Background Traffic-Aware Rate Adaptation for IEEE 802.11: Implementation and Test-bed Experimental Results

Shao-Cheng Wang
shaochew@ufl.edu

Ahmed Helmy
helmy@ufl.edu

Department of CISE, University of Florida, Gainesville, FL., U.S.A.

IEEE 802.11-based devices employ rate adaptation algorithms to dynamically switch data rates to accommodate the fluctuating wireless channel conditions. In this paper, we design and implement a new Background traffic aware rate adaptation algorithm (BEWARE) in Linux-based device driver. The proposed rate adaptation algorithm makes rate decisions by on-the-fly estimating the expected packet transmission time which captures both current wireless channel and background traffic conditions. Our test-bed experiment results show that BEWARE outperforms other rate adaptation algorithms by up to 150% in various indoor and outdoor scenarios.

I. Introduction

With the multiple transmission data rates specified in the IEEE 802.11 standards, IEEE 802.11-based stations implement rate adaptation algorithm (RAA) to dynamically select the best data rate that yields the highest performance in the given wireless channel conditions. The effectiveness of many RAAs [1]-[5] has been extensively evaluated under various wireless channel conditions, when there is only one station in the network. Furthermore, in multiple-user environment, several studies [6][7] reported that the performance of some types of RAAs, e.g. Automatic Rate Fallback (ARF)[1], degrades drastically because the RAA mistakenly lowers its data rate when the consecutive frame losses are caused by collision losses not by wireless losses. The studies in [6] and [7] further propose to use RTS/CTS to filter out collision losses from rate decision process to improve performance in multiple-user environment.

While these proposals provide significant improvements compared to RAAs without loss differentiation capability, our earlier study [8] observed that existing RTS-based loss differentiation schemes do not perform well in all background traffic scenarios. The fundamental problem is that background traffic from other contending stations changes the throughput ranking of the operating data rates. Therefore, we designed a new Background traffic aware Rate Adaptation Algorithm (BEWARE) that explicitly addresses the mixed effects from wireless and collision losses. We found BEWARE's superior performance over other RAAs for up to 250% under various simulated background traffic and wireless scenarios. In this paper, we describe our implementation efforts including the challenges and different trade-offs we face when we deal with the real hardware. We also conduct a series of systematic experiments to evaluate and compare BEWARE's performance in real-world scenarios.

II. BEWARE Design

The center part to the BEWARE design is to estimate the expected packet transmission time of each data rate that attributes the combined costs of wireless channel errors and background traffic contentions. We gather the occurring probability and duration of the busy/idle medium events and failed/successful transmission events happen in MAC layer backoff procedure as illustrated in Fig. 1. We then use a previously validated model to calculate the expected packet transmission time accordingly. The rate selection engine then uses this metric to find the data rate that yields the highest throughput in the given wireless channel and background traffic condition.

While we try to implement this design on open source MADWIFI [9] driver based on Atheros chipsets, one of the challenges we face is in obtaining some of the parameters needed for the algorithm. Particularly, MADWIFI leaves the control and feedback of backoff procedure details in the firmware, so it is not possible for us to control or even know

This work was supported in part by NSF.

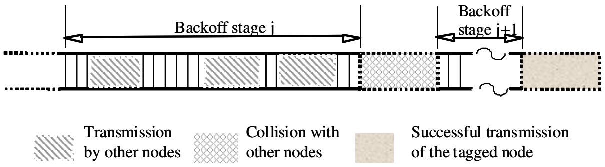

Backoff stage j
Backoff stage j+1
Transmission by other nodes
Collision with other nodes
Successful transmission of the tagged node

Figure 1. Packet transmission and collision events during IEEE 802.11 MAC backoff

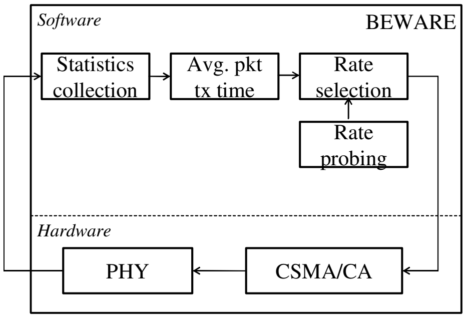


Figure 2. Structure of BEWARE design

exactly how many and how long backoff events (busy or idle) happen in a particular backoff stage. Therefore, we turn to other parameters that can represent the aggregated effects on the length of individual backoff stages. We further revise the model so that it not only takes the new parameters, but also reduces the computation complexity in real-world hardware.

In the following, we describe the functions and implementations of different BEWARE modules as shown in Fig. 2.

II.A. Statistics Collection/Processing

After the packet transmission completes, we keep track of the length of each non-retransmitting successful transmission. We then subtract it by the actual packet transmission time (T_{succ}) so that we can log the actual 1st backoff stage duration ($T_{1st\text{-}stage}$). We also keep track of failed packet transmission time (T_{fail}) Such records are further processed with exponentially weighted moving average (EWMA) to smooth out the biases to the sudden changes in current wireless channel and collision conditions. This module also collects frame error probability, P_{fail}, by counting the ratio of failed packet transmission attempts and total packet transmission attempts.

II.B. Expected Packet Transmission Time Calculation

Once we have the parameters from the previous module, we can derive the overall backoff duration by the cumulative effects from the successive backoff stages:

$$T_{avg} = \sum_{n=1}^{m}[(2^{(n-1)} * T_{1st-stage} + (n-1)T_{fail} + T_{succ}) * P_{fail}^{(n-1)} * (1 - P_{fail})]. \tag{1}$$

We can see that, in this equation, we estimate the length of the *n-th* backoff stages other than the 1st backoff stage as $2^{(n-1)}$ times of $T_{1st\text{-}stage}$, according to the 802.11 DCF binary backoff operation. The overall backoff procedure duration is then estimated by the combinations of corresponding probabilities that the transmission succeed at the *n-th* backoff stage. Note that T_{fail} and T_{succ} in Eq. 1 represent the length of failed and successful transmissions, which are already known by the transmitting station.

II.C. Rate Probing

Periodically, BEWARE sends packets at a data rate other than the current one to update the expected transmission time of other data rates. In order to avoid the common rate-probing pitfalls reported in [3], BEWARE limits the frequency of packet probing to a fraction (~5%) of the total transmission time. In addition, BEWARE does not probe data rates that suffer from excessive failures for most recent packet attempts.

II.D. Rate Selection Decisions

The rate selection module constantly compares the expected packet transmission time of current data rate and that of others, and decides to change operating data rate whenever it finds a data rate yields the shorter transmission time (and thus highest throughput) beyond a certain threshold. BEWARE also implements a short-term frame loss reaction mechanism in case wireless channel conditions change too rapidly. That is, the rate selection module forces data rate to decrease one level when the packets exhaust all retries for three times consecutively.

III. Experimental Results

We conduct a series of systematic experiments to evaluate and compare BEWARE's performance in real-world scenarios, including indoor and outdoor environments, different number of background traffic stations and traffic patterns. The objective of the experiments is to not only help us understand BEWARE's performance in different scenarios, but also expose BEWARE in the dynamics of real-world situations where simulations may not be able to capture.

III.A. Experiment Setup

Our experimental setup consists of one Cisco AP-1230 802.11a/b/g access point and laptops equipped with Proxim Orinoco Gold 802.11a/b/g combo PCMCIA cards. The laptops run Ubuntu Linux with kernel version 2.6.24.5 and modified MADWIFI driver based on version 0.9.4.

We conduct both indoor and outdoor experiments in the University of Florida campus. The indoor environment is an office/lab setting with concrete walls separating the rooms and many metal cubical partitions within the lab. For outdoor experiments, we choose an open garden area between two buildings on campus. We choose one Line-of-Sight (LOS) location in the open area with direct distance about 28m and one non-LOS (NLOS) location at the side that is blocked by two building poles and the direct distance is about 35m away from the AP.

We conduct each experiment with multiple runs, and present the results that are averaged over all runs. In order to provide fair comparisons among different RAAs, we choose channel 40 of 802.11a and conduct the experiments during late evenings or weekends to minimize impacts from external factors, such as people walking around.

We compare the performance of BEWARE with ARF and ARF-RTS. We know from previous studies that, while ARF suffers from "rate-poisoning" problem when there is some background traffic in the network, ARF-RTS is the solution proposed by later studies [6][7] that has been widely accepted by the community for its ability in helping RAAs deal with background traffic. However, we have shown in our previous study [8] that, using RTS to differentiate the losses between wireless losses and collisions can sometimes be misleading and resulting in performance degradations. We believe that comparing BEWARE's performance with these algorithms provides a good overall picture for understanding how different rate adaptation algorithms perform in real-world scenarios with different wireless loss and background traffic environments.

III.B. Indoor Performance

The layout of indoor experiments is shown in Fig. 3. We place up to 3 background traffic stations next to the AP. Each background traffic station is configured to transmit continuous UDP packets with payload size 500 bytes long, and uses the lowest data rate to ensure that the background traffic is detectable at the farthest range of the AP. We then place one RAA-enabled station in the three different indoor locations to investigate the RAAs' effectiveness under mixed wireless loss and contention conditions. Location #1 is within 1m to the AP so that we can examine the RAAs' performance when the wireless condition is almost perfect. Location #2 is about 12m away from the AP, with average SINR 26 to 24 db, and obstructed by 2 concrete walls in the line-of-sigh from the AP location. Location #3 is further down with direct distance about 20m and is also obstructed with 2 concrete walls. The average SINR at this location is 16 to 18 db.

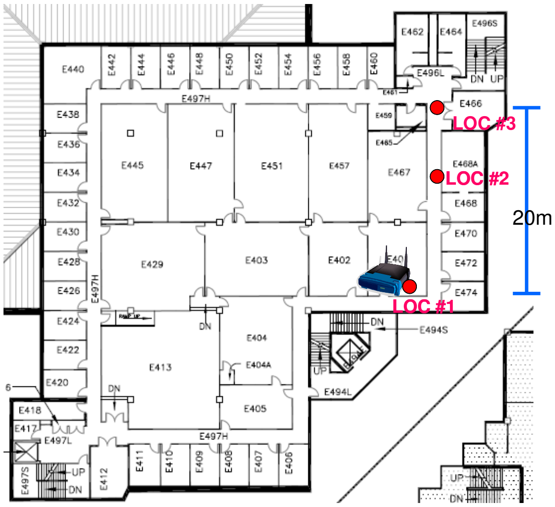


Figure 3 Indoor experiment layout

In Fig. 4, we plot the performance of BEWARE normalized by either ARF-RTS or ARF, at three different locations and with different number of background traffic stations. The two thin solid lines show that, at location #1 where RAA-enabled station is just next to the AP, BEWARE does not provide significant performance improvement against ARF-RTS & ARF. On the other hand, when we move the RAA-enabled station to location #2 (dotted lines) and location #3 (thick solid lines), we can see from Fig. 4 that BEWARE consistently outperforms ARF-RTS, ARF, in all background traffic scenarios. At location #3, BEWARE's performance improvements over ARF-RTS are more significant, when compared with the performance at location. #2. In addition, BEWARE's performance improvement increases with more background traffic in the network.

III.C. Outdoor Performance

In outdoor experiments, we place 2 background traffic stations next to the AP and one RAA-enabled station in the LOS and NLOS location, as described in Sec. III-A. We compare the performance of BEWARE, ARF, and ARF-RTS at these two

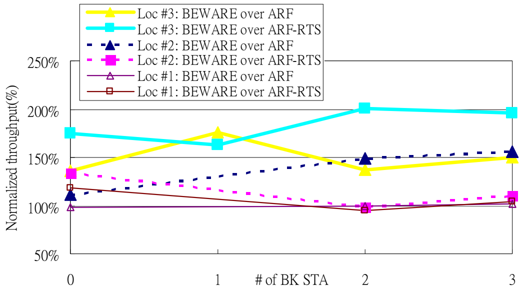
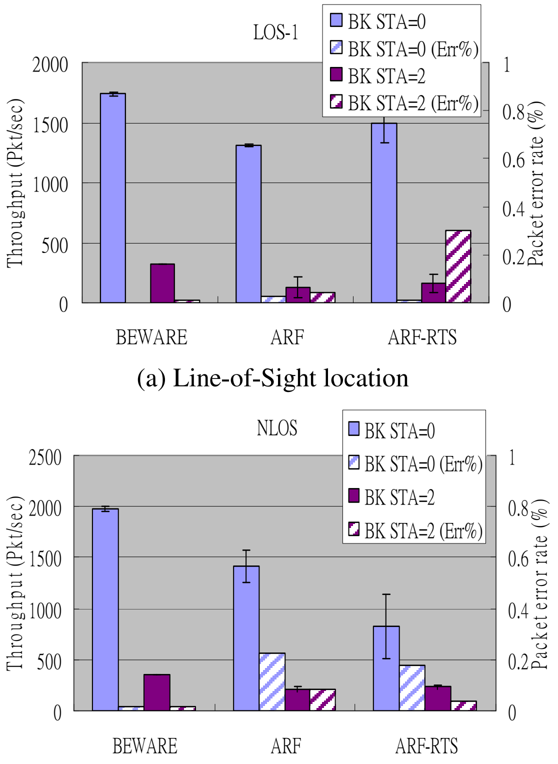


Figure 4. Normalized throughput for BEWARE over ARF and BEWARE over ARF-RTS in indoor environment with number of background traffic stations.



(a) Line-of-Sight location

(b) Non-Line-of-Sight location

Figure 5. Performance of BEWARE, ARF, and ARF-RTS at different locations in the outdoor environment.

locations, with and without both background traffic stations turned on.

As we can see from Fig. 5, BEWARE consistently outperforms ARF and ARF-RTS, in both locations and in both background traffic levels. BEWARE's performance advantage is more significant when there are more background traffic in the network. In addition, BEWARE's packet loss rate is always < 2% in all scenarios evaluated. On the other hand, in this outdoor experiment, both ARF and ARF-RTS suffer from substantial packet loss rate, up to 18% in no background traffic scenario and up to 35% in 2 background traffic station scenario.

IV. Conclusion

In this paper, we design and implement a novel background traffic-aware rate adaptation, BEWARE, that uses transmission information available to real-world hardware driver to estimate the effectiveness of the data rates in given wireless and contention conditions. We show that BEWARE outperforms other RAAs up to 150% under various wireless loss and contention conditions, and the observations are consistent with the simulation findings we report in [8].

References

[1] A. Kamerman, L. Monteban, "WaveLAN-II: A High-Performance Wireless LAN for the Unlicensed Band," Bell Labs Technical Journal, pp. 118–133, Summer '97.

[2] M. Lacage, M. H. Manshaei, T. Turletti, "IEEE 802.11 rate adaptation: a practical approach," ACM MSWiM '04

[3] S. Wong, H. Yang, S. Lu, V. Bharghavan, "Robust Rate Adap-tation in 802.11 Wireless Networks," ACM MOBICOM '06.

[4] J. Bicket. Bit-rate Selection in Wireless Networks. MIT Master's Thesis, '05.

[5] Gavin Holland, Nitin Vaidya, and Paramvir Bahl, "A Rate-Adaptive MAC Protocol for Multi-Hop Wireless Networks," ACM MobiCom '01

[6] J.S. Kim, S.K. Kim, S.H. Choi, D. Qiao, "CARA: collision-aware rate adaptation for IEEE 802.11 WLANs," IEEE INFOCOM '06.

[7] Q. Pang, V.C.M. Leung, and S.C. Liew, "A Rate Adaptation Algorithm for IEEE 802.11 WLANs Based on MAC-Layer Loss Differentiation," IEEE BRAODNETS '05.

[8] S. Wang and A. Helmy, "BEWARE: Background trafffic-aware rate adaptation algorithm," IEEE WoWMoM '08.

[9] MADWIFI, http://sourceforge.net/projects/madwifi/