Analysis of Hello-Based Link Failure Detection in Wireless Ad hoc Networks

Alvin Valera Hwee-Pink Tan
Institute for Infocomm Research (I^{2}R)
1 Fusionopolis Way
#21-01 Connexis, Singapore 138632
Email:{acvalera, hptan}@i2r.a-star.edu.sg

***Abstract*—Wireless ad hoc routing protocols must employ accurate and rapid link failure detection mechanisms in order to maintain valid multihop routes and provide high data delivery rates. *Hello-based failure detection* is the predominant failure detection mechanism due to its ease of implementation. Despite its prevalence, no analytical work has been carried out to better understand its fundamental behavior. In this paper, we study the performance of hello-based link failure detection via analysis and experimentation. Our analytical results, which are validated by experimental results, show the existence of optimal hello beaconing parameters which depend on network conditions such as traffic load, link failure rate and hello delivery rate. These results can be applied in real-world network deployments for obtaining the optimal hello beaconing parameters that can provide the highest data delivery rate.**

I. Introduction

Wireless ad hoc networks are becoming an attractive and practical solution at providing flexible and extended wireless coverage over large areas. As such networks are expected to provide high delivery rates, routing protocols must be designed to minimize packet loss even in the face of numerous difficulties including highly dynamic multihop topologies, lossy and noisy communication channels, and sporadic connectivity. These difficulties essentially contribute to persistent link failures which emphasizes the need for *accurate* and *rapid* link failure detection mechanism.

Link failure detection in wireless ad hoc networks can be performed using either periodic hello beaconing [1]–[3] or link layer feedback [4], [5]. Due to its ease of implementation, hello-based failure detection is the predominant failure detection mechanism employed by wireless ad hoc routing protocols [6]. In spite of this, no analytical work has been carried out to understand its trade-offs and performance under varying network conditions. In this paper, we derive an analytical model for hello-based failure detection that provides a lower bound on the packet delivery ratio. We perform experiments to validate the model and show that packet delivery ratio can be maximized through the use of optimal beaconing parameters which depend on network conditions such as traffic load, link failure rate and hello delivery rate.

The remainder of this paper is organized as follows. Section II presents the related work. Section III presents the main contribution of this paper which is the formulation of an analytical model for hello-based failure detection while Section IV presents the model verification through experimentation. Section V concludes the paper with a summary of the important findings.

II. Related Work

The use of keep-alive packets (referred to as *hello*) for link status monitoring has its origins in wired networks [7]. It has been adapted to wireless networks, in particular to wireless ad hoc networks where it has been used by many routing protocols for maintaining local connectivity [3], [8]–[10].

As the characteristics of wireless links differ significantly from that of wired links, numerous difficulties arose with the use of hello beacons in wireless ad hoc networks [1], [2]. Several studies [1], [2], [11], [12] proposed mechanisms to improve the performance of hello but to the best of our knowledge, no analytical work has been carried out to understand the fundamental behavior of hello-based failure detection under varying network conditions (*e.g.*, load, link failure rate and hello delivery rate).

III. Analysis

A. Network Model and Assumptions

A wireless ad hoc network is modeled as a graph $G = (V, E)$ where V is the set of nodes and E is the set of links. A link $(i, j) \in E$ and is said to be "up" if i and j are directly connected and can bi-directionally communicate with each other. Link failures are modeled similar to that in [13] where link failure rate r_{LF} (failures per second) is equal for all links in E.

B. Properties of Hello-Based Link Failure Detection

Every node in the network broadcasts hello packets at a constant interval T_B. When a node i fails to receive K consecutive hellos from a neighbor node j, i declares that the link (i, j) is "down". The detection delay δ has a uniform distribution on $[(K-1)T_B, KT_B]$. Hence, the **average detection delay** $\bar{\delta}$ can be expressed as

$$\bar{\delta} = (K-1)T_B + \frac{T_B}{2} = \frac{(2K-1)T_B}{2} \qquad (1)$$

where K is an integer ≥ 1 and $T_B > 0$.

Hello-based failure detection may trigger false positives which occur whenever a node i fails to receive K consecutive

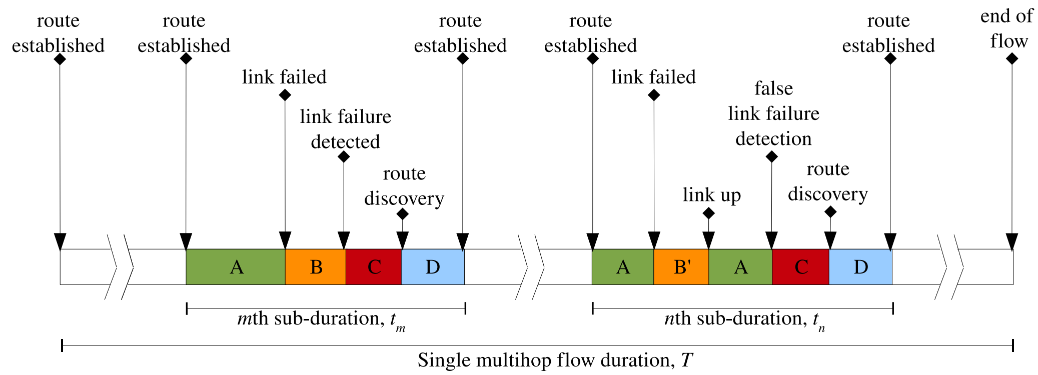


Fig. 1. Analytical framework to model the impact of link failures on a single multihop flow.

hellos from j even though link (i,j) is up. If p_B is the probability of receiving a hello when link is up, then the false positive probability is $(1-p_B)^K$. Since hellos are sent at $1/T_B$, then the **false detection rate** r_{FD} (false detections per second) for every link is

$$r_{FD} = \frac{1}{T_B}(1-p_B)^K. \tag{2}$$

Note that $p_B < 1$ when a link experiences high bit error rates and severe contention [14], [15].

In addition to false positives, hello-based failure detection may also miss true failures. This happens when a link (i,j) goes down for a duration less than the minimum detection delay, or $t_{fail} < (K-1)T_B$ where t_{fail} is the link failure duration. If $P\{t_{fail} < (K-1)T_B\}$ is the probability that a link failure has duration less than $(K-1)T_B$, then the **missed detection rate** (undetected failures per second) for every link is

$$r_{MD} = r_{LF}P\{t_{fail} < (K-1)T_B\}. \tag{3}$$

C. Routing Protocol Analytical Framework

To determine the effect of link failures, we introduce an analytical framework that captures the common operations of single-path on-demand protocols [3], [4] during a single multihop flow. We consider a flow from a source node h to a destination node k. Packets are generated at h at a rate of λ packets per second.

In the framework as shown in Figure 1, a flow with duration T is subdivided into M sub-durations. The figure illustrates two sub-durations. In the mth sub-duration which has duration t_m, a true failure detection occurs. The sub-duration is divided into four phases labeled A–D. Right after route establishment, phase A begins wherein the discovered l_m-hop route is used for sending packets to destination k. When a link along the path fails, phase B, which is the link failure detection delay, begins. Once failure is detected, phase C commences wherein the node that encountered the failure sends route error message to upstream nodes. We refer to phase C as the *route invalidation* phase. Upon receipt of route error at the source, it initiates a route discovery. Phase D is essentially the route search time. When a route is established, a new sub-duration commences.

In the nth sub-duration, the occurrence of a missed detection and false failure detection are illustrated. The missed failure duration is indicated by phase B' which is shorter than the detection delay. Whereas, the false failure detection occurs with the transition from phase A to phase C (phase B does not occur since no link actually failed). Note that missed detections do not trigger any of the phases and cannot exist in a sub-duration by itself. For generality, t_m need not be equal to $t_i, \forall \in M, i \neq m$. Likewise, l_m need not be equal to $l_i, \forall \in M, i \neq m$.

The framework makes some simplifying assumptions: (*i*) route discoveries are always successful and no packets are dropped during phase D; (*ii*) routing protocol does not perform local repair; and (*iii*) route error messages always reach the source. From these assumptions, it is obvious that losses can only be incurred during phases B, B' and C of every sub-duration. This is because during these time periods, h continues to send packets along the path as it is still oblivious to the link failure downstream or the route invalidation that is in progress. Node h only stops sending after it has received a route error message.

D. Single-Flow Multi-hop Packet Delivery Ratio

We now consider the single-flow packet delivery ratio $\theta = \bar{N}_r/N_s$ when hello-based failure detection is employed, where N_s is the number of packets sent while $\bar{N}_r$ is the average number of packets received. To obtain θ, we simply subtract the number of lost packets at every sub-duration m from N_s. From the analytical framework, packets are lost in phases B, B' and C of every sub-duration. Let t_m^B, $t_m^{B'}$ and t_m^C be the time duration of phases B, B' and C at sub-duration m. Then the number of lost packets, N_l is

$$N_l = \lambda\left[\sum_{m\in M_t}(t_m^B + t_m^C) + \sum_{m\in M_m} t_m^{B'} + \sum_{m\in M_f} t_m^C\right], \tag{4}$$

where $M_t \subseteq M$ is the set of sub-durations where true failure detections occurred, $M_m \subseteq M$ is the set of sub-durations where missed detections occurred, and $M_f \subseteq M$ is the set of sub-durations where false detections occurred. Since $M_t \cup M_f = M$ (note that M_m is not included in the union as missed detections do not exist in a sub-duration by itself), we can re-arrange (4) as

$$N_l = \lambda \left[\sum_{m \in M_t} t_m^B + \sum_{m \in M_m} t_m^{B'} + \sum_{m \in M} t_m^C \right]. \quad (5)$$

This expression groups losses into three factors: (*i*) packets lost due to link failure detection delay, $N_l' = \lambda \sum_{m \in M_t} t_m^B$; (*ii*) packets lost due to undetected failures, $N_l'' = \lambda \sum_{m \in M_m} t_m^{B'}$; and (*iii*) packets lost due to route invalidation, $N_l''' = \lambda \sum_{m \in M} t_m^C$.

1) Packet Loss Due to Link Failure Detection Delay: It is obvious that the quantity t_m^B represents the failure detection delay at sub-duration m. Since $E[t_m^B] = \bar{\delta}, \forall m \in M_t$, then the average number of packets lost due to failure detection delay is

$$\bar{N_l'} = E\left[\lambda \sum_{m \in M_t} t_m^B\right] = \lambda |M_t| \bar{\delta} = \lambda |M_t| \frac{(2K-1)T_B}{2},$$

where $|M_t|$ is the number of true failure detections over the flow duration T. Note that $|M_t|$ can actually be expressed in terms of r_{LF}, r_{MD}, T, and the path length from h to k. Suppose that L_{max} is the longest path from h to k during the flow, then

$$\bar{N_l'} \leq \lambda T L_{max}(r_{LF} - r_{MD}) \frac{(2K-1)T_B}{2}. \quad (6)$$

In a special case where the path length $l_m = L, \forall m \in M$ (*i.e.*, the path discovered after every failure is of the same length as the previous path), the above inequality changes to an equality:

$$\bar{N_l'} = \lambda T L(r_{LF} - r_{MD}) \frac{(2K-1)T_B}{2}. \quad (7)$$

2) Packet Loss Due to Undetected Failures: During an undetected failure of link (i, j), node i, which is upstream of the failed link, continues to send packets across the link. These packets eventually get dropped as the receiver j is momentarily unreachable. Since the failure duration $t_m^{B'} < (K-1)T_B \leq \delta$, $\forall m \in M_m$,

$$E\left[\sum_{m \in M_m} t_m^{B'}\right] < |M_m| \bar{\delta} = |M_m| \frac{(2K-1)T_B}{2},$$

where $|M_m|$ is the number of undetected failures over the flow duration T. Once again, $|M_m|$ can be expressed in terms of r_{MD}, T, and the path length from h to k. The average number of lost packets due to undetected failures $\bar{N_l''}$ is therefore

$$\bar{N_l''} < \lambda T L_{max} r_{MD} \frac{(2K-1)T_B}{2}. \quad (8)$$

3) Packet Loss Due to Route Invalidation: This loss is triggered whenever a failure detection (whether true or false) occurs at an intermediate node $i \neq h$. When i detects a failure of link (i, j), it removes its route entry to k and drops all queued packets destined for k. After which, i sends a route error message to its upstream node. Upon receipt of the message, the upstream node performs the same set of actions. This process is repeated until the message reaches h which immediately initiates a route discovery. This means that as long as h does not receive a route error message, it will continue to forward packets along the path. Such forwarded packets will eventually get dropped the moment they reach a node that does not have a route to k.

The time duration t_m^C therefore depends on the per-hop delay of sending route error messages and the hop count of the point of failure from h. If τ is the per-hop delay, then if the failure is encountered by a node i that is d_m hops away from h, then $t_m^C = \tau d_m$. Hence, the average number of lost packets due to route invalidation $\bar{N_l'''}$ can be expressed as

$$\bar{N_l'''} = E\left[\lambda \tau \sum_{m \in M} d_m\right] = \lambda \tau E\left[\sum_{m \in M} d_m\right].$$

The expected value of $\sum_{m \in M} d_m$ can be expressed in terms of r_{LF}, r_{MD}, r_{FD}, and T. Every link along the path from h to k is detected to fail an average of $(r_{LF} - r_{MD} + r_{FD})T$ times during the entire flow. Thus, $\bar{N_l'''}$ can be simplified as

$$\begin{aligned} \bar{N_l'''} &\leq \lambda \tau \sum_{n=1}^{L_{max}-1} n(r_{LF} - r_{MD} + r_{FD})T \\ &\leq \lambda T \tau (r_{LF} - r_{MD} + r_{FD}) \frac{L_{max}(L_{max}-1)}{2}. \end{aligned} \quad (9)$$

Note that the summation is up to $L_{max} - 1$ since the node that is L_{max} hops away from the source is already the sink (*i.e.*, the sink will never experience downstream link failures as it is the end of the route). In the special case where $l_m = L, \forall m \in M$,

$$\bar{N_l'''} = \lambda T \tau (r_{LF} - r_{MD} + r_{FD}) \frac{L(L-1)}{2}. \quad (10)$$

4) Packet Delivery Ratio: For the entire flow duration, the number of packets sent $\bar{N_s} = \lambda T$. Subtracting the total number of lost packets, the packet delivery ratio θ can be computed as

$$\theta = \frac{\lambda T - (\bar{N_l'} + \bar{N_l''} + \bar{N_l'''})}{\lambda T} = 1 - \frac{\bar{N_l'} + \bar{N_l''} + \bar{N_l'''}}{\lambda T}.$$

Substituting (6), (8), and (9) to the above equation, we obtain the following inequality which indicates the lower bound for θ

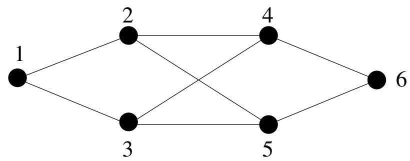


Fig. 2. Topology to experimentally validate the model.

TABLE I
EXPERIMENTAL CONFIGURATIONS

Parameter	Value(s)
Transmit power	18 dBm
MAC protocol	IEEE 802.11b
Unicast data rate	11 Mb/s
Packet size	1400 bytes
λ	$\{25, 50, 100\}$ pkt/sec
K	$\{1, 2, 3, 4\}$
T_B	$\{125, 250, 500, 1000, 2000\}$ ms

$$\theta > 1 - \frac{L_{max}}{2}\Big\{r_{LF}(2K-1)T_B + (r_{LF} - r_{MD} + r_{FD})(L_{max}-1)\tau\Big\}. \quad (11)$$

This expression highlights the competing requirements of link failures, false detections, and missed detections on the beaconing parameters K and T_B:

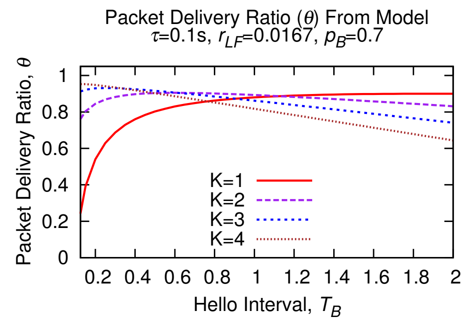
- Link failures contribute the highest losses as they factor in both detection delay and route invalidation. These losses are unavoidable but can be reduced by by choosing low K and T_B to shorten detection delay.
- False detections contribute losses due to unnecessary route invalidation. From (2), these losses can be reduced by choosing high K and T_B.
- Missed detections reduce losses due to route invalidation as they do not trigger the route invalidation phase. This implies that K and T_B may be chosen such that short-term link failures need not be detected if the resulting losses of not detecting them is smaller than the resulting losses of detecting them.

The current analytical framework implicitly assumes that link failures along the path from h to k do not overlap or occur simultaneously. This may not hold especially when link failures are frequent and the path from h to k is long. Observe that when several links fail almost at the same time, only the route error message due to the failed link (i, j) closest to the source h will reach h (because the route error message from the further links need to pass through (i, j) which already failed). Thus, the effect of overlapping failures is to reduce route invalidation and consequently reduce packet loss.

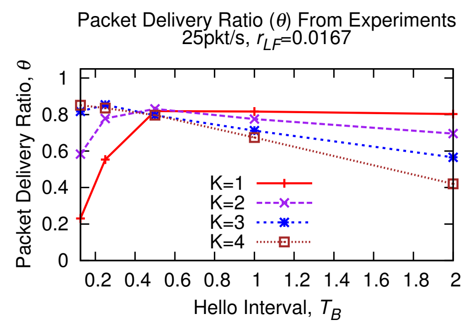
IV. MODEL VERIFICATION AND OPTIMIZATION OF BEACONING PARAMETERS

We validate the model for the packet delivery ratio θ by performing indoor experiments. We position six routers in an indoor environment to form the topology shown in Figure 2. We used AODV (aodv-uu implementation [16]) as the routing protocol and performed modifications to dynamically configure K and T_B.

Node 1 was configured to send CBR traffic to node 6 for 300 seconds. Nodes 2–5 were made to fail alternately twice every minute, with every failure lasting for exactly 10 seconds. The alternating node failure scheme ensured that there was always a route to the destination and that the length of the route was always 3. Table I provides a summary of the configuration used in the experiments. Note that $K = 2$ and $T_B = 1000$ ms are the typical values used by AODV.



(a)



(b)

Fig. 3. Packet delivery ratio at packet sending rate of 25 pkt/sec.

Note that the above configurations are valid for the special case where $l_m = L, \forall m \in M$. Moreover, since the failure time is greater than 8 seconds (the longest failure detection delay), $r_{MD} = 0$. From these, we can obtain a simpler expression for θ using (7), (10), and (2):

$$\theta = 1 - \frac{L}{2}\Big\{r_{LF}\left[(2K-1)T_B + (L-1)\tau\right] + \frac{(1-p_B)^K}{T_B}\left[(L-1)\tau\right]\Big\}. \quad (12)$$

Figures 3, 4 and 5 show θ when $\lambda = \{25, 50, 100\}$ packets per second, respectively. The values for τ and p_B used in the model were determined from the experiments while the value for r_{LF} was calculated since the number of link failures was known. Note that (12) does not show any direct dependence on λ. However, (12) is still affected by λ through p_B as the latter has been observed to be highly sensitive to the packet sending rate. From the experiments, p_B was determined to be 0.85,

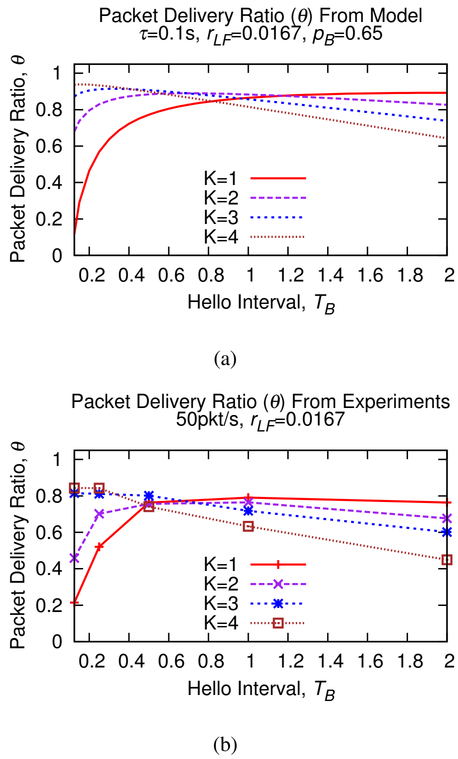


Fig. 4. Packet delivery ratio at packet sending rate of 50 pkt/sec.

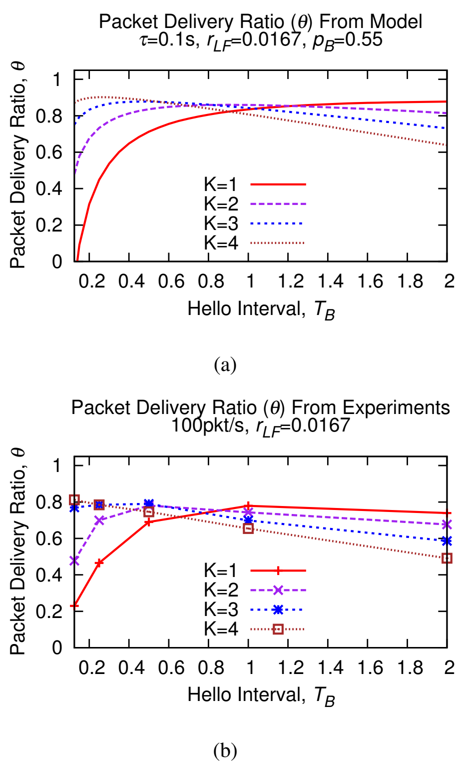


Fig. 5. Packet delivery ratio at packet sending rate of 100 pkt/sec.

0.7, 0.65, and 0.55 when λ was 0, 25, 50, and 100 packets per second, respectively. This sensitivity is due to the fact that when contention is increased (when λ is higher), hellos are more prone to loss due to collisions as they are sent broadcast (*i.e.*, without retry attempt) than data packets which are sent unicast (*i.e.*, with retry attempts) [15].

For each K, the obtained θ from experimental results are generally lower but follow the trend as T_B is varied from 125 ms to 1 second. The lower θ from experiments can be explained by losses due to contention which is not considered by the model. When $\lambda = 100$ and $K = 1$, the model tends to over-estimate the losses as the resulting θ obtained from the model is lower than the θ obtained from experiments. This is due to the "non-overlapping failures" assumed by the model. As mentioned, losses are expected to be lower when failures overlap due to reduced instances of route invalidation.

We can observe from both model and experiment that there is a value for T_B where an optimal θ for every K can be obtained. This can be determined by solving for the first derivative of θ with respect to T_B and equating it to zero as follows:

$$\frac{d\theta}{dT_B} = \frac{L}{2}\left[-r_{LF}(2K-1) + \frac{(1-p_B)^K(L-1)\tau}{T_B^2}\right] = 0.$$

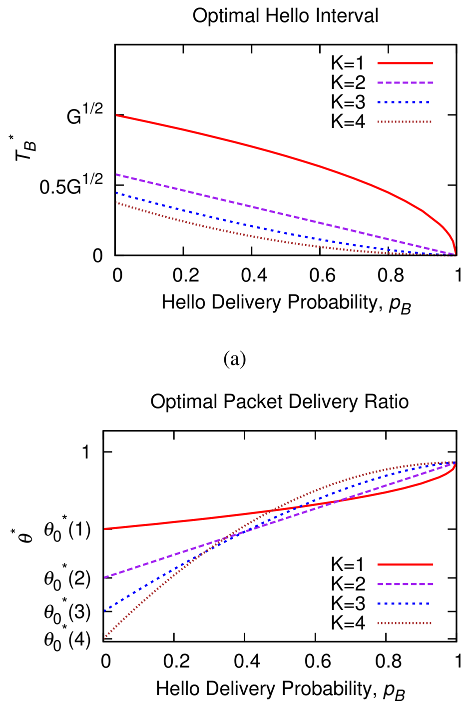
From this, we can obtain the optimal value for $T_B = T_B^*$ which provides the highest θ. Solving the above equation for T_B and ignoring the negative root, T_B^* is given by

$$T_B^* = \sqrt{\frac{(1-p_B)^K(L-1)\tau}{r_{LF}(2K-1)}} = \sqrt{\frac{(1-p_B)^K}{(2K-1)}G}, \qquad (13)$$

where $G = (L-1)\tau/r_{LF}$. Given T_B^*, we can obtain the optimal $\theta = \theta^*$ by substituting (13) into (12):

$$\theta^* = 1 - \frac{Lr_{LF}}{2}\left\{2\sqrt{(2K-1)(1-p_B)^K G} + Gr_{LF}\right\}. \quad (14)$$

We plot (13) and (14) as a function of p_B in Figure 6. From Figure 6a, it is clear that the optimal value for T_B is inversely proportional to K. Furthermore, the optimal T_B decreases as p_B increases. From Figure 6b, we can see that the optimal K (and consequently T_B) depends on p_B. For $p_B < 0.5$, $K = 1$ provides the best θ while for $p_B > 0.5$, $K = 4$ provides the best θ. Although counter-intuitive, this outcome can be explained by the following: At low p_B values, the false detection probability is exceedingly high and is the dominant factor for packet loss. Thus, choosing $K = 1$ in tandem with the corresponding T_B^* from Figure 6a provides the lowest false detection rate and consequently, the lowest packet loss. Meanwhile at high p_B values, detection delay becomes the dominant factor as false detection probability is significantly low. Thus, choosing $K = 4$ in conjunction with the corresponding T_B^* from Figure 6a provides the lowest detection delay and consequently, the lowest packet loss.



(a)

(b)

Fig. 6. Optimal hello interval and packet delivery ratio. In (b), $\theta_0^*(x)$ denotes the value when (14) is substituted with $K = x$ and $p_B = 0$.

V. Conclusion

Accurate and timely detection of link failures is important in order to maintain valid multihop routes in wireless ad hoc networks. Hello-based failure detection is still the predominant failure detection mechanism employed by many routing protocols.

In this paper, we derived an analytical model for hello-based failure detection that provides a lower bound on the packet delivery ratio. The model captures the competing requirements of link failures, false detections, and missed detections on the beaconing parameters K and T_B. Our analytical results, which are validated by experiments, show that the performance of hello-based failure detection can be optimized by selecting appropriate parameter values for K and T_B given the network conditions such as traffic load, link failure rate, and hello delivery rate. When hello delivery rate is low (in high load conditions), choosing K and T_B that minimizes false failure detections is preferred. When hello delivery rate is high (in light load conditions), choosing K and T_B that minimizes failure detection delay is preferred. In choosing T_B, one must also ensure that the control overhead which is $1/T_B$ packets per second, is not excessive as it may cause severe contention.

In the future, we plan to extend the analytical model to quantify the effects of: (*i*) route repair, which may reduce losses when successful but increase losses when unsuccessful; (*ii*) queuing losses when route discovery is prolonged; and (*iii*) overlapping or simultaneous failures.

References

[1] I. Chakeres and E. Belding-Royer, "The utility of hello messages for determining link connectivity," in *Proc. IEEE WPMC 2002*, vol. 2, Oct. 2002, pp. 504–508.

[2] V. Giruka and M. Singhal, "Hello protocols for ad-hoc networks: Overhead and accuracy tradeoffs," in *Proc. IEEE WOWMOM 2005*, 2005, pp. 354–361.

[3] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," Jul. 2003, IETF RFC 3561 (Experimental).

[4] D. Johnson, D. Maltz, and J. Broch, "DSR the dynamic source routing protocol for multihop wireless ad hoc networks," in *Ad hoc Networking*, C. Perkins, Ed. Addison-Wesley, 2001, pp. 139–172.

[5] A. C. Valera, W. K. Seah, and S. Rao, "Improving protocol robustness in ad hoc networks through cooperative packet caching and shortest multipath routing," *IEEE Trans. Mob. Comput.*, vol. 4, no. 5, pp. 443–457, 2005.

[6] C. Tschudin, P. Gunningberg, H. Lundgren, and E. Nordström, "Lessons from experimental manet research," *Ad Hoc Networks*, vol. 3, no. 2, pp. 221–233, Mar. 2005.

[7] L. L. Peterson and B. S. Davie, *Computer Networks: A Systems Approach*. Morgan Kaufmann Publishers, 2000.

[8] B. Bellur and R. Ogier, "A reliable, efficient topology broadcast protocol for dynamic networks," in *Proc. IEEE INFOCOM 1999*, vol. 1, Mar. 1999, pp. 178–186.

[9] S. Basagni, I. Chlamtac, V. R. Syrotiuk, and B. A. Woodward, "A distance routing effect algorithm for mobility (dream)," in *Proc. ACM MobiCom 1998*. New York, NY, USA: ACM, 1998, pp. 76–84.

[10] P. Jacquet, P. Muhlethaler, A. Qayyum, A. Laouiti, L. Viennot, and T. Clausen, "Optimized link state routing protocol. draft-ietf-manet-olsr-04.txt," work in Progress.

[11] F. Ingelrest, N. Mitton, and D. Simplot-Ryl, "A turnover based adaptive hello protocol for mobile ad hoc and sensor networks," in *Proc. IEEE MASCOTS 2007*, 2007, pp. 9–14.

[12] A. C. Valera, H.-P. Tan, and W. K. Seah, "Improving link failure detection and response in ieee 802.11 wireless ad hoc networks," in *Proc. IEEE PIMRC 2010*, 2010, pp. 1814–1819.

[13] G. Egeland and P. E. Engelstad, "The availability and reliability of wireless multi-hop networks with stochastic link failures," *IEEE J.Sel. A. Commun.*, vol. 27, no. 7, pp. 1132–1146, 2009.

[14] D. Aguayo, J. Bicket, S. Biswas, G. Judd, and R. Morris, "Link-level measurements from an 802.11b mesh network," in *Proc. ACM SIGCOMM 2004*, Aug. 2004.

[15] S. Das, H. Pucha, K. Papagiannaki, and Y. Hu, "Studying wireless routing link metric dynamics," in *Proc. ACM IMC 2007*, 2007, pp. 327–332.

[16] E. Nordström, "Aodv-uu: Ad-hoc on-demand distance vector routing," Aug. 2008, [Online]. Available: http://core.it.uu.se/core/index.php/AODV-UU [Accessed: Sept 3, 2011].