be $5500, e.g., $500 for Intel’s rural connectivity platform (RCP), a special WiFi node with high-gain directional antenna designed for rural settings, with a $5000 tower [1]. Intel’s RCP was shown to deliver 6 Mbps over 100 km. The cost per Mb per km in this case is $18.3. Note that we have also considered node failures with multihop chain backhaul, where as a long-distance link would be inactive if either of the nodes fails.

B. Node failure rate

We also modeled failures affecting a larger region as given in Section II-B. Simulation of Fig. 4 is executed with regional failure model with typical parameter values from Section II-B with $p_f = 0.1$ to produce Fig. 5. Interestingly, chains with redundant nodes are still exhibiting some resilience whereas simple chain is completely inoperative in Fig. 5. A broader view of the results of this experiment is available in Fig. 6, where $P(n)$ is plotted against $d$. Comparing this figure with Fig. 3, which is drawn for the similar settings except with iid

\[ P(n) \text{ vs. number of nodes when } p_f = 0.1 \text{ and regional failures are also possible.} \]

\[ P(n) \text{ vs. distance between nodes when } p_f = 0.1 \text{ and regional failures are also possible.} \]

failures with $p_f = 10^{-3}$, we can see that when separation between nodes are smaller, there are larger number of nodes affected by the regional failures and the network reliability is small for all topologies. For larger separation, a higher $p_f$ with weaker links are the causes of lower reliability when compared with Fig. 3. Fig. 6 shows optimum values for $d$ for different chains yielding best $P(n)$.

V. CONCLUSION

In this paper, upper bound on reliability of wireless multihop chain networks is studied in terms of probability of successful packet delivery. Our analysis shows that it is possible to deploy a WiFi multihop chain backhaul spanning long distances with reasonable resilience against uncertain radio propagation and node failures which also costs less than the existing state-of-the-art of WiFi long-distance point-to-point backhaul. Improvement in robustness of chain networks can be achieved by adding redundancies in network topology. Although, a practical deployment should also consider other factors, such as, terrain factors, QoS parameters, etc.

REFERENCES


