Mobile Information Systems 5 (2009) 81–99
DOI 10.3233/MIS-2009-0074
IOS Press

A simulation based analysis of the impact of IEEE 802.15.4 MAC parameters on the performance under different traffic loads

D. Rohm[a], M. Goyal[a,*], H. Hosseini[a], A. Divjak[b] and Y. Bashir[b]
[a]*University of Wisconsin Milwaukee, Milwaukee, WI 53201, USA*
[b]*Johnson Controls, Milwaukee, WI 53202, USA*

Abstract. IEEE 802.15.4, a MAC/PHY protocol for low power and low data rate wireless networks, is emerging as the popular choice for various monitoring and control applications. Depending on the application, the traffic load on an IEEE 802.15.4 network may vary over a wide range. The performance of the protocol, measured in terms of the packet loss probability and the packet latency, depends upon the prevailing traffic load among the nodes competing for channel access, the level of interference from the hidden nodes and the configuration of IEEE 802.15.4 MAC parameters. In this paper, we analyze via simulations the impact of different configurable MAC parameters on the performance of beaconless IEEE 802.15.4 networks under different traffic loads and under different levels of interference from the hidden nodes. Based on this analysis, we suggest the values of IEEE 802.15.4 MAC parameters that results in a good tradeoff between the packet loss probability and the packet latency under different conditions.

Keywords: IEEE 802.15.4 MAC, wireless sensor networks, CSMA, hidden nodes

1. Introduction

IEEE 802.15.4 [1] is a leading MAC/PHY 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 [20]. 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.

Suppose a number of IEEE 802.15.4 source nodes are sending data to one or more destination nodes. A source node competes with all other source nodes in its radio range for access to the transmission channel using the CSMA/CA algorithm implemented in IEEE 802.15.4 MAC operation. The node may fail to get access to the transmission channel even after repeated attempts if too many nodes are competing

*Corresponding author: M. Goyal, EMS919, UW Milwaukee, 3200 N Cramer Street, Milwaukee, WI 53201, USA. Tel.: +1 414 229 5001; Fax: +1 414 229 6958; E-mail: mukul@uwm.edu.

for channel access. The competition for channel access depends upon the the prevailing traffic load on the network, which in turn is determined by the number of nodes competing for channel access and their packet generation rates. Even if the node manages to gain access to the transmission channel, its transmission may collide with that of a *hidden* node, i.e. a node outside the radio range of the source node but within the radio range of the destination node. For a given traffic load/hidden node interference scenario, the performance of an IEEE 802.15.4 node, measured in terms of the loss rate and the latency for the packets it transmits, is heavily influenced by the configuration of IEEE 802.15.4 MAC parameters in the network. IEEE 802.15.4 specification [1] suggests default values for different MAC parameters. However, the default configuration may not yield the most desirable tradeoff between the packet loss rate and the packet latency in all situations. In fact, it may be difficult to determine a single IEEE 802.15.4 MAC configuration that results in optimal performance in all situations.

In this paper, we analyze the impact of IEEE 802.15.4 MAC parameters, namely *macMinBE/macMaxBE*, *macMaxCSMABackoffs* and *macMaxFrameRetries*, on the performance of IEEE 802.15.4 nodes, competing with each other for access to the transmission channel using *beaconless* operation of IEEE 802.15.4 MAC protocol, under different traffic loads and under different levels of interference from *hidden* nodes. The performance is measured in terms of the packet loss probability and the packet latency. This study is based on NS2 [14] simulations using an extensively improved version [4] of the IEEE 802.15.4 module. The objective is to determine the appropriate values of IEEE 802.15.4 MAC parameters that results in a good tradeoff between the packet loss probability and the packet latency for a given traffic load range. A preliminary version of this analysis, based on the impact of *macMinBE/macMaxBE* and *macMaxCSMABackoffs* parameters in the absence of hidden nodes, appeared in [18].

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, 5 and 6 present the simulation results regarding the impact of *macMinBE/macMaxBE*, *macMaxCSMABackofffs* and *macMaxFrameRetries* parameters respectively on the performance of nodes in a beaconless IEEE 802.15.4 network under different traffic loads and under different levels of interference from hidden nodes. Section 7 presents a 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.

[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].

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 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.

Thus, in IEEE 802.15.4 MAC operation, a packet can be lost either due to a *channel access failure* or a *collision failure*. In this paper, we use the *packet loss rate*, the fraction of packets that a node loses because of *channel access failures* or *collision failures* and the *packet latency*, 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, as the performance metrics.

2.1. Collisions in beaconless IEEE 802.15.4 MAC operation

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 upto 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 [8]. Note that the second collision window exists only if no collision takes place in the first collision window.

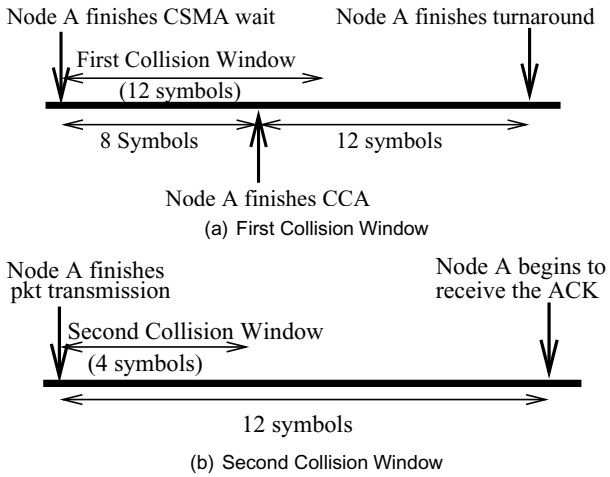

Fig. 1. Collision windows in beaconless IEEE 802.15.4 operation.

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 reported in this paper 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 2.4 GHz band and no transmission is lost due to PHY level noise. The simulated network topology (Fig. 8) consists of two sets of nodes: the nodes under *observation* and the *hidden* nodes. The simulation results presented in this paper report the loss rate/latency for *observed* nodes. The hidden nodes are outside the radio range of the observed nodes and vice versa. All observed nodes are in each other's radio range. Same is true for the hidden nodes. The destination node is in the radio range of both observed as well as hidden nodes. Each observed/hidden node sends packets to the destination node as per a poisson distribution with average rate 5 packets/second. Since the average time interval (200 ms) between successive packets generated at a node is more than the typical packet latency, the nodes operate mostly in *unsaturated* mode. 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 among the observed nodes is varied by changing the number of observed nodes in the range 10 through 60. The interference level from hidden nodes is varied by changing the number of hidden nodes in the range 0 through 20. In each simulation, a certain number of observed nodes (between 10 and 60) and a certain number of hidden nodes (between 0 and 20) send packets to their common destination. Since each node generates on average 5 packets/second, the simulated average traffic load among observed nodes varies in range 50 to 300 packets/second and the traffic load on hidden packets varies in range 0 to 100 packets/second. Note that with 133 byte packet size, a packet transmission takes

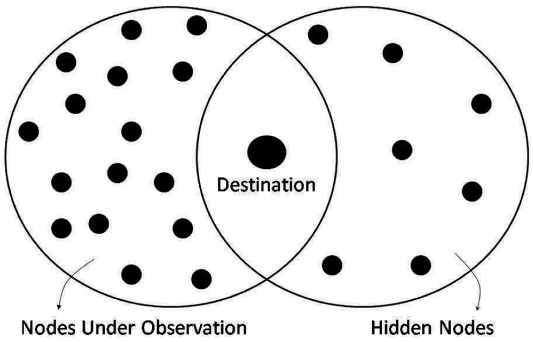

Fig. 2. Simulated Network Topology.

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 a significantly overloaded network (300 packets/second) with a large range of hidden node traffic.

The simulations were setup such that all the nodes complete their *association* with the *coordinator*, the destination node, before the packet generation begins. The nodes send packets to the coordinator for more than 3000 seconds. The simulations were performed using the ns-2 simulator [14]. We have significantly improved the IEEE 802.15.4 module in ns-2 simulator removing several bugs [4] and implemented a Zigbee [24] routing module as well. The modified IEEE 802.15.4 module, including the Zigbee routing implementation, is publicly available [4].

The performance metrics used in this study are the packet loss probability and the packet latency for the observed nodes. 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. In the simulations, we measure for each observed node the probability of channel access failure for a transmission attempt, the probability of collision for a transmission and the overall packet loss probability. 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 this paper 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[2] and the value of the *macMaxFrameRetries* parameter varied between 0 and 7, the range of values allowed for the parameter by IEEE 802.15.4 specification [1].

4. Impact of *BE* (= *macMinBE* = *macMaxBE*) value on IEEE 802.15.4 performance

Let us first consider the situation when no hidden nodes are present. Figure 3 shows the impact of increasing the BE value on different performance metrics as the number of observed nodes and hence their trafic load increases while there are no hidden nodes present. In these simulations, the *macMaxCSMABackoffs* and *macMaxFrameRetries* parameters are maintained at their default values (4 and 3 respectively). For sake of clarity, we display the curves for BE values 3,5 and 7 only.

Figure 3(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 (Fig. 3(b)).

These observations can be explained as follows. Suppose certain nodes are competing for channel access at a certain time instant. 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 (Fig. 3(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,

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

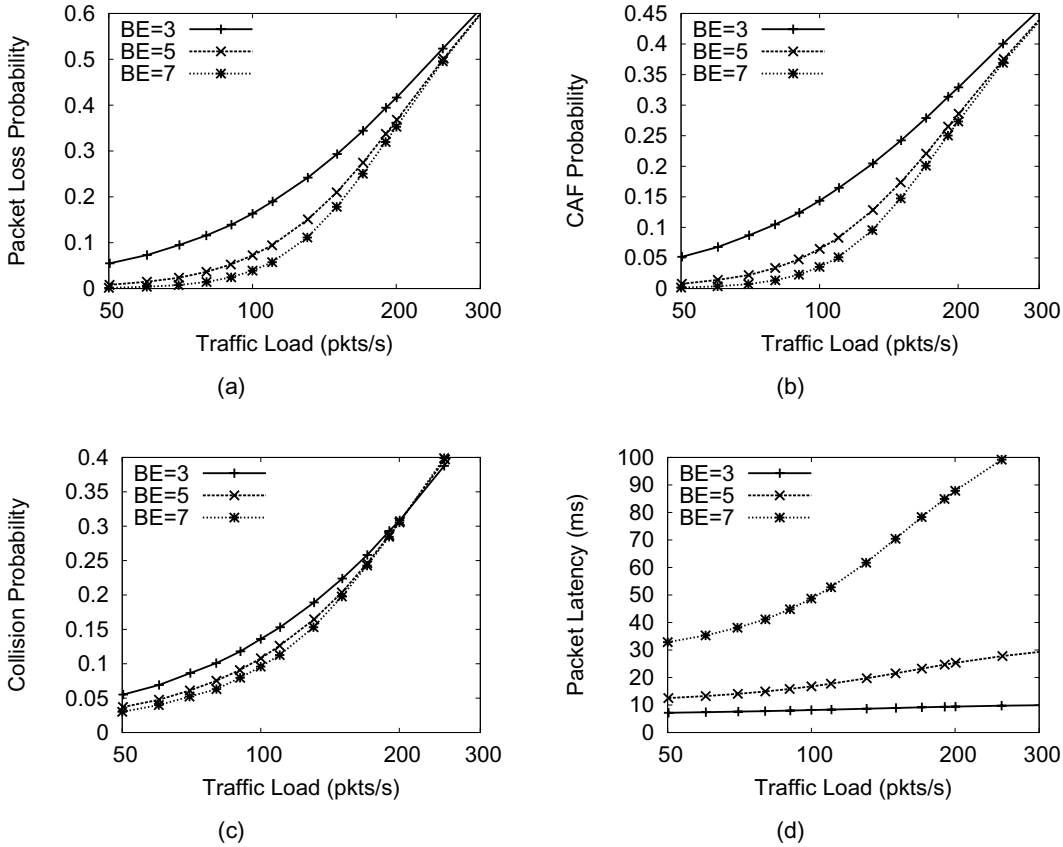

Fig. 3. The impact of macMinBE/macMaxBE value on performance when no hidden nodes are present.

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 3(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. BE values 7 and higher result in lowest packet losses but produce such high latency values that they are unlikely to be useful for most of the applications. This is especially true if a packet needs to travel over a multi-hop route from its source to destination and hence the latency values at each hop add up. However, as Fig. 3(a) shows, BE value 5 does not significantly increase the packet loss probability compared to a BE value of 7 and results in much better latency. For this reason, BE value 5 is likely to be best for the applications that need low packet loss rates as well as low latency. Applications with stringent latency requirements may use BE value 3 and under but would have to suffer significant packet loss rates. *Overall, we can conclude that BE value 5 presents the best tradeoff between the packet loss probability and the latency.*

The results shown in Fig. 3 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 value 5 to offer the best tradeoff between the packet loss probability and the latency.

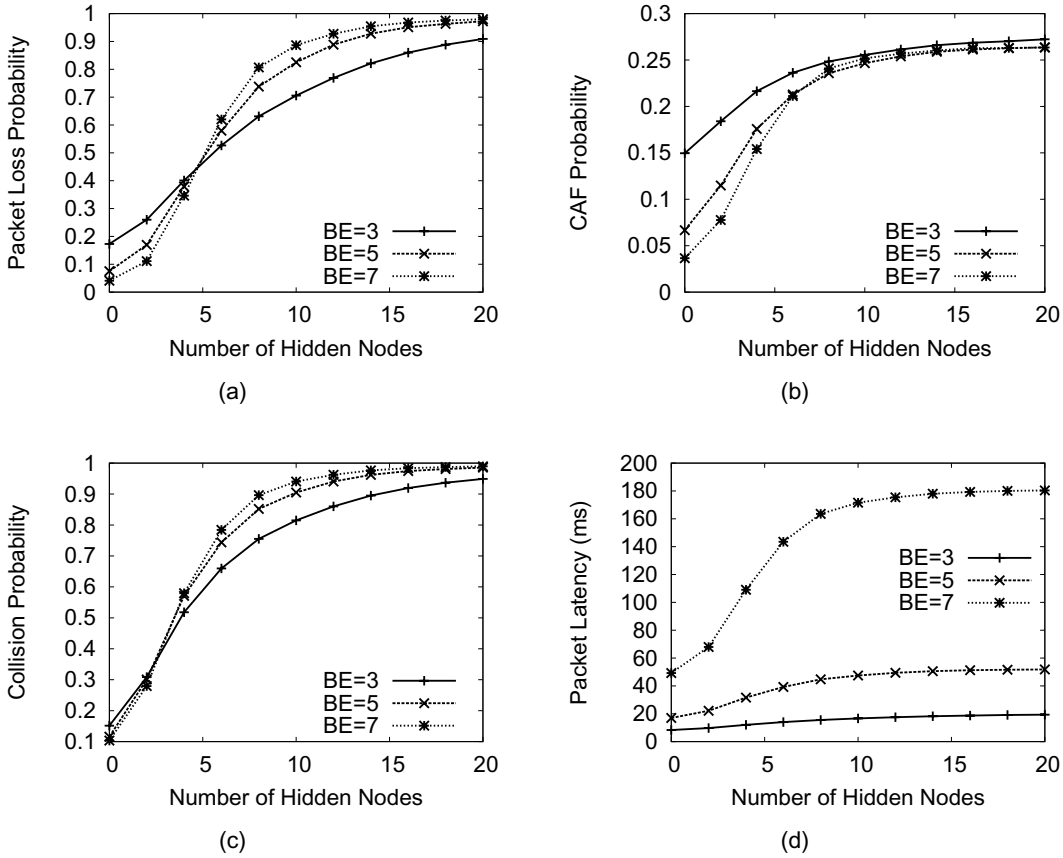

Fig. 4. The impact of macMinBE/macMaxBE value as the number of hidden nodes increases while the number of observed nodes is 20.

4.1. Impact of BE value in the presence of hidden nodes

Next, we consider the situation when hidden nodes are present. Figure 4 shows the values of different performance metrics for BE values 3, 5 and 7 as the number of hidden nodes increase from 0 to 20 while the number of observed nodes stays fixed at 20. Since the hidden nodes and the observed nodes are not in each other's radio range, a hidden node can transmit at the same time as an observed node. The collision causes both nodes to attempt another transmission of their packets. Thus, the presence of hidden nodes increases the number of transmissions required to send a packet for both observed and hidden nodes, thereby resulting in still more collisions. The probability of collision for a transmission quickly deteriorates as the number, and hence the interference level, of hidden nodes increases (Fig. 4(c)). The resulting increase in the number of transmissions causes the probability of CCA failure, and hence that of channel access failures, to increase as well (Fig. 4(b)). The overall result is that the packet loss probability for observed nodes increases rapidly with increase in the number of hidden nodes (Fig. 4(a)).

As Fig. 4(a) shows, when the number of hidden nodes is small, increase in BE helps reduce the packet loss probability. However, as the number of hidden nodes increases, increase in BE increases the packet loss probability. When the transmissions from hidden nodes are relatively infrequent, the increase in BE increases the range of CSMA wait times that results in lower probability of CCA failures and collision and hence lower probability of packet loss. However, as the number of hidden nodes and hence

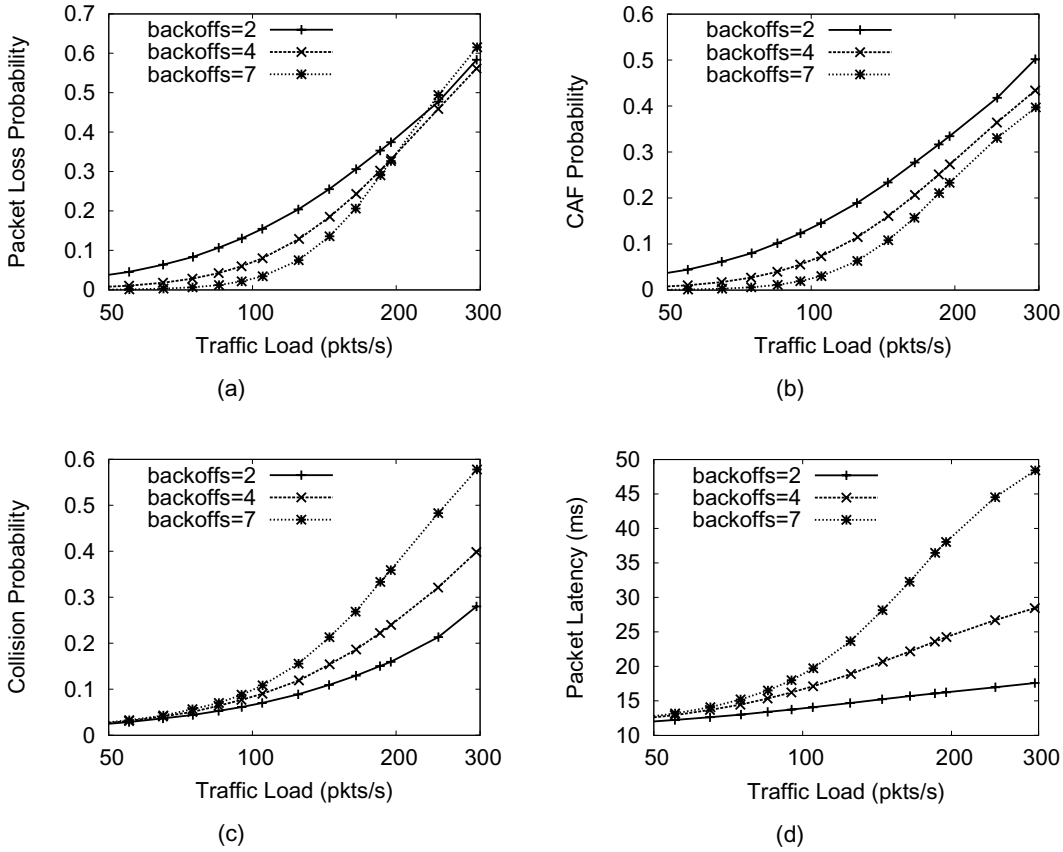

Fig. 5. Impact of *macMaxCSMABackoffs* value on performance when no hidden nodes are present.

transmissions from hidden nodes increase, the increase in CSMA wait times, resulting from increase in BE, has no beneficial impact. It results in increase in the packet latency (Fig. 4(d)). It fails to reduce the probability of collision as most of the collisions are being caused by transmissions of hidden nodes. In fact, the probability of collisions worsens with increase in BE (Fig. 4(c)) as increased latency causes more nodes to compete for channel access. The increase in BE also fails to have any significant impact on reducing the probability of channel access failure (Fig. 4(b)) as the number of packet transmissions, and hence the probability of CCA success/failure, largely depend on the interference from hidden nodes.

Figure 4(a) clearly shows that increase in the level of interference from hidden nodes has a devastating impact on the performance irrespective of the BE value. Figure 4 showed the case when the number of observed nodes was 20 and hence the total traffic load of the observed nodes is quite moderate (100 packets per second). The impact of hidden nodes worsens as the number/traffic load of observed nodes increases. As we will see later, the other IEEE 802.15.4 MAC parameters, namely *macMaxCSMABackoffs* and *macMaxFrameRetries*, also fail to alleviate debilitating impact of hidden nodes.

5. Impact of *macMaxCSMABackofs* value on IEEE 802.15.4 performance

Figure 5 shows the impact of *macMaxCSMABackoffs* value on the performance as the number of observed nodes increase and there are no hidden nodes. 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 (Fig. 5(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 (Fig. 5(c)). However, as Fig. 5(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 (Fig. 5(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 retransmissions 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 30 ms) and lower packet loss rates than other experimented values for traffic loads upto 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.

5.1. Impact of macMaxCSMABackoffs value in the presence of hidden nodes

Figure 6 shows the values of different performance metrics for *macMaxCSMABackoffs* values 0, 2 and 4 as the number of hidden nodes increase from 0 to 20 while the number of observed nodes stays fixed at 20. The collision probability (Fig. 6(c)) and hence the packet loss probability (Fig. 6(a)) increases rapidly with increase in the number of hidden nodes for all *macMaxCSMABackoffs* values. As Fig. 6(c) shows, the collision probability worsens with increase in *macMaxCSMABackoffs* value. This is because a higher *macMaxCSMABackoffs* value decreases the probability of channel access failures and hence increases the number of transmissions by both observed and hidden nodes. As Fig. 6(a) shows, when the number of hidden nodes are few, the channel access failures cause most of the packet loss and hence higher *macMaxCSMABackoffs* value decreases the packet loss probability. With increase in the number of hidden nodes, the collision failure becomes the main reason for packet

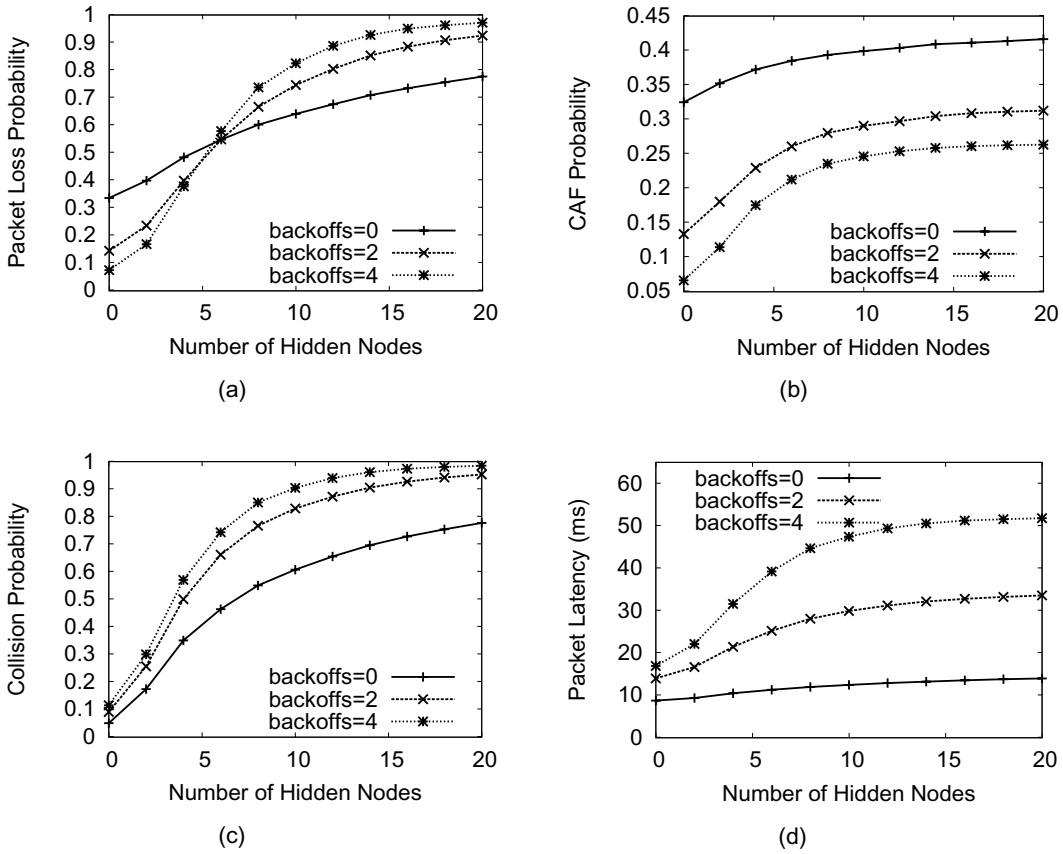

Fig. 6. The impact of macMaxBackoffs value as the number of hidden nodes increases while the number of observed nodes is 20.

loss and hence higher *macMaxCSMABackoffs* value increases the packet loss probability (Fig. 6(a)). The value 0 for *macMaxCSMABackoffs* means that a packet is abandoned as soon as a CCA failure is encountered. As expected, such a policy leads to a significant increase in channel access failures as Fig. 6(b) shows. However, the resulting decrease in the number of packet transmissions helps reduce the probability of collisions (Fig. 6(c)) and the overall probability of packet loss (Fig. 6(a)) over higher values of *macMaxCSMABackoffs* parameter. Overall, we can conclude that, as was the case with BE, the *macMaxCSMABackoffs* value is also largely inconsequential in mitigating the effect of a large number of hidden nodes.

6. Impact of *macMaxFrameRetries* value on IEEE 802.15.4 performance

Figure 7 shows the impact of *macMaxFrameRetries* value on the performance as the number of observed nodes increase and there are no hidden nodes. The label *retries* in the figures refers to *macMaxFrameRetries*. In these simulations, the *macMinBE* and *macMaxBE* parameters are set to value 5 each and *macMaxCSMABackoffs* parameter is set to its default value 4. For sake of clarity, we show curves for only selected *macMaxFrameRetries* values.

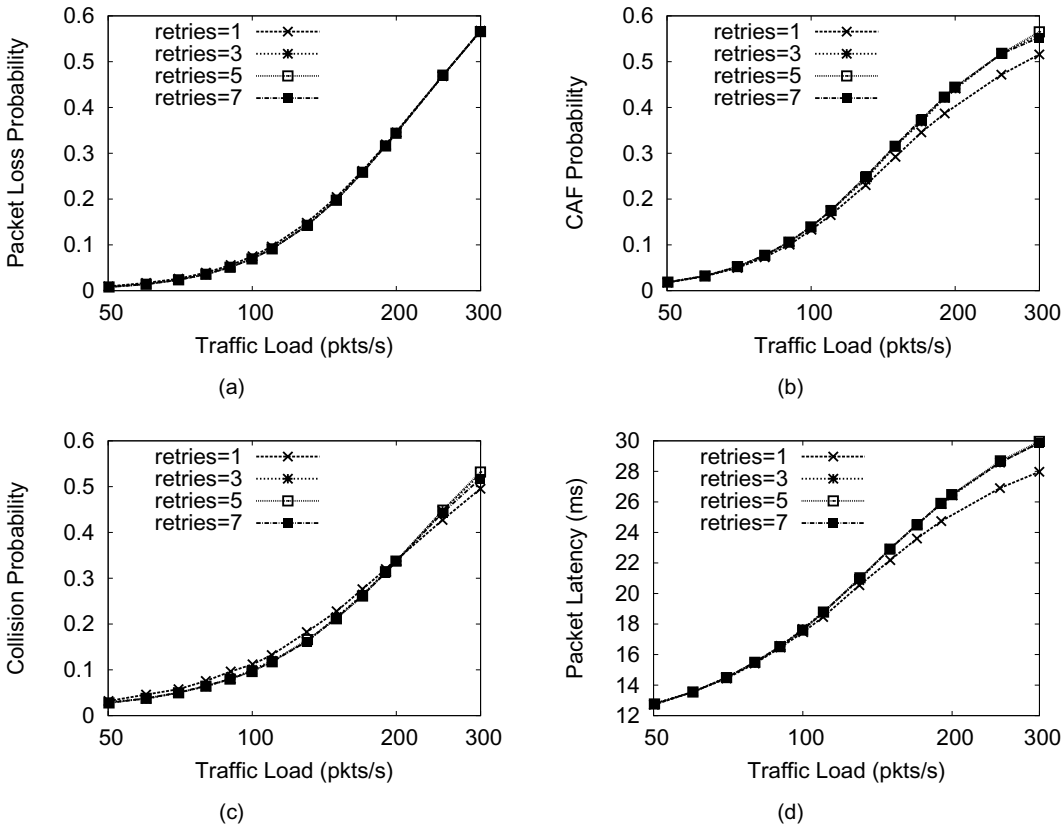

Fig. 7. Impact of macMaxFrameRetries value on performance in the absence of hidden nodes.

Figure 7(a) suggests that any increase in the *macMaxFrameRetries* value beyond 1 does not cause any noticable change in the packet loss probability. However, if we zoom into the packet loss probability curves (Fig. 8), it it clear that there is a small decrease in the packet loss probability for traffic loads upto 150 packets/second or so as *macMaxFrameRetries* value in increased from 1 to 3. Any further increase in the *maxMaxFrameRetries* value does not yield any improvement in the packet loss probability. This result can be attributed to the fact that, although the probability of collision for an individual transmission may be significant (Fig. 7(c)), very few packets are lost due to *collision failures* (i.e. $1 + macMaxFrameRetries$ back-to-back collisions). Figure 9 shows the fraction of losses due to *channel access failure* at different traffic loads and for different *macMaxFrameRetries* values. Note that in the absence of hidden nodes, even for *macMaxFrameRetries* value 1, more than 80% of the packet losses are due to channel access failures. This is true even for small traffic loads at which the probability of packet loss itself is very small. The small number of collision failures taking place with *macMaxFrameRetries* value 1 are mostly eliminated as *macMaxFrameRetries* value increases to 3. Thus, increasing the *macMaxFrameRetries* value beyond 1 does not yield any significant benefits in terms of packet loss probability. Note that this observation hold true in only those scenarios where no packet loss takes place due to signal corruption on the transmission channel. If noise/interference (e.g. 802.11 interference) levels are high in the transmission channel, we expect a larger fraction of packet loss to take place due to collision failures. This scenario has not been investigated in this paper.

As expected and as Fig. 7(b) shows, the change in *macMaxFrameRetries* value does not cause any

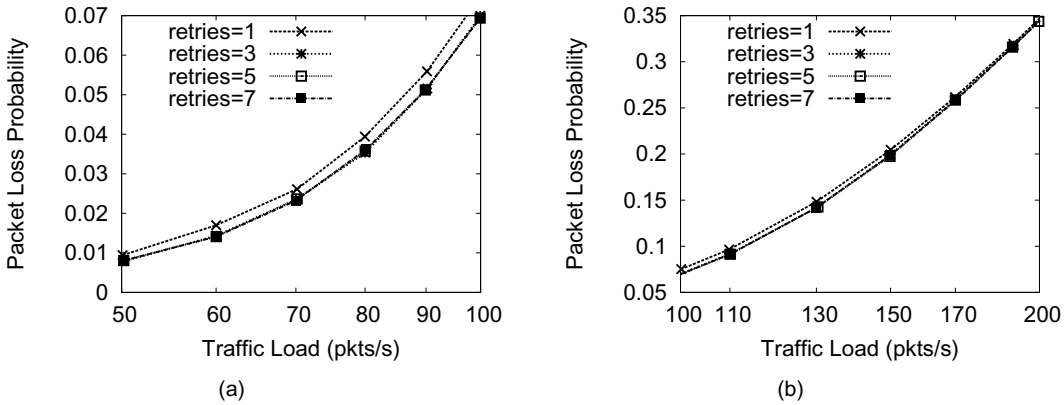

Fig. 8. Zooming in the packet loss probability results regarding the impact of macMaxFrameRetries value in the absence of hidden nodes.

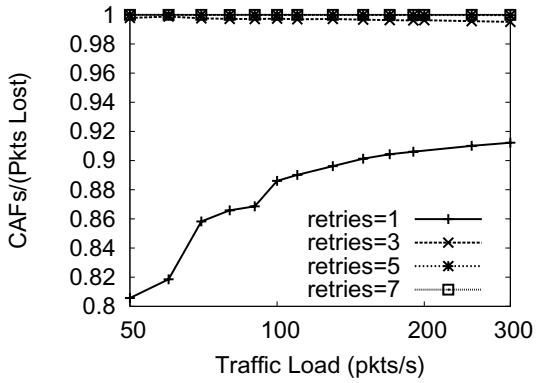

Fig. 9. Ratio of *channel access failures* to total number of lost packets in simulations with different macMaxFrameRetries values in the absence of hidden nodes.

noticable change in the probability of channel acess failures (CAF) except at higher traffic loads. The CAF probability at a given traffic load is primarily determined by the *macMinBE/macMaxBE* and *macMaxCSMABackoffs* parameter values. The *macMaxFrameRetries* parameter has some impact on the CAF probability only at high traffic loads. As Fig. 7(b) shows, at high traffic loads, increase in the *macMaxFrameRetries* value from 1 to 3 causes some increase in the CAF probability as the number of (re)transmissions increase which increases the likelihood of finding the transmission channel busy when a CCA is performed. As per Fig. 7(b), any further increase in the *macMaxFrameRetries* value is not observed to have any noticable impact on the CAF probability.

The probability of collision for an individual transmission is also observed to be largely uneffected by the *macMaxFrameRetries* value (Fig. 7(c)). The probability of collision, as well as the probability of CCA failure, largely depends on how many nodes are competing for channel access at a given time. As we increase the *macMaxFrameRetries* value, we allow a packet to contend for channel access for a longer time and hence compete with a larger set of other nodes, which should increase the probability of collision. However, at low traffic loads, the collisions and hence retransmissions are infrequent. Increasing the *macMaxFrameRetries* value would not have any impact since a packet does not need that many retransmissions for successful delivery. At higher traffic loads, the probability of collision

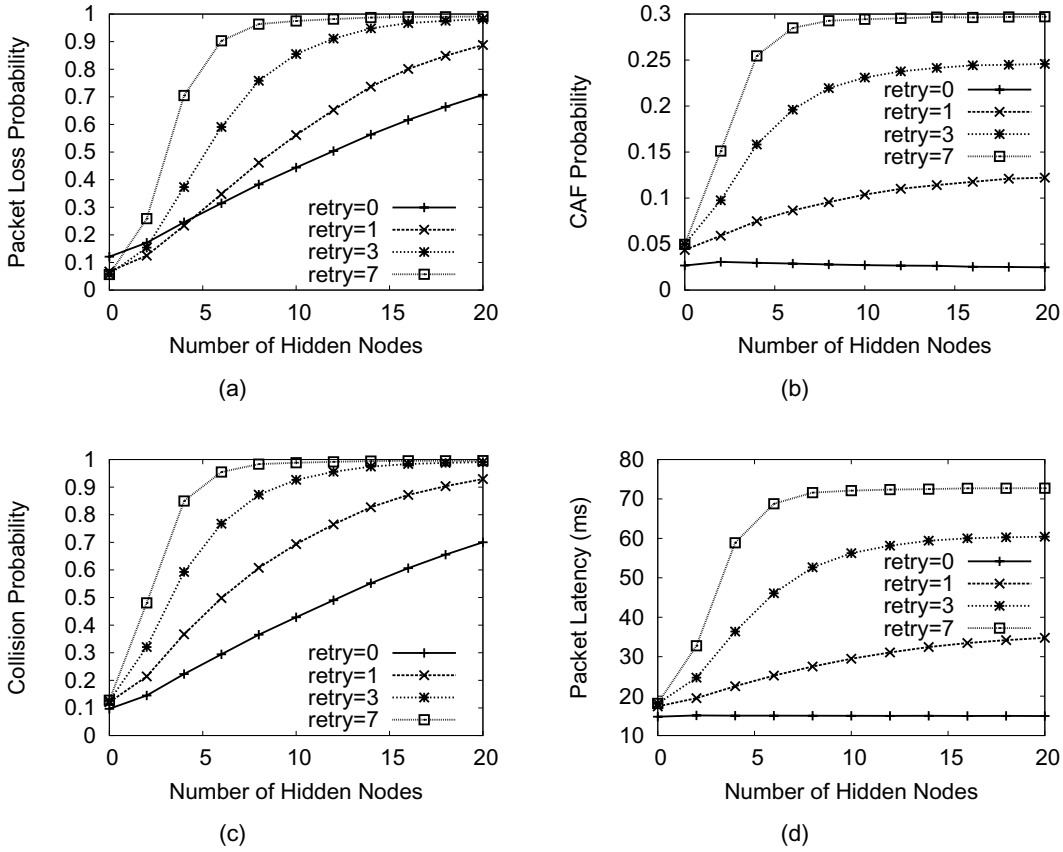

Fig. 10. The impact of macMaxFrameRetries value as the number of hidden nodes increases while the number of observed nodes is 20.

is significant. So, we may expect that increasing the *maxMaxFrameRetries* value should increase the number of transmissions a packet may go through before successful delivery or collision failure. However, this turns out not to be the case since, at high traffic loads, the number of actual transmissions on the channel is so high that a packet is very likely to encounter repeated CCA failures and suffer a channel access failure. Thus, even at high traffic loads, we fail to see any appreciable increase in the probability of collision for a transmission as we increase the value of *macMaxFrameRetries* parameter. This arguement is corroborated by only a marginal increase in the packet latency with increase in the *macMaxFrameRetries* value even at high traffic loads (Fig. 7(d)).

The observations made above regarding the impact of *macMaxFrameRetries* value in the absence of hidden nodes hold true for other *macMaxCSMABackoffs* values as well. In light of these observations, it is clear that *macMaxFrameRetries* $= 3$ is a good setting for this parameter in the absence of hidden nodes. Note that this setting is also the default setting for the parameter as per IEEE 802.15.4 specification [1].

6.1. Impact of macMaxFrameRetries value in the presence of hidden nodes

Figure 10 shows the values of different performance metrics for different values of *macMaxFrameRetries* parameter as the number of hidden nodes increase from 0 to 20 while the number of observed

nodes stays fixed at 20. As was the case with *BE* and *macMaxCSMABackoffs* parameters, the *macMaxFrameRetries* parameter also proves to be largely ineffectual in protecting the observed nodes from the hidden nodes. In the presence of hidden nodes, the increase in the number of transmissions by both observed and hidden nodes, resulting from the increase in the *macMaxFrameRetries* value, hurts both the channel access failure probability (Fig. 10(b)) and the probability of collision (Fig. 10(c)) and hence the overall packet loss probability (Fig. 10(a)) and the packet latency (Fig. 10(d)). In fact, setting *macMaxFrameRetries* value to 0, which essentially means not caring if the acknowledgement for the packet is received or not, results in the best performance as this setting provides the maximum reduction in the number of packet transmissions. Combining this observation with that made in Section 5.1, it seems that setting both *macMaxCSMABackoffs* and *macMaxFrameRetries* parameters to 0 is the best option when the interference from hidden nodes is significant. However, such values for these parameters would clearly result in poor performance in the absence of hidden nodes.

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. Additionally, most papers on IEEE 802.15.4 focus on the beacon-enabled mode of operation. Koubaa et al. [11] performed a simulation based evaluation of the impact of different configuration parameters, including *macMinBE,* on the performance of beacon mode operation of IEEE 802.15.4 MAC and 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. [19] observed that, under *saturated* [3] 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. Ha et al. [5] argued that an individual CCA failure need not necessarily mean high level of channel contention and hence incrementing BE for every individual CCA failure is not justified. They suggested incrementing BE when *macMaxCSMABackoffs* number of consecutive CCA failures occur or when no ack is received for a packet transmission. Further, rather than resetting BE to 0 at the beginning of a new transmission attempt, they suggested retaining the final BE value from the previous transmission attempt, although this value is decremented by 1 if the previous transmission attempt was successful. Zhang et al. [22] suggested a dynamic algorithm to automatically select an appropriate BE value for use in a beacon-enabled network. Their algorithm uses the time it takes to complete a successful CCA in order to estimate the number of nodes in the network, and then select an appropriate BE value.

Some papers prescribed using different BE values to achieve service differentiation. Koubaa et al. [10] suggested using lower *macMinBE* values to achieve low latency for time critical traffic in beacon mode IEEE 802.15.4 networks. Ko et al. [9] suggested allowing nodes that need to transmit frequently to use lower than normal *macMinBE*. Youn et al. [21] suggested achieving priority based service differentiation in IEEE 802.15.4 networks by chosing the CSMA wait duration using different gaussian distribution for different priorities.

Many papers [13,15–17] have suggested that the coordinator should dynamically assign BE values to the associated devices in a beacon-enabled network based on the information it has regarding the individual/total traffic loads and the number of nodes in the cluster. Pang et al. [15] suggested that the

[3] Where a node always has a packet to send.

coordinator determine the BE value to be used by its associated devices during a superframe based on observed channel contention in the previous superframe and convey it to the associated devices in the beacon message. Lee et al. [13] suggested a scheme where the coordinator conveys the BE value to be used by a device for the next transmission in the acknowledgement for the previous transmission.

In our literature search, we could find only a few papers that analyze 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 latency while ignoring any detrimental effect such a setting may have on the packet loss rates. Tao et al. [19] observed that *macMinBE/macMaxBE* parameters have more direct influence on the network throughput than *macMaxCSMABackoffs* parameter. We did not find any papers analyzing the impact of *macMaxFrameRetries* parameter on IEEE 802.15.4 performance.

There are some papers that suggest strategies to mitigate the hidden node problem in beacon-enabled IEEE 802.15.4 networks. Hwang et al. [7] suggested having the coordinator detect hidden node situations and modify grouping, and thus scheduled awake periods, to avoid hidden nodes. Harthikote-Matha et al. [6] concluded that hidden nodes have a significant impact on throughput and energy efficiency in IEEE 802.15.4 slotted CSMA and suggest using higher BO values, thus longer active periods, to improve throughput and reduce energy use. Zheng and Lee [23] observed that the majority of collisions in a beacon enabled star environment with many hidden nodes are the result of the hidden node problem. Koubbaa et al. [12] suggested a hidden-node avoidance mechanism that detects hidden nodes and groups these nodes into different active periods.

8. Conclusions

In this paper, we analyzed the impact of *macMinBE/macMaxBE*, *macMaxCSMABackoffs* and *macMaxFrameRetries* parameters on the performance of beaconless IEEE 802.15.4 networks under different traffic load conditions and under different levels of interference from the hidden nodes.

The main conclusions regarding the impact of *macMinBE/macMaxBE, macMaxCSMABackoffs* and *macMaxFrameRetries* parameters when the interference from hidden nodes is not significant are as follows.

At low to moderate traffic loads,[4] increasing the *macMinBE/macMaxBE* values, beyond their default values, helps reduce the loss rates at the expense of increased packet latency. Consider the set of nodes competing for channel access at any given time. At low/moderate traffic loads, this set consists of only a small number of nodes. Another node may not generate a packet to transmit, and hence join this set, for relatively long time. Increasing the *macMinBE/macMaxBE* values increases the range of CSMA wait times. Thus, competing nodes become less likely to finish their CSMA waits when another node is performing RX-to-TX turnaround or transmitting a packet. Thus, increasing the *macMinBE/macMaxBE* values leads to reduction in both the probability of collisions as well as CCA failures. Increasing the *macMaxCSMABackoffs* value allows a node to tolerate more CCA failures in a transmission attempt before a *channel access failure* is declared and hence helps reduce the packet loss rate. The downside of increasing the *macMinBE/macMaxBE* and *macMaxCSMABackoffs* values is increased packet latency due to increased CSMA wait times as well as more CSMA waits per transmission attempt on average.

[4]Compared to the theoretical maximum throughput that can be carried on a IEEE 802.15.4 network. For example, with 133 byte long packets, the theoretical maximum throughput was earlier calculated to be 208.33 packets/second.

The *macMaxFrameRetries* parameter does not have any significant impact on performance as repeated collisions are rare and most of the packet loss takes place due to channel access failures.

Once the traffic load crosses a threshold, configurations with higher (than default) values for *macMinBE/macMaxBE* and *macMaxCSMABackoffs* parameters result in higher loss rates than the default configuration. At high traffic loads, the set of nodes competing for channel access at any given time is large. Hence, increasing the range of CSMA wait times does not reduce the probability of a node finishing its CSMA wait during the time when another node is doing RX-to-TX turnaround or transmitting a packet. Thus, increasing the *macMinBE/macMaxBE* does not help. Similarly, increasing the number of CCA failures allowed in a transmission attempt only increases the time a packet stays in competition for channel access, thereby exasperating the competition. Hence, increasing the *macMaxCSMABackoffs* value does not help either. As in case of low traffic loads, the *macMaxFrameRetries* parameter does not have a significant impact on performance under heavy traffic loads either. Overall, it appears that *CSMA/CA* based IEEE 802.15.4 MAC does not work very well under high traffic load scenarios and it may not be possible to avoid high loss rates just by manipulating the configuration.

When the interference from hidden nodes is significant, the best strategy is to reduce the number of transmissions. This can be done by setting both *macMaxCSMABackoffs* and *macMaxFrameRetries* parameters to 0. However, our investigation suggests that altering the values of IEEE 802.15.4 MAC parameters is mostly ineffective in dealing with the problem of hidden nodes. If the frequency of transmissions from the hidden nodes is significant, IEEE 802.15.4 operation essentially breaks down. The use of *request to send/clear to send* (RTS/CTS) mechanism, used in IEEE 802.11 networks to deal with hidden nodes, may be useful in IEEE 802.15.4 networks as well if such RTS/CTS packets are significantly smaller than the data packets, which themselves are less than 133 bytes in size. However, the use of RTS/CTS mechanism in IEEE 802.15.4 operation may increase the complexity and hence cost of IEEE 802.15.4 hardware. Another option is to allow the use of multiple transmission channels to deal with hidden nodes. If the hidden nodes use a different transmission channel, their transmissions won't affect the regular nodes. Such a scheme would require the destination nodes to listen on multiple channels. This is plausible in IEEE 802.15.4 networks if the destination nodes are mostly *mains*-powered *full function devices* [1]. However, the assignment of transmission channels to use by different sensor nodes is a non-trivial problem. One may require a higher-level tool to split the sensor nodes into *islands*, where nodes with in an island are in each other's radio range, and assign different transmission channels to different islands.

References

[1] Part 15.4: WirelessMAC and PHY layer specifications for low-rate wireless personal area networks, IEEE Std 802.15.4–2006, 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, T. Watteyne, T. Winter and D. Barthel, Urban WSNs Routing Requirements in Low Power and Lossy Networks. Internet-Draft draft-ietf-roll-urban-routing-reqs-02, IETF, October 2008. Work in progress.

[4] M. Goyal, Zigbee/IEEE 802.15.4 module for NS2 simulator, 2008.

[5] J.Y. Ha, T.H. 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) (May 2007), 461–463.

[6] M. Harthikote-Matha, T. Banka and A.P. Jayasumana, Performance degradation of IEEE 802.15.4 slotted CSMA/CA due to hidden nodes. Local Computer Networks, 2007. LCN 2007. 32nd IEEE Conference on, pages 264–266, Oct. 2007.

[7] L.-J. Hwang, S.-T. Sheu, Y.-Y. Shih and Y.-C. Cheng, Grouping strategy for solving hidden node problem in IEEE 802.15.4 LR-WPAN. Wireless Internet, 2005. Proceedings. First International Conference on, pages 26–32, July 2005.

[8] 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) (April 2008), 238–240.
[9] J.-G. Ko, Y.-H. Cho and H. Kim, Performance evaluation of IEEE 802.15.4MAC with different backoff ranges in wireless sensor networks. Communication systems, 2006. ICCS 2006. 10th IEEE Singapore International Conference on, pages 1–5, Oct. 2006.
[10] 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. In Proc. of the Workshop of Real-Time Networks, Satellite Workshop to ECRTS 2006, July 2006.
[11] A. Koubaa, M. Alves, B. Nefzi and E. Tovar, A comprehensive simulations study of slotted CSMA/CA for IEEE 802.15.4 wireless sensor networks, *In IEEE International Workshop on Factory Communication Systems* **27** 2006, 183–192.
[12] A. Koubaa, R. Severino, M. Alves and E. Tovar, H-NAMe: Specifying, implementing and testing a hidden-node avoidance mechanism for wireless sensor networks.
[13] 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.
[14] S. McCanne and S. Floyd, ns network simulator.
[15] A.-C. Pang and H.-W. Tseng, Dynamic backoff for wireless personal networks. Global Telecommunications Conference, 2004. GLOBECOM '0, *IEEE* **3** (Nov.-3 Dec. 2004), 1580–1584.
[16] 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.
[17] 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.
[18] D. Rohm, M. Goyal, H. Hosseini, A. Divjak and Y. Bashir, *Configuring Beaconless Ieee 802.15.4 Networks Under Different Traffic Loads*, In Proceedings of IEEE 23rd International Conference on Advanced Information Networking and Applications (AINA-09), May 2009.
[19] Z. Tao, S. Panwar, D. Gu and J. Zhang, Performance analysis and a proposed improvement for the IEEE 802.15.4 contention access period, *Proc. of IEEE WCNC* **4** (2006), 1811–1818.
[20] A. Wheeler, Commercial applications of wireless sensor networks using zigbee, *IEEE Communications Magazine* **45**(4) (April 2007), 70–77.
[21] M.J. 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.
[22] Y. Zhang, P. Xu, G. Bi and F.S. Bao, *Analysis of energy efficiency and power saving in IEEE 802.15.4*, IEEE Wireless Communications and Networking Conference, pages 3330–3334, 2007.
[23] J. Zheng and M.J. Lee, Low rate wireless personal area networks (lr-wpans) – NS2 simulation platform.
[24] Zigbee Alliance, Zigbee specification, December 2006.

Dawn Rohm is currently a graduate student at the University of Wisconsin Milwaukee working under the supervision of Dr. Mukul Goyal. She also works as an instructor and unix systems administrator at St. Norbert College in De Pere, Wisconsin. She received her M.S. in Computer Science from the University of Wisconsin – Milwaukee in 2000, and her B.S. in Mathematics/Computer Science from St. Norbert College in 1997.

Mukul Goyal is an Assistant Professor in Computer Science department at University of Wisconsin Milwaukee. He received a PhD in Computer and Information Science from Ohio State University. His research interests include the performance evaluation of computer networks.

Hossein Hosseini is currently the Chair of Computer Science at University of Wisconsin-Milwaukee (UWM), where he has developed Computer Engineering Program and Computer Networks Curriculum. He is a co-director of the Computer Networks Laboratory at UWM. He earned his MS and PhD degrees from Iowa State and University of Iowa, in 1977, and 1982; respectively. His area of interest includes Computer Networks, Computer Architecture, and Fault-Tolerance. He has published over 100 referred journal and conference papers. He has graduated over 60 master and 9 PhD students. He has received funding from NSF and industry. He has served as an editor of a journal, and program committee members for several international conferences.

Yusuf Bashir is a senior engineer at Johnson Controls, Inc, Milwaukee Wisconsin. He received his BS and MS in electrical engineering from Temple University, Philadelphia, PA. His research interests include wireless communications and routing algorithms. He is involved in the application of wireless technology in building automation and IT systems.

August Divjak is a senior staff engineer at Johnson Controls, Inc, Milwaukee Wisconsin. He received his BS in electrical engineering from Milwaukee School of Engineering (MSOE), Milwaukee, Wisconsin. His research interests include wireless communications and systems modeling. He is involved in the application of wireless technology and control technology in building automation.