8

The Performance of Wireless Mesh Networks with Apparent Link Failures

Geir Egeland[1], Paal E. Engelstad[2], and Frank Y. Li[3]
[1]*Department of Electrical and Computer Engineering, University of Stavanger*
[2]*Simula and Telenor Corporate Development, University of Oslo*
[3]*Department of Information and Communication Technology, University of Agder*
Norway

1. Introduction

A wireless multi-hop network is a network consisting of a group of nodes interconnected by the means of wireless links. The nodes in such a network, which are often self-configured and self-organized, communicate with each other over multiple hops through a routing protocol. Examples of such networks include Wireless Mesh Networks (WMNs) IEEE802.11s (2010), Mobile Ad Hoc Networks (MANETs) Chlamtac et al. (2003) and Wireless Sensor Networks (WSNs) Gharavi & Kumar (2003). The performance and the reliability of these networks depend heavily on the routing protocol's capability to detect link failures between neighboring nodes as well as its link-maintenance mechanism to recover a path from source to destination when a link-failure happens.

While MANETs generally appear more dynamic due to node mobility, the network topology for WMNs and WSNs remains comparatively stable. No matter which network form is concerned, however, these networks exhibit ad hoc features since wireless links are intrinsically unreliable. In the majority of cases, link failures are present in a multi-hop network regardless of the use of link-maintenance mechanisms. Sometimes link failures are unavoidable, such as when a mobile node deliberately leaves a network or is subject to the exhaustion of its battery power. In another case a link would cease to be operative when two nodes move outside each others' radio transmission range. In addition to these, a set of link failures which we refer to as *apparent link-failures* exist. They are primarily caused by radio links being vulnerable to radio induced interference, but also appear when a link-maintenance mechanism erroneously assumes a link to be inoperable due to *loss of beacons*. A beacon is a short packet transmitted periodically to a node's one-hop neighbors and its purpose is to detect neighbors and to keep links alive. Beacons are normally broadcast, and are thus not acknowledged, i.e. they are unreliable and vulnerable to overlapping transmissions from hidden nodes Tobagi & Kleinrock (1975). Moreover, common protection mechanisms against hidden nodes (such as RTS/CTS of the IEEE 802.11 MAC protocol IEEE802.11 (1997)) are not applicable, since unicast data transmission using RTS/CTS will only provide protection for packet reception at the node that issued the CTS.

1.1 Motivation and methods

Although a huge number of efforts have been made in the research community during the past decade on various facets of wireless multi-hop networks, little attention has been paid to the reliability aspect of such networks. In this chapter, we propose an analytical model for apparent link-failures in static mesh networks where the location of each node is carefully planned (referred to hereafter as *planned mesh network*). A planned mesh network typically appears as a consequence of the high costs associated with interconnecting nodes in a network with wired links. For example, ad hoc technology can in a cost-efficient manner, extend the reach of a wired backbone through a wireless backhaul mesh network. Apparent link-failures are often a significant cause for performance degradation of mesh networks, and thus a model is needed in order to diminish their effect. For instance, with a model in place it is possible to detect and avoid undesirable topologies that might lead to a high frequency of such failures.

The proposed model makes use of the assumption that the probability of losing a beacon due to a packet collision with transmissions from hidden nodes (p_e), is much larger than the probability of losing beacons due to transmissions from one-hop neighbors (p_{coll}). The probability that a receiving node considers a link to be inoperative at the time a beacon is expected, is then estimated through analysis using a Markov model. Furthermore, an algorithm which is used for determining the number of hidden nodes and the associated traffic pattern is introduced so that the model can be applied to arbitrary topologies.

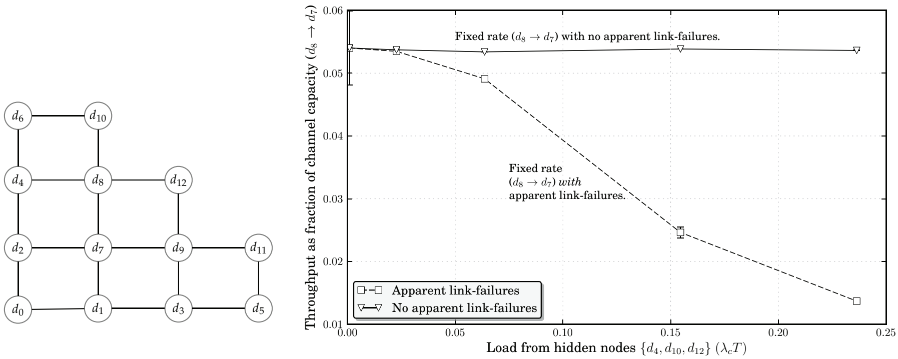
1.2 Significance of our results

By avoiding poorly planned topologies, not only the reliability of mesh networks can be increased, but also the general performance of such networks can be improved. Apparent link-failures are often a significant cause for performance degradation of ad hoc networks since erroneous routing information may be spread in the network when apparent link-failures happen. Also, it might lead to a disconnected topology or less optimal routes to a destination. Analysis of a real life network Li et al. (2010) has demonstrated that it takes a significant amount of time to restore failed links Egeland & Li (2007). An example of the effect of these failures is illustrated in Fig. 1. Using a well known network simulator ns2 (2010) we have measured the throughput from node $d_8 \rightarrow d_7$ in the topology shown in Fig. 1(a). As the load from the hidden nodes increases, the throughput from node $d_8 \rightarrow d_7$ is reduced, because the routing protocol forces the data packets to traverse longer paths in order to bypass the apparent link-failure or simply because node d_7 drops packets when buffers are filled as a result of having no operational route to node d_8. The throughput would remain relatively stable if the apparent link-failures were eliminated, as seen from the "No apparent link failure" graph in Fig. 1(b).

The model presented in this chapter allows a node to calculate the probability of losing connectivity to its one-hop neighbors caused by beacon loss. Utilizing the model, we demonstrate how a node in a mesh network operated on the *Optimized Link State Routing* (OLSR) Clausen & Jacquet (2003) routing protocol can apply the apparent link-failure probability as a criterion to decide when to unicast and when to broadcast beacons to surrounding neighbors, thus improving the packet delivery capability.

1.3 Related work

In Voorhaen & Blondia (2006) the performance of neighbour sensing in ad hoc networks is studied, however, only parameters such as the transmission frequency of the Hello-messages and the link-layer feedback are covered. In Ray et al. (2005) a model for packet collision and the effect of hidden and masked nodes are studied, but only for simple topologies, and the work is not directly applicable to the Hello-message problem. The work in Ng & Liew (2004) addresses link-failures in wireless ad hoc networks through the effect of routing instability.



(a) Example topology (b) Throughput from node $d_8 \to d_7$

Fig. 1. Performance with and without apparent link-failures. The possibility of apparent link failures is artificially removed by not allowing the links to time out when beacons are lost.

Here the authors study the throughput of TCP/UDP in networks where the routing protocol falsely assumes a link is inoperable. However, what causes a link to become unavailable to the routing protocol is not studied. A model for packet collision and the effect of hidden and masked nodes are studied in Ray et al. (2004), but only for simple topologies, and the work is not directly applicable to loss of beacons. Not much published work relates directly to the modeling of apparent link-failures caused by loss of beacons. In Egeland & Engelstad (2009) the reliability and availability of a set of mesh topologies are studied using both a distance-dependent and a distance-independent link-existence model, but the effects of beacon-based link maintenance and hidden nodes are ignored. Here it is assumed that apparent link-failures are a result of radio-induced interference only. The work in Gerharz et al. (2002) studies the reliability of wireless multi-hop networks with the assumptions that link-failures are caused by radio interference.

2. Network model

2.1 Network terminology

This chapter reuses the terminology of wireless mesh networks in order to describe the architecture of a planned mesh network, more specifically of the IEEE 802.11s specification IEEE802.11s (2010) of mesh networks. In this terminology a node in a mesh network is referred to as a *Mesh Point* (MP). Furthermore, an MP is referred to as a *Mesh Access Point* (MAP) if it includes the functionality of an 802.11 access point, allowing regular 802.11 Stations (STAs) access to the mesh infrastructure. When an MP has additional functionality for connecting the mesh network to other network infrastructures, it is referred to as a *Mesh Portal* (MPP). A mesh network is illustrated in Fig. 2.

A mesh network can be described as a graph $G(V, E)$ where the nodes in the network serve as the vertices $v_j \in V(G)$. Any two distinct nodes v_j and v_i create an edge $\epsilon_{i,j} \in E(G)$ if there is a direct link between them. In order to provide an adequate measure of network reliability, the use of probabilistic reliability metrics and a probabilistic graph is necessary. This is an undirectional graph where each node has an associated probability of being in an operational state, and similarly for each edge, i.e. the random graph $G(V, E, p)$ where p is

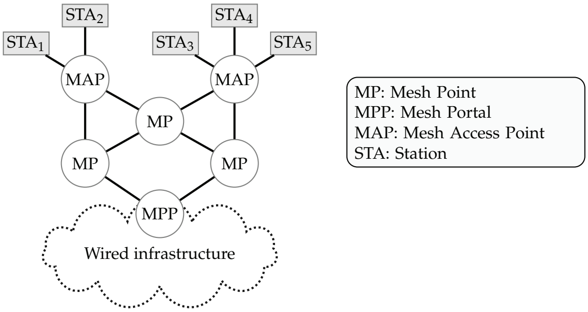


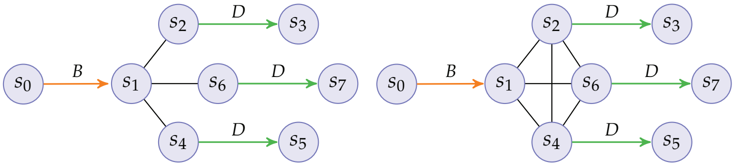
Fig. 2. A wireless mesh network connected to a fixed infrastructure.

the link-existence probability. An underlying assumption in the analysis is that the existence of a link is determined independently for each link. This means that the link $\epsilon_{s,d}$ may fail independently of the link $\epsilon_{i,j} \in E(G) \setminus \{\epsilon_{s,d}\}$. As the link failure probability in general is much higher than the node failure probability, it is natural to model the nodes $v_j \in V(G)$ in the topology as invulnerable to failures. Thus, a mesh network can be described and analyzed as a random graph.

2.2 Link maintenance using beacons

In a multi-hop network, links are usually established and maintained proactively by the use of one-hop beacons which are exchanged between neighboring nodes periodically. Beacons are broadcast in order to conserve bandwidth, as no acknowledge messages are expected from the receivers of these beacons. Thus, the link status of every link on which a beacon is received can be effectively obtained through beacon transmissions. Since broadcast packets are not acknowledged, beacons are inherently unreliable. A node anticipates to receive a beacon from a neighbor node within a defined time interval and can tolerate that beacons occasionally will be missing due to various error events like channel fading or packet collision. However, a node failed to receive a number of $(\theta+1)$ consecutive beacons will accredit that the node on the other side of the link is permanently unreachable and that the link is inoperable. The value of the configurable parameter θ is a tradeoff between providing the routing protocol with stable and reliability links (a large θ), and the ability to detect link-failures in a timely and fast manner (a small θ). Since beacons are broadcast, they are unable to take the advantage of the Request-To-Send/Clear-To-Send (RTS/CTS) signaling that protects the IEEE 802.11 MAC protocol's IEEE802.11 (1997) unicast data transmission against hidden nodes. Although some beacon loss is avoided using RTS/CTS for the *unicast data traffic* in the network, it will only affect the links of the node that issues the CTS. The consequence is that beacons will be susceptible to collisions with traffic from hidden nodes *even if* RTS/CTS is enabled. Thus, the utilization of a link may be prevented if the link is assumed to be inoperable due to beacon loss. Examples of routing protocols that make use of beacons are the proactive protocol OLSR Clausen & Jacquet (2003) and an optional mode of operation for the reactive *Ad hoc On-Demand Distance Vector* (AODV) routing protocol Perkins et al. (2003).

A major difference between various beacon-based schemes is how the routing protocol determines if a failed link is operational again. Stable links are desirable, and introducing a link too early can lead to a situation where a link oscillates between an operational and a non-operational state. A solution that avoids this situation is by measuring the Signal-to-Noise Ratio (SNR) of the failed link and define the link as operational only when



(a) Isolated hidden nodes (b) Connected hidden nodes

Fig. 3. Sample topologies where the hidden nodes $\{s_2, s_4, s_6\}$ are isolated or connected. When the hidden nodes send data (D), this may collide with the beacons (B) sent by node s_0.

both beacons are being received and the received SNR is above a defined threshold Ali et al. (2009). However, if SNR measurement is not available or not practical, a simple solution is to introduce some kind of hysteresis by requiring a number of consecutive beacons to be received $(\theta_h + 1)$ before the link is assumed to be operational. This is the solution chosen in this analysis.

3. Apparent link-failures due to beacon loss

3.1 Assumptions for the beacon-based link maintenance

Before we can determine the apparent link-failure probability, a model for identifying losing a single beacon caused by overlapping transmissions must be found. In order to simplify the analysis, the model is based upon three assumptions. First, it is assumed that a beacon sent by a node has a negligible probability of colliding with a beacon from any of the neighboring nodes. This is a fair assumption, since beacons are short packets that are transmitted periodically and at a random instant at a relatively low rate. Secondly, it is assumed that the probability of a beacon colliding with a data transmission from any of the (non-hidden) neighboring nodes also is negligible, i.e. $p_e \gg p_{coll}$. This assumption is also fair, since a MAC layer often has mechanisms that reduce such collisions to a minimum. Examples of such mechanisms are the collision avoidance scheme of the IEEE 802.11 MAC protocol with randomized access to the channel after a busy period, and the carrier- and virtual sense of the physical layer. Accordingly to the IEEE 802.11 standard, a beacon will be deferred at the transmitter if there is ongoing transmission on the channel. Therefore, the probability that beacons are lost, is a result of *overlapping data packet transmissions from hidden nodes only.* Thirdly, we make the assumption that the packet buffers of a node can be modeled as an $M/M/1$ queue Kleinrock (1975) and that the packet arrival rate is Poisson distributed with parameter λ_c and that the channel access and data packet transmission times are exponential distributed with parameter $1/\mu$.

These assumptions allow us to verify the model in a simple manner. Even though traffic in a real network may follow other distributions, the results presented later in the chapter suggest that the assumptions are fair. The bounds for beacon loss probability based on a large number of random independent traffic scenarios will be presented, and these capture more of the characteristics of the traffic in a real-life network.

3.2 Probability of losing a beacon p_e

Consider the topology in Fig. 3(a). We need to find firstly the probability (p_e) that the beacon from s_0 and a data packet from the hidden node s_2 collide. Let $q_{s_2}(0)$ denote the probability of

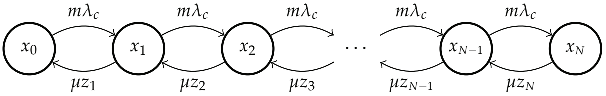


Fig. 4. A Markov model of the total number of packets waiting to be transmitted by the m hidden nodes, where λ_c is the packet arrival rate, $1/\mu$ is the service time and z_n is the average number of the m hidden nodes transmitting simultaneously.

node s_2 having zero packets awaiting in its buffer. p_e can be expressed as Dubey et al. (2008):

$$\begin{aligned} p_e &= \Pr\{\text{Collision}|q_{s_2}(0) > 0\} \cdot \Pr\{q_{s_2}(0) > 0\} \\ &\quad + \Pr\{\text{Collision}|q_{s_2}(0) = 0\} \cdot \Pr\{q_{s_2}(0) = 0\} \\ &= (1 - p_0) \cdot 1 + (1 - e^{-\lambda_c \omega_b / T_p}) \cdot p_0 \end{aligned} \tag{1}$$

where p_0 is the probability that the hidden node s_2 has zero packets awaiting to be transmitted. The parameters T_p and ω_b represent the average transmission time of the data packet and of the beacon packet, respectively. Both these transmission times are assumed to be exponentially distributed. The probability that a node has i data packets in its packet queue is given by $p_i = (1-\rho)\rho^i$, where $\rho = \lambda_c/\mu$, thus $p_0 = 1 - \rho$ Kleinrock (1975).

3.2.1 Isolated hidden nodes

We will now evaluate the probability that a beacon collides with data transmissions from a set of hidden nodes using the topology illustrated in Fig. 3(a). In this sample topology, the hidden nodes are assumed to be *isolated*, i.e. outside the transmission range of each other. Individually, the probability that one of them sends a data packet which overlaps with a beacon from node s_0 is given by Eq. (1) (denoted p_e). The number of data packets from $\{s_2, s_4, s_6\}$ overlapping with a beacon from s_0 is binomially distributed $B(m, p_e)$ where m is the number of hidden nodes. The probability that a beacon is lost can then be expressed as:

$$p_e^I = \sum_{k=1}^{m} \binom{m}{k} p_e^k (1 - p_e)^{m-k}. \tag{2}$$

3.2.2 Connected hidden nodes

In Fig. 3(b) the hidden nodes are all within radio transmission range of each other. When all the hidden nodes are connected, the calculation of the beacon loss probability is not as straightforward, and we need to make further simplified assumptions. Firstly, it is assumed that the nodes access the common channel according to a *1-persistent* CSMA protocol Kleinrock & Tobagi (1975). This might seem like a contradiction, since it was stated earlier that we assumed a MAC protocol that reduces the collisions between non-hidden neighbours to a minimum. However, for the case where the hidden nodes are connected, there will be a parameter (z_n) in the model that can be set to control to which extent transmissions between the hidden nodes are permitted to collide with each other. Secondly, it is assumed that the arrival rates at the different hidden nodes are not coupled, hence a Markov model can be used for the analysis.

Consider the Markov chain illustrated in Fig. 4. Each state represents the sum of all packets queuing up in the m hidden nodes. Here z_n is the average number of hidden nodes transmitting when a total of n packets are distributed amongst the hidden nodes.

We are now able to find the probability of being in state x_0, which is the case for which none of the hidden nodes have packets awaiting transmission (p_0^C). Using standard queuing theory Kleinrock (1975), it can easily be shown that this probability is given by:

$$p_0^C = \left[1 + \sum_{i=1}^{N} (m\rho)^i \left(\prod_{n=1}^{i} z_{n,i} \right)^{-1} \right]^{-1}, \quad \rho = \frac{\lambda_c}{\mu} \tag{3}$$

where $z_{n,i}$ is the average number of the m nodes transmitting simultaneously and is calculated according to:

$$z_n = \begin{cases} \dfrac{\sum_{k=1}^{n} k \binom{m}{k} \binom{n-1}{k-1} (1-\rho^m)}{\sum_{k=1}^{n} \binom{m}{k} \binom{n-1}{k-1}} & \substack{n<m, \\ \rho=\lambda_c/\mu} \\ \dfrac{\sum_{k=1}^{m-1} k \binom{n-1}{k-1} (1-\rho^m)}{\sum_{k=1}^{m-1} \binom{n-1}{k-1}} + m\rho^m & \substack{n\geq m, \\ \rho=\lambda_c/\mu.} \end{cases} \tag{4}$$

The probability that one or more of the m nodes having zero packets in its buffer, given the sum of packets in the buffers is n, is given by the term $1 - \rho^m$ in Eq. (4). The combinations of k of m buffers containing packets, constrained by a total sum of n packets is given by $\binom{n-1}{k-1}$.
By substituting p_0 in Eq. (1) with p_0^C (Eq. (3)), the probability that transmissions from the connected hidden nodes overlap with a beacon can be calculated as:

$$p_e^C = 1 - p_0^C \cdot e^{-\lambda_c \omega_b / T_p}. \tag{5}$$

Before attempting to model more complex traffic patterns, i.e. arbitrary packet flows between different nodes, we must ensure that the basic model is capturing all possible transmission configurations. In fact, the initial model did not take into account the possibility that a neighbouring node receiving the beacon could be transmitting any data packets. Therefore, an approximate model will be provided, where the channel access time of the neighbouring node receiving the beacon is also taken into account. This model will be used in the next sub-section when random traffic patterns is analysed.
Again, consider the sample topology illustrated in Fig. 3(a). Let us assume that node s_1 has a traffic load with the rate λ_c and the probability that it gains access to the channel in order to transmit a packet is p_{s_1}. If the nodes $\{s_1, s_2, s_4, s_6\}$ are modelled as M/M/1 queues, the probability that e.g. node s_2 has no packets in its buffer can be expressed as:

$$q_{s_2}(0) = \left[1 + \sum_{k=1}^{N} \left(\frac{\rho}{1 - \rho p_{s_1}} \right)^k \right]^{-1} , \rho = \lambda_c / \mu. \tag{6}$$

An approximate expression for p_{s_1} is the probability that none of the neighbour nodes of s_1 have a packet in its buffer. The probability p_{s_1} is then given by $\prod_{i \in \{2,4,6\}} q_{s_i}(0)$ and can now be written as:

$$p_{s_1} \approx \left[1 + \sum_{k=1}^{N} \left(\frac{\rho}{1 - \rho p_{s_1}} \right)^k \right]^{-m} \tag{7}$$

where solutions for p_{s_1} can be found numerically and $m = |\{s_2, s_4, s_6\}|$. For the case of isolated hidden nodes in Fig. 3(a), the parameter p_0 in Eq. (1) can now be expressed as $q_{s_i}(0)$ in Eq. (6).

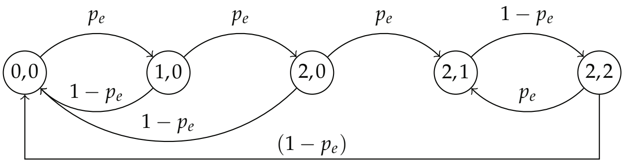


Fig. 5. A Markov model of a link-sensing mechanism with θ=2 and θ_h=1. The probability of losing a single beacon (p_e) is random and independent.

For the connected hidden nodes in Fig. 3(b), the probability p_{s_1} is equal to $1/(m+1)$, since each of the $m+1$ nodes gets an equal share of the common channel. Thus, p_0^C is rewritten as:

$$p_0^C = \left[1 + \sum_{i=1}^{N} (m\rho)^i \left(\prod_{n=1}^{i} z_{n,i} \left[1 - \frac{1}{m+1}\right]^i \right)^{-1} \right]^{-1}. \tag{8}$$

When the hidden nodes are connected, i.e. within each others transmission range, a packet arriving at one of the hidden nodes might have to wait until an ongoing transmission is finished before it is transmitted. When all the buffers are filled, the m hidden nodes will transmit simultaneously after an ongoing transmission is finished, thus emptying the buffers at a rate of $m \cdot \mu$. If we however change the model for the connected case, and enforce that the hidden nodes access the channel once at a time, the rate of emptying the buffers of the hidden nodes is reduced to μ, and can be calculated using Eq. (8) with z_n=1$\forall n$. The model will now resemble the IEEE 802.11 MAC protocol, which has mechanisms that aim to reduce collisions on the channel to a minimum. This will represent an *upper bound* for the beacon loss probability. We can now use the beacon loss probabilities in Eqs. (1)–(8) to calculate the link-failure probability p_f.

3.3 A model for apparent link-failures

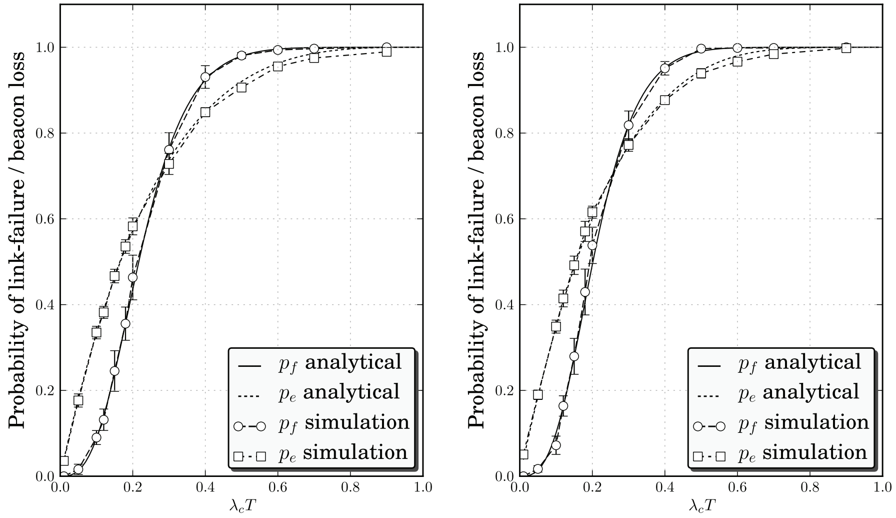
If we assume that the event of losing a beacon is random and independent, apparent link-failures can be analyzed using a Markov model as shown in Fig. 5 where the state variable $s_{i,j}$ describes the number of $i \in [0,\theta]$ beacons lost and $j \in [0,\theta_h]$ the number of beacons received in the hysteresis state. Solving the state equation in the model, it is easy to show that the probability of apparent link-failure (p_f) is the sum of the state probabilities $\sum_{j=1}^{\theta_h} p_{i,j}$. Thus, p_f can be expressed as:

$$p_f = \frac{(2-p_e)p_e^3}{(p_e^3 - p_e + 1)} \tag{9}$$

where p_e is the probability of losing a single beacon.

3.4 Analysis of the model's performance

In order to test the model's accuracy, a discrete-event simulation model was used. The simulator can model a two-dimensional network where every node transmits with the same power on the same channel. The sensing range (r_{cp}) of the physical layer is equal to the transmission range (r_{rx}). Even though this is not the case in a real-life network, it simplifies our analysis and provides to certain extent of topology control. Every node experiences the same path loss versus distance and has the same antenna gain and receiver sensitivity. A node receives a packet correctly only if the packet does not overlap with any other packet



(a) Results for Fig. 3(a)

(b) Results for Fig. 3(b)

Fig. 6. The probability of losing a beacon (p_e) and the probability of link-failure (p_f) for the topologies in Fig. 3. The simulation results are shown with a 95% confidence interval.

IP/MAC layer	Values	Physical layer	Values	Simulation	Values
Beacon/ Data	30/ 100 bytes	Propagation model	Free Space	Simulation/ transient time	900s/25s
MAC protocol	CSMA/CA	Data rate	11Mbps	Traffic/ Distribution	Poisson
Queue Length	50	Turn time	10 μs	Replications	50 times

Table 1. Simulation parameters.

transmitted by a node within its range. The propagation delay is assumed to be negligible and the nodes are static. The beacon-loss probability (Eqs. (1)–(8)) was verified in Egeland & Engelstad (2010), using both the simulation model and the widely used *ns2* network simulator ns2 (2010).

The results in Fig. 6 show the beacon loss probability (p_e) and the link-failure (p_f) probability for the topologies in Fig. 3. Both analytical and simulated results are shown. The simulation parameters are listed in Tab. 1. As can be verified from the figure, the results from our simulation model match well with the analytical results. The results confirm that the model provides sufficient accuracy, even though the model assumes that the length of the data packets are exponential distributed while a fixed packet length is used in the simulations.

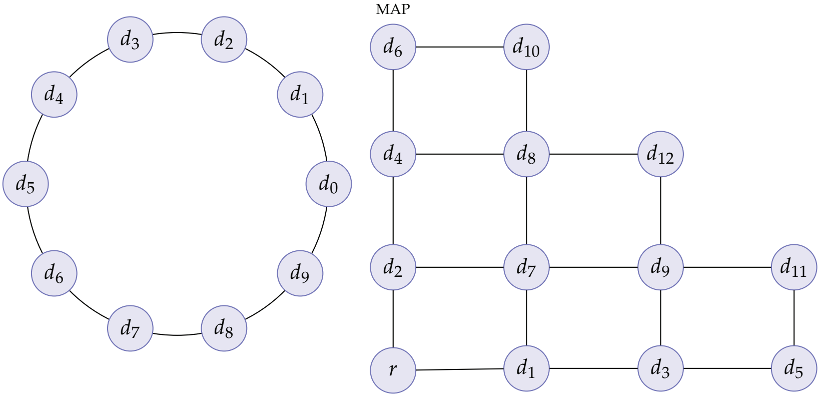
4. Apparent link-failures in arbitrary mesh topologies

4.1 Link-failure probability for complex traffic patterns

The apparent link-failure probability in Eq. (9) is only applicable for a topology with a specific connectivity between the nodes. In order to apply the apparent link-failure model on links in an arbitrary mesh topology with a given traffic pattern, an algorithm is needed to determine the number of hidden nodes and the associated traffic pattern that have impact on the rate of which the hidden nodes empty their buffers.

A wireless mesh topology can also be described as a *directed graph* $G=(V,E)$, where the nodes in the network serve as the vertices $v_j \in V(G)$ and any pair of nodes $v_j \to v_i$ creates an edge $\epsilon_{i,j} \in E(G)$ if there is a direct link between them. A random traffic pattern where a set of nodes transmit data over a link $\epsilon_{i,j} \in E(G)$ with the probability p_{tx} will also form a directed graph $S(V,E,p_{tx})$ that is a subset of G. It is assumed that every node $v_j \in S$ generates data packets at the same rate. Algorithm (1) calculates the number of neighbor nodes (h_u) of the vertice n that are hidden from a vertice $i \in V(G) : \epsilon_{i,n} \in E(G)$ where $h_u = |\{j, \forall j : j \in V(G) \wedge \epsilon_{n,j} \in E(G) \wedge \exists \epsilon_{j \to k \in V(S)} \in E(S)\}|$. In addition, it returns a flag (0|1) that indicates whether or not vertice n transmits data traffic. Applying Eq. (9) on these parameters will give the upper bound link-failure probability p_f for the link $\epsilon_{n \to i}$.

For the calculation of the lower bound, an average value for the number of hidden nodes is used, which is denoted h_l in Alg. (1). The rationale behind this is that for a set of nodes $R \subseteq V(S)$ hidden from node i, the carrier sense nature of the MAC protocol will in the case of two nodes $\{k,z\} \in R$ where $\exists z \neq k : \epsilon_{z,k} \in E(G)$ result in that only a subset of the nodes in R can transmit data at any given time. The parameter h_l is the average number of nodes in R that transmit data at a given time. For the calculation of the lower bound this will give a more accurate estimate than using h_u as the number of hidden nodes in Eq. (2).



(a) Topology: Ring with 10 nodes

(b) Topology: Connected MAPs with redundant MPs

Fig. 7. The distribution of nodes in two example mesh topologies.

4.2 Random pattern of bursty traffic

In this section we investigate how the analyzes of the topologies in Fig. 3 can be applied to more complex mesh topologies. Without loss of generality, we now focus on the two topologies in Fig. 7 as examples, observing that the analysis can easily be generalized for any arbitrary mesh topology. The topologies in Fig. 7 do not resemble the topologies in Fig. 3, but equations Eqs. (1)–(9) will together with Alg. (1) be able provide an upper and lower bound for the apparent link-failure probability p_f.

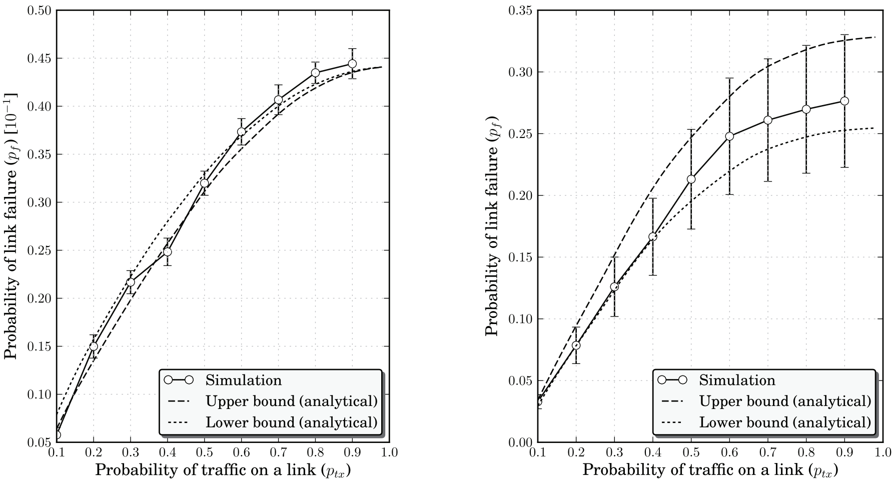
The simplest approach to analyzing a bursty traffic pattern is to generate a snapshot of the traffic in the topology. We assume that the time between each snapshot is sufficiently long

Algorithm 1 $\vec{H}(G,S)$

```
Require: An undirected graph $G(V,E)$, a directed graph $S \subseteq G$.
$H \leftarrow \emptyset$
for $i \in V(G)$ do
    $J \leftarrow \{j, \forall j : \epsilon_{i,j} \in E(G)\}$
    for $n \in J$ do
        $R \leftarrow \{r, \forall r \neq i : \epsilon_{n,r} \in E(G)\}$
        for $k \in R$ do
            if $|\{j, \forall j : \epsilon_{k,j} \ \in E(S)\}| > 0 \wedge k \notin G_i$ then
                $h_u \leftarrow h_u + 1$
            end if
        end for
        $N \leftarrow \emptyset$
        for $k = 0$ to $2^{|R|}$ do
            $n_i \leftarrow 0; ca \leftarrow \emptyset$
            for $p = 0$ to $|R|$ do
                if $k \xrightarrow{rshift} p\&1 \wedge \epsilon_{n,R_p} \in E(S)$ then
                    $ca \leftarrow ca \cup \epsilon_{n,R_p}$
                    $n_i \leftarrow n_i + 1$
                end if
            end for
            if not $[\exists z{:}\epsilon_{n,z}{\in}ca \wedge \exists w{\neq}z{:}\epsilon_{n,w}{\in}ca{:}\epsilon_{z,w}{\in}E(G)]$ then
                $N \leftarrow N \cup n_i$
            end if
        end for
        $h_l \leftarrow \lceil\!\lceil \frac{1}{|N|} \sum_{k=0}^{|N|} N_k \rceil\!\rceil$
        $\vec{L} \leftarrow (i,n)$
        $H \leftarrow \{H\} \cup \{(\vec{L}, h_u, h_l, |\{j, \forall j : \epsilon_{n,j} \ \in E(S)\}|?0:1))\}$
    end for
end for
return $H$
```

for the traffic patterns of each snapshot to be considered independent and that for each link in the topologies in Fig. 7, a burst of data packets is transmitted with the probability p_{tx}. Each node generates data packets within a burst according to a Poisson process with the rate parameter λ_c. If the topology is described as a graph $G(V,E)$, the traffic pattern given by the graph $S(V,E,p_{tx}){\subseteq}G$ is a snapshot that will represent a possible data transmission pattern. By generating a large number of random snapshots for a given p_{tx} $\left(S_{i\in\{0,M\}}\right)$, the overall average apparent link-failure probability for a given λ_c can be found.

Fig. 8 shows the average upper and lower bound for the apparent link-failure probability for λ_c=0.2. The apparent link-failure probability for the topologies in Fig. 7 is calculated using Alg. (1) and Eqs. (1)–(9) on the randomly generated traffic patterns. The figure also shows simulation results for the average apparent link-failure. As the simulation results demonstrate, the analytical upper and lower bounds provide a good indicator of the average link-failure probability even though it can be seen that the gap between the upper and lower bound increases as $p_{tx}{\to}1$. This is a result of a complex traffic pattern and interaction between the nodes that the simple model does not incorporate. At low values for p_{tx}, the model's upper and lower bound is as expected, more accurate.



(a) Results for topology in Fig. 7(a)

(b) Results for topology in Fig. 7(b)

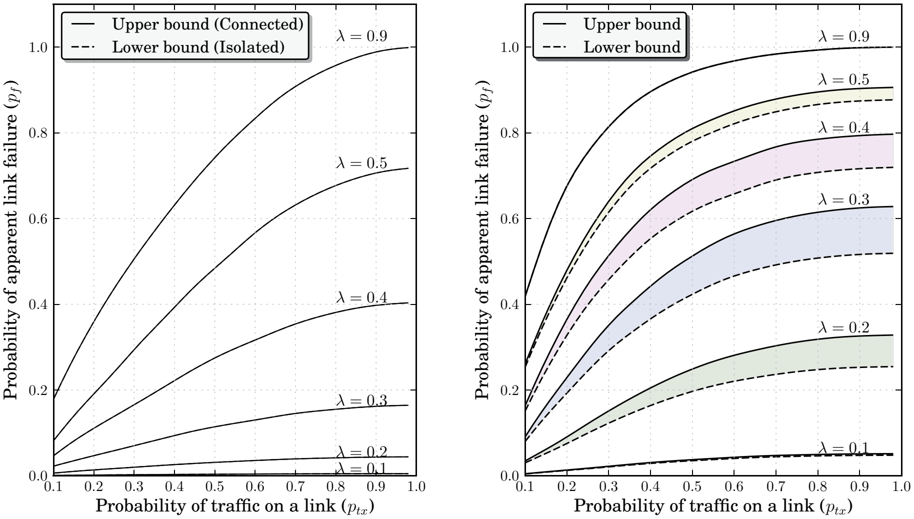
Fig. 8. Apparent link-failure probability for Fig. 7 ($\lambda_c = 0.2$). Simulation results are shown with a 95% confidence interval.

In Fig. 9 the upper and lower bound link-failure probability for different values of λ_c is shown. As can be seen from the figure, for small and large values of λ_c, the gap between lower and upper bound is negligible. The reason for this is that when $\lambda_c \gtrsim 0$, the sum of the packets awaiting transmission in the buffers of the hidden nodes is almost zero in both the isolated and the connected cases. Therefore, the apparent link-failure probabilities are almost identical. For the case when $\lambda_c \lesssim 1$, the sum of packets awaiting transmission in the buffers of the hidden nodes is always greater that zero, i.e. there is always a packets waiting to be transmitted. Hence, the difference in apparent link-failure probability is almost negligible. For $0.2 < \lambda_c < 0.6$, there exist various combinations of empty and non-empty buffers for the isolated and the connected cases, thus it is expected that there will be a difference in the upper and lower bound.

5. Network availability

If a network operates successfully at time t_0, the network reliability yields the probability that there were no failures in the interval $[0, t]$ Shooman (2002). The analysis of network reliability assumes for simplicity that there are no link repairs in the network. This is not exactly true for mesh networks, since a link-maintenance mechanism will ensure that a failed link is restored. The metric used to describe repairable networks is *availability*. The network availability is defined as the probability that at any instant of time t, the network is up and available, i.e. the portion of the time the network is operational Shooman (2002). This section focuses on the availability at the steady-state, found as $t \to \infty$, i.e. when the transient effects from the initial conditions are no longer affecting the network.

A typical availability measure is the k-terminal availability, namely the probability that a given subset k of K nodes are connected. For a graph $G(V, E, p)$, the k-terminal availability for the k nodes $\subseteq V(G)$ can be found as:



(a) Results for topology in Fig. 7(a)

(b) Results for topology in Fig. 7(b)

Fig. 9. Analytical results for the upper/lower bound of the apparent link-failure probability for the topologies in Fig. 7.

$$P_A(K = k) = \sum_{i=w_k(G)}^{|E(G)|} T_i^k(G)(1-p)^i p^{|E(G)|-i} \tag{10}$$

$$= 1 - \sum_{i=\beta(G)}^{|E(G)|} C_i^k(G) p^i (1-p)^{|E(G)|-i} \tag{11}$$

where $T_i^k(G)$ in Eq. (10) denotes the tieset with cardinality i, i.e. the number of subgraphs connecting k nodes with i edges. Furthermore, $w_k(G)$ is the size of the minimum tieset connecting the k nodes. In Eq. (11), $C_i^k(G)$ denotes the number of edge cutsets of cardinality i and $\beta(G)$ denotes the cohesion.

5.1 *k*-terminal availability with apparent link-failures

The network availability (Eq. (11)) is a measure of the robustness of a wireless mesh network and is determined by the structure and the link-failure probability of the links, provided the node-failure probability is negligible.

For a topology described as a graph G, which includes $k-1$ different distribution nodes $d_i \in V(G)$ and a set of root nodes $r_i \in V(G)$ (normally one root node serves a set of distribution nodes), a distribution node corresponds to a MAP while the root node corresponds to an MPP, according to the terminology of IEEE 802.11s. For normal network operation, the transit traffic in an IEEE802.11s network is directed along the shortest path between a root node r and each distribution node, $d_i \in G(V)$. The network is not operating as expected if a distribution node is disconnected from the root node, i.e. the network has failed. Thus, the network is fully operational only if there is an operational path between the root node and each of the distribution nodes. This is true if, and only if, the root node r and the $k-1$ distribution nodes are all connected. Thus, the reliability of the network may be analyzed using the k-terminal reliability.

The expression for the network availability in Eq. (11) assumes a fixed and identical link-failure probability for all the links in a topology. However, the apparent link-failure model can provide exact probabilities for every link in a topology. In the following we compare the availability using an average apparent link-failure probability with the availability using an exact and a simulated-based apparent link-failure probability.

5.1.1 k-terminal availability based on an average p_F (P_A^a)

As in Section 4, the average apparent link-failure probability is calculated according to Eqs. (1)–(9) and Alg. (1). For a number of $|S|=|\{S_0,\ldots,S_{M-1}\}|=5000$ random patterns of bursty traffic, the average apparent link-failure probability is expressed as:

$$\overline{p}_F = \frac{1}{|S|\times|E(G)|}\sum_{s\in S}\sum_{\epsilon_{i,j}\in E(G)} p_f(i,j)_s \times p_f(j,i)_s \tag{12}$$

where p_f is calculated according to Eq. (9). The k-terminal availability based on an undirectional average link-failure probability is given by:

$$P_A^a\left[G(V,E,\overline{p}_F)\right] = 1 - \sum_{i=\beta}^{|E(G)|} C_i\left(\overline{p}_F\right)^i\left(1-\overline{p}_F\right)^{|E(G)|-i} \tag{13}$$

5.1.2 k-terminal availability using simulation (P_A^m)

Using a Monte Carlo simulation, the availability of each topology is calculated where the existence of a link $\epsilon_{i,j}\in E(G)$ depends on the probability $1-p_F(i,j)$. An estimate for the k-terminal availability can then be calculated for $s\in S$ ($|S|=5000$) random bursty traffic patterns as:

$$P_A^m\left[G(V,E,p_F)\right] = \frac{1}{|S|}\times\left[\begin{array}{l}\text{Number of graphs where}\\ k\text{ nodes are connected}\end{array}\right] \tag{14}$$

5.1.3 k-terminal availability using exact calculation (P_A^e)

Since we can calculate the apparent link-failure probability of every link, it is also possible to calculate an exact value for the k-terminal availability. Let us define $L\subseteq E(G)$ as a set of links that are removed from the graph $G(V,E)$. For a traffic pattern $s\in S$, we define:

$$T(L)_s = \prod_{\forall\epsilon_{i,j}\in L} p_F(i,j)_s\times\prod_{\substack{\forall\epsilon_{q,r}\in\\ E(G)\setminus L}}\left[1-p_F(q,r)_s\right]. \tag{15}$$

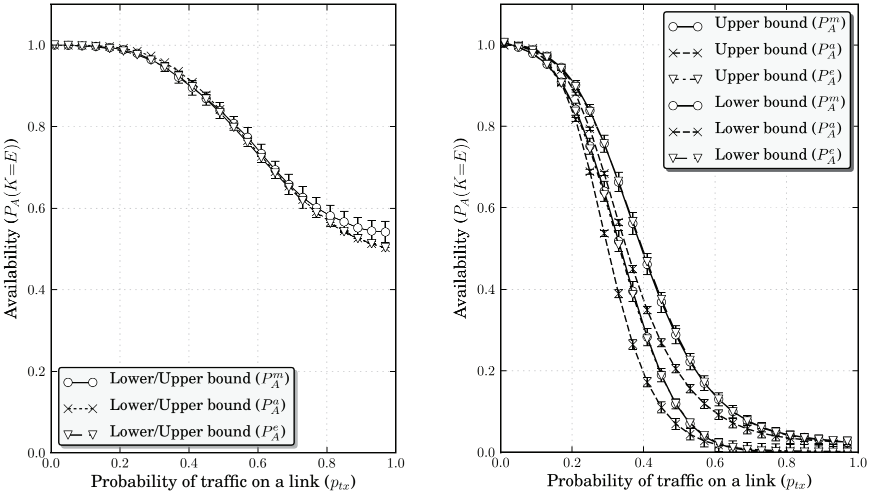
An exact calculation of the k-terminal availability for $|S|$ bursty traffic patterns is then given by:

$$P_A^e\left[G(V,E,p_F)\right] = 1-\frac{1}{|S|}\sum_{s\in S}\sum_{\substack{\forall L:V_k(G)\subseteq V(G)\\ \text{is not connected}}} T(L)_s. \tag{16}$$

5.1.4 Availability of example topologies

In this section we apply Eqs. (13)–(16) on the topologies in Fig. 7 using a scenario where the network is configured to allow the STAs to access the MAPs at one frequency band (e.g. using 802.11b or 802.11g) and use another frequency band for the communication between the MPs.

Since the extra equipment cost of such a configuration often is minimal compared with the costs associated with site-acquisition, it is anticipated that many commercial mesh networks will implement a MAP at each MP in the network. For such a configuration, the *all-terminal* availability ($P_A(K{=}k)$) of the network is of interest, which is shown in Fig. 10 (upper and lower bound). The figure shows that the all-terminal availability based on an average p_F (P_A^a) differs slightly from the exact calculations (P_A^e) for the topology in Fig. 7(b). This is caused by the fact that nodes at the border of the topology have fewer neighbors than the nodes in the center area of the topology. For larger 2D-grid topologies, this effect will be reduced and we will have $P_A^a \approx P_A^e$. This is easy to deduce, since the average number of neighbors in an $N \times N$ grid network is $4-4/N$. As N increases, the nodes in the network experience comparable one-hop neighbor/hidden node conditions, due to the topology's regular structure. This is also illustrated in Fig.11(b), where the availability is calculated without the border nodes, i.e. $P_A(\{c_0,\dots,c_8\})$.



(a) Results for topology Fig.7(a)

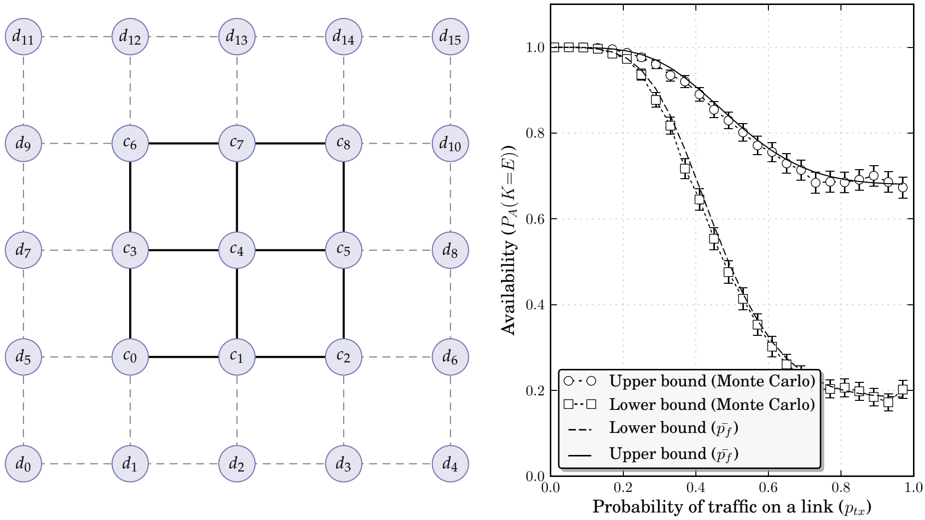
(b) Results for topology in Fig.7(b)

Fig. 10. The upper/lower bound all-terminal availability, $P_A(K{=}k)$ for the topologies in Fig. 7 (λ_c=0.4).

6. A random geometric graph model approach to apparent link-failures

The main drawback in the previous sections is that it does not take into account correlations between different links. For example, if two ad hoc nodes s_a and s_b are physically very close to each other, and another ad hoc node s_c is farther away, the existence of the links $\epsilon_{a,c}$ and $\epsilon_{b,c}$ is expected to be correlated in reality. So far Eqs. (1)–(9) do not model this correlation.

In this section, we further extend the apparent link-failure model to encompass random geometric graphs Haenggi et al. (2009). A *random geometric graph* $G(V,E,r)$ is a geometric graph in which the $n = |V(G)|$ nodes are independently and uniformly distributed in a metric space. In other words, it is a random graph for which a link between two nodes s_a and s_b exists if, and only if, their Euclidean distance is such that $\| s_a - s_b \| \le r_0$, where r_0 is the transmission range of the nodes.



(a) Every node transmits with probability $p_{tx} = 1$ and at rate $\lambda_c = 0.4$

(b) Upper and lower bound all-terminal reliability for the nodes $\{c_0, \ldots, c_8\}$.

Fig. 11. Illustration of the border effect. Since every node in $\{c_0, \ldots, c_8\}$ experiences equal amount of hidden nodes, using the average apparent link-failure probability ($\overline{p}_f$) gives the same all-terminal reliability measure as the Monte Carlo simulation.

6.1 The node degree

We first establish an expression for the probability that n_0 of all n nodes are within a certain area A_0 in the system plane Ω. The expected number of nodes per unit area is then $\rho = n/\Omega$. This probability is in Bettstetter (2002) shown to be:

$$P(d = n_0) = \frac{\left(\frac{A_0}{\Omega} n\right)^{n_0}}{n_0!} \cdot e^{-\frac{A_0}{\Omega} n} = \frac{(\rho A_0)^{n_0}}{n_0!} \cdot e^{-\rho A_0} \tag{17}$$

for large n and large Ω. If a node's radio transmission range r_0 covers an area $A_0 = \pi r_0^2$, the probability that a randomly chosen node has n_0 neighbors is:

$$P(d = n_0) = \frac{\left(\rho \pi r_0^2\right)^{n_0}}{n_0!} \cdot e^{-\rho \pi r_0^2}. \tag{18}$$

A probabilistic bound for the minimum node degree of a homogenous ad hoc network is shown to be Bettstetter (2002):

$$P(d_{min} \geq n_0) = \left(1 - \sum_{i=0}^{n_0 - 1} \frac{(\rho \pi r_0^2)^i}{i!} \cdot e^{-\rho \pi r_0^2}\right)^n. \tag{19}$$

6.2 Average number of hidden nodes of an area A_0

For a given node density and transmission range, we now find the average number of hidden nodes for any given node. Consider the intersecting circles in Fig. 12. Let us assume that the

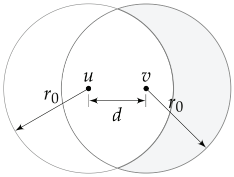


Fig. 12. Analysis of area containing hidden nodes when node u sends a beacon to node v.

points u and v represent to nodes separated by a distance d, each with a transmission range of r_0. If each node covers region S_u and S_v when they transmit a packet, we are interested in finding the area S_{v-u}, since if any node is located in this area, this node will appear hidden from node u. From Tseng et al. (2002) this area is given by $|S_{v-u}| = |S_v| - |S_{u\cap v}| = \pi r^2 - \text{INTC}(d)$, where $\text{INTC}(d)$ is the intersection area of the two circles:

$$\text{INTC}(d) = \int_{d/2}^{r_0} \sqrt{r_0^2 - x^2}dx. \tag{20}$$

When the node v is randomly located within u's transmission range, the average area of S_{v-u} is:

$$S_{v-u} = B_0 = \frac{3\sqrt{3}}{4\pi}\pi r_0^2 \tag{21}$$

If n nodes are randomly and uniformly distributed on an area Ω following a homogenous Poisson point process, the probability of finding b_0 nodes in the area B_0 is given by Eq. (17), substituting A_0 with B_0. Thus,

$$P(d = b_0) = \frac{(\rho B_0)^{b_0}}{b_0!} \cdot e^{-\rho B_0} = \frac{\left(\rho \frac{3\sqrt{3}}{4\pi}\pi r_0^2\right)^{b_0}}{b_0!} \cdot e^{-\rho \frac{3\sqrt{3}}{4\pi}\pi r_0^2}. \tag{22}$$

6.3 Connectivity

A topology is said to be *k-connected* ($k = 1,2,3,\ldots$) if for each node pair there exist at least k mutually independent paths connecting them. For a topology described as a graph $G(V,E)$ where $|V(G)| = n$, the probability that G, with $n \gg 1$ where each node has a transmission range r_0 and a homogenous node density ρ is k-connected is Bettstetter (2002):

$$P(G \text{ is } k\text{-connected} \approxeq P(\text{node } i \text{ has } d_{min} \geq k),\ \forall i \in V(G). \tag{23}$$

A beacon from node u to v in Fig.12 will fail to be received if any nodes in the area B_0 (S_{v-u}) transmit a data packet. The apparent link-failure probability with m hidden nodes ($p_f(m)$) is given by Eq. (9). From Eq.(22), we can easily find the probability that node u in Fig. 12 has zero hidden nodes to be $e^{-\rho B_0}$. The probability that the link between node u and v is operational if k nodes are located within node u's transmission range can be calculated as:

$$p_{ok}(k) = e^{-\rho B_0} + \sum_{m=1}^{n-k} \frac{(\rho B_0)^m}{m!} \cdot e^{-\rho B_0} \left(1 - \left[p_f(m)\right]^2\right). \tag{24}$$

If we make the assumption that the one-hop links of node u fail independently, the probability that k of the links are operational is:

$$P(\text{node } u \text{ is } k\text{-connected}) = P(d_{min} \geq k) = \sum_{i=k}^{n} (1 - [1 - p_{ok}(k)]^i) \cdot \frac{(\rho A_0)^i}{i!} \cdot e^{-\rho A_0}. \tag{25}$$

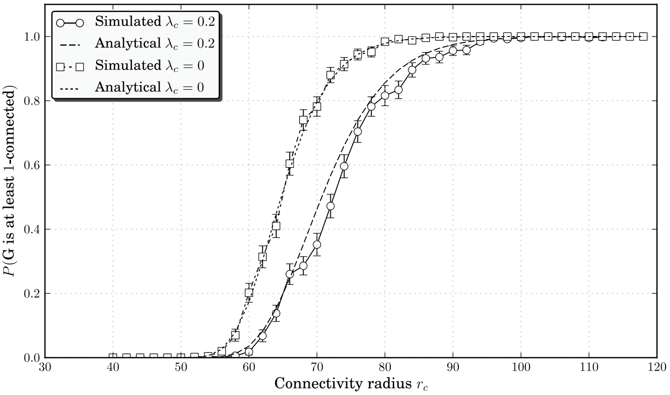


Fig. 13. $P(k\text{-connected})$ with usual Euclidian distance metric. $A = 1000 \times 1000$ ($\rho = 5 \cdot 10^{-4}$)

The probability that a graph $G(V,E)$ where $|V(G)|$ is k-connected is given by:

$$P(G \text{ is } k\text{-connected}) \approxeq \left(\sum_{i=k}^{n} (1-[1-p_{ok}(k)]^i) \cdot \frac{(\rho A_0)^i}{i!} \cdot e^{-\rho A_0} \right)^n . \tag{26}$$

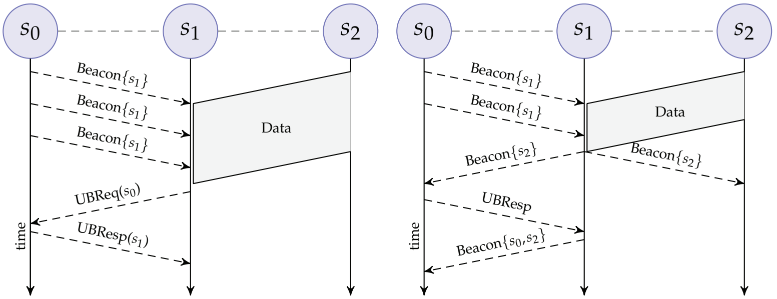
Fig. 13 shows the probability of a topology with $n = 500$ nodes being at least 1-connected, i.e. $P(d_{min} \geq 1)$. The apparent link-failure probability (p_f) is calculated using the lower bound. Every node in the topology transmits data packets with probability $p_{tx} = 1$ which are Poisson distributed with parameter λ_c. Both analytical and Monte Carlo simulation results are shown. The simulation results are based on 1000 randomly generated topologies from which links are removed based on traffic load and the number of hidden nodes of a link. As the figure shows, the simulation results match well with the analytical model. Also, the probability that the topology is connected increases as the transmission range of the nodes is gradually increased, which is as expected. The figure also demonstrates that more neighbors are needed in order to have a connected topology as λ_c, i.e. the traffic rate of the hidden nodes is increased.

7. Using unicast beacon in the presence of apparent link-failures

Having studied the probability of apparent link-failures and its effect on network availability, it is also of interest to explore the measures for diminishing the influence of apparent link-failures. There are several methods for this purpose, such as:

- **Increasing beacon loss parameter (θ):** This method will require more consecutive beacon loss before a node determines that the link is inoperable. However, in cases where a node or a link becomes permanently unavailable due to other reasons than apparent link-failures, this will result in a longer time interval before a new route is calculated; and
- **Reducing hysteresis (θ_h)**: This method will bring a link back to operational much faster, however it can result in oscillation between an operational and non-operational state of the link.

Another simple yet effective solution to apparent link-failures is to introduce *unicast beacon transmissions*. This method has the advantage that the MAC layer will retransmit the beacon



(a) Explicit unicast beacon (b) Implicit unicast beacon

Fig. 14. Handshake of UBReq and UBResp messages.

a defined number of times if an acknowledge is not received. In addition, it is possible to protect the beacon using the RTS/CTS signalling of the MAC layer.

A request for a beacon is called a *Unicast Beacon Request* (UBReq) message and a response to this is called a *Unicast Beacon Response* (UBResp) message. Both these messages can be the same packet format as normal beacon, with the difference that they use a unicast destination address instead of a broadcast destination address. A unicast beacon can be triggered in either end of a link. Consider the topology in Fig. 14(a). Let us assume that node s_0 has discovered s_1 as a neighbor and vice versa. Then, at some point node s_2 transmits data such that node s_1 fails to receive the beacons from node s_0. Node s_1 can then send a UBReq message to node s_0 which answers with a UBResp message. This prevents node s_1 from defining the one-hop link to node s_0 as inoperable. The UBReq and UBResp messages will also be vulnerable to overlapping transmissions from hidden nodes. To overcome this, the link sensing mechanism can protect the UBReq and UBResp messages using RTS/CTS at the MAC layer.

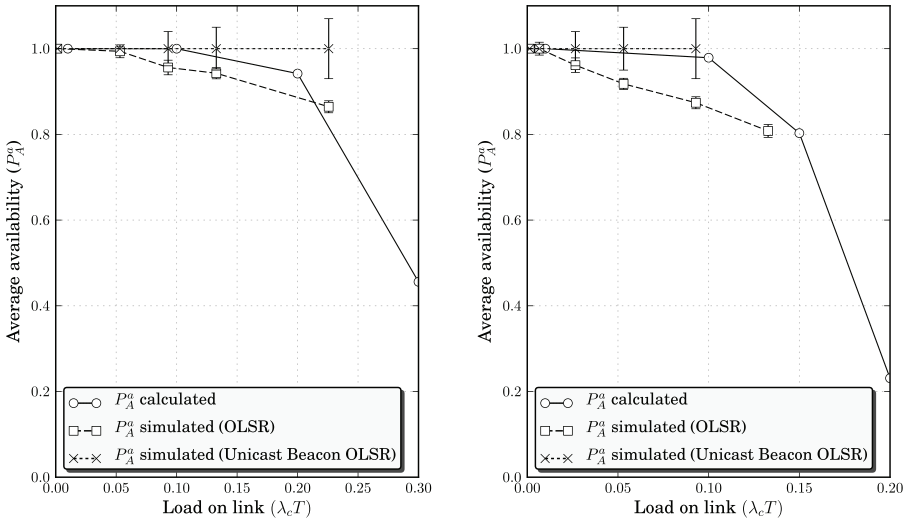
Now consider Fig. 14(b). A UBResp could also be triggered implicitly if node s_0 receives broadcast beacons from node s_1 but fails to find its address in the beacon message. This indicates that s_1 has not received broadcast beacons from node s_0. Node s_0 could therefore send a UBResp message to node s_1, indicating that it can hear node s_1, whereupon node s_1 will include s_0 in its next beacon.

We implemented the unicast beacon scheme in ns2 by modifying the OLSR routing protocol, allowing unicast beacons to be protected by RTS/CTS signalling. Using *No Route To Host* packets drop as an indicator, we can calculate the availability of a network. The simulation parameters are shown in Table 2 and the topologies are shown in Fig.7.

IP/MAC layer	**Values**	**Physical layer**	**Values**	**Simulation**	**Values**
Data	1500 bytes	Propagation model	Free Space	Simulation/ transient time	500s/25s
MAC protocol	CSMA/CA	Data rate	11Mbps	Traffic/ Distribution	Poisson
Queue Length	10			Replications	50 times

Table 2. ns2 simulation parameters.

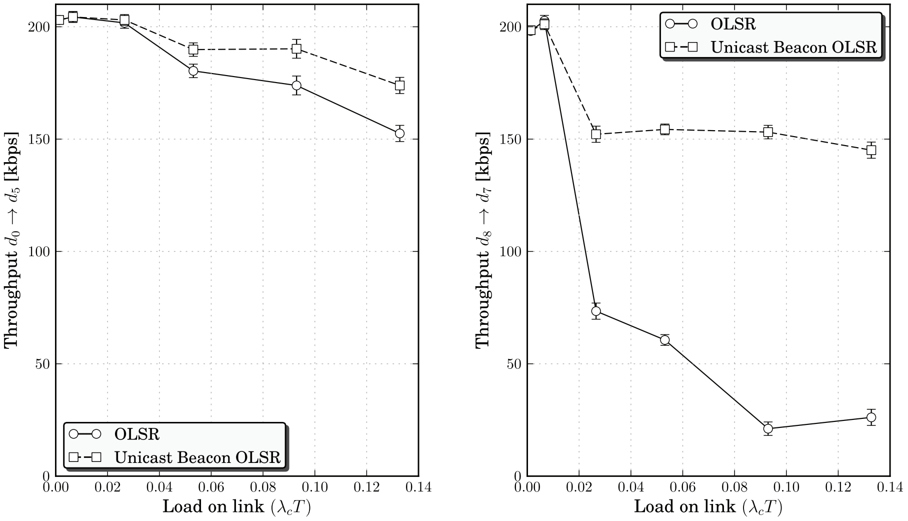
Fig.15 illustrates the all-terminal availability. The analytical and simulated results are shown for normal OLSR beacon scheme. As can be observed from the figure, the simulated average availability for OLSR is much lower than the analytical one. This is as expected, since our



(a) Availability for the topology in Fig.7(a)

(b) Availability for the topology in Fig.7(b)

Fig. 15. Average availability for the topologies in Fig.7. Results for standard beacon transmission and unicast beacon transmission protected by RTS/CTS are shown.



(a) Throughput node $d_0 \rightarrow d_5$ in Fig.7(a)

(b) Throughput node $d_8 \rightarrow d_7$ in Fig.7(b)

Fig. 16. Average throughput for the topologies in Fig.7. Results for standard beacon transmission and unicast beacon transmission protected by RTS/CTS are shown. The source nodes transmit at a fixed rate of 200 kbps while the load on all links is gradually increased.

simple model does not take MAC retransmissions into account. MAC retransmissions will increase the average load (λ_c) on the channel, thus increasing the probability of beacon loss.The figure also shows that the simulated results from unicast beacon scheme provide much higher availability as the load on the channel increases.

8. Conclusions

This chapter introduces an approximate model for the probability of apparent link-failures in beacon-based link maintenance schemes. The model is extended to provide a rough upper and lower bound for arbitrary topologies. Through extensive simulations, it has been confirmed that the model provides acceptable accuracy for simple topologies. Furthermore, more advanced topologies with random traffic patterns and bursty traffic have been studied, where the model can provide an average upper and lower bound for the link-failure probability with satisfactory accuracy. In addition, the work has demonstrated how the apparent link-failure model can be used to investigate the availability of mesh topologies and that using an average apparent link-failure probability can serve as a good indicator for the availability of a given topology. However, the *k*-terminal reliability problem is known to belong to a class of NP-complete problems Valiant (1979), which has similar complexity as calculating the exact network availability. Applying approximate methods to the *k*-terminal probability is possible, but this is a topic for future work. In order to provide intuition about the effects of apparent link-failures in large network with randomly distributed nodes, random geometric graph analysis has been applied. Based on existing work on random geometric graphs, we have extended our link-failure model so that connectivity calculations can be performed for topologies where apparent link-failures are present.

Last but not least, a simple remedy for apparent link-failures has been introduced where unicast beacons are used to mitigate beacon loss caused by overlapping transmissions. This solution has been implemented for the OLSR routing protocol and the performance improvements have been verified using the *ns2* simulation tool.

9. References

Ali, H. M., Naimi, A. M., Busson, A. & Vèque, V. (2009). Signal strength based link sensing for mobile ad-hoc networks, *Telecommunication Systems* 42(3-4): 201–212.

Bettstetter, C. (2002). On the minimum node degree and connectivity of a wireless multihop network, *MobiHoc '02: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, ACM, New York, NY, USA, pp. 80–91.

Chlamtac, I., Conti, M. & Liu, J. J.-N. (2003). Mobile ad hoc networking: Imperatives and challenges, *Ad Hoc Networks, Elsevier* 1(1): 13–64.

Clausen, T. & Jacquet, P. (2003). Optimized link state routing protocol (olsr), ietf rfc 3626.

Dubey, A., Jain, A., Upadhyay, R. & Charhate, S. (2008). Performance evaluation of wireless network in presence of hidden node: A queuing theory approach, *Modeling and Simulation, 2008. AICMS 08. Second Asia International Conference on*, pp. 225–229.

Egeland, G. & Engelstad, P. E. (2009). The availability and reliability of wireless multi-hop networks with stochastic link failures, *IEEE J.Sel. A. Commun.* 27(7): 1132–1146.

Egeland, G. & Engelstad, P. E. (2010). A model for the loss of Hello-Messages in a wireless mesh network, *IEEE ICC 2010 - Ad-hoc, Sensor and Mesh Networking Symposium*, Cape Town, South Africa.

Egeland, G. & Li, Y, F. (2007). Prompt route recovery via link break detection for proactive routing in wireless ad hoc networks, *10th International Symposium Wireless Personal Multimedia Communications (WPMC)*, Jaipur, India.

Gerharz, M., Waal, C. D., Frank, M. & Martini, P. (2002). Link stability in mobile wireless ad hoc networks, *In Proceedings of the 27th Annual IEEE Conference on Local Computer Networks (LCN'02)*.

Gharavi, H. & Kumar, S. (2003). Special issue on sensor networks and applications, *Proceedings of the IEEE* 91(8).

Haenggi, M., Andrews, J., Baccelli, F., Dousse, O., Franceschetti, M. & Towsley, D. (2009). Guest editorial: geometry and random graphs for the analysis and design of wireless networks, *Selected Areas in Communications, IEEE Journal on* 27(7): 1025 –1028.

IEEE802.11 (1997). Wireless LAN medium access control (MAC) and physical layer (PHY) specification.

IEEE802.11s (2010). Lan/man specific requirements - part 11: Wireless medium access control (mac) and physical layer (phy) specifications: Amendment: Ess mesh networking.

Kleinrock, L. (1975). *Theory, Volume 1, Queueing Systems*, Wiley-Interscience.

Kleinrock, L. & Tobagi, F. (1975). Packet switching in radio channels: Part i–carrier sense multiple-access modes and their throughput-delay characteristics, *Communications, IEEE Transactions on* 23(12): 1400–1416.

Li, F., Bucciol, P., Vandoni, L., Fragoulis, N., Zanoli, S., Leschiutta, L. & Lázaro, O. (2010). Broadband internet access via multi-hop wireless mesh networks: Design, protocol and experiments, *Wireless Personal Communications* .
URL: *http://dx.doi.org/10.1007/s11277-009-9907-9*

Ng, P. C. & Liew, S. C. (2004). Re-routing instability in ieee 802.11 multi-hop ad-hoc networks, *Local Computer Networks, 2004. 29th Annual IEEE International Conference on*, pp. 602–609.

ns2 (2010). The Network Simulator NS-2, `http://www.isi.edu/nsnam/ns/`.

Perkins, C., Belding-Royer, E. & Das, S. (2003). Ad hoc on-demand distance vector (aodv) routing, ietf rfc 3561.

Ray, S., Carruthers, J. B. & Starobinski, D. (2004). Evaluation of the masked node problem in ad-hoc wireless lans, *IEEE Transactions on Mobile Computing* 4: 430–442.

Ray, S., Starobinski, D. & Carruthers, J. B. (2005). Performance of wireless networks with hidden nodes: a queuing-theoretic analysis, *Comput. Commun.* 28(10): 1179–1192.

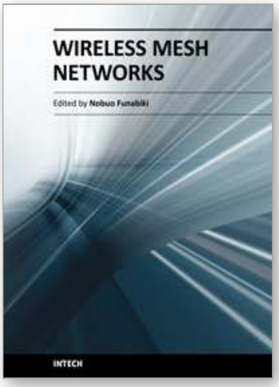
Shooman, M. L. (2002). *Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design*, John Wiley and Sons, Inc.

Tobagi, F. & Kleinrock, L. (1975). Packet switching in radio channels: Part ii–the hidden terminal problem in carrier sense multiple-access and the busy-tone solution, *Communications, IEEE Transactions on* 23(12): 1417–1433.

Tseng, Y.-C., Ni, S.-Y., Chen, Y.-S. & Sheu, J.-P. (2002). The broadcast storm problem in a mobile ad hoc network, *Wirel. Netw.* 8(2/3): 153–167.

Valiant, L. G. (1979). The complexity of computing the permanent, *Theor. Comput. Sci.* 8: 189–201.

Voorhaen, M. & Blondia, C. (2006). Analyzing the impact of neighbor sensing on the performance of the olsr protocol, *Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, 2006 4th International Symposium on*, pp. 1–6.



WIRELESS MESH NETWORKS

Edited by Nobuo Funabiki

INTECH

ISBN 978-953-307-519-8
Hard cover, 308 pages
Publisher InTech
Published online 14, January, 2011
Published in print edition January, 2011

The rapid advancements of low-cost small-size devices for wireless communications with their international standards and broadband backbone networks using optical fibers accelerate the deployment of wireless networks around the world.â€¨The wireless mesh network has emerged as the generalization of the conventional wireless network. However, wireless mesh network has several problems to be solved before being deployed as the fundamental network infrastructure for daily use. The book is edited to specify some problems that come from the disadvantages in wireless mesh network and give their solutions with challenges. The contents of this book consist of two parts: Part I covers the fundamental technical issues in wireless mesh network, and Part II the administrative technical issues in wireless mesh network,. This book can be useful as a reference for researchers, engineers, students and educators who have some backgrounds in computer networks, and who have interest in wireless mesh network. It is a collective work of excellent contributions by experts in wireless mesh network.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821