TKN Telecommunication Networks Group

Technical University Berlin

Telecommunication Networks Group

Packet Loss Discrimination in Multi-Cell 802.11 Wireless LANs

Murad Abusubaih, Berthold Rathke

abusubaih@tkn.tu-berlin.de

Berlin, October 2008

TKN Technical Report TKN-08-010

TKN Technical Reports Series

Editor: Prof. Dr.-Ing. Adam Wolisz

Abstract

Packet loss in 802.11 WLANs can occur either due to collision or a signal that is not strong enough at the receiver antenna. A challenging issue is the determination of packet loss cause once it occurs, which is a key for improving the performance of 802.11 WLANs. This report proposes and evaluates an algorithm to achieve this goal. The core of this algorithm is power level statistics at the receiver MAC. It learns from the received power levels of both correct and corrupted packets and decides whether a packet is lost due to collision or a weak signal.

Contents

Chapter 1

Introduction

Recently, there has been a great interest in the design of WLAN management algorithms for improving users' QoS, particularly in dense deployments. The trend is to develop a self-reconfigurable network that is able to learn the environment, share information and adapt its parameters as necessary. In this context, numerous rate selection, channel selection, channel access, and power adjustment algorithms have been proposed. One major goal of such algorithms is adaptability to the dynamical changes in the wireless environment.

With current 802.11 products, the only feedback to the sender is the ACK packet, which indicates successful packet reception. If ACKs do not arrive, the sender does not know the reason. In this case: backoff, rate selection, power, channel selection are candidate actions to be taken. Obviously, only based on lack of ACKs, it is quite hard for the sender to decide on the right action to be executed. Different strategies have been proposed for reaction to the absence of ACKs. In most implementations, the cause of failure is firstly attributed to collisions, thereby the contention window is doubled and the sender enters the backoff state. Depending on the used strategy, after some number of unsuccessful transmission trials, a failure is then attributed to weak signals, triggering the rate selection algorithm. Clearly, if a frame is dropped due to a weak signal, doubling the contention window will waste the airtime, leading to serious performance degradation. Also, when collisions occur often, the rate selection will unnecessarily reduce the transmission rate.

This blind reaction can be overcome if communicating nodes are able to diagnose the cause of failure and invoke the proper adaptation algorithm. In this case, if insufficiently strong signal arrives at the receiver, the proper action would be a tune of transmit power level, transmission rate, or perhaps invoke of handoff procedure. On the other hand, if packets are not ACKed due to collisions, it would be better for the sender to tune backoff, the operational channel, or even negotiate a change of the access scheme in case of high interference.

To this end, a method to diagnose the cause of packet losses is a key for effective WLAN management algorithms. This report proposes and evaluates one method towards this goal.

1.1 Relevant Work

Witehouse et. al. [1] have shown that if two frames arrive at the receiver of a node with certain timing and power levels characteristics (the second frame arrives after the preamble and header of the first frame and the power level of the second frame is significantly higher than that of the first frame), then it is possible for the node to conclude that a collision had definitely occurred and the receiver synchronizes and receives the new frame. The authors propose a mechanism by which a node detects the new frame. A node achieves this by observing a significant jump of received power and searching for headers while decoding the first frame. The proposed approach was implemented for sensor networks, on a platform that allows at any time low-level access to timing and power parameters which is not the case with 802.11 implementations, which provides power level indication (RSSI) at the MAC for each frame. The algorithm may not detect all collisions since a collision is assumed only if significant power levels between the first frame and a new coming one is observed.

Another attempt was done by Yun and Seo [2]. They proposed a mechanism for collision detection in 802.11 links based on RF energy measurements. The authors assume that a WLAN adapter (at the receiver) can measure the duration of RF energy pulse (the time span a receiver detects energy above the sensitivity threshold) on a channel during packet reception. The physical layer reports the measurement result to the MAC layer. As the packet duration is known to the sender (from the Length and Rate information), the sender deduces a collision to have occurred if the duration of energy measured at the receiver and sent back to the sender is larger than the packet duration. Obviously, this approach only works with some configurations of packet length and their relative phase shift. The approach introduces overhead due to the backward transmission of measurements from receivers to senders. Moreover, experimental evaluations conducted in [6] concluded that the efficiency of the proposed mechanism might be poor in practice.

Pang et. al. [3] have modified the 802.11 MAC and used explicit negative acknowledgment (NAK) for the purpose of differentiating frame losses due to intra-BSS collisions and weak signal. The authors assume that if all STAs in a WLAN BSS are close enough and can hear one another, a collision occurs only when more than one station sends data frame in the same time slot. In this case, collision on initial bits may happen and both the header and body will be corrupted (i.e. the receiver can neither receive the header nor the payload of the collided packet). Based on this observation, the authors propose that a receiver sends back a NAK if the MAC header is correctly received but the MAC body of the frame is wrong. Upon receiving the NAK, the sender concludes that a link error has occurred. If neither ACK nor NAK arrives at the sender, collision is assumed to have occurred. It is clear that the algorithm fails if a sent NAK frame does not arrive at the sender for some reason or if STAs are not within the range of each other.

In [4, 5], collision detection has been used to improve rate adaptation algorithms. The authors assume that RTS/CTS is always signaled before data packets. Assuming negligible transmission error probability of an RTS frames, a loss after the exchange of RTS/CTS is attributed to channel errors since RTS/CTS reserve the medium for the next packet. In addition to the overhead imposed by the exchange of RTS/CTS, this differentiation mechanism may fail in the presence of hidden nodes across multiple Basic Service Sets (BSSs).

Recently, Sharvan et. al. [6] proposed a new measurement-based approach for discriminating packet collisions and losses due to bad channel conditions in 802.11 systems. Their approach is based on explicit sending back of complete frames in error along with the Received Signal Strength Indicator (RSSI) values to the sender. The authors rely on their observations indicated that data bits which follow the preamble is seldom found in error, due to receiver synchronization using the physical layer preamble. This includes source and destination MAC addresses. In the 802.11 standard, the RSSI is defined as a measure of the power level observed at the receiver antenna, measured during the PCLP (Physical Layer Convergence Protocol) of an arriving packet [9]. The intuition behind using RSSI is experimental observations that the RSSI of packets suffering from signal attenuations is usually lower than that of packets suffering from collisions. It has been observed that the RSSI of 98% of packets received in error was below -73dBm. Similarly, the authors observed that 98% of packets in error due to fading have a BER of 12% or less, while only 24% of packets in error due to collision have BERs of 12% or less. This means that about 75% of packets corrupted due to collisions have BER greater than 12%. The sender then uses the RSSI value (sent back from the receiver) and a BER value (computed at the as the ratio of incorrect bits in the packet sent back from the receiver) for the discrimination of packet loss. It employs some empirical rules to identify the cause of error assuming that the receiver was able at least to decode the MAC header of the frame in error. Particularly, if any metric (RSSI, or computed BER) indicates a collision, the algorithm outputs collision as result. The main drawback of this approach is that the RSSI value can not capture collisions unless the PLCPs of colliding packets overlap. This is due to the fact that the RSSI is measured during the reception of PLCP. Another drawback is the dependency of the decision rule on a fixed cut-off RSSI value (-73dBm), where the used value may not apply to any deployment scenario in general. The associated overhead with this approach is rather high due to packets relay-back between senders and receivers.

Another recent algorithm has been proposed by Malone et al. in [7]. The proposed algorithm differentiates between two types of packet losses. The first is losses due to intra-BSS collisions and the second is losses due to weak signals or hidden node. The algorithm is executed at the sender side utilizing MAC sensing statistics of busy and idle periods. The collision probability is estimated as the proportion of busy slots due to transmissions by other stations(i.e # of Busy Slots/(# of Idle Slots + # of Busy Slots)). A busy slot is defined as the event that a node has detected the medium as busy due to transmissions of one or more other nodes, and has suspended its backoff until NAV, DIFS/EIFS indicate that the backoff can resume. An idle slot is defined as the event that a node has seen the medium as idle and, if backoff is in progress, has decremented its backoff counter. The probability of success is computed as the ratio of successfull transmits to attempted transmits. Knowing the probability of successfull transmission and the probability of collisions, the authors compute the probability of channel error. The authors extend their work in [8] to discriminate between losses due to noise/weak signal and hidden node (interference). They do that by sending a packet as a sequence of fragments. The authors assume that the first fragment is the only one subject to collisions while subsequent fragments are subject to noise. One concern about this discrimination method is that not all 802.11 packets are normally fragmented. Also, in a wireless environment, sensing results at the sender side is usually not enough to infer collisions at the receiver. Moreover, excessive fragmentation introduces additional overhead.

1.2 Report Structure

The rest of this report is organized as follow: Chapter two details our packet loss discrimination algorithm. Chapter three evaluates the performance of proposed approach via detailed simulation experiments and chapter four concludes this report.

Chapter 2

Packet Loss Discrimination

2.1 System Model

We consider an ESS 802.11 WLAN (see figure 2.1) composed of $\boldsymbol{N}$ APs and $\boldsymbol{M}$ stations (STAs). All APs are connected to a single distribution system (DS). APs provide communication services to the $\boldsymbol{M}$ STAs that reside within their coverage area. APs are assumed to operate on non-overlapping channels. Some APs might be assigned the same channel. At any time instant, a STA is associated to a single AP. The coverage areas of APs are assumed to overlap.

2.2 Problem Statement

The question is how could we enable 802.11 WLAN nodes to accurately diagnose the cause of packet loss. Particularly, how could we differentiate if a packet has been corrupted as a result of collision or channel errors.

2.3 Receiver-Oriented Loss Discrimination

In 802.11 there are two types of collisions. The first type occurs when a new packet arrives while the radio of the receiving node is already synchronized and receiving a packet (may be during header reception). If the stronger packet arrives while the receiver radio is synchronized and receiving a packet of weaker signal, the new packet will corrupt the tail of the first packet, thereby leading to corruption of both packets. However, if the first packet is strong enough relative to the new packet arrived (Capture works), the first (stronger) packet will be correctly received, i.e. the interfering new packet will not impact the first stronger packet. We call this interference *tolerated interference.*

As an 802.11 standard feature, the RSSI value is defined in the standard as a measure of

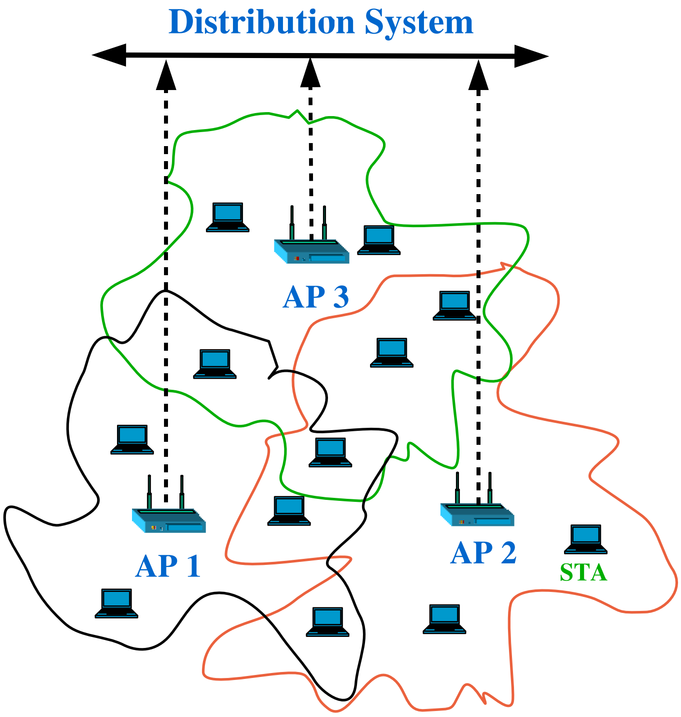

Figure 2.1: Network Model

the power level observed at the receiver antenna, measured during the PCLP (Physical Layer Convergence Protocol) of an arriving packet [9]. Note that the specific details of implementation for acquiring this value (e.g. # of samples, a method to compute a final value from numerous samples) is not explicitly provided by the standard and left to manufactureres.

In [6], the authors have experimentally observed a relation between the RSSI value of received packets and interference. Particularly, it has been shown that the RSSI value at a receiver increases when an interfering node is active. However, from the definition of RSSI, it turns out that an interfering signal contributes to the RSSI of a packet only if it arrives during the reception of the PLCP of this packet, i.e the RSSI value is the sum of the desired signal and interfering signal(s) only if interfering signal(s) arrive during the reception of the PLCP as illustrated in figure 2.2. Although the two packets in figure 2.2(a) overlap, the signal power of the new packet will not influence the RSSI of frame F1. This occurs when the transmitting nodes of the two frames are hidden from each other. In contrast, frame F2 in figure 2.2(b) will increase the RSSI of frame F1 as it arrives during the reception of PLCP of frame F1.

As the RSSI value does not always provide complete information about potential inter-

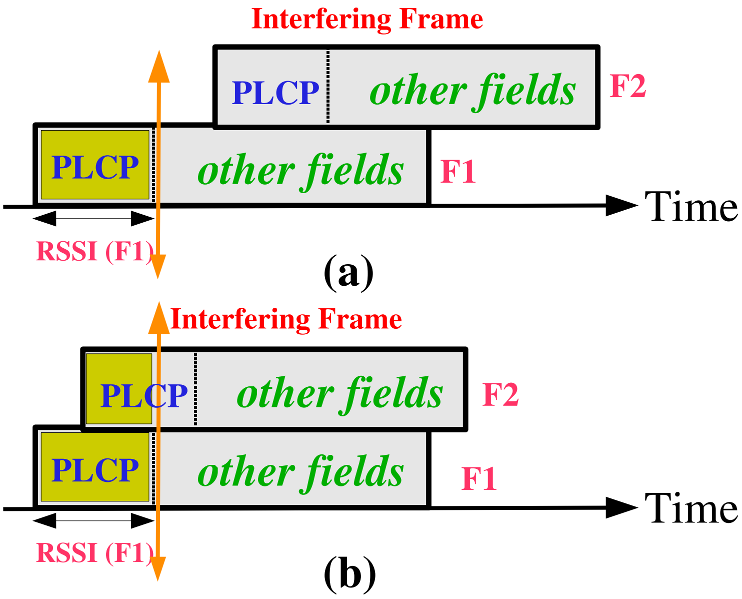

Figure 2.2: Impact of Interfering Signal on RSSI

fering signal(s) during a reception of a packet, we would like to follow the above observations while suggesting the usage of the Received Channel Power Indicator (RCPI) [10] as a measure of the channel power (signal, noise, and interference) of a received IEEE 802.11 frame. Unlike RSSI, which is measured during PLCP reception, RCPI shall be measured over the entire frame on the channel and at the antenna connector used to receive that frame [10]. Again, the standard does not explicitly specify the details for acquiring the RCPI value and leaves that to manufacturers. Nonetheless, we assume hereafter that the RCPI value is an average power level measured over the entire frame.

In further considerations, we assume that the receiver is able to correctly decode the MAC header of a packet that arrives first. Observations in [6] indicated that this assumption is reasonable due to receiver synchronization using the physical layer preamble. Further we assume that the RCPI values of both correct and corrupted packets are available at the MAC layer.

Generally, the received instantaneous power of packet k at node i, $Px_{ik}(t)$ can be expressed as:

$$Px_{ik}(t) = S_{ik}(t) + I_{ik}(t) + n_{ik}(t) \tag{2.1}$$

where $S_{ik}(t)$ is the instantaneous received power of the actual/desired signal of packet k at node i, $I_{ik}(t)$ is the instantaneous power received from one or more interferers at node i during the reception of packet k, and $n_{ik}(t)$ is the instantaneous thermal noise power.

Assuming that $n_{ik}(t)$ is constant and an $RCPI_{ik}$ value is obtained by sampling and averaging the received instantaneous power $Px_{ik}(t)$ at node i over the whole length of packet k, then we have:

$$RCPI_{ik} = S_{ik} + I_{ik} + n_{ik} \tag{2.2}$$

where S_{ik}, I_{ik} , and n_{ik} are the contributions of the desired signal, interference signals, and the thermal noise to the $RCPI_{ik}$ value, respectively.

The probability that node i receives packet k incorrectly is then given as:

$$P_{ik}[Failure] = P\left[\frac{S_{ik}}{I_{ik} + n_{ik}} < \delta\right] \tag{2.3}$$

where δ is the minimum signal to interference and noise ratio (SINR) for a correct reception of a packet.

From equation 2.3, it is clear that:

- It is possible for the receiver of node i to correctly decode a packet k even in the presence of some interference I_{ik} (Capture effect).
- If I_{ik} exceeds some threshold I_{th}, the received packet will contain errors. **An increase in I_{ik} will result in an increase in the corresponding $RCPI_{ik}$, which value depends on the duration and strength of I_{ik}.**
- **If I_{ik} is below or equal I_{th}, then packet failure has to be attributed to a decrease in S_{ik} (i.e weak signal).**

A receiver discriminates between packet losses as follows:

Algorithm 1 Receiver-Oriented Loss Discrimination Algorithm

```
$Q_i(x)$ = The x % quantile RCPI value of a training sample of correctly received
    packets at node $i$.
$RCPI_{ik}$ = RCPI of packet $k$ received by node $i$.
for every packet $k$ received in error
        if ($RCPI_{ik} > Q_i(x)$)
                Cause = Collision.
        else
                Cause = Channel error.
```

Due the fact that a packet may still be captured and successfully received in the presence of some interference (i.e tolerated interference), the algorithm uses a quantile

RCPI value $Q_i(x)$ of correctly received packets as a threshold with which the $RCPI_{ik}$ of a corrupted received packet is compared for the sake of discrimination. Specifically, $Q_i(x)$ is the RCPI value below which fall $x\%$ of RCPI values of correctly received packets at node i. In our evaluations, $Q_i(x) = 70\%$ was found to achieve a good estimation accuracy.

Obviously, using these statistics (power of correct and corrupted packets), it is also possible to estimate the amount of untolerated interference at the receiver of node i, i.e. the amount of interference from neighboring nodes that really causes packet loss at node i. This can be estimated over a period of time T as follows:

$$\hat{I}_i = RCPIFailed_i - Q_i(x) \tag{2.4}$$

where $RCPIFailed_i$ is the average RCPI value of incorrectly received packets due to interference at node i during T. The main advantage of this estimation is that it can be performed on-the-fly. Nodes are not required to cease their transmitters and sense the medium for potential interferers.

Chapter 3

Performance Evaluation

In this chapter we assess the performance of our proposed approach for diagnosing the cause of packet loss in 802.11 WLANs. We have conducted detailed simulation experiments using the NCTUns simulation package [13]. The MAC protocol of NCTUns is ported from NS-2 network simulator which indeed implements the complete IEEE 802.11 standard MAC protocol to accurately model the contention of users for the wireless channel.

3.1 Performance Evaluation Strategy

For the evaluation of our algorithm, we look at the estimated collisions and the actual/true collisions. Specifically, during each second, we sum the number of collisions as estimated by our algorithm and the total number of actual collisions (number of times the receive module of the simulator at the receiving node decides a collision to have occurred and drops the packet under reception as a result of this decision). We compare the two values.

In order to incorporate different wireless conditions and assess the ability of the algorithm to capture the dynamical changes: First, we use different traffic patterns. Second, we increase the collision rate in the network by tuning the maximum contention window CW_{max}. Third, we increase the BER by randomly decreasing the SNR (per packet). We compare the performance of our algorithm with the ones proposed recently in [6] and [7], which we also have implemented in our simulation tools.

3.2 Simulation Scenario

3.2.1 Simulation Setup

The scenario is comprised of 4 BSSs and 40 STAs. The four APs are configured over the same channel. APs and STAs implement the 802.11b technology and use the DCF MAC protocol. The STAs are randomly distributed in the coverage area of the APs.

At the physical layer, we have used a two ray ground reflection path loss model with the received power P_{rx} given as:

$$P_{rx} = \frac{P_{tx} G_{tx} G_{rx} h_{tx} h_{rx}}{d^2} \tag{3.1}$$

where P_{tx} is the transmit power (in mW), G_{tx},G_{rx} denote the transmitter and receiver antenna gains respectively, h_{tx} and h_{rx} are the antenna heights of transmitter and receiver, and d is the distance between them. The received power is further attenuated by Rayleigh fading. A Rayleigh fading model provided by the NCTUns simulator is used. It takes as parameters the received power P_{rx} and a fading variance set to its default value of 10dB. The received power level of a packet (with respect to both path loss and fading attenuations) is computed at the beginning of the packet and assumed to be constant over the whole packet length. It is passed to an error module provided by the simulator along with packet length and modulation type. This module determines whether a received packet is correct or corrupted due to fading and path loss attenuation.

The aggregated combined power level (our RCPI) of two packets if one arrives while the other is being received is computed at the receiver as follows:

$$P_{total} = \frac{P_f T_f + P_n T_{overlapp}}{T_f} \tag{3.2}$$

where P_f is the received power level of the first packet, T_f is the duration time of the first packet, P_n is the received power level of the new incoming packet and $T_{overlapp}$ is the time it overlaps with the first packet.

A sender selects a physical transmission rate based on the distance d to the receiver and the rate remains fixed during the simulation time (i.e no rate adaptation is used). Table 3.1 lists the values of the parameters as used in simulations.

Packet capturing is modeled in the simulator as follows: While simulating packet reception time (a function of physical rate, packet size), if a new packet arrives and the power level of the first packet is greater than the power level of the new packet by at least the Capture Threshold (used to be 10dB), then the first packet is assumed to be received and the new packet is ignored.

Parameter	**Value**	**Parameter**	**Value**
PLCP header T_H	48 μs	T_{SIFS}	10 μs
PLCP preamble T_P	144 μs	T_{DIFS}	50 μs
Cell overlap	20 %	T_{Slot}	20 μs
Fading Variance	10 dB	$W_{\min}$	31
APs/STAs Tx Power	100 mW	$W_{\max}$	1023
d $\leq$ 40	11Mbps	40 < d $\leq$ 80	5.5Mbps
80 < d $\leq$ 120	2Mbps	d > 120	1Mbps

Table 3.1: Constant Parameters

3.2.2 Experiment Description

All STAs download UDP traffic from a server via their APs. Traffic was generated with the stg traffic tools that come with the NCTUns simulator. The profile is provided in tables 3.2. APs transmit data packets to the STAs. For every received packet, if the MAC at a receiving node has decided to drop a packet, a STA uses the proposed algorithm to determine the cause of packet drop. Whenever the algorithm guesses a collision as the reason of a dropped packet, a corresponding counter is incremented. Another counter is incremented whenever the receive module of simulator decides a collision. The values of both counters are logged every second. The RCPI quantile point $Q_i(x)$ was selected by each node i using a 70% (i.e. x=70) quantile of correctly received packets.

Simulation Time	Offered Load (Pkt/s)	Packet Size (B)
0 - 120	100	Randomly between 200 and 1500

Table 3.2: Traffic Profile

3.3 Evaluation Results

3.3.1 Diagnosing Packet Loss

Figures 3.1 plots the actual number of collisions and that estimated by our algorithm and the algorithms of Rayanchu et. al [6] and Malone et.al [7] with the traffic profile of table 3.2. The figure shows that our proposed approach outperforms the other two approaches. The difference between the actual/true number of collisions and the one estimated by our algorithm observed at the beginning of the simulation time is due to the algorithm learning phase (i.e. time until enough number of correctly received packets is used for the computation of a good quantile point, Quantile Learning Phase).

As the approach of [6] does not capture the interference of packets that arrive after the preamble of the packet being received (the power of those packets do not contribute to the RSSI value of the packet being received), it was found to estimate less number of collisions.

Now, we increase the collision probability by decreasing the maximum size of the contention window CW_{max}. The results are plotted in figure 3.2. The figure shows that our approach better tracks the increased number of collisions due to the decrease in the size of maximum contention window. Although the approaches of Rayanchu and Malone show an increase in estimated collisions as the CW_{max} decreases, their estimations are not accurate enough specially for small CW_{max}.

Finlay, we increase the BER by decreasing the SNR (i.e. in fact we want to increase the number of dropped packets due to weak signal). We plot the results in figure 3.3. Since the approach of Rayanchu bases the diagnosis on a fixed cut-off value of the RSSI, collision estimations with this approach are not close to the actual number of collisions. In contrast, our approach which learns from the history of correctly received packets, the fluctuations in the received signal power do not impact its ability of discriminating the cause of errors. It was found to overperform the other two approaches in this scenario.

3.3.2 Interference Estimation

We have used equation 2.4 for estimating the interference. Every second, we compare the total amount of estimated interference with the total number of actual collisions. Since both parameters have different units, we normalized both values by the maximum of each and plot the curves together in figure 3.4. The figure shows a good correlation between the two curves, i.e the estimated interference tracks the actual collisions in the network.

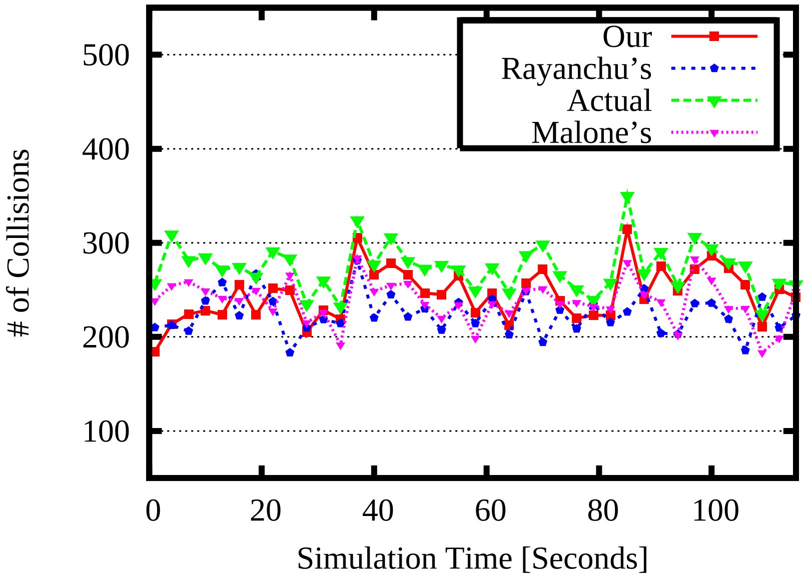

Figure 3.1: Actual and Estimated number of collisions.

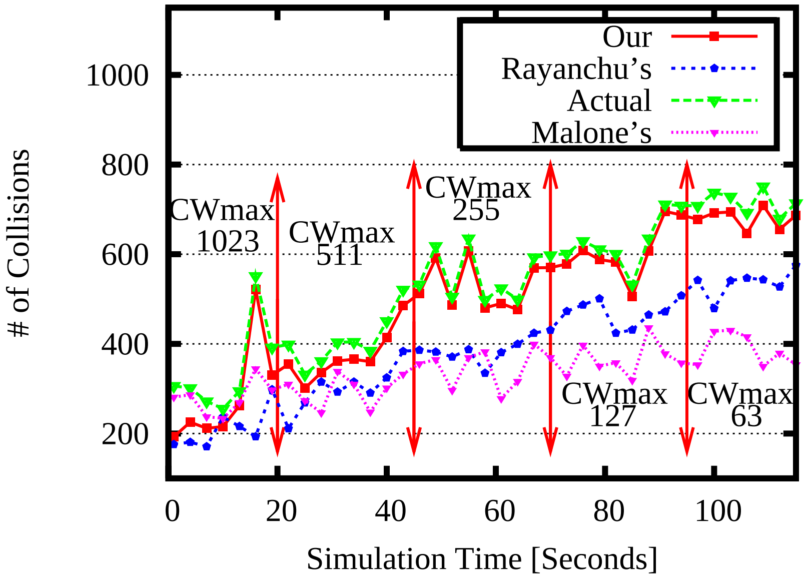

Figure 3.2: Actual and Estimated number of collisions for different CW_{max} values.

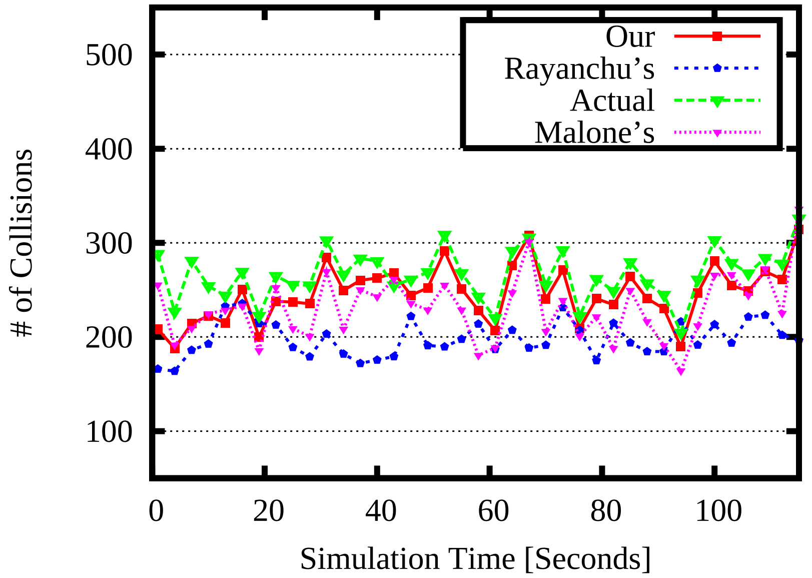

Figure 3.3: Actual and Estimated number of collisions with random per packet decrease of SNR.

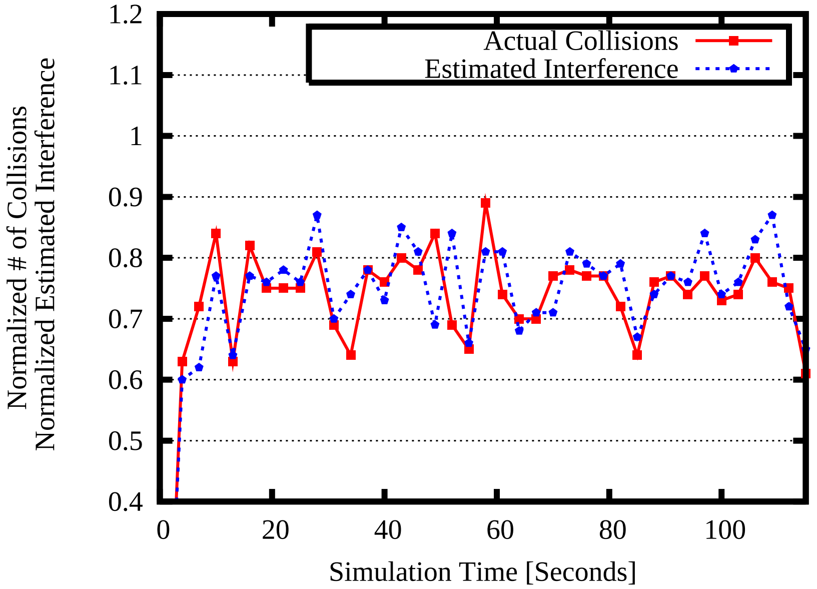

Figure 3.4: Comparison between Actual number of collisions and amount of Interference estimated by equation 2.4.

Chapter 4

Conclusions

This report proposes a method for diagnosing the cause of packet loss in 802.11 WLAN. It differentiates between losses due to collisions or weak signals. Simulation studies has shown that the proposed approach has a great potential in improving the accuracy of estimation.

Bibliography

[1] K. Whitehouse, A.Woo, F. Jiang, J. Polastre, and D Culler. Exploiting the capture effect for collision detection and recovery. *In Proceedings of EmNetS11*, 2005

[2] Ji-Hoon Yun and Seung-Woo Seo. Collision detection based on RF energy duration in ieee 802.11 wireless lan. *In Proceedings of Comsware*, 2006

[3] Qixiang Pang, Soung C. Liew, and Victor C. M. Leung. Design of an Effective Loss-Distinguishable MAC Protocol for 802.11 WLAN. *IEEE COMMUNICATIONS LETTERS*, 2006

[4] S. Wong, S. Lu, H. Yang, and V. Bhargavan. Robust rate adaptation for 802.11 wireless networks. *In Proceedings of ACM Mobicom*, 2006

[5] J. Kim. Cara: Collision-aware rate adaptation for ieee 802.11 wlans. *In Proceedings of INFOCOM06*, 2006

[6] S. Rayanchu, A. Mishra, D. Agrawal, S. Saha, and S. Banerjee. Diagnosing Wireless Packet Losses in 802.11: Separating Collision from Weak Signal. *In Proceedings of IEEE INFOCOM08*, April, 2008.

[7] D. Malone, P. Clifford, and D. J. Leith. MAC layer channel quality measurement in 802.11. *IEEE COMMUNICATIONS LETTERS*, February, 2007.

[8] Domenico Giustiniano, David Malone, Douglas J. Leith and Konstantina Papagiannaki. Experimental Assessment of 802.11 MAC Layer Channel Estimators. *IEEE COMMUNICATIONS LETTERS*, December, 2007.

[9] IEEE Std. 802.11-2007, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std. 802.11, 2007 edition.

[10] IEEE Std. 802.11k-2008, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 7: Radio Resource Measurement , IEEE Std. 802.11k, February, 2008.

[11] Chi Pan Chan, Soung Chang Liew, and An Chan. Many-to-One Throughput Capacity of IEEE 802.11 Multi-hop Wireless Networks. *IEEE TRANSACTIONS ON MOBILE COMPUTING*, 2007.

[12] Li Bin Jiang and Soung Chang Liew. Improving Throughput and Fairness by Reducing Exposed and Hidden Nodes in 802.11 Networks. *IEEE TRANSACTIONS ON MOBILE COMPUTING*, vol. 7, no. 1, January 2008.

[13] http://nsl.csie.nctu.edu.tw/nctuns.html.

[14] D. Chiu and R. Jain Analysis of the Increase and Decrease Algorithms for Congestion Avoidance in Computer Networks *Journal of Computer Networks and ISDN Systems*, vol. 17,Nr.1, pp. 1-14, June, 1989.