Dynamic Backoff for IEEE 802.15.4 Beaconless Networks

D Rohm, M Goyal
University of Wisconsin Milwaukee
Milwaukee, WI 53201 USA
{dmgibson,mukul}@uwm.edu

1. Introduction

IEEE 802.15.4 [1] is a leading standard for low power and low data rate wireless sensor networks. IEEE 802.15.4 based wireless technology offers lower installation and maintenance costs and hence is increasingly replacing the existing wired technologies in applications such as building automation, home/environment monitoring, industrial control and smart metering. Deployed/future IEEE 802.15.4 based networks may range from few nodes in a room to several thousand nodes spread sporadically or densely over a large geographical area [3]. The nodes may generate traffic infrequently or at a steady rate or in occasional bursts. The overall traffic load on an IEEE 802.15.4 network may be fairly static or vary unpredictably over a wide range. Clearly, proper configuration is important for successful operation of an IEEE 802.15.4 network in given operating conditions.

In this paper, we examine the impact of *macMinBE/ macMaxBE* and *macMaxCSMABackoffs* parameters on the performance of *beaconless* operation of IEEE 802.15.4 MAC layer under different traffic loads. The performance is measured in terms of the packet loss probability and the packet latency. We also develop a dynamic scheme to automatically configure the macMinBE, macMaxBE and macMaxCSMABackoffs parameters. Our dynamic scheme estimates the traffic load on the network through examination of packet loss rates as observed at a particular node. Based on the perceived network traffic load, maxMinBE, macMaxBE, and maxMaxCSMABackoffs are modified. We present data that shows how this dynamic algorithm outperforms the default standard configuration.

The rest of the paper is organized as follows. Section 2 provides an overview of the packet transmission process in beaconless IEEE 802.15.4 MAC operation as well as describes different *collision* scenarios. Section 3 describes the simulation setup as well as the network performance metrics used for this study. Sections 4 and 5 present simulation results analyzing the impact of *macMinBE/macMaxBE* and *macMaxCSMABackofffs* parameters respectively and make recommendations regarding suitable values for these parameters under different traffic loads. Section 6 presents a dynamic backoff algorithm and simulation results for the new algorithm. Section 7 presents a brief survey of previous work on configuring IEEE 802.15.4 networks. Finally, Section 8 concludes the paper.

2. Packet Transmission in Beaconless IEEE 802.15.4 MAC Operation: CSMA/CA and Retransmissions

Beaconless IEEE 802.15.4 uses unslotted CSMA/CA. A transmission attempt begins with a CSMA wait for a random number of *backoff periods* between 0 and $2^{BE} - 1$, where BE can have a value between *macMinBE* and *macMaxBE* (by default 3 and 5 respectively). A backoff period is the time required to transmit 20 *symbols*, where a symbol is equivalent to 4 bits, on a 250 Kbps channel. Once the CSMA wait is over, the node determines if the channel is available for transmission. This *clear channel assessment* (CCA) is performed over a time duration of 8 symbols. If the CCA fails (i.e. the channel is found to be busy), the node increments *BE* (up to *macMaxBE*), repeats the CSMA wait and the CCA. If the CCA fails even after *macMaxCSMABackoffs* (by default 4) re-attempts, a *channel access failure* (CAF) is declared and no further attempt is made to send the packet. If the CCA succeeds, the node performs an RX-to-TX turnaround[1] and transmits the packet.

The packet transmission may get involved in a *collision*. In the next section, we describe different scenarios that result in a collision in beaconless IEEE 802.15.4 networks. In the absence of a collision, the receiver node receives the packet and may optionally send an acknowledgement (ACK) back to the source node. Note that the CSMA/CA process is not repeated for the sending of an ACK. The receiving node simply performs an RX-to-TX turnaround of

[1] The IEEE 802.15.4 nodes are typically *half-duplex* in nature, i.e. they can not perform both the *transmit* (TX) and *receive* (RX) operations at the same time. The *RX-to-TX* or *TX-to-RX* turnaround time is required to be less than 12 symbols [1].

its radio (again up to 12 symbols) and immediately sends the ACK. As described in the next section, an ACK may also be involved in a collision and thus get lost. The result of an ACK collision is the same as that of a packet collision. If an ACK is required, the source node reattempts to send the packet after waiting for *macAckWaitDuration* symbols (54 symbols for 2.4 GHz PHY operation) after finishing the packet transmission. A failure is declared if no ACK is received even after *macMaxFrameRetries* (by default 3) retransmissions. Such a failure is referred to as the *collision failure* in the subsequent discussion.

In beaconless IEEE 802.15.4 networks, collisions may take place either due to *hidden* nodes or due to non-negligible *RX-to-TX* (and *TX-to-RX*) turnaround times.

Hidden nodes: Some nodes in the network may not be in the hearing range of a node (say node *X*) and hence may transmit a packet at the same time as node *X*. Such nodes are called *hidden* nodes for node *X*. If node *Y*, the destination of node X's transmissions, can hear these hidden nodes, any concurrent transmission by a hidden node would cause node *Y* to drop node *X*'s transmission.

Collisions due to turnaround time: As mentioned earlier, an IEEE 802.15.4 node may take up to 12 symbols to turn around from *RX* mode to *TX* mode and vice-versa. This non-negligible turnaround time may cause packet collisions to take place in the following situations:

1) Suppose, a number of nodes, all in each other's hearing range, are competing for channel access and all of them are doing the CSMA wait at a certain time, hence the transmission channel is idle. Suppose, node *A* is the first node to wake up at time t. Node *A* performs a CCA till time $t + 8$, which is guaranteed to succeed, and then performs an *RX-to-TX* turnaround that finishes at time $t + 20$. The transmission channel would continue to be idle until time $t + 20$ when node *A* begins its packet transmission. Thus, if another node finishes its CSMA wait between times t and $t + 12$, its CCA would succeed and its subsequent packet transmission would collide with that of node *A*. Figure 1(a) refers to this 12 symbol duration as the *first collision window*. Note that the first collision window is actually equal to the *RX-to-TX* turnaround time.

2) A destination node (say *B*) needs to complete an *RX-to-TX* turnaround before it can send the acknowledgement for a packet. If another node finishes its CSMA wait during the first 4 symbols of this turnaround, its CCA would succeed and its packet transmission would collide with node *B*'s acknowledgement. Figure 1(b) refers to this 4 symbol duration as the *second collision window*. Clearly, the second collision window is the result of CCA duration being less than the *RX-to-TX* turnaround time.*To eliminate the second congestion window, we suggest increasing the CCA duration to a value larger than 12 symbol RX-to-TX turnaround time.* The same suggestion has been independently made in [5]. Note that the second collision window exists only if no collision takes place in the first collision window.

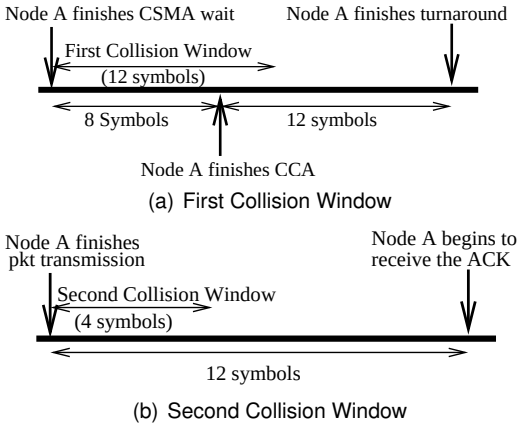


Figure 1. Collision Windows

3) A destination node would ignore a packet transmission if it begins before the destination has completed the *TX-to-RX* turnaround after sending the acknowledgement for the previous transmission. Even though this situation does not involve a collision, its impact is same as that of a collision.

3. Simulation Setup and Performance Metrics

The simulations make the following assumptions. The IEEE 802.15.4 MAC layer operates in the beaconless mode and all the packets require MAC level acknowledgement. The CCA is performed over 16 symbols to ensure that an ACK is never involved in a collision. The IEEE 802.15.4 PHY layer operates in 2.4GHz band and no transmission is lost due to signal attenuation/corruption over the channel. In this paper, we investigate the scenario where hidden nodes are not a significant problem. Hence, in our simulations, we ensure that all the nodes are in each other's radio range and thus there are no hidden nodes.[2] Each node generates traffic for the common coordinator as per a poisson distribution with average rate 5 packets/second. The simulations were performed with several different packet sizes although the results presented here were obtained using 133 byte long packets, which is the maximum allowed size for an IEEE 802.15.4 PHY frame including the 5 byte *synchronization header* and 1 byte *PHY header* [1].

The traffic load across simulations is varied by changing the number of nodes, excluding the coordinator, in the range $\{10, 12, \ldots, 22, 26, \ldots, 38, 40, 50, 60\}$. In each simulation, a certain number of nodes (between 10 and 60)

[2]Understanding how to counter the impact of hidden nodes by properly configuring IEEE 802.15.4 parameters is a part of our ongoing research.

send packets to their common coordinator. Since each node generates on average 5 packets/second, we simulate average traffic loads ranging from 50 to 300 packets/second. Note that with 133 byte packet size, a packet transmission takes channel time of 300 symbols (266 symbols for packet transmission + 12 symbols for receiver's RX-to-TX turnaround + 22 symbols for 11 byte acknowledgement transmission). Hence a 2.4 GHz channel, with channel capacity 250 Kbps (or 62500 symbols/second), can carry at most 208.33 ($= 62500/300$) packets per second. Thus, the simulations cover a wide range of traffic load scenarios from a lightly loaded network (50 packets/second) to significantly overloaded network (300 packets/second). Additionally, performance data was only collected after the network reached a steady state where association with the coordinator and route discoveries have already been completed.

In order to analyze how the dynamic algorithm reacts to changes in the network traffic load, we also performed simulations with variable traffic loads. Our variable rate simulations also wait until after the network has reached a steady state before collecting data. Variable rate simulations start with a traffic load of 50 pps which is maintained for 100 seconds. Every 100 seconds the traffic load changes. The traffic loads through the simulation are 50, 100, 150, 300, 150, 100, 300, 100 packets per second starting at times 9100, 9200, 9300, 9400, 9500, 9600, 9700, and 9800 respectively.

The network performance metrics used in this study are the packet loss probability and the packet latency. The packet loss probability is the probability that the MAC layer fails to send a packet to its destination. As discussed earlier, the packet loss can take place due to a channel access failure (CAF) or a collision failure. The packet loss probability for a node is simply the fraction of packets lost by the node during the simulation run. The CAF probability is the probability that a packet encounters *(1 + macMaxCSMABackoffs)* consecutive CCA failures. The CAF probability for a node is calculated as the number of CAFs it suffers divided by the total number of transmission attempts it makes. The probability of collision for a transmission by a node is calculated as the ratio of total number of collisions experienced by the node during the simulation and the total number of transmissions (transmission attempts excluding the ones that ended in CAF) it makes. Note that the probability of collision for a transmission is not the same as the probability of collision failure. A collision failure occurs only when (1 + *macMaxFrameRetries*) back-to-back collisions take place during the transmission of a packet or its ACK. The packet latency is defined as the time interval between the instants when the IEEE 802.15.4 MAC layer receives a packet for transmission and when it reports the success or failure in sending the packet back to the higher layer. The packet latency for a node is calculated as the average latency for the packet it generates. The performance metrics values reported in the subsequent sections are averages across all the nodes in the simulation. The 95% confidence intervals associated with these values were always observed to be within a few percentage of the average.

As described in the previous section, in IEEE 802.15.4 MAC operation, the CSMA wait time depends on the BE value. For each transmission attempt, BE is initialized to *macMinBE* and each CCA failure causes it to increase by 1 until it reaches a maximum (*macMaxBE*). Thus, the CSMA wait duration depends on how many CCA failures have already taken place in the current transmission attempt. To simplify our investigation, we eliminate this dependency by setting *macMinBE* and *macMaxBE* to the same value, referred to henceforth simply as BE. Thus, in our simulations, the CSMA wait time simply depend on BE irrespective of the CCA failures experienced so far in the current transmission attempt. In this study, we experimented with *macMinBE*(=*macMaxBE*) values 3 through 8. The value of the *macMaxCSMABackoffs* parameter used in the simulations varied in range 0 through 7[3]. Although we performed simulations with different values of the *macMaxFrameRetries* parameter as well, the parameter was observed not to have much impact on the performance. We believe that the true impact of the *macMaxFrameRetries* parameter can only be determined when collisions are a frequent occurance in the network, i.e. in the presence of a significant number of hidden nodes. Analyzing the impact of *macMaxFrameRetries* parameter on beaconless IEEE 802.15.4 performance in the presence of hidden nodes is part of our ongoing research.

4. Impact of *BE* (*macMinBE/macMaxBE*) Value

Figure 2 shows the impact of increasing the BE value on different performance metrics as the trafic load on the network increases. In these simulations, the *macMaxCSMABackoffs* and *macMaxFrameRetries* parameters are maintained at their default values (4 and 3 respectively). Figure 2(a) reveals that, at low traffic loads, the increase in BE can significantly reduce the packet loss probability for a given traffic load. However, as the traffic load increases, the reduction in the packet loss probability with increase in BE becomes less significant. At very high traffic loads, the packet loss probability becomes very high irrespective of the BE value. The CAF probability for a transmission follows essentially the same trend as the packet loss probability (Figure 2(b)).

[3] Although IEEE 802.15.4 specification [1] limits *macMaxCSMABackoffs* to a maximum value of 5, we found merit in increasing the parameter's value beyond this limit (Section 5).

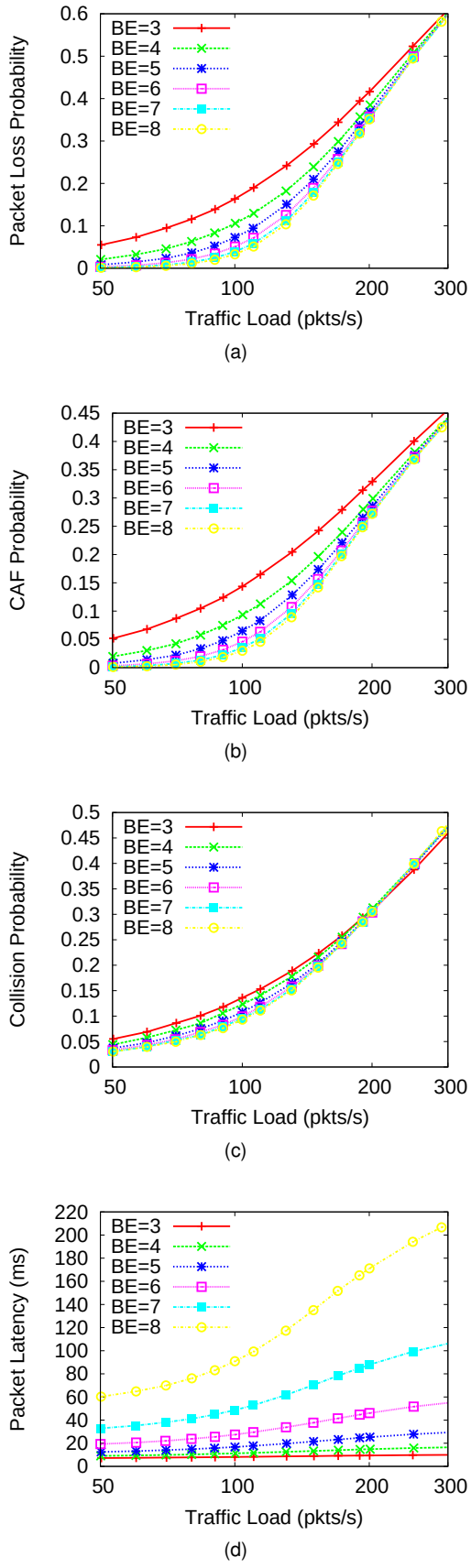


Figure 2. Impact of macMinBE/macMaxBE value

These observations can be explained as follows. Suppose certain nodes are competing for channel access at a certain time. At low traffic loads, the size of this set is small and there are no new additions to it, i.e. no new node gets a packet to send, for a relatively long time. The increase in BE increases the range of CSMA wait times, which in turn causes the packet transmissions to be spread throughout this time. Thus, a node becomes less likely to sense the transmission channel while another node is in middle of a transmission. Moreover, as packets are successfully transmitted, there is less competition for channel access and hence the CAF probability goes down. At high traffic loads, the number of nodes competing for channel access at a certain time may be large and new nodes continuously enter the set of competing nodes as some nodes leave. Thus, increasing the range of CSMA wait times to spread out the packet transmissions does not help much.

Similar to the CAF probability, the collision probability also reduces with increase in BE at low traffic loads, although the reduction is not as significant as for the CAF probability (Figure 2(c)). At high traffic loads, the collision probability increases slightly with increase in BE. As we discussed earlier, in the absence of hidden nodes, the non-negligible RX-to-TX turnaround time is the reason collisions take place. At low traffic loads, increase in BE increases the range of CSMA wait times. Thus, a node is less likely to finish its CSMA wait during the turnaround time of a node about to begin its packet or ACK transmission. Since the turnaround time is required to be less than 12 symbols [1], the increase in range of CSMA wait times causes only a modest decrease in the collision probability. The slight increase in the collision probability with increase in BE at high traffic loads can be due to several factors. First, higher BE values result in slightly lower CAF probability even at high traffic loads. Thus, higher BE values cause more packet transmissions which may result in more collisions. Secondly, higher BE values increase the packet latency which means that the number of nodes competing for channel access at any given time increases, which again results in more collisions.

Figure 2(d) shows that, despite lower collision rates at low traffic loads, the packet latency is consistently higher for higher BE values. This is because the longer CSMA waits overshadow the effect of fewer retransmissions due to collisions. As mentioned earlier, BE values 7 and 8 result in lowest packet losses but produce such high latency values that they are likely to be useful only for those applications that can tolerate very high latencies. However, as Figure 2(a) shows, BE value 6 does not significantly increase the packet loss probability compared to a BE value of 7 or 8. For this reason, BE value 6 is likely to be best for the applications that need low packet loss rates and can tolerate *per-hop* packet latencies up to 50 ms. Applications with

more stringent latency requirements may benefit from BE value 5. Lower BE values would be useful for only those applications that can tolerate packet losses but need minimum packet latencies.

The results shown in Figure 2 were obtained using 133 byte long packets. The simulations were repeated with several smaller packet sizes as well and the results obtained were qualitatively similar. In particular, we always found BE values 5 and 6 to offer the best tradeoff between the packet loss probability and the latency.

5. Impact of *macMaxCSMABackoffs* Value

The simulation results regarding the impact of *macMaxCSMABackoffs* value on beaconless IEEE 802.15.4 operation are displayed in Figure 3. The label *backoffs* in the figures refers to *macMaxCSMABackoffs*. In these simulations, the *macMinBE* and *macMaxBE* parameters are set to value 5 each and *macMaxFrameRetries* parameter is set to its default value 3. To allow easy observation of main results, we show curves for *macMaxCSMABackoffs* values 2, 4 and 7 only.

It is clear that the increase in the *macMaxCSMABackoffs* value reduces the CAF probability across all traffic loads (Figure 3(b)) as more CCA failures are allowed in a transmission attempt before a channel access failure is declared. Reduction in the CAF probability means that more transmissions take place, which translates to a higher probability of collision for a transmission (Figure 3(c)). However, as Figure 3(c) shows, the increase in the probability of collision, with increase in *macMaxCSMABackoffs* value, is not substantial for traffic loads up to 100 packets/sec. The decrease in the CAF probability dominates the increase in the collision probability and causes the overall packet loss probability to go down with increase in *macMaxCSMABackoffs* value for traffic loads up to 200 packets/sec. For higher traffic loads, the increase in the collision probability becomes large enough to neutralize the impact of reduced CAF probability and the overall packet loss probability becomes slightly higher for larger *macMaxCSMABackoffs* values.

The increase in the *macMaxCSMABackoffs* value also causes an increase in the packet latency (Figure 3(d)), which becomes significant at higher traffic loads, as a packet has less chance to be abandoned because of a channel access failure and more chance to be retransmitted due to collisions. The substantial increase in the packet latency and the collision probability at higher traffic loads, with increase in the *macMaxCSMABackoffs* value, can be attributed to their mutual dependence. Higher packet latency means that a packet competes with a larger number of other packets for access to the transmission channel, which results in more collisions. More collisions, in turn, mean more retransmis-

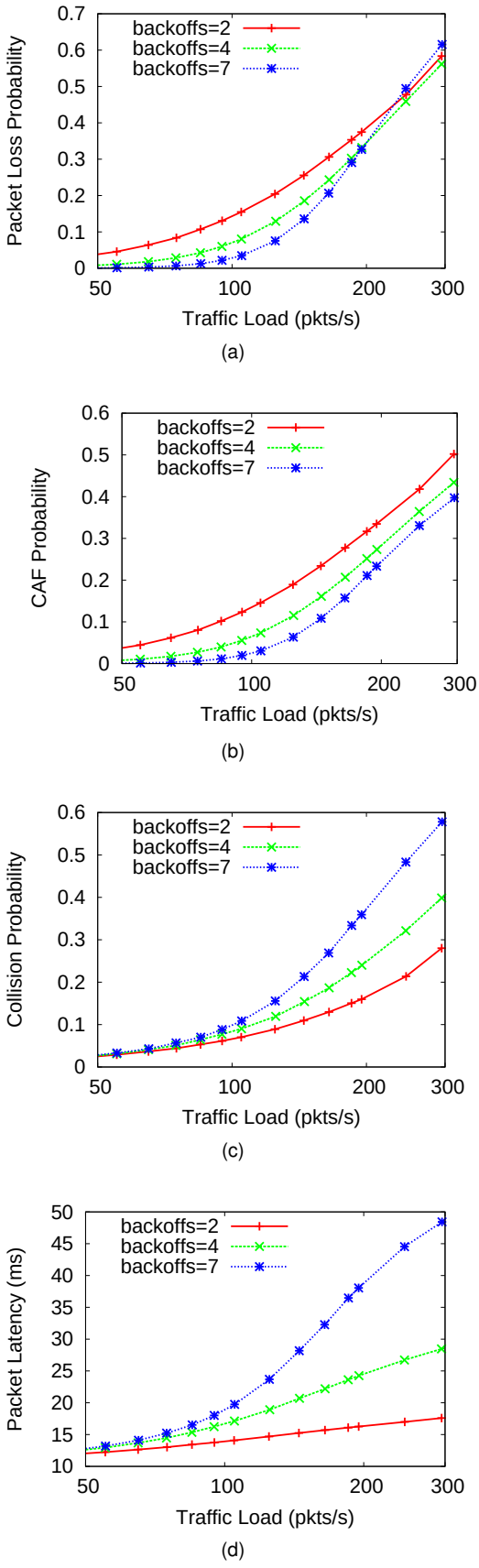
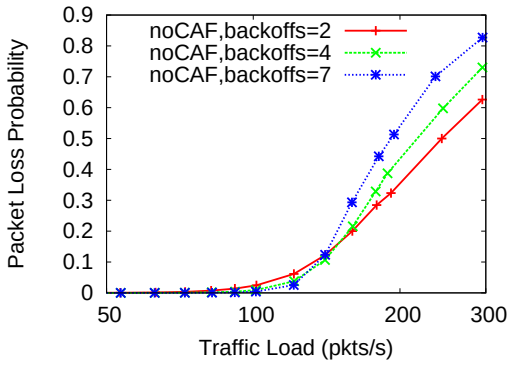
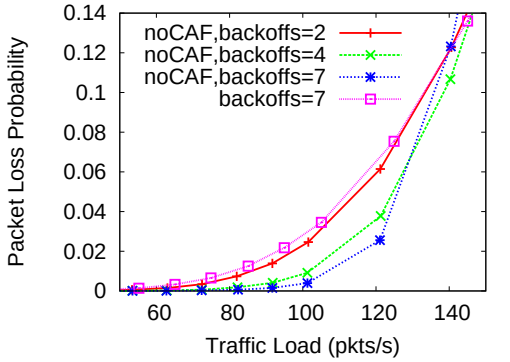


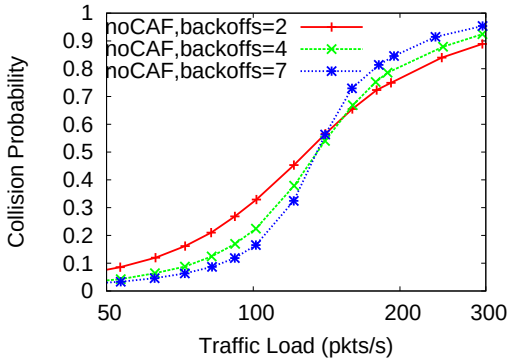
Figure 3. Impact of *macMaxCSMABackoffs* value with Channel Access Failures allowed



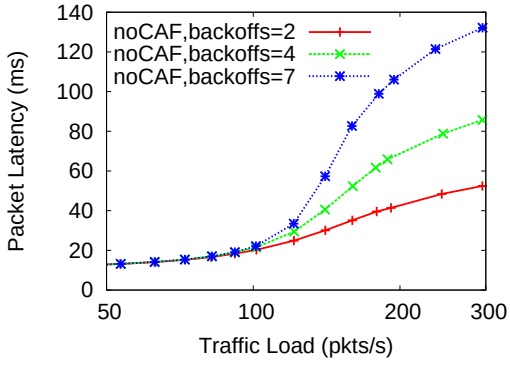
(a)



(b) CAF allowed versus CAF disabled



(c)



(d)

Figure 4. Impact of *macMaxCSMABackoffs* value with Channel Access Failures disabled

sions of a packet and hence higher latency. Simulations with smaller packet sizes revealed essentially the same trends as described above with the differences easily accounted for by the change in the packet size.

The simulation results show that setting the *macMaxCSMABackoffs* parameter to value 7 results in a reasonable packet latency (less than 30ms) and lower packet loss rates than other experimented values for traffic loads up to a certain threshold. This threshold value is observed to be about 150 packets/sec for 133 byte long packets and gets higher for smaller packet sizes. As IEEE 802.15.4 specification [1] limits the *macMaxCSMABackoffs* parameter to a maximum value 5, we suggest modifying the standard to allow higher values for the parameter. At traffic loads higher than this threshold, setting *macMaxCSMABackoffs* parameter to value 4, which is also the default value for the parameter, gives the best tradeoff between the packet loss rate and the packet latency.

The results discussed above suggest that, at low and moderate traffic loads, further reductions in the packet loss probability can be obtained if we eliminate the restriction imposed by the IEEE 802.15.4 standard on how many times a node can perform CCA without success while attempting to send a packet. The IEEE 802.15.4 standard requires a packet to be abdandoned if *(1 + macMaxCSMABackoffs)* consecutive CCA failures take place, characterizing the situation as a *channel access failure*. Rather than abandoning the packet, we consider treating a channel access failure the same way as a collision. Under this modification, a node would start the next attempt to send the packet (resetting the *NB* parameter to 0 and *BE* to *macMinBE*) when it encounters *(1 + macMaxCSMABackoffs)* consecutive CCA failures in the current transmission attempt or when it fails to receive an acknowledgement for the packet transmission. As before, a node can make atmost *(1 + macMaxFrameRetries)* attempts to send a packet.

The simulation results under the modified scheme are shown in Figure 4. The performance curves for the modified scheme are labeled with prefix *noCAF*. As Figure 4(b) shows, the modification indeed leads to lower loss probability than the standard scheme for traffic loads up to a threshold (140 packets/second for 133 byte packets). Note that the packet loss probability values under the modified scheme with *macMaxCSMABackoffs* value 2 are very close to the values under the standard scheme with *macMaxCSMABackoffs* value 7. Increasing the *macMaxCSMABackoffs* value from 2 to 4 and then to 7 under the modified scheme causes continuous, albeit diminishing, reductions in the packet loss probability for traffic loads up to the 140 packets/second threshold. At higher traffic loads, the packet loss probability increases with increase in the *macMaxCSMABackoffs* value (Figure 4(a)).

The observed change in the packet loss probability for

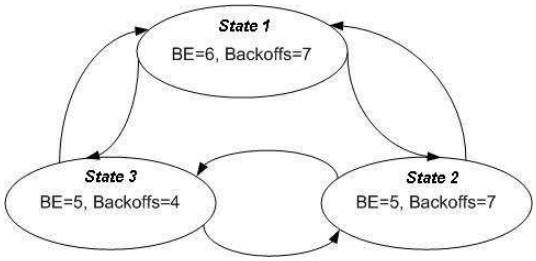


Figure 5. Dynamic Algorithm

different *macMaxCSMABackoffs* values under the modified scheme can be explained on the basis of the observed change in the collision probability. Figure 4(c) displays the collision probability for a transmission for different *macMaxCSMABackoffs* values under the modified scheme, where the erstwhile channel access failures are also counted as the collisions. Note that, for traffic loads up to the 140 packets/second threshold, the collision probability decreases with increases in *macMaxCSMABackoffs* value and vice versa for higher traffic loads. Clearly, for traffic loads up to the threshold, the decrease in the number of erstwhile channel access failures with higher *macMaxCSMABackoffs* values dominates any increase in the actual collisions due to more transmissions taking place. At higher traffic loads, the impact of increase in the number of actual collisions dominates. Note that, under the modified scheme, the increase in the *macMaxCSMABackoffs* value leads to significant increase in the packet latency at traffic loads higher than the 140 packets/second threshold (Figure 4(d)). Simulations with smaller packet sizes gave similar results except that the threshold traffic load was larger.

A comparison of Figure 3(a) and Figure 4(a) reveals that, for 133 byte long packets, the modified scheme results in lower loss rates than the standard scheme for traffic loads up to a threshold (about 150 packets/second) and vice versa for the higher traffic loads. Further, an examination of Figures 4(b) and 4(d) reveals that under the modified scheme, setting *macMaxCSMABackoffs* to value 4 gives the best tradeoff between the packet loss probability and the packet latency for traffic loads up to the threshold. Similar behavior was observed for lower packet sizes with the threshold traffic load being correspondingly higher. Since an IEEE 802.15.4 network can be expected to operate in the low/moderate (less than the threshold) traffic load regime most of the time, there is some merit in modifying the IEEE 802.15.4 standard to include the modified scheme as a configurable option.

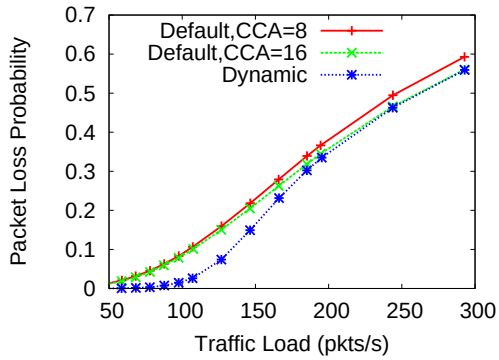
6. Dynamic Backoff Algorithm

The proposed dynamic backoff algorithm tunes the parameters *macMinBE*, *macMaxBE*, and *macMaxCSMABackoffs* for currently observed network traffic loads. The goal of the algorithm is to decrease packet loss rates and increase throughput while maintaining reasonable latencies. To this end, we attempt to maintain average latency values of 40 ms or below. Note that this algorithm could easily be adapted to an alternative acceptable latency value. Our algorithm estimates the current network traffic load by monitoring packet loss rates over previous packets. Centralized algorithms which may be able to calculate such information precisely involve more overhead than is practical for IEEE 802.15.4 devices where energy conservation is critical. As a result, the proposed algorithm estimates the recent network by observing the results of previous transmission attempts.

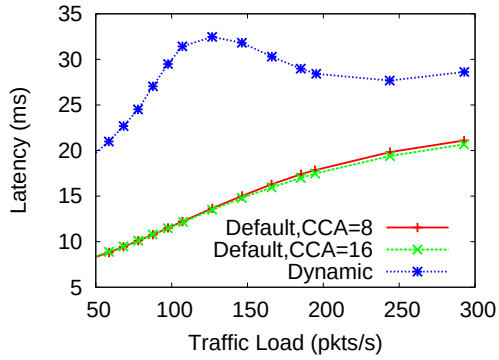
The state diagram depicting our dynamic algorithm can be seen in figure 5. For networks with very low traffic rates (50 to 140 packet/s in our simulations), the dynamic algorithm uses a configuration of *macMinBE*/*macMaxBE*=6 and *macMaxCSMABackoffs*=7. This configuration is refered to as state 1 in figure 5. At approximately 140 packets/s, the average latency begins exceeding the 40 ms threshold. At this point, the algorithm detects the higher latency values and transitions to state 2 (*macMinBE*/*macMaxBE*=5, *macMaxCSMABackoffs=7*) in an effort to lower the packet latencies. It can be noted that in terms of packet loss, state 1 remains optimal above the 140 packets per second threshold, but because the latency values become excessive, it is necessary to transition to state 2. Additionally, if average packet loss rates jump above 30%, indicating a traffic load exceeding 200 packets/s, transition is made to state 3 (*macMinBE*/*macMaxBE*=5, *macMaxCSMABackoffs=4*).

From state 2, transition can be made back to state 1 if both the packet loss rate drops below 15% and the latency below 40 ms. A packet loss rate below 15% indicates that the traffic load has dropped below 140 packets per second, and thus the state 1 configuration is again optimal. The requirement that the average packet latency be below 40 ms is a safe guard to ensure the latency requirement and to prevent a possibly ping pong effect between state 1 and state for a network with a constant traffic load. State 2 will transition to state 3 if either the loss rate reaches 30%, indicating a traffic load exceeding 200 packets/s, or if the average latency still exceeds 40 ms. Finally, from state 3, the algorithm will transition to state 1 if the traffic load goes below 140 packets/s (loss rate below 15%) and the average latency is below 40 ms.

State 3 transitions to state 2 if the average latency is below 40 ms and the traffic load is less than 200 packets/s (30% packet loss) but greater than 140 packets/s (packet loss of 15%). State 3 may otherwise transition to state 1

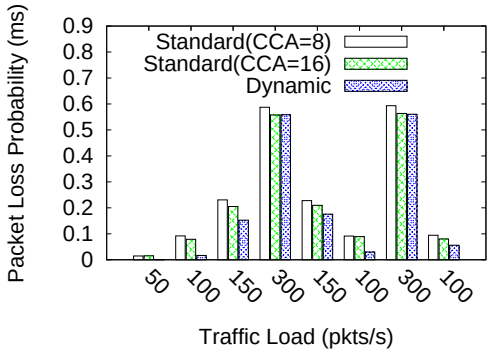


(a) Packet Loss

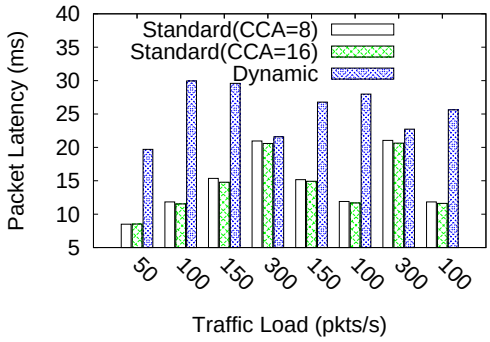


(b) Latency

Figure 6. Dynamic vs. Standard



(a) Packet Loss



(b) Latency

Figure 7. Variable Traffic Load Performance

if the traffic load drops below 140 packets/s (15% packet loss) and the average latency is below 40 ms.

Figure 6(a) shows much improved performance for our Dynamic algorithm over the standard default settings. The improvement is significant even when you compare our dynamic algorithm to the standard default configuration with a clear channel assessment (CCA) time of 16 instead of the standard 8. This shows that the improvement is not just due to increasing the CCA time to 16, but a result of our dynamic configuration. The dynamic algorithm does result in higher latencies than the IEEE 802.15.4 standard implementation; however, the decrease in packet loss and increase in throughput outweighs the disadvantage of increased latencies for most applications, and again, the algorithm can be easily reconfigured to tolerate higher or lower latency values. The largest improvement in packet loss rates is seen at lower traffic rates. This is a result of the increase of backoff exponent values to 6 and the number of CSMA backoffs to 7. At higher traffic rates, the results of our dynamic algorithm are similar to the standard using a CCA value of 16. This is because the configuration at high traffic loads (*macMinBE*/*macMaxBE*=5,*macMaxCSMABackoffs=4*) is a near match to the standard configuration (*macMinBE*=3,*macMaxBE*=5,*macMaxCSMABackoffs=4*).

In variable rate simulations, our dynamic algorithm quickly adapts to changes in network traffic levels. Figures 7(a) and 7(b) show average values for all nodes over the 100 second time period that a given traffic load is in effect. As can be seen in figure 7(a), our dynamic algorithm reacts and outperforms the standard default in most cases. At lower traffic load levels, our algorithm again shows significant improvement over the standard. At higher traffic loads, our algorithm performs similarly compared to the standard. 7(b) shows average latency values over these 100 second timeframes staying below 35 ms for all traffic loads. This is even better than our requirement of staying below a 40 ms average.

As can be seen in figure 8(a), and 8(b) this dynamic algorithm does a good job of estimating the current network traffic load and adjusting its configuration. 8(a) shows nearly perfect matches to the component configurations. Latency values match exactly at lower and higher traffic rates, while the midrange traffic loads gradually follow the trend as it transitions. This is because the final dynamic algorithm we implemented moves to state 2 at an earlier point in an effort

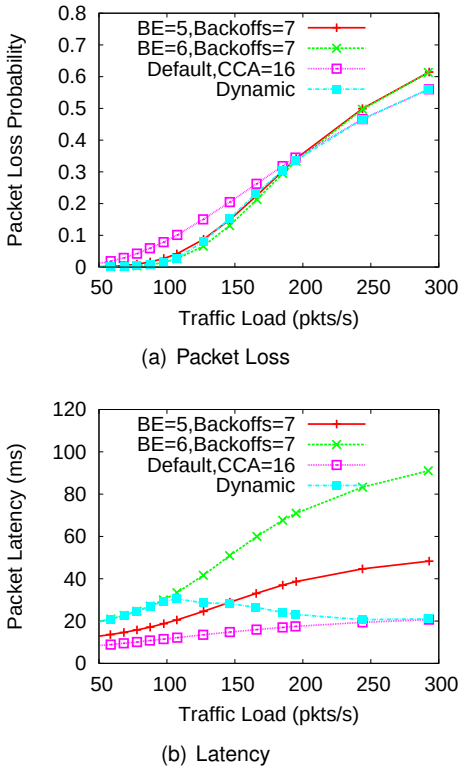


Figure 8. Dynamic Algorithm

to maintain average latency values below 40 ms.

The configuration window of 40 packets was carefully chosen to allow the dynamic algorithm to react quickly to changes in the network traffic load while also avoiding bouncing between configuration states. The smaller the window of packets between configuration changes, the more responsive the algorithm is to changes in the network. For example, with the jump from 100 packet/s to 300 packet/s, the response times were 2, 5 and 13 seconds for window sizes of 20, 40, and 80 respectively. The change from 300 packet/s to 100 packet/s takes even longer to adjust the configuration with 21, 28, and 67 seconds respectively. The response time when analyzing 80 packets at a time is likely too slow for most applications. While the response time for a window size of 20 packets is faster, figure 9(a) shows the algorithm jumping around as it reacts too hastily. For these reasons, we believe that a window size of 40 packets will provide the best performance.

7. Related Work

The use of IEEE 802.15.4 standard in commercial applications is still at an early stage and hence there are not many papers that investigate proper configuration of IEEE 802.15.4 MAC paremeters. Koubaa et.al.[8] observed that the packet loss rate in a beacon enabled network can be reduced at the cost of increasing the packet latency by increasing the *macMinBE/macMaxBE* values. Tao et. al. [13] observed that, under *saturated*[4] conditions in beacon enabled networks of more than 4 nodes, increase in *macMinBE/macMaxBE* values from $(3/5, 3/3)$ to $(4/6, 5/5)$ respectively improves the network throughput.

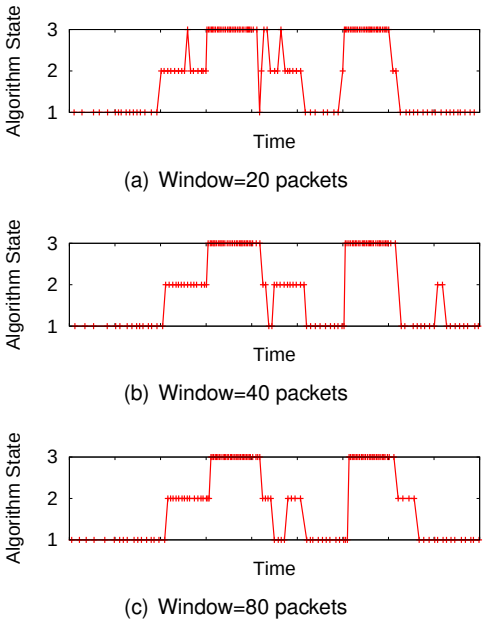


Figure 9. Algorithm States for a Single Node

Additionally, many papers prescribe using different BE values to achieve service differentiation. Koubaa et. al.[7] suggest using lower *macMinBE* values to achieve low latency for time critical traffic in beacon mode IEEE 802.15.4 networks. Ko et.al. [6] suggest allowing nodes that need to transmit frequently to use lower than normal *macMinBE*. Youn et.al. [14] suggest achieving priority based service differentiation in IEEE 802.15.4 networks by chosing the CSMA wait duration using different gaussian distribution for different priorities. Ha et.al. [4] suggest a scheme for determining BE value for a new send attempt based on the final BE value reached in the previous send attempt. Finally, there are many papers [10, 9, 11, 12] that require the coordinator to dynamically assign BE values to the associated devices since the coordinator may have access to useful information such as the individual/total traffic loads and the number of nodes in the cluster.

As per our literature search, only a few papers have so far analyzed the impact of *macMaxCSMABackoffs* value on IEEE 802.15.4 operation. Athanasopoulos et.al. [2] suggested using *macMaxCSMABackoffs* value 1, rather than default 4, to reduce the power consumption and the packet

[4] where a node always has a packet to send

latency while ignoring any detrimental effect such a setting may have on the packet loss rates. Tao et.al. [13] observed that *macMinBE/macMaxBE* parameters have more direct influence on the network throughput than *macMaxCSMABackoffs* parameter.

8. Conclusion

In this paper, we analyzed the impact of *macMinBE/macMaxBE* and *macMaxCSMABackoffs* parameters on the performance of beaconless IEEE 802.15.4 networks. We have also proposed a dynamic algorithm that adjusts itself to observed changes in the network traffic load. Network traffic loads are estimated by monitoring latency and packet loss rates at each individual node. This is important as it avoids additional communications for the nodes that would be necessary in a centrally managed algorithm. Finally, we have shown that this algorithm is able to quickly adapt to changes in the observed network traffic load.

References

[1] IEEE standard for information technology- telecommunications and information exchange between systems- local and metropolitan area networks- specific requirements part 15.4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs). *IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003)*, 2006.

[2] A. Athanasopoulos, E. Topalis, C. Antonopoulos, and S. Koubias. 802.15.4: The effect of different back-off schemes on power and qos characteristics. *Wireless and Mobile Communications, 2007. ICWMC '07. Third International Conference on*, pages 68–68, March 2007.

[3] M. Dohler and T. Watteyne. Urban WSNs Routing Requirements in Low Power and Lossy Networks. Internet-Draft draft-ietf-roll-urban-routing-reqs-00, Internet Engineering Task Force, Sept. 2008. Work in progress.

[4] J. Y. Ha, T. Kim, H. S. Park, S. Choi, and W. H. Kwon. An enhanced CSMA-CA algorithm for IEEE 802.15.4 LR-WPANs. *Communications Letters, IEEE*, 11(5):461–463, May 2007.

[5] T. O. Kim, J. S. Park, H. J. Chong, K. J. Kim, and B. D. Choi. Performance analysis of IEEE 802.15.4 non-beacon mode with the unslotted CSMA/CA. *IEEE Communications Letters*, 12(4):238–240, Apr. 2008.

[6] J.-G. Ko, Y.-H. Cho, and H. Kim. Performance evaluation of IEEE 802.15.4 MAC with different backoff ranges in wireless sensor networks. *Communication systems, 2006. ICCS 2006. 10th IEEE Singapore International Conference on*, pages 1–5, Oct. 2006.

[7] A. Koubaa, M. Alves, B. Nefzi, and Y. Song. Improving the IEEE 802.15.4 slotted CSMA/CA MAC for time-critical events in wireless sensor networks. *Workshop of Real-Time Networks, Satellite Workshop to ECRTS 2006*, July 2006.

[8] A. Koubaa, M. Alves, and E. Tovar. A comprehensive simulation study of slotted CSMA/CA for IEEE 802.15.4 wireless sensor networks. *Factory Communication Systems, 2006 IEEE International Workshop on*, pages 183–192, 27, 2006.

[9] B.-H. Lee and H.-K. Wu. A delayed backoff algorithm for IEEE 802.15.4 beacon-enabled LR-WPAN. *Information, Communications and Signal Processing, 2007 6th International Conference on*, pages 1–4, Dec. 2007.

[10] A.-C. Pang and H.-W. Tseng. Dynamic backoff for wireless personal networks. *Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE*, 3:1580–1584 Vol.3, Nov.-3 Dec. 2004.

[11] H. M. Park, W. C. Park, S. J. Lee, and G.-Y. Lee. Modified backoff scheme for MAC performance enhancement in IEEE 802.15.4 sensor network. In *2007 WSEAS International Conference on CIRCUITS, SYSTEMS, SIGNAL and TELECOMMUNICATIONS*, January 2007.

[12] V. P. Rao and D. Marandin. Adaptive backoff exponent algorithm for Zigbee (IEEE 802.15.4). In *Next Generation Teletraffic and Wired/Wireless Advanced Networking*, volume 4003 of *Lecture Notes in Computer Science*, pages 501–516. Springer-Verlag, 2006.

[13] Z. Tao, S. Panwar, D. Gu, and J. Zhang. Performance analysis and a proposed improvement for the IEEE 802.15.4 contention access period. *Wireless Communications and Networking Conference, 2006. WCNC 2006. IEEE*, 4:1811–1818, 0-0 2006.

[14] M. Youn, Y.-Y. Oh, J. Lee, and Y. Kim. IEEE 802.15.4 based QoS support slotted CSMA/CA MAC for wireless sensor networks. *Sensor Technologies and Applications, 2007. SensorComm 2007. International Conference on*, pages 113–117, Oct. 2007.