Measuring the Reliability of 802.11 WiFi Networks

David Murray, Terry Koziniec, Michael Dixon
School of Engineering and IT
Murdoch University
Perth, Australia
D.Murray@murdoch.edu.au

Kevin Lee
School of Science and Technology
Nottingham Trent University
Nottingham, UK
Kevin.Lee@ntu.ac.uk

***Abstract*—Over half of the transmission time in WiFi networks is dedicated to ensuring that errors are corrected or detected. Despite these mechanisms, many studies have concluded that frame error rates vary. An increased understanding of why frames are lost is a pragmatic approach to improving real world 802.11 throughput. The potential beneficiaries of this research, include rate control algorithms, Modulation and Coding Schemes, simulation models, frame size selection and 802.11 configuration guidelines. This paper presents a measurement study of the factors which correlate with packet loss in 802.11 WiFi. Both passive and active approaches were used to investigate how the frame size, modulation and coding scheme and airtime effect the loss rate. Overall, packet errors were high. The size of frames were not a major determinant of the loss rate. The loss rate decreased as the airtime of transmissions reduced but at substantially lower rates than those suggested in simple packet error models. Future work will further try to isolate and investigate specific errors, such as head on collisions in the preamble.**

Keywords—802.11, WiFi, Reliability, Measurement, Packet loss)

I. Introduction

It is widely known that the throughput of 802.11 WiFi networks, in optimal radio conditions, are at best half the reported data rate [1]. These throughput reductions are a consequence of MAC layer sharing mechanisms and error detection, such as Automatic Repeat reQuest (ARQ). Despite the use of Forward Error Correction (FEC), packet losses recorded in real world measurement studies are high, varying between 5% and 45% [2], [3]. The exploratory study presented in this paper is an attempt to determine the extent and cause of 802.11 WiFi packet losses. Identification of the primary cause of packet loss may enhance the design of more efficient loss detection/correction mechanisms.

This paper initially describes the scenarios that might cause packet loss and discusses the current loss prevention mechanisms. An experimental approach is used to measure the occurrence of packet loss in a range of real world environments. A seminal paper, by Aguayo et al. published using early 802.11b networks, found that link distance and SNR had only a very weak correlation with the packet loss rate [4], citing multi path fading from reflections as a possible cause. This paper presents an updated view from the perspective of modern wireless LANs. This work helps to highlight where future research may have the largest impact.

II. Background

A. The cause of packet loss in 802.11 wireless networks

There are numerous ways that packet loss can manifest in 802.11 wireless networks, as follows.

1) Head-on Collisions:

WiFi networks use a CSMA/CA protocol called Distributed Coordination Function (DCF) to share the medium. After a transmission has ended, all stations seeking access to the medium will pick a random number and count down to zero. If a node counts to zero, it will begin transmitting. All other stations, will overhear the transmission and defer access. If two nodes pick the same random number and begin transmitting simultaneously, the result will be an indecipherable transmission.

2) Hidden nodes

Transmission errors can also be caused by hidden nodes. This occurs when two competing stations cannot overhear each other’s transmission. Fortunately, numerous experimental studies have shown that, in LAN scenarios, the carrier sensing range is greater than the transmission range [5], [6]. The authors have not found any experimental evidence or observations investigating how commonly hidden node problems occur.

3) Background interference

Background wireless noise can be caused by various non-802.11 coexisting network types such as Bluetooth or Zigbee [7]. There are also many other sources of interference which may arise from non data communications devices such as microwave ovens and cordless phones [8].

4) Aggressive rate control

Wireless links actively modify the transmission rate by changing the Modulation and Coding Scheme (MCS). The modulation determines the number of bits per symbol and the coding scheme determines the amount of FEC. Onoe [9] and Minstrel [10] are examples of open source rate control algorithms. Onoe [9] determines the success rate of the current data rate every second. If the packet loss rate is less than 10%, over a fixed invocation period, the transmission rate is increased. Onoe is considered a conservative rate control algorithm [9].

$$Throughput = (\text{Prob\_success\_trans}/\text{Airtime\_of\_1\_packet}) \quad (1)$$

Minstrel [10] works by keeping an exponentially weighted moving average of the potential throughput at different data rates. The estimated throughput is calculated independently for each data rate and is shown in equation 1. The rate providing the highest throughput is the one which is used.

Minstrel attempts to send packets at higher and lower data rates to constantly probe whether the data rate should be increased or decreased. Therefore, unless the station is connected at the highest rate, the algorithm is certain to cause packet loss by testing packets at data rates that are higher than may realistically be supported.

Rate control is implementation specific and many algorithms are not publicly available. The Minstrel rate control algorithm continuously probes the optimal data rate limit and a degree of packet loss is not only inevitable, but a necessary consequence of finding and utilising the most efficient rate. While it is difficult to know the precise usage of different rate control algorithms in current 802.11 WiFi networks, it is likely that most algorithms will allow or cause a degree of packet loss.

B. *The extent of packet loss in 802.11 wireless networks*

Using basic packet error models, the probability of an error should increase exponentially with the packet size. Equation 2 shows this rate; where pBE is the probability of bit error and z is the frame size. The accuracy of this equation will heavily depend on the distribution of wireless errors. This study demonstrates the extent to which packet size and air time are linked with the loss rate in modern 802.11 WiFi networks.

$$LossProbability = (1 - \mathrm{pBE})^{z} (2)$$

C. *How packet loss is prevented in 802.11 wireless networks*

Collisions, hidden nodes and background interference make the wireless medium inherently unreliable. Packet losses that are not recovered at the link layer cause dramatic reductions in the TCP window and throughput, as TCP will interpret them as congestion. 802.11 WiFi uses Forward Error Correction (FEC) and Automatic Repeat Request (ARQ) to prevent packet losses from being recovered by TCP.

1) FEC

FEC is the addition of redundant bits, which enable the correction of errors at the receiver. FEC is particularly effective against a commonly modelled form of interference called Additive White Gaussian Noise (AWGN). Depending on the modulation, the FEC, or coding rate, varies between 50% and 16%. Post FEC loss rates in real 802.11 WiFi networks have been found to vary between 5% and 45% [2], [3]. The mechanism to recover these packets, which are indecipherable after FEC, is called ARQ.

2) ARQ

Packets where the interference or noise is too great to be corrected by FEC are detected and recovered through the use of ARQ. This link layer reliability mechanism positively acknowledges all packets. Every data frame that does not receive an acknowledgement is retransmitted. In some cases, the data frame may have been successful, but the returning acknowledgement is lost. The loss of this acknowledgement also causes a retransmission. Under perfect conditions, with no retransmissions, the overhead of this scheme is approximately 25% of the total transmission time [11] in 802.11a/b/g networks. In more recent 802.11 amendments, block acknowledgements have been used to reduce this overhead.

Given that 16-50% of transmission time is used by FEC to fix errors and an additional 25% of time is used for ensuring link layer reliability, a greater understanding of the factors causing packet loss has the potential to greatly improve the real world performance of WiFi networks.

III. Problem Statement and Related Work

Analysis of the factors causing packet loss using simulators or link emulators is erroneous. Some WiFi manufacturers specify that the range of SNR values which produce loss rates between 10% and 90% is a narrow 3dB [12]. Emulations, where the sender is directly connected to the receiver via a cable and variable attenuator also support this narrow, 3dB, margin for error [4].

Real world experiments [4], contradict the results of simulators and link emulators. They suggest that the range of SNRs where packet loss may occur is significantly wider than 3dB. The difficulties in creating mathematical models, wireless simulations or emulations that can account for real world wireless networks are well known [13], [6], [4]. Due to the evidence [14], demonstrating the vastly different behaviour between emulated and real word links, the investigation presented in this paper uses real world data.

To the authors' best knowledge, there are two studies that have used a similar experimental methodology to determine loss rates over real 802.11 WiFi LANs. These previous experimental studies have measured packet loss rates and found variations between 5% and 45% at different time periods [2]. A study by Rodrig et al. recorded a mean, pre-ARQ packet loss rate of 28% [3]. These 5% to 45% packet loss rates are occurring despite 25%-50% of the transmission time being used by FEC.

This paper re-examines transmission success rates and the range of factors that correlate with packet losses. Careful analysis may provide clues to help locate the predominant cause of packet loss. Understanding why wireless networks lose packets is very important and it is possible that much needed experimentation in this area has been neglected due to the methodological difficulties in obtaining data from which generalised conclusions can be made. The significance of this study is the volume of wireless packet captures which have been obtained from a wide range of network types and the analysis of loss rates against modulation, frame size and airtime.

IV. Methodology

The goal of this study was to obtain real world measurements on packet losses in WiFi networks. Two approaches were taken: passive and active. The passive approach captures the effects of a wide range of devices and

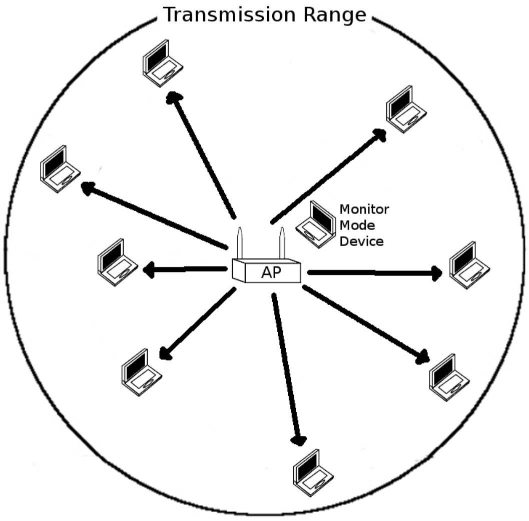

Figure 1: Passive Test Topology: Only transmissions sourced from the AP are used for analysis

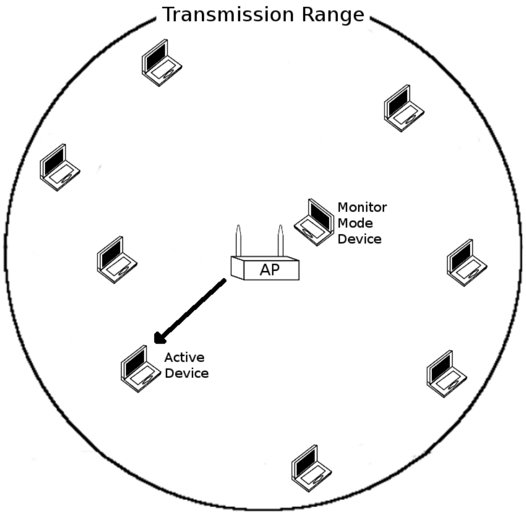

Figure 2: Active Test Topology: Only transmissions sourced from the AP, and destined to the active device are used for analysis

settings. The active method trades the range of devices and settings for greater control over the variables in use.

Both passive and active methods involved the use of monitor mode 802.11 network cards to capture over the air traffic. Monitor mode allows the capture of raw link layer information. The methodology used for 802.11 measurements has been the subject of numerous academic papers [15], [16], [17]. These papers unanimously agree that the most accurate way to measure packet loss is by monitoring the medium and measuring the number of packets with the 802.11 retransmitted flag set to 1 [15], [16], [17]. In this study, a monitoring device is placed next to the AP. Only frames transmitted from the wireless Access Point (AP) to the wireless client are used for statistical analysis as the wireless monitor might only capture a subset of frames transmitted from the client to the AP, skewing the results. The aspects specific to the passive and active approaches are detailed in the following sections.

A. *Passive measurement*

Few studies have investigated packet losses in real 802.11 WiFi networks because measurements from each AP are not repeatable, and many environmental factors are uncontrollable. Background noise and interference vary over time. To combat these problems, traffic was captured over a long duration to minimise any bias introduced by individual clients or events. An entire weeks worth of data was captured for every AP.

The interference encountered by different WiFi hotspots will vary. A range of scenarios and environments including high and low density office environments to household APs in suburban and urban settings, were used. Permission was obtained from all the network owners who ensured that all data was encrypted. Furthermore, the capture length was set such that only the data-link layer headers of each packet are stored. This study was approved by the Murdoch University Human Research Ethics Committee (Permit No:2014/149). Figure 1 shows the design of the passive experiments. The passive measurement data set was filtered based on the source MAC address of the AP in use. This ensures that the data set only consisted of packets sent from the AP and to wireless clients. As the data being analysed is limited to frames transmitted within a foot of the monitor mode packet capturing device, we believe that the captured data set is complete.

B. *Active measurement*

Using a passive capture method relinquishes control over some variables. In the passive captures, frames <200 bytes and >1400 bytes made up over 90% of the frames. The active measurement tests permitted control over the frame sizes in the sample. In the active tests, a script continually sent different sized ICMP messages between the wireless client and the AP. The data set was filtered, after the capture, to only contain the desired data. These active tests made it possible to obtain representative samples of a range of different packet sizes which were not present in sufficient quantities in the passive measurement tests. Figure 2 shows the design of the active experiments. The difference between the passive and active studies is the introduction of the passive wireless client. Only frames transmitted from the AP to the active client were used for analysis.

V. Results

This study investigated correlations with loss rates. Within tests, there were a vast number of continuously changing variables. Losses caused by collisions, hidden nodes, random interference and faulty drivers are just a subset of the operations occurring in the background that are neither controlled or measured. In some cases, these aspects are unable to be measured. In other cases, actively controlling these aspects may reduce the validity of the study. Due to aggressive rate selection mechanisms, searching for the best possible data rate will create some spurious errors [9], [10]. Looking at previous experimental work, as well as the rate control algorithms themselves, the authors do not believe that the number of these errors would exceed 10% [9], [10]. Any data points which did not constitute a sufficient proportion, 2% of the captured data packets, were omitted from the results.

A. Modulation and coding

Some previous work has shown that there are compromised data rates. Bianchi et al. states that; 802.11b at 11 Mb\/s is more reliable than 802.11g at 6 Mbps [18]. Due to prior work [18], stating that there are certain weak data rates, this study analysed the percentage of lost packets based on the data rate or the modulation and coding scheme. Table 1 shows the data rate and the level of FEC in 802.11a/g 802.11n 1x1 MIMO and 802.11n 2x2 MIMO. As shown in Table 1, the same coding rates and FEC is used in 802.11a/g and 802.11n. While there were a range of factors effecting loss rates, the data does not indicate that there is a single particularly weak data rate.

TABLE I. MODULATION AND CODING SCHEME FOR 802.11AGN

Modulation	**BPSK**	**QPSK**		**16-QAM**		**64-QAM**		
Coding	**1/2**	**1/2**	**3/4**	**1/2**	**2/3**	**2/3**	**3/4**	**5/6**
802.11a/g	6	12	18	24	36	48	54	-
802.11n 1x1	6.5	13	19.5	26	39	52	58.5	65
802.11n 2x2	13	26	39	52	78	104	117	130

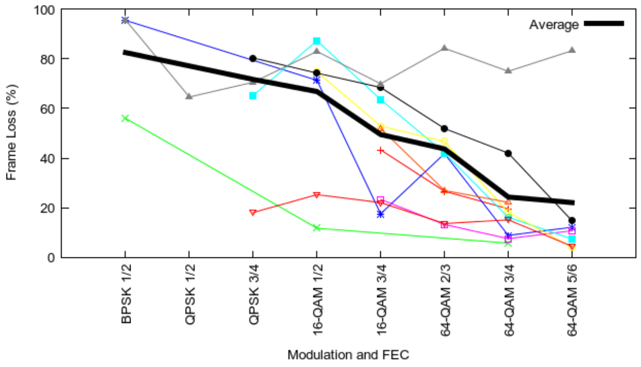

Figure 4 Passive Tests – Transmission rate and loss rate

The trend in the data does show that clients connected at higher modulation and coding schemes are more likely to successfully deliver their packets. Clients connected at low data rates are significantly more likely to have frame errors. Many configuration rules state that for high bandwidth WLANs, slow clients should be prevented from connecting, as their packets will consume significant airtime. This study further shows that, not only will their packets consume more airtime, they will also suffer frequent retransmissions.

Using the collected data, it is impossible to determine the exact reason(s) why transmissions from stations connecting at faster speeds have more reliable transmissions, however, it is possible to hypothesise, such that future work may target these factors. One possibility is that the preamble is more robust on connections which are capable of connecting at higher data rates. Problems with preamble sync have been suggested in prior work [19]. Another possibility is that clients connected at higher data rates send frames which, on average, spend less time in the air. This might make them less prone to random bursts of interference. The idea that dropping to a lower data rate does not necessarily increase the probability of successful transmissions is well known amongst those that have worked on rate control algorithms [4], [10]. If increased airtime is the main factor in packet losses, in current WiFi networks, then the following investigation of frame sizes should show that losses increase with the frame size.

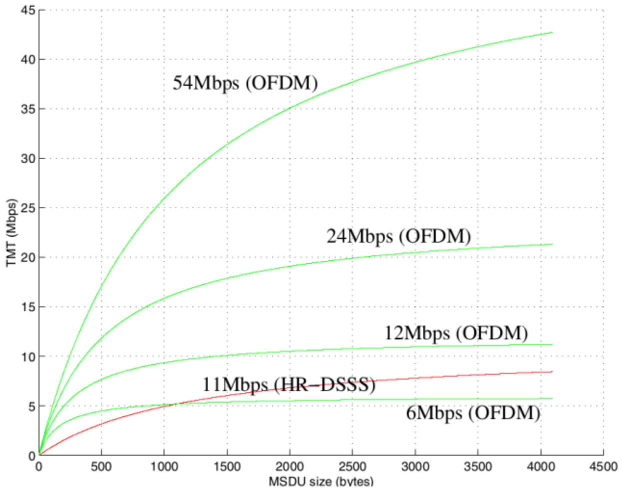

Figure 3 TMT: Theoretical Maximum Throughput

B. Frame size

The frame size used in wireless networks can have a large impact on performance. As each frame has a fixed overhead, larger frames will reduce overheads and can potentially increase throughputs. Figure 4 demonstrates how higher throughputs can be achieved simply by increasing the frame size. This graph assumes that there are no packet losses in the wireless network. If packet losses increase with the packet size, then real world performance is unlikely to scale in the manner suggested in Figure 4.

Great efforts were made in the 802.11n standardisation process to create mechanisms to aggregate multiple 1500 byte frames. Aggregating multiple frames is attractive because the default, 1500 byte, frame size becomes increasingly inefficient as the data rate increases. A standard 1500 byte frame becomes inefficient, as the data rate increases, due to MAC and PHY overheads, such as the preamble and media contention, which increase in their relative size with data rate increases. Larger frames sizes amortise these costs. Recent work has also demonstrated the potential TCP benefits derived from using a larger Internet packet size [20].

A serious impediment, to the use of a larger transmission unit, is the uncertainty over increased loss rates at larger frames sizes. Larger data frames have a higher probability of being dropped than smaller frames [2]. The extent to which frame losses increase with the packet size depends on the reason for lost packets. Some prior work, by Sridhara et al. [19], investigated errors using an emulated setup. The conclusion of this study was that, when errors are caused by collisions the packet error rate is independent of the frame size. Sridhara et al. [19] differentiated this from scenarios which were noise limited, where the probability of errors grows exponentially with the frame size.

Real Internet packets have bimodal distribution, with the majority of packet sizes falling below 200 bytes or between 1400 and 1500 bytes [21]. The results showing the percentage of lost packets in the passive measurement test are shown in Table 2. These results from the passive measurement suggest that there is no observable difference between the packet loss rate of packets <200 bytes and >1400 bytes.

TABLE II. PACKET LOSS MEASURED IN PASSIVE STUDY

Scenario	< 200 byte packets lost	< 1400 byte packets lost	Change
Lib 5GHz	15.5%	10%	-5.5%
Lib 2.4GHz	30.7%	27.6%	-3.1%
Ubiquiti 2.4 GHz	18.6%	16.6%	-2.0%
Buffalo 2.4GHz	29.2%	30.8%	+1.6%
SC 2.4GHz	72.0%	82.3%	+10.3%
TP-Link 2.4GHz	11.0%	7.2%	-3.8%
Cisco 2.4GHz	14.1%	7.4%	-6.7%

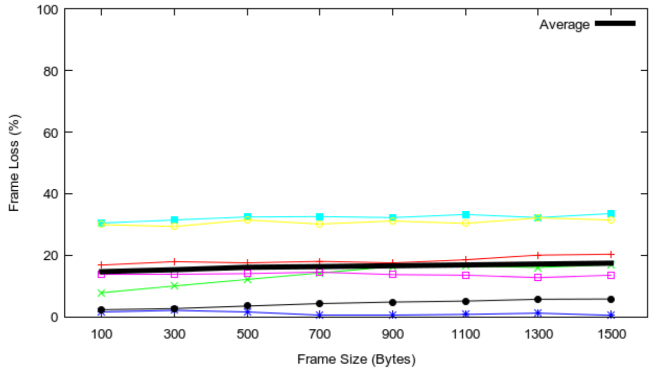

Figure 5: Active Tests – Frame Size and loss rate

Active tests were also performed and allowed control of the sample packet size. A representative sample of a wide range of packet sizes were possible and the results are shown in Figure 5. The active results also suggest that the packet size did not contribute significantly to the packet error rate.

C. Airtime

The previous results suggest that the frame size, in bytes, did not have an observable effect on the packet loss rate. However, frame size may also be interpreted as the amount of time a frame exists in the air. This value, referred to as the airtime, is the size, in bytes, divided by the data rate, plus physical layer preambles. Aguayo et al. [4] found that sometimes lower bit rates perform more poorly than higher bit rates, due to the amount of time the packet spends in the air. Work on rate control algorithms also supports the idea that reduced airtime can also reduce the exposure to interference [10]. The results of the passive and active studies are shown in Figure 6 and Figure 7. Note that the scale of the x-axis in Figure 7 and Figure 7 is logarithmic. The results suggest that the packets which spend less time in the air, were less likely to be lost [4], [10].

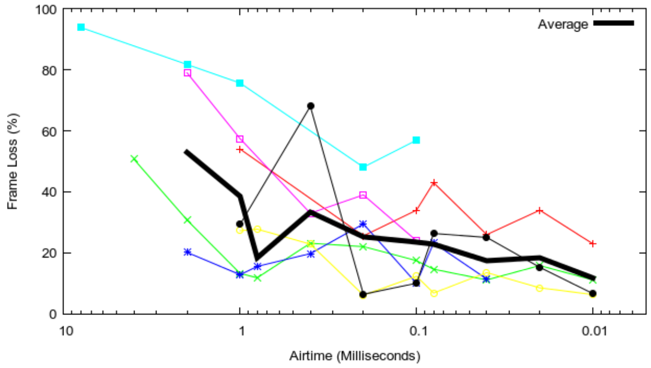

Figure 6: Passive Tests – Airtime and loss rate

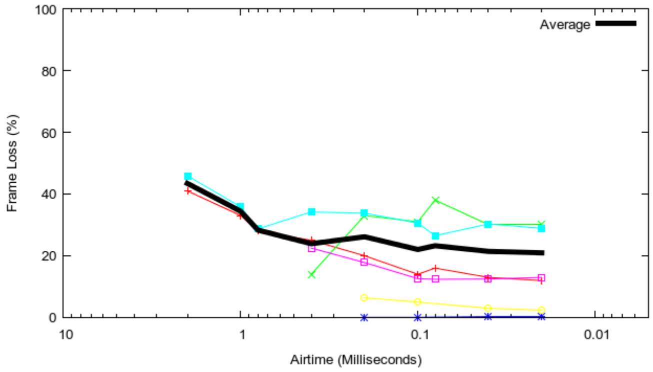

Figure 7: Active tests: Airtime and loss rate

Interestingly, the packet size did not have an observable effect on the loss rate yet the modulation and the airtime did. Further research is required to investigate whether there are artefacts that are independent of the length, which are robust for clients that can support high data rates and fragile for clients at lower speeds. The preamble will be a specific area of enquiry in future research.

D. Preamble and Guard Interval

The most common configuration measured was a short preamble and a long guard interval. Both are the default settings for modern APs. Data on preamble length and guard interval was measured however the data recorded in these types of studies are inadequate for meaningful analysis. The preamble is a sequence of symbols which are sent to synchronise the sending and receiving radios. Most APs in this study used the short preamble, because they were transmitting the majority of packets using the 802.11a/g/n standards where support is mandatory. Long preambles were used for 802.11b transmissions and therefore comparisons between the success rate of short and long preambles are likely to represent the difference between 802.11b and 802.11a/g/n transmission mechanisms. Reporting these numbers would therefore be fraught with bias.

The guard interval is a period of silence between every transmitted wireless symbol and is required to allow multi-path reflections to die down before the beginning of a subsequent symbol. Comparing the short and long guard intervals would suffer from similar bias to short and long preambles. The short guard interval is only an option 802.11n/ac deployments and therefore the results of a comparison might be more likely to represent the difference between 802.11a/b/g and 802.11n/ac success rates.

VI. Conclusions and Future Work

The number of packet losses occurring, in this and prior measurement studies [2, 3], is large enough to be considered an important topic requiring serious consideration. The results suggest that frames, which spend less time in the air, were less likely to be lost but at proportionally lower rates than simple channel error models suggest. Frames transmitted at high data rates, were also more likely to be successful than those transmitted at low data rates. Both the passive and active studies found that the size of the packet, in bytes, did not significantly effect the probability of loss. While this study alone does not permit any strong conclusions about the precise cause of packet loss, there are implications for a number of research areas.

Reducing the airtime by 10 times, on average, reduces the loss rate by approximately 10%. As the results suggest that the frame size has little effect on the loss rate, we suggest that larger wireless frames, may have a highly beneficial effect on overall throughputs. Future research should investigate the extent to which the packet size effects the loss rate in 3G and 4G networks. If future 3G and 4G experiments continue to suggest that packet loss does not increase at larger packet sizes then perhaps the current MTU used on the Internet requires fresh consideration [20]. The link layer throughput benefits, when using a larger frame size, are significant.

If the major cause of frame loss was hidden nodes or continuous background noise then losses would have increased exponentially with the size. As frame losses did not increase exponentially, or proportionally, with either the packet size or airtime, we suggest that they are not the main reason for losses in the capture. Future work will isolate an 802.11 WiFi network in coax cable with the specific intention of investigating the preamble, as well as head on and mid-air collisions.

References

[1] J. Jun, P. Peddabachagari, and M. Sichitiu, "Theoretical maximum throughput of IEEE 802.11 and its applications," in Network Computing and Applications, 2003. NCA 2003. Second IEEE International Symposium on, pp. 249–256, 2003.

[2] A. P. Jardosh, K. N. Ramachandran, K. C. Almeroth, and E. M. Belding-Royer, "Understanding link-layer behavior in highly congested ieee 802.11b wireless networks," in Proceedings of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis, E-WIND '05, (New York, NY, USA), pp. 11–16, ACM, 2005.

[3] M. Rodrig, C. Reis, R. Mahajan, D. Wetherall, and J. Zahorjan, "Measurement-based characterization of 802.11 in a hotspot setting," in Proceedings of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis, E-WIND '05, (New York, USA), pp. 5–10, ACM, 2005.

[4] D. Aguayo, J. Bicket, S. Biswas, G. Judd, and R. Morris, "Link- level measurements from an 802.11b mesh network," in Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications, SIGCOMM '04, (New York, NY, USA), pp. 121–132, ACM, 2004.

[5] X. Liu, A. Sridharan, S. Machiraju, M. Seshadri, and H. Zang, "Experiences in a 3g network: interplay between the wireless channel and applications," in Proceedings of the 14th ACM international conference on Mobile computing and networking, MobiCom '08, (New York, NY, USA), pp. 211–222, ACM, 2008.

[6] G. Anastasi, E. Borgia, M. Conti, and E. Gregori, "Wi-fi in ad hoc mode: a measurement study," in Pervasive Computing and Communications, 2004. PerCom 2004. Proceedings of the Second IEEE Annual Conference on, pp. 145–154, 2004.

[7] S. Pollin, I. Tan, B. Hodge, C. Chun, and A. Bahai, "Harmful coexistence between 802.15.4 and 802.11: A measurement-based study," in 3rd In- ternational Conference on Cognitive Radio Oriented Wireless Networks and Communications, CrownCom 2008, pp. 1–6, 2008. [8

[8] CiscoSystems, "20 myths of wi-fi interference: Dispel myths to gain high- performing and reliable wireless," 2007.

[9] S. Pal, S. Kundu, K. Basu, and S. Das, "IEEE 802.11 Rate Control Algorithms: Experimentation and Performance Evaluation in Infrastructure Mode," in Passive and Active Measurement Conference, PAM'06, pp. 30–31, 2006.

[10] F. Fietkau and D. Smithies, "Minstrel Rate Control Algorithm Documentation." http://wireless.kernel.org/en/developers/Documentation/mac80211/RateControl/minstrel, 2014.

[11] D. Murray, T. Koziniec, and M. Dixon, "D-proxy: Reliability in wireless networks," in APCC 2010 Asia Pacific Conference on Communications, pp. 129–134, 2010.

[12] Intersil-Corporation, "ISL3873 Wireless LAN Integrated Medium Access Controller with Baseband Processor." Whitepaper Online, 2000.

[13] D. Kotz, C. Newport, and C. Elliott, "The mistaken axioms of wireless-network research," July 2003.

[14] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Predictable 802.11 packet delivery from wireless channel measurements," SIGCOMM Com- put. Commun. Rev., vol. 41, Aug. 2010.

[15] Y.-C. Cheng, J. Bellardo, P. Benk ̈o, A. C. Snoeren, G. M. Voelker, and S. Savage, "Jigsaw: solving the puzzle of enterprise 802.11 analysis," SIGCOMM Comput. Commun. Rev., vol. 36, pp. 39–50, Aug. 2006.

[16] J. Yeo, M. Youssef, and A. Agrawala, "A framework for wireless lan monitoring and its applications," in Proceedings of the 3rd ACM workshop on Wireless security, WiSe '04, (New York, NY, USA), pp. 70–79, ACM, 2004.

[17] U. Deshpande, C. McDonald, and D. Kotz, "Refocusing in 802.11 wireless measurement," in Proceedings of the 9th international conference on Passive and active network measurement, PAM'08, (Berlin, Heidelberg), pp. 142–151, Springer-Verlag, 2008.

[18] G. Bianchi, F. Formisano, and D. Giustiniano, "802.11b/g link level measurements for an outdoor wireless campus network," in World of Wireless, Mobile and Multimedia Networks, WoWMoM 2006. International Symposium on a, pp. 6 pp.–530, 2006.

[19] V. Sridhara, S. Hweechul, and S. Bohacek, "Performance of 802.11b/g in the interference limited regime," in Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th International Conference on, pp. 979–984, Aug 2007. [20

[20] D. Murray, T. Koziniec, K. Lee, and M. Dixon, "Large MTUs and internet performance," in 2012 IEEE 13th International Conference on High Performance Switching and Routing (HPSR), pp. 82–87, 2012.

[21] D. Murray and T. Koziniec, "The State of Enterprise Network Traffic in 2012," in 18th Asia-Pacific Conference on Communications (APCC), 2012.