Modeling and exploiting the relation between packet losses and hidden traffic

Marc Portoles-Comeras, Albert Cabellos-Aparicio, Pablo Serrano, Josep Mangues-Bafalluy,
José Núñez-Martínez, Marc Solé, Albert Banchs, Jordi Domingo-Pascual

***Abstract*—Nowadays, it is common to find multiple WLAN deployments coexisting in shared spaces. The resulting interference between transmissions represents an important source of performance degradation, specially those originating from hidden traffic. This note explores the relation between hidden traffic and packet losses, using renewal theory to show that losses constitute *biased* samples of hidden traffic. Building on the developed analytical model, the paper derives the optimal frame length that maximizes throughput in the presence of hidden traffic. The results are validated using an 802.11 WLAN in-lab setting.**

***Index Terms*—WLAN, packet probing, measurements, renewal theory, hidden node interference.**

I. Introduction

CSMA networks (e.g., 802.11 WLANs) may suffer from the *hidden terminal* problem. This interference is caused by traffic that is not detected (i.e., sensed) at the sender-side of the communication, but results in a packet loss due to simultaneous transmissions at the receiver-side.

This work uses renewal theory to obtain a *generic* and *simple* model to characterize packet losses due to hidden traffic, showing that the frame length introduces a significant bias in the perceived losses. The model is generic in the sense that it is not specific to e.g. a technology or modulation and coding scheme (MCS), yet it can be easily translated into practical setups, as it is done in the validation experiments. The model is simple as it results analytically tractable, supporting the development of practical application of the results. Indeed, the article unveils an inherent trade-off between the protocol efficiency (i.e., payload time over total time) and the losses due to hidden traffic, and derives a closed-form expression for the optimal payload length to maximize throughput.[1]

This study differs from recent related works [3]–[6] in various aspects, which we summarize next. In [3] authors analyze the 802.11 saturation throughput with hidden nodes and validate the model using simulations. In their model, which is tailored to 802.11, all stations use the same frame size and no attempt is made to derive an optimal length, while our model is technology-agnostic and is validated with using experimentation. In [4] authors model the interactions between "coupled" flows in saturation, accounting for the *capture effect* and the lack of carrier sense. The model, which extends Bianchi's [7] to account for packet overlaps, is validated through experimentation. Here we follow a different approach to analyze the impact of a non-saturated hidden interferer on a reference flow, this resulting in a simple yet effective model that, furthermore, supports the derivation of a closed-form expression for the optimal frame length. In [5] authors analyze the case of 802.11b under 802.15.4 interference using a model and simulations, and recommend some values for the packet length based on the distance to the interferer. In contrast, our approach does not require considering the details of specific standards, radio propagation or MCS, and it is validated with experimentation (both the analysis and the derivation of the optimal frame length). Finally, in [6] authors propose an algorithm to estimate the derivative of throughput with respect to packet length, to maximize performance. The scheme is a heuristic that relies on tuning some parameters and the use of a lookup table, and is evaluated via simulations. In contrast, here we first propose an analytical model to characterize the impact of hidden traffic and validate it using experimentation, and then build on these solid foundations to derive a closed-form expression for the optimal packet length, which is also validated in a real-life testbed.

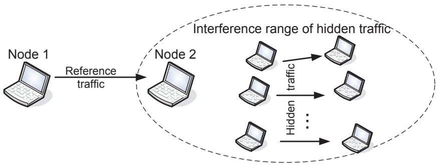

Figure 1. Reference scenario. Transmissions in the presence of hidden traffic

The rest of the paper is structured as follows. Section II proposes the model of the inter-relation between packet losses and hidden traffic load. This model is experimentally validated in Section III. Section IV derives the optimal frame length in the presence of hidden traffic and experimentally validates the results, and Section V concludes the letter.

II. A model of the inter-relation between loss and hidden traffic load

A. Scenario and assumptions

We consider the scenario depicted in Fig. 1, in which node 1 is sending data to node 2 (we refer to this traffic as *reference traffic*), and there is *hidden traffic* from other wireless sources that cannot be sensed by node 1, but will result in collisions at node 2. We assume that the behaviour of the hidden traffic is independent from the reference traffic, and that RTS/CTS is not used.[2]

We denote with T_n the time instant when the n-th packet of the reference traffic is sent, and with τ_n its length ($n = \{1, 2, \ldots\}$). Note that τ_n is determined by the packet length

[1] Note that this is only one of the potential practical applications of the results, and that other applications may include link quality metrics for taking routing decisions [1], or for access point selection strategies [2].

[2] Not only RTS/CTS is seldom used in real deployments, but also it can be ineffective [8] and degrade the overall network performance due to exposed nodes [9].

L_n, the transmission rate r_n and the headers time τ^h, i.e., $\tau_n = L_n/r_n + \tau^h$. For simplicity we assume constant transmission durations ($\tau_n = \tau,\ \forall n$) and Poisson arrivals.

We assume that hidden traffic can be modelled after an alternating renewal process, which is illustrated in Fig. 2. The process alternates between an *ON* (or busy) state, when hidden traffic is present but Node 1 senses the medium as idle, and an *OFF* (or idle) state, when there is no hidden traffic. The durations of busy periods form a random sequence $\{Z_k : k = 1, 2, ...\}$ that we assume as i.i.d with distribution function F_{on}, and the duration of idle periods follows the process $\{Y_k : k = 1, 2, ...\}$ that is also assumed to be drawn from a sequence of i.i.d durations with distribution function F_{off}. The addition of *busy* and *idle* durations forms the sequence $\{X_k = Z_k + Y_k\}$, with distribution function F. $\{X_k\}$ describes the sequence of inter-arrival times of the renewal process $\{N(t) = \sup\{k : \sum_{i=1}^{k} X_i \le t\}\}$.

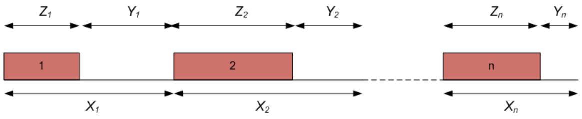

Figure 2. An alternating renewal process for the hidden traffic.

Let us denote as $U(t)$ the process *utilization* describing the *ON/OFF* state of the hidden traffic process at an instant t.

$$U(t) = \begin{cases} 1 & \text{hidden traffic present (busy)} \\ 0 & \text{no hidden traffic (idle)} \end{cases} \tag{1}$$

The long-term average-time that hidden traffic transmissions are using the wireless medium can be expressed as

$$\lim_{t\to\infty} P[U(t) = 1] = \frac{\mathbb{E}[Z_k]}{\mathbb{E}[Z_k] + \mathbb{E}[Y_k]} = u_h. \tag{2}$$

B. Model for the packet losses due to hidden traffic

In our scenario, where the senders of the reference and the hidden traffic cannot sense each other, packet losses are caused by the superposition of the above two processes. This is illustrated in Fig. 3, in which the $(n-1)$-th transmission is successful but the n-th transmission overlaps with the beginning of a new busy state, and therefore results in a collision.[3]

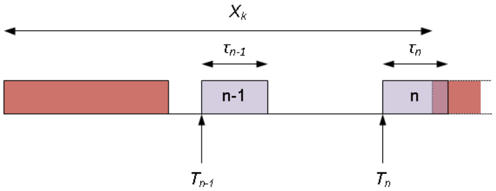

Figure 3. Modeling packet losses based on the superposition, in time, of reference and hidden traffic

Based on the above, the limiting probability of losing a packet (P_l) from the Poisson-arriving process $\{T_n\}$ can be expressed as,

$$\lim_{n\to\infty} P_l(\tau) = u_h + \varepsilon(\tau), \tag{3}$$

which is composed of two terms. The first one (u_h) corresponds to the average activity of hidden traffic that zero-length frames would measure, and is a consequence of the PASTA principle.[4] The second one ($\varepsilon(\tau)$), is caused by the non-zero duration of the packets from the reference traffic, and can be seen as a positive bias on the experienced hidden activity. More specifically, these "additional" experienced losses over u_h correspond to the cases when a packet arrives during the OFF period of the hidden traffic, but a new busy period starts before the transmission finishes. Note that if $Y_k < \tau$, i.e., the OFF period is shorter than the transmission length, the packet will always be lost, while in case $\tau < Y_k$, the packet could be successfully delivered (see Fig. 3),

To compute $\epsilon(\tau)$, we define the reward sequence $W_k = \min(Y_{k-1}, \tau)$, i.e., the amount of time during the OFF interval of the k-th period in which if a packet from the reference traffic is transmitted, it will collide with the hidden traffic. Let us define $R(t)$ as the cumulated reward by time t, such that $R(t) = \sum_0^{N(t)} W_n$. Based on this, the elementary renewal-reward theorem leads to

$$\varepsilon(\tau) = \lim_{t\to\infty} \frac{1}{t} R(t) = \frac{\mathbb{E}[W_k]}{\mathbb{E}[X_k]} = \frac{\mathbb{E}[\min(Y_{k-1}, \tau)]}{\mathbb{E}[X_k]} = \frac{\tau \cdot \Pr(\tau < Y_k) + \mathbb{E}[Y_k | Y_k \le \tau] \cdot \Pr(\tau > Y_k)}{\mathbb{E}[X_k]} = \frac{\tau \cdot (1 - F_{\text{off}}(\tau)) + \mathbb{E}[Y_k | Y_k \le \tau] \cdot F_{\text{off}}(\tau)}{\mathbb{E}[X_k]}. \tag{4}$$

Remarks. It is worth noting that the reward sequence is bounded by τ, and therefore $\mathbb{E}[W_k] \le \tau$. In the limiting case that the OFF periods are always longer than the transmission lengths (i.e., $F_{\text{off}} \approx 0$), the equality holds, while in case that the OFF periods are always shorter ($F_{\text{off}} \approx 1$), it can be seen that all packets from the reference traffic will be lost, as $P_l \approx u_h + \mathbb{E}[Y_k]/\mathbb{E}[X_k] = 1$.

III. Experimental validation

A. Testbed setup

In order to evaluate the model given by (3)-(4) in a real setting, we have set up the in-lab scenario illustrated in Fig. 4, which consists of two reference nodes, node (1) sending the reference traffic to node (2), several hidden traffic sources (h_i) and destinations (r_i), and three monitor devices used to capture traffic at different points of the communication to adequately measure the various performance figures (e.g., collisions, channel occupation). All nodes are equipped with 802.11b/g cards based on Atheros chipset, and we use coaxial cables and attenuators to replicate the reference scenario of Fig. 1. Experiments are run and controlled using the EXTREME Testbed facility.[5]

[3] Note that throughout the paper we do not consider the *capture effect* [10], as our scheme is oblivious to its impact: in case transmissions from the reference traffic capture the channel, these transmissions cannot be distinguished from successful transmissions in the absence of hidden traffic; in case they do not capture the channel, it will be undistinguishable from *regular* collisions.

[4] The assumption of using Poisson probing and the PASTA argument can be relaxed when the processes involved are mixing [11], which is the case of traffic patterns observed in Internet [12].

[5] http://iptechwiki.cttc.es/EXTREME_Testbed

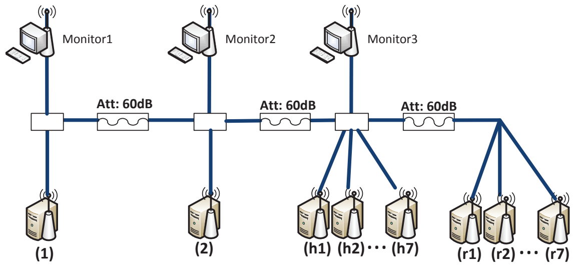

Figure 4. Experimental setup used to validate the model in an 802.11 setting

In all experiments, node (1) generates the multicast reference traffic to node (2), and node h_i generates hidden traffic to node r_i for all i, all of them using the `mgen` generation tool.[6] The reference traffic is constantly backlogged, while the hidden traffic generation rate is varied during the experiments to assess the accuracy of the model for different values of the airtime occupation.

B. Performance evaluation

We validate the accuracy of the analytical model for a variety of scenarios. More specifically, for the case of hidden traffic we used the $\{6, 12, 24, 54\}$ Mbps MCS, the traffic generation rates $\lambda = \{200, 500, 1000\}$ packets/s, and a fixed frame length of 1500 B. In order to accurately estimate the distribution of F_{off}, which not only depends on the generation process (Poissonian) but also on the impact of channel access rules (i.e., post-backoff rules) and the fidelity of the traffic generator [13], for every experiment we use the tracefile obtained by `Monitor3`. For the reference traffic, we used the $\{6, 12, 24\}$ Mbps MCS, while frame length is varied between 164 B and 1564 B to obtain and adequate sampling of τ.

The resulting values for the frame loss ratio P_l are depicted in Fig. 5, with lines depicting the results from the analytical model, and box-and-whisker plots representing the values from 20 measurements. According to the figure, the model is able to accurately predict the results from experimentation, as for all airtime occupation values the analytical results closely match the numbers from the testbed. The figure also confirms that P_l has a strong dependence of τ, thus confirming the dramatic impact of the bias term $\epsilon(\tau)$ characterized by equation (4).

IV. Optimal Packet Size Under Hidden Traffic

With the above, we have confirmed the good accuracy of the model (3)-(4) to predict the losses due to hidden traffic, which is the main contribution of the letter. Here we give one potential application of the model, namely, deriving the closed-form expression for the optimal frame size in a WLAN scenario with hidden traffic, to illustrate its usefulness.

A. The trade-off on the useful airtime

The protocol efficiency η_p determines the relative amount of time the medium is actually devoted to sending user data. Given a total frame length τ, the time required for headers τ^h, and an average guard time g that accounts for protocol operations between transmissions (e.g., backoff), the protocol efficiency can be computed as

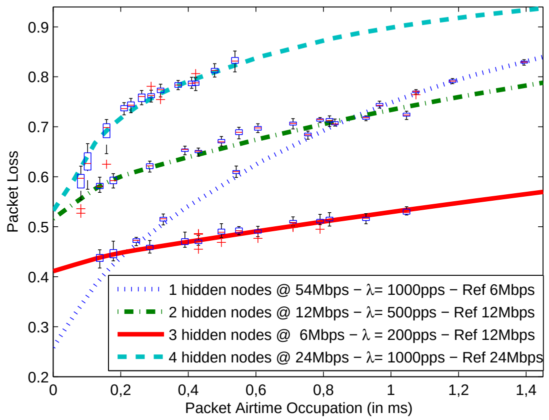

Figure 5. Packet Loss in the presence of hidden traffic. Experimental validation of the model

$$\eta_p = \frac{\tau - \tau^h}{\tau + g}, \tag{5}$$

which is an increasing function of τ. In the presence of hidden traffic, though, each frame has a loss probability equal to $P_l = u_h + \epsilon(\tau)$, and therefore the success probability p_s is a decreasing function of τ. Based on this trade-off between η_p and p_s, the optimal frame length τ^* results from solving the following maximization problem:

$$\tau^* = \max_{\tau} \eta_p p_s = \max_{\tau} \frac{\tau - \tau^h}{\tau + g}(1 - (u_h + \varepsilon(\tau))). \tag{6}$$

B. Linear approximation for P_l

We next address the derivation of a closed-form expression for τ^* based on (6). To this aim, we first note that according to Fig. 5, $P_l(\tau)$ can be approximated by a linear function for relatively large values of τ, which is the region of interest.[7] In this way, if we express P_l as

$$P_l \approx \hat{u_h} + \alpha\tau, \tag{7}$$

and substitute it in (6), performing the derivative to compute the maximum leads to the following expression for the optimal transmission duration (we omit the details for space reasons):

$$\tau^* = \sqrt{(\tau^h + g)(g + \frac{1 - \hat{u_h}}{\alpha})} - g. \tag{8}$$

We illustrate the accuracy of the linear approximation in Fig. 6, using the following two configurations:

- Case 1: We use the 12 Mbps MCS for the reference traffic and 6 Mbps MCS for the hidden traffic, which generates packets at a 200 packets/s rate.
- Case 2: We use 24 Mbps for both reference and hidden traffic. Hidden traffic is generated at 1000 packets/s.

The numerical values of the u_h and α parameters (provided in the figure) are computed using packet lengths five times

[6] http://cs.itd.nrl.navy.mil/work/mgen

[7] Overly small values of the occupation, i.e., $\tau \approx 0$, would correspond to almost-zero throughput.

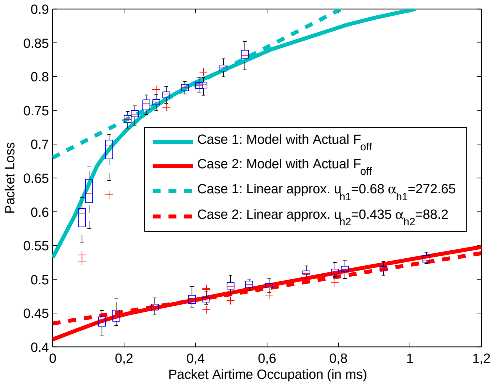

Figure 6. Linear approximation of the packet loss using packet loss samples of packets in the range 500Bytes-1500Bytes

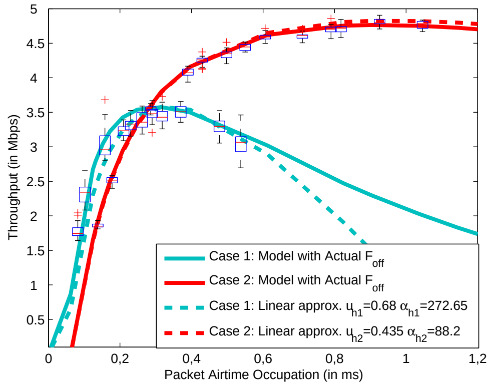

Figure 7. Throughput vs. Packet Size (Airtime Occupation) trade-off in an 802.11 setting. Boxplots are generated using experimental data and the curves stem from applying the loss model

longer than the frame overhead, i.e., $\tau > 5\tau_h$. The figure confirms that, for the region of interest, there is a good accuracy between the exact model (3) and the linear approximation (7).

C. Experimental validation

Here we validate the accuracy of (8) to compute the optimal frame length under hidden traffic, comparing its performance against results from experimentation. We consider the same two configurations as in the previous section, in which we already provided the numerical figures for u_h and α. Based on the default settings of the `madwifi` driver, the guard time is given by $g = 106$ μs, while the τ^h overheads for each case are $\tau_1^h = 68$ μs and $\tau_2^h = 47$ μs, respectively.

To validate the expression to compute τ^*, we perform a sweep on the packet size (in steps on 10 B) and measure the throughput obtained, repeating each experiment 20 times. We also compute the throughput predicted using the complete model, and the one using the linear approximation. The results are depicted in Fig. 7, in which we use box-and-whisker plots to represent the values from experiments, solid lines for the complete model, and dashed lines for the approximation. The results show that the linear approximation provides enough accuracy to compute the throughput in the range where it is maximum, thus being effective to obtain the optimal value for τ. This is confirmed by the numbers in Table I, in which for Case (1) the difference in packet lengths between the exhaustive search and the model is well below 9%, while for Case (2) it is below 4%. We conclude from these results that our model for the losses caused by hidden traffic can be effectively used to derive the optimal transmission length to maximize throughput.

Table I
OPTIMAL FRAME LENGTH FOR THE SCENARIOS CONSIDERED.

Scenario	Model	Experiment	Error
Case 1	867 B	800 B	8%
Case 2	1335 B	1296 B	3%

V. CONCLUSIONS

This letter explores the relation between packet losses and hidden traffic transmissions by means of renewal theory. The study models the relation between the time that it takes to transmit a packet and its loss probability, illustrating a trade-off with the protocol efficiency. As an example of a use-case for the model, we have derived the closed-form expression for the optimal transmission length under hidden traffic. The results have been experimentally validated in an 802.11 WLAN.

ACKNOWLEDGMENT

This work was partially supported by the Spanish Ministry of Science and Innovation under grants TEC2010-10440-E and TEC2011-29700-C02-01 and by Generalitat de Catalunya under grant 2009-SGR-940.

REFERENCES

[1] J. Padhye, S. Agarwal, V. Padmanabhan, L. Qiu, A. Rao, and B. Zill. *Estimation of Link Interference in Static Multi-hop Wireless Networks.* In ACM/USENIX Internet Measurement Conference (IMC) 2005.

[2] B. Kauffmann, F. Baccelli, A. Chaintreau, V. Mhatre, K. Papagiannaki, C. Diot, *Measurement-Based Self Organization of Interfering 802.11 Wireless Access Networks.* in IEEE INFOCOM, 2007.

[3] B. Jang and M. L. Sichitiu. *IEEE 802.11 saturation throughput analysis in the presence of hidden terminals* IEEE/ACM Transactions on Networking, April 2012

[4] J. Camp, E. Aryafar, and E. Knightly, *Coupled 802.11 Flows in Urban Channels: Model and Experimental Evaluation.* IEEE/ACM Transactions on Networking, 20(5):1635-1648, October 2012.

[5] D. Gil Yoon, S. Young Shin, W. Hyun Kwon, H. Seong Park, *Packet Error Rate Analysis of IEEE 802.11b under IEEE 802.15.4 Interference* In Proc. of VTC 2006-Spring, Melbourne, Australia, May 2006

[6] M. Krishnan, E. Haghani, A. Zakhor, *Packet Length Adaptation in WLANs with Hidden Nodes and Time-Varying Channels*, IEEE GLOBECOM 2011 Houston, TX, December 2011

[7] G. Bianchi, *Performance analysis of the IEEE 802.11 distributed coordination function.* IEEE J. Sel. Areas Commun., vol. 18, no. 3, pp. 535547, Mar. 2000.

[8] K. Xu, M. Gerla, M., Sang Bae. *How effective is the IEEE 802.11 RTS/CTS handshake in ad hoc networks.* In IEEE Global Telecommunications Conference (GLOBECOM), November 2002.

[9] L. B. Jiang, S. C. Liew. *Improving Throughput and Fairness by Reducing Exposed and Hidden Nodes in 802.11 Networks.* IEEE Transactions on Mobile Computing 7, 1 (January 2008), 34-49.

[10] P. Patras, H. Qi, D. Malone. *Exploiting the Capture Effect to Improve WLAN Throughput.* IEEE WoWMoM, San Francisco, USA, Jun. 2012

[11] F. Baccelli, S. Machiraju, D., and J. C. Bolot. *The role of PASTA in network measurement.* In Proc. of SIGCOMM'06. ACM, New York, NY, USA 2006

[12] M. M. Bin Tariq, A. Dhamdhere, C. Dovrolis, and M. Ammar. *Poisson versus periodic path probing (or, does PASTA matter?).* ACM SIGCOMM IMC, Berkeley, CA, USA 2005.

[13] Botta, A., Dainotti, A., Pescape, A. *Do you trust your software-based traffic generator?* IEEE Communications Magazine, Sept. 2010.