A Stochastic Model for Beaconless IEEE 802.15.4 MAC Operation

M. Goyal*,a, D. Rohma, W. Xiea, S.H. Hosseini, K.S. Trivedi**,b, Y. Bashirc, A. Divjakc

aUniversity of Wisconsin - Milwaukee, Milwaukee WI 53201, USA
bDuke University, Durham NC 27708, USA
cJohnson Controls Inc., Milwaukee WI 53202, USA

Abstract
IEEE 802.15.4 is a popular choice for MACPHY protocols in low power and low data rate wireless sensor networks. In this paper, we develop a stochastic model for the beaconless operation of IEEE 802.15.4 MAC protocol. Given the number of nodes competing for channel access and their packet generation rates, the model predicts the packet loss probability and the packet latency. The model can also account for the impact of hidden nodes in certain situations. We compared the model predictions with NS2 simulation results and found an excellent match between the two for a wide range of the packet generation rates and the number of competing nodes in the network.

Key words: IEEE 802.15.4, Wireless Sensor Networks, Medium Access Control Protocols, Stochastic Analysis, Unslotted Carrier Sense Multiple Access

1. Introduction
IEEE 802.15.4 [1] provides physical (PHY) and medium access control (MAC) layer functionality in low power and low data rate wireless sensor
networks (WSN). Wireless communication among sensor devices, enabled by IEEE 802.15.4 technology, is increasingly replacing the existing wired technology in a wide range of monitoring and control applications in home, urban, building and industrial environments [2, 3, 4, 5]. IEEE 802.15.4 MAC operation is based on carrier sense multiple access with collision avoidance (CSMA/CA). Thus, an IEEE 802.15.4 node competes with all the nodes in its radio range for access to the transmission channel.

The CSMA/CA based networks are known to suffer from performance deterioration with increase in the number of nodes competing for channel access at any given time, which in turn depends on both the total number of nodes in each other’s radio range and their packet generation rates. Although, in currently deployed IEEE 802.15.4 based networks, an individual node typically has only a small number of nodes in its radio range, this situation will probably change in future. Future IEEE 802.15.4 networks may consist of several thousand nodes distributed over a large area and an individual node may possibly have hundreds of nodes in its radio range [3]. Although IEEE 802.15.4 is designed to be a low data rate protocol, it is not uncommon for IEEE 802.15.4 nodes to occasionally have relatively high packet generation rates (of the order of few packets per second) over some time intervals. A combination of large number of nodes in each other’s radio range and high packet generation rates may have a severe impact on the functionality of the WSN. Thus, it is important to understand how the performance - the packet loss probability and the packet latency - over a single hop in an IEEE 802.15.4 based network changes as the number of nodes in each other’s radio range and/or their packet generation rates increase.

In this paper, we develop a stochastic model for popular beaconless operation of IEEE 802.15.4 MAC protocol. Given the number of nodes competing for channel access and their packet generation rates, the model can very accurately predict the packet loss probability as well as the packet latency. Under certain conditions, the model can also take in account the impact of transmissions by hidden nodes on the packet loss probability and latency. Thus, the stochastic model presented in this paper can serve as a useful tool in the design of WSNs based on IEEE 802.15.4. This paper is a significant expansion of a preliminary version [6] and contains the following additional material:

- This paper includes a comprehensive survey of published literature regarding the modeling of CSMA-based protocols;
• This paper includes a detailed explanation of the impact of signal to noise ratio deterioration on IEEE 802.15.4 PHY-level packet loss rates. This explanation is a part of the argument regarding why it is reasonable to ignore such impact while modeling IEEE 802.15.4 performance;

• This paper extends the stochastic model presented in [6] to account for the impact of hidden nodes, under certain conditions, on the packet loss probability and latency in a beaconless IEEE 802.15.4 network.

The rest of the paper is organized as follows. Section 2 presents a brief overview of IEEE 802.15.4 PHY and MAC protocols. Section 3 contains a comprehensive survey of the existing work on stochastic modeling of CSMA based protocols. Section 4 describes the impact of signal to noise ratio on IEEE 802.15.4 PHY-level packet loss rates. Section 5 describes different ways a packet collision may occur in the operation of a beaconless IEEE 802.15.4 network. Section 6 presents the stochastic model for beaconless IEEE 802.15.4 MAC operation and Section 7 evaluates the model’s accuracy by comparing model predictions against simulation results. Finally, Section 8 concludes the paper.

2. About IEEE 802.15.4

As mentioned before, IEEE 802.15.4 protocol provides PHY and MAC layer functionality in low power and low data rate WSNs. Typically, IEEE 802.15.4 constitutes the PHY/MAC layer of a larger protocol suite (e.g. Zigbee [7]), where the upper layers provide multi-hop routing and other functionality to allow formation of large-scale WSNs.

2.1. Packet Transmission and Reception in IEEE 802.15.4 PHY Operation in 2450 MHz Range

IEEE 802.15.4 PHY layer is responsible for transmission and reception of data to/from the radio channel and can operate in many different frequency ranges. Popular 2450 MHz operation of IEEE 802.15.4 PHY layer offers a maximum data rate of 250 Kbps and is based on direct sequence spread spectrum (DSSS) technology employing offset quadrature phase-shift keying (O-QPSK) modulation. There are 16 communication channels available in 2450 MHz range and each channel is 5 MHz wide.
Table 1: 32-chip PN Sequences for 4-bit Symbols [1]

Each packet in 2450 MHz PHY operation begins with a 5 byte (or 10 symbols\(^1\)) long synchronization header and a 1 byte (or 2 symbols) long PHY header. These fields are followed by a variable length (up to 127 bytes) PHY payload. The actual transmission takes place 1 symbol (or 4 bits) at a time. A 4-bit long symbol is translated to one of 16 nearly orthogonal 32-chip long pseudo-random noise (PN) sequences shown in Table 1. The PN sequences for successive data symbols are concatenated and the resulting chip stream is modulated onto the carrier using O-QPSK with even-indexed chips being modulated onto the in-phase carrier and odd-indexed chips modulated onto the quadrature-phase carrier.

The packet reception at the PHY layer works as follows. The received signal is demodulated to retrieve the chip stream and the individual 32-chip sequences. A received sequence is compared against 16 valid PN sequences and the one showing the smallest hamming distance from the received sequence is chosen as the transmitted sequence and is translated back to the corresponding symbol. Here, the hamming distance refers to the number of chip positions the two chip sequences differ in [8]. Thus, a transmitted symbol will be correctly identified as long as the hamming distance between the received sequence and the transmitted sequence is smaller than the hamming distance between the received sequence and any other valid sequence. Any error in identifying the transmitted symbols is likely to be identified when the packet checksum is calculated and compared with the checksum carried in the packet’s header.

\(^1\)Each symbol consists of 4 bits.
In this paper, we assume the popular 2450 MHz range operation of IEEE 802.15.4 PHY layer.

2.2. IEEE 802.15.4 MAC Operation

IEEE 802.15.4 MAC operation has two modes - beacon-enabled and beaconless. The beacon-enabled mode allows splitting of time into multiple active durations with a cluster consisting of a coordinator and its associated nodes having exclusive access to the transmission channel during its active duration. The coordinator broadcasts a beacon to inform other nodes in the cluster about the beginning of the cluster’s active duration. The cluster nodes compete for channel access during their active period using a slotted CSMA/CA algorithm. In the beaconless operation, there is no division of time into active durations and a node competes for channel access with other nodes in its radio range using an unslotted CSMA/CA algorithm. In this paper, we have focused on the beaconless operation of IEEE 802.15.4 MAC layer.

As per the unslotted CSMA/CA algorithm, the source node begins a transmission attempt with a CSMA wait for a random number of backoff periods (=20 symbols each) between 0 and $2^{BE} - 1$. Here, $BE$ refers to a variable called the backoff exponent that is initially set to the value of $macMinBE$ parameter (by default 3). After the CSMA wait, the source 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 the value of $macMaxBE$ parameter, which is 5 by default) and repeats the procedure. If the CCA fails even after $macMaxCSMABackoffs$ (by default 4) CSMA waits, a channel access failure is declared and any further attempt to transmit the packet is abandoned. If the CCA succeeds, the source node performs an RX-to-TX turnaround and transmits the packet. The propagation delay for the packet is expected to be negligible. On receiving the packet, the destination node performs an RX-to-TX turnaround and sends the acknowledgement (ACK) if required by the source. No CSMA wait is performed for ACK transmission. As discussed in Sect. 5, the transmitted
packet or its ACK may suffer a collision. In this case, the source node waits for the *macAckWaitDuration* (typically 54 symbols for 2.4GHz operation) for the ACK to arrive and then proceeds with next attempt to transmit the packet. The source node can make up to *macMaxFrameRetries* (3 by default) further attempts to transmit the packet and receive the ACK. The failure to receive an ACK even after *macMaxFrameRetries* +1 attempts causes the IEEE 802.15.4 MAC layer to accept failure in sending the packet. Such a failure is referred to as *collision failure* in the following discussion.

3. Stochastic Models of CSMA based Protocols: An Overview

*Carrier Sense Multiple Access* (CSMA) protocols require a node to listen to the channel (*sense the carrier*) and proceed with the transmission only if the channel is idle [9]. Such carrier sensing can significantly reduce the probability of collision among transmissions if the propagation delays between nodes are much smaller than the packet transmission times. In their seminal work [9], Kleinrock and Tobagi classify CSMA protocols as either *non-persistent* or *p-persistent* and analyze their throughput-delay performance. In non-persistent CSMA, the failure to find the channel idle causes a node to undergo a random CSMA wait before sensing the channel again. Therefore, IEEE 802.15.4 MAC can be classified as a nonpersistent CSMA protocol.

Another seminal work in CSMA/CA analysis is Bianchi’s model [10] of IEEE 802.11 *distributed coordination function* (DCF) [11]. Bianchi presented a model for IEEE 802.11 DCF operation where a fixed number of nodes compete for channel access under the *saturated* condition, i.e. each node begins the process of sending the next packet as soon as the process for the previous packet is over. The model assumes that the probability of collision for a packet transmission is fixed irrespective of the number of collisions already suffered by the packet. This assumption allows the state of a single node to be modeled as a *discrete-time markov chain* [12], which is then used for further analysis. Bianchi’s model for IEEE 802.11 DCF operation inspired a number of models for slotted, i.e. beacon-enabled, IEEE 802.15.4 operation [13, 14, 15, 16, 17, 18, 19, 20, 21].

Next, we present an overview of the existing analytical models for both beacon-enabled and beaconless IEEE 802.15.4 MAC operation. Beacon-enabled (or slotted) 802.15.4 operation differs from the beaconless (or unslotted) 802.15.4 operation in several ways. Apart from the difference arising from slotted/unslotted nature of CSMA/CA algorithm used in two modes,
some differences that significantly affect the modeling process are as follows.

In beacon-enabled operation, a node needs to verify that the transmission channel is idle for two consecutive backoff periods before it can begin the packet transmission. This means that a node needs to have two back-to-back CCA successes, where the CCAs are performed at the beginning of two back-to-back backoff periods, before it can transmit a packet. In beaconless operation, only one CCA success is required for packet transmission. In beacon-enabled operation, the channel time is divided into superframes, where each superframe has an active period as well as an inactive period. The active period is further divided into the contention access period (CAP) and contention free period (CFP). In both modes of operation, the CSMA wait is a random number of backoff periods in the range $0$ to $2^{BE} - 1$. However, in beacon-enabled operation, if the chosen CSMA wait duration is larger than the remaining CAP duration, the countdown of the number of remaining backoff periods in the CSMA wait is paused at the end of the CAP and resumed at the start of the CAP in the next superframe. Further, in beacon-enabled operation, when a node completes its CSMA wait, it determines if the remaining steps in the packet transmission process (2 CCAs, packet transmission and ACK reception) can be completed before the end of the CAP. If this is not possible, the node waits for the start of the CAP in the next superframe and repeats the whole procedure starting with another randomly chosen CSMA wait.

Ramachandran et.al. [22] analyzed beacon-enabled IEEE 802.15.4 operation by modeling the behavior of an individual node and the transmission channel using two inter-related discrete time markov chains. This model assumes that the CSMA wait duration during a particular backoff stage is determined as per a geometric distribution with the same mean value as the uniform distribution suggested in IEEE 802.15.4 specification. This assumption allows the probability that the CSMA wait during a particular backoff stage gets over in a given backoff slot to be fixed irrespective of the time already spent in the CSMA wait. Our model makes a similar assumption: the CSMA wait duration is assumed to be an exponentially distributed continuous variable with same mean as the uniform distribution suggested in IEEE 802.15.4 specification.

Singh et.al. [23] presented a markov renewal sequence based model for beacon-enabled IEEE 802.15.4 operation where a fixed number of nodes compete for channel access under saturated condition. The authors then adapted the model for the situation where the packet generation rate at each node

7
is finite. At finite rates, each node is assumed to contend for channel access for only a fraction of time ($\rho$), which is used to determine the probability that a certain number of nodes ($m$) are contending at any given time. Using $m$ as the number of "saturated" mode nodes, the authors determine the expected rate at which the packets depart (either after successful transmission or discard) for given $\rho$ value. $\rho$ is determined as the value that makes the packet departure rate at a node equal to the packet generation rate. Our model is similar to Singh’s model in the sense that our model is also based on calculating the probability that a certain number of nodes are contending for channel access at any given time.

Some other stochastic models focussed on beacon-enabled IEEE 802.15.4 operation are briefly discussed next. Tao et.al. [13] presented a model, based on a discrete time markov chain, for beacon-enabled operation where a fixed number of saturated state nodes compete for channel access. Misic et.al. [14] used a discrete time markov chain to model the CSMA/CA behavior in beacon-enabled operation. This markov chain was then used as a building block to model the operation of a node, where a node can send packets to its coordinator via direct transmission or receive packets from the coordinator via indirect transmissions. Jung et.al. [24] presented a discrete markov chain model for beacon-enabled operation under unsaturated traffic conditions taking in account the inactive periods in the superframes and the possibility of a transmission getting deferred until the next superframe. Pollin et.al. [15] used a discrete markov chain to model the behavior of a node sending unacknowledged packets in a beacon-enabled network. In [16], Pollin et.al. upgraded their model to include packet acknowledgements. Ling et.al. modeled beacon-enabled IEEE 802.15.4 operation of a node under saturated traffic conditions as a multi-level renewal process [25]. Shu et.al. [26] used a non-stationary markov chain to determine the fraction of nodes that are able to successfully send their unacknowledged packets during a superframe in a beacon-enabled scenario.

Kim et.al. [27] presented a model for beaconless IEEE 802.15.4 MAC operation. This paper also identified the two collision windows (described in Sect. 5) in beaconless IEEE 802.15.4 operation and the need for CCA duration to exceed the RX-to-TX turnaround time in order to avoid collisions involving ACKs. This paper models an IEEE 802.15.4 node as an $M/G/1$ queue with the packet latency (i.e. the time MAC layer takes to successfully transmit or discard the packet) as the service time of the queue. The model assumes that the CCA duration is set to be more than the turnaround time.
and hence no ACK collisions are possible. The main weakness of this model is that it completely ignores the collisions in packet transmissions under the assumption that such collisions are infrequent. This assumption is not true in high traffic load situations. In Section 5, we described how multiple packet transmissions may collide with each other under beaconless IEEE 802.15.4 operation. Later in this paper (Section 6.6), we calculate the probability of collision for a transmission. As demonstrated in Fig. 9, the probability of collision is significant at high traffic loads and hence the beaconless IEEE 802.15.4 model we present takes such collisions into account.

Finally, we briefly discuss other previous work that has influenced our model. Burchfield et.al. [28] calculated the average time spent doing CSMA waits during a transmission attempt for a given level of channel activity and thus the total time required for a transmission attempt in beaconless IEEE 802.15.4 MAC operation. However, the authors did not attempt to determine the channel activity level when a number of nodes, generating traffic at a certain rate, compete for channel access. Additionally, the paper identified extra latencies in the packet transmission process in IEEE 802.15.4 hardware implementations. These extra latencies originate from interrupt service times, limited available memory and processor-transceiver communication latency and prevent actual throughput from reaching the theoretical maximum values. Timmons and Scanlon [29] studied the possible life times of IEEE 802.15.4 based sensors implanted in the human body. As part of this study, the authors determined the average number of CSMA waits required in a transmission attempt given a certain probability of finding the channel idle during a CCA. However, the authors did not describe how this later probability is to be calculated when a given number of nodes, generating traffic at a certain rate, compete with each other for channel access.

4. Impact of Signal to Noise Ratio on IEEE 802.15.4 PHY-level Packet Loss Rate

In this section, we evaluate the impact of signal to noise ratio (SNR), defined as the ratio of the signal and noise energy levels in the communication channel, on the PHY-level packet loss rates on an IEEE 802.15.4 link under the additive white gaussian noise and Rayleigh fading models [30]. We show that IEEE 802.15.4 PHY-level packet loss rate has a step-like response to the SNR deterioration. In other words, the packet loss rate is largely unaffected by SNR deterioration as long as SNR is more than a threshold. However,
even a small (less than 10 dB; some times as small as 3 dB) deterioration in
SNR beyond this threshold causes the packet loss rate to approach 1. This
result implies that SNR is either good enough so that the PHY noise has
negligible impact on IEEE 802.15.4 operation or SNR is so bad that IEEE
802.15.4 operation is not possible. Thus, it is reasonable to ignore the PHY
noise in the modeling process.

In the following discussion, Section 4.1 calculates the probability that an
IEEE 802.15.4 PHY node fails to correct an \( n \)-chip error in the received 32-
chip sequence sent for a 4-bit symbol. Section 4.2 builds on this analysis to
determine the probability of receiving a packet in error on an IEEE 802.15.4
link operating in 2450 MHz range given the signal to noise ratio (SNR) under
additive white gaussian noise and Rayleigh fading models. This section also
analyzes the impact of SNR deterioration on the IEEE 802.15.4 PHY-level
packet loss rate.

### 4.1. The Probability of Symbol Error in IEEE 802.15.4 PHY Operation

As mentioned in Section 2.1, the receiver correctly identifies the transmis-
ted symbol if the hamming distance between the received and the transmitted
sequence is smaller than the hamming distance between the received sequence
and any other valid sequence. In this section, we calculate the probability
that the receiver fails to identify the transmitted symbol correctly, i.e., the
hamming distance between the received sequence and the transmitted se-
quence is equal to or higher than that between the received sequence and
another valid sequence.

Table 2 shows the hamming distance between each pair of 32-chip PN
sequences shown in Table 1. Table 2 shows that each valid chip sequence
differs from other valid chip sequences in at least 12 positions and atmost 20
positions. A closer look reveals that each valid chip sequence has:

- a hamming distance of 12 from 2 other valid chip sequences;
- a hamming distance of 14 from 2 other valid chip sequences;
- a hamming distance of 16 from 3 other valid chip sequences;
- a hamming distance of 18 from 2 other valid chip sequences; and
- a hamming distance of 20 from 6 other valid chip sequences.

Consider the following scenario:
Table 2: Hamming distance between each pair of 32-chip PN Sequences

- The hamming distance between the received 32-chip sequence \( R \) and the sent 32-chip sequence \( S \) is \( x \);

- The hamming distance between the received sequence \( R \) and another valid 32-chip sequence \( A \) is \( y \);

- The hamming distance between sequence \( S \) and sequence \( A \) is \( d \);

- Sequences \( R \) and \( A \) differ in \( z \) of the \( d \) chips, where \( S \) and \( A \) are different, and in \( y - z \) of the \( 32 - d \) chips, where \( S \) and \( A \) are same.

The last point mentioned above implies that sequences \( R \) and \( S \) differ in \( d - z \) of the \( d \) chips, where \( S \) and \( A \) are different, and in \( y - z \) of the \( 32 - d \) chips, where \( S \) and \( A \) are same. In other words, \( x = d - z + y - z = d + y - 2z \). Thus, \( x < y \) if \( d < 2z \). Thus, the receiver will not mistake \( A \) as the sent sequence as long as \( d < 2z \) or \( z > d/2 \).

Since the minimum hamming distance between any two valid chip sequences is 12, any 5 or fewer chip errors between the sent and the received sequences can always be corrected. This is because, in these cases, the sent sequence would still have smaller hamming distance from the received sequence than any other valid sequence. Similarly, it can be shown that 26 or more chip errors between the sent and the received sequence can never be corrected. This is because, in these cases, every other valid sequence will have a smaller or equal hamming distance from the received sequence than the sent sequence. For example, if the hamming distance between the sent (\( S \)) and received (\( R \)) sequence is 26 and that between the sent and another valid sequence (\( A \)) is 12, then the maximum hamming distance between \( R \)
4.2. Signal to Noise Ratio Versus Packet Error Rate in 2450 MHz IEEE 802.15.4 PHY Operation

As discussed in Section 2.1, the chip sequences for successive data symbols are concatenated and the resulting chip stream is modulated onto the carrier using offset quadrature phase shift keying (O-QPSK). In this section, we combine the probability of a chip error for an O-QPSK modulated chip stream for a given signal to noise ratio (SNR) with the symbol error probability determined in the previous section to obtain the PHY-level packet error rate for 2450 MHz IEEE 802.15.4 operation.

The probability of bit error (or the bit error rate) for an O-QPSK modulated signal under additive white gaussian noise (AWGN) is given by [8]:

\[ B = \frac{1}{2} \text{erfc}(\sqrt{\gamma}) \]  

(1)
where \( \text{erfc} \) is the complementary error function, \( \gamma \) is the ratio of the signal energy to the noise energy.

AWGN does not take in account the impact of fading. The probability of bit error (or the bit error rate) for an O-QPSK modulated signal under Rayleigh fading model, which represents the scenario where there is no significant line of sight component between the transmitter and receiver, is given by [8]:

\[
B = \frac{1}{2} \left( 1 - \sqrt{\frac{\gamma}{1 + \gamma}} \right)
\]  

(2)

where \( \gamma \) is the signal to noise ratio.

If \( B \) is the probability of receiving a chip in error and \( P_{\text{symerr}}(n) \) is the probability of symbol error when \( n \) chips are received in error (Table 4.1), the probability \( S \) of interpreting a symbol incorrectly (or the symbol error rate) is given by:

\[
S = \sum_{n=1}^{32} {32 \choose n} B^n (1 - B)^{32-n} \times P_{\text{symerr}}(n)
\]  

(3)

A packet is received in error if any of its symbols is received in error. Thus, if a packet is \( m \) bytes (or \( 2^m \) symbols) long, the probability \( P \) of receiving a packet in error (or the packet error rate) is given by:

\[
P = 1 - (1 - S)^{2^m}
\]  

(4)

Figures 1(a) and 1(b) show the deterioration in bit, symbol and packet error rates as the SNR deteriorates under AWGN and Rayleigh fading model respectively. The packet error rates are calculated assuming the packet size to be 133 bytes (or 266 symbols), which is the maximum possible packet size under IEEE 802.15.4. These figures clearly illustrate that the packet error rate quickly deteriorates from 0 to 1 as the SNR deteriorates beyond a threshold. Figures 1(c) and 1(d) present a close up view of the same information focusing on the region of sudden transition in the packet error rate. As these figures show, the packet error rate changes from 0 to 1 as the SNR deteriorates from 1 dB to -3 dB under AWGN model and from 6 dB to -1 dB under Rayleigh fading model. The step-like increase in the packet error rate with SNR deterioration is due to the packet error rate’s dependence on the symbol error rate, which in turn depends on the bit error rate. As the figures show, the SNR deterioration results in moderate increase in the
Figure 1: The impact of SNR deterioration on the bit, symbol and packet error rates for 2450 MHz Operation of IEEE 802.15.4 PHY layer.

bit error rate that causes much steeper increase in the symbol error rate, which in turn causes almost step-like increase in the packet error rate. Thus, we can conclude that the PHY-level packet error rate on an IEEE 802.15.4 link shows a step-like increase from 0 to 1 as the SNR deteriorates beyond a threshold.

5. Packet Collision Scenarios in Beaconless IEEE 802.15.4 Networks

Even though the IEEE 802.15.4 nodes use a collision avoidance algorithm to compete for channel access, collisions do occur for reasons described next. Hidden nodes: Some nodes in a WSN 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. However, 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:

- 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 2 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.

- A destination node (say B) needs to complete an RX-to-TX turnaround before it can send the ACK 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 ACK. Figure 3 refers to this 4 symbol duration as the second collision window. Note that the second collision window is the result of CCA duration being less than the RX-to-TX turnaround time. Also, note that the second collision window exists only if no collision takes place in the first collision window.

- A destination node would ignore a packet transmission if it begins before the destination has completed the TX-to-RX turnaround after sending the ACK for the previous transmission. Even though this situation does not involve a collision, its impact is same as that of a collision.
Corruption due to PHY noise/interference: A packet transmission may get incorrigibly corrupted due to PHY level noise or interference from sources like microwave ovens or WiFi transmissions. The consequent discarding of the packet transmission by the destination has the same impact as a collision.

6. A Stochastic Model for Beaconless IEEE 802.15.4 MAC Operation

6.1. The Network Scenario Being Modeled

In this paper, we develop a stochastic model to predict the packet loss probability and latency for a group of source nodes (i.e., the nodes that originate packets) in a network that are in each other’s radio range and hence compete with each other for channel access to send packets to one or more destination nodes. These source nodes are referred to as the regular nodes in the subsequent discussion. In addition to the regular nodes, the network may have a number of hidden source nodes that are outside the radio range of regular nodes (and hence can not use CSMA to prevent concurrent transmissions with regular nodes) but with in the radio range of the destination node(s) of the regular nodes. Hence, concurrent packet transmissions by a regular node and a hidden node would result in a collision.

In general, each regular node may have its own set of hidden nodes with each such hidden node having arbitrary sets of nodes in its radio range and out of it. This general situation is mathematically intractable. In this paper, we consider the particular situation where the source nodes are arranged in one or more groups such that the nodes in each group are in each other’s radio range but outside the radio range of nodes in other groups. One such group consists of the regular nodes. The nodes in other groups are hidden nodes for the regular nodes. Further, each group of hidden nodes is “independent” in the sense that the nodes in this group dont have their own hidden nodes. In other words, the destinations for a group of hidden nodes are not in the radio range of other nodes. Figure 4 illustrates this scenario.
The stochastic model, presented in this paper, does not take in account the impact of PHY level noise on the packet loss probability and latency. As explained in Section 4, the probability that a packet suffers incorrigible corruption due to PHY noise undergoes very sudden transition from almost 0 to almost 1 as the signal to noise ratio (SNR) deteriorates. This means that SNR is either good enough so that the PHY noise has negligible impact on IEEE 802.15.4 operation or SNR is so bad that IEEE 802.15.4 operation is not possible. Thus, it is reasonable to ignore the PHY noise in the modeling process.

Further assumptions regarding the network being modeled are as follows:

- The destination nodes do not send packets;
- Clear channel assessment (CCA) fails if there is a transmission by any node in the radio range during any part of the CCA duration; otherwise, the CCA succeeds.

Suppose the first assumption does not hold true and a destination node needs to send/forward packets. Depending on its MAC implementation, the destination node may ignore any packets it receives while it is trying to send a packet. The packet send procedure involves CSMA wait followed by a CCA. If the CCA succeeds, the node does an RX-to-TX turnaround and transmits the packet. Being half-duplex in nature, a node can not receive a packet while it is transmitting one. However, whether a packet received during the CSMA wait is accepted or not is implementation dependent. A node may choose to accept the received packet and postpone the packet transmission to a later time or it may choose to discard the received packet and continue with the packet transmission. If a node chooses to accept the received packet, the model presented in this paper may still be used to evaluate the performance; otherwise not. Note that a large number of application scenarios exist in home, building and industrial environments where the sensor nodes convey information to their directly reachable controllers which then forward the information further over the wired infrastructure. The first assumption holds true in these scenarios and the model presented in this paper is directly applicable. The assumption does not hold true in case of multi-hop networks where a node needs to forward a received packet further on its way to the destination node. Predicting the end-to-end performance in a multi-hop network using beaconless IEEE 802.15.4 at MAC layer, where a
Figure 4: The "hidden node" scenario being modeled: The regular nodes and multiple groups of "independent" hidden nodes

node ignores received packets while it is trying to send a packet, is an open research problem out of scope for this paper.

The second assumption is related to the implementation of CCA mechanism. IEEE 802.15.4 standard specifies three CCA modes [1]:

- **energy above threshold**, where CCA fails if the detected energy during the CCA duration exceeds a threshold;

- **carrier sense only**, where CCA fails if the node detects an IEEE 802.15.4 compliant signal with same modulation and spreading characteristics as the particular IEEE 802.15.4 PHY used by the node;

- an **AND/OR** combination of the previous two modes.

The assumption regarding CCA is valid in all three modes except when the energy threshold is set too high.

6.2. Modeling Methodology and Assumptions

The stochastic model makes the following assumptions:

- The number of regular source nodes in $n$.

- The time interval, $t$, between two consecutive packet send events at each regular node is exponentially distributed with rate $1/T$, i.e. $T = E(t)$. 


The time interval, $h$, between two consecutive transmissions by the hidden nodes is exponentially distributed with rate $1/H$, i.e. $H = E(h)$. Later in the paper (Section 6.10), we offer guidance on how $H$ may be estimated for the "hidden node" scenarios being modeled.

A destination node is always able to complete the $TX$-to-$RX$ turnaround in time between the transmission of an ACK and receipt of the next packet meant for it. The assumption is reasonable since the $TX$-to-$RX$ turnaround time is required to be less than 12 symbols or 0.192ms (for 2.4GHz PHY).

A node finishes service to a packet before the next packet is generated, i.e. there is no queueing delay component in the packet latency. The assumption is reasonable since the maximum packet latency at IEEE 802.15.4 MAC layer, with default values for different IEEE 802.15.4 MAC parameters, is 10688 symbols or $171.008$ ms (for 2.4GHz PHY), which is generally less than the time interval between two packet send events at a node in typical WSN applications.

The stochastic model takes $n$, $T$ and $H$ values as input and generates the expected values for the packet loss probability, $L(n, T, H)$, and the packet latency, $D(n, T, H)$, at steady state.

Let $m$ be the random variable denoting the number of regular active nodes at any given time. A regular node is considered active only while it has a packet to send and hence is competing for channel access with other regular active nodes. Later in this section, we show that the probability of CCA failure, $\alpha(m, H)$ and the probability of collision for a transmission, $\beta(m, H)$, are functions of $m$ and $H$. The $\{\alpha, \beta\}$ values for given $m$ and $H$ values can

---

4 A node makes at most 4 attempts to send a packet and receive the acknowledgement. During a transmission attempt, the node performs up to 5 CSMA waits to find the channel idle. With initial and maximum BE values 3 and 5 respectively, the maximum durations, including the CCA durations, of 5 allowed CSMA waits are 148, 308, 628, 628 and 628 symbols, totalling to 2340 symbols. Suppose the node finds the channel idle after the fifth CSMA wait. So, the node will additionally spend 12 symbols in $RX$-to-$TX$ turnaround, up to 266 symbols in packet transmission (maximum packet size at PHY layer is 133 bytes) and up to 54 symbols ($macAckWaitDuration$) in waiting for the acknowledgement. Thus, the maximum duration of a transmission attempt is 2672 (= 2340 + 12 + 266 + 54) symbols and the maximum value of the packet latency is $4 \times 2672 = 10688$ symbols.
be used to determine the corresponding packet loss probability $\lambda(m, H)$ and the corresponding packet latency $\delta(m, H)$.

The number of regular nodes that are active at any given time vary depending on the total number of regular nodes ($n$), their packet generation behavior characterized by average inter-packet interval $T$ and the hidden node behavior characterized by average inter-transmission interval $H$. The stochastic model is based on the assumption that the probability that $m$ regular nodes are active at any given time is same as the probability that $m - 1$ regular nodes get a new packet to send while a regular active node is sending its current packet, i.e. during a time interval equal to the steady state packet latency $D(n, T, H)$. Thus, for given values of $\{n, T, H\}$, $m$ is a function of packet latency $D(n, T, H)$, which in turn is a function of $\delta(m, H)$ and hence $m$ (for a given value of $H$). The model exploits this cyclic relationship between $m$ and $D(n, T, H)$ to determine $D(n, T, H)$, which can readily be translated to the expected value for packet loss probability $L(n, T, H)$ as described later.

In the following, we describe the dependence of probabilities $\{\alpha, \beta\}$ on $\{m, H\}$ and the dependence of packet loss probability ($\lambda$) and packet latency ($\delta$) on probabilities $\{\alpha, \beta\}$. We begin this discussion with the relationship between the average CSMA wait duration, $w$, and the probability of CCA failure, $\alpha$. This is followed by a description of the life cycle of an active period, the time duration enveloping each overlapping set of transmissions by the regular active nodes. The life cycle of an active period helps us derive the probabilities $\alpha$ and $\beta$ in terms of $m$ and $H$.

6.3. Modeling The CSMA Wait Duration

During a packet transmission attempt, a node does a CSMA wait before performing the CCA. The CCA failure causes $BE$ value to be incremented (up to $macMaxBE$, by default 5) and the CSMA wait to be repeated (up to $macMaxCSMABackoffs$ times, by default 4). The CSMA wait duration is a randomly selected number of backoff periods (=20 symbols each) in the range $[0, 2^{BE} - 1]$, where each number in the range is equally likely to be selected. With $\alpha$ as the probability of CCA failure, a node would perform on average $1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4$ CSMA waits during a packet transmission attempt. Let $w$ denote the random variable corresponding to a CSMA wait duration. With $macMinBE$ and $macMaxBE$ parameters at their default values (3 and 5 respectively), i.e., with 3 and 5 as the initial and maximum values of $BE$, the
The expected value of a CSMA wait duration (in terms of backoff periods) can be expressed as the following continuous and monotone increasing function of $\alpha$, the probability of CCA failure:

$$E_w(\alpha) = \frac{3.5 + 7.5\alpha + 15.5\alpha^2 + 15.5\alpha^3 + 15.5\alpha^4}{1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4}$$ (5)

Even though the CSMA wait duration is discrete in nature, we model it as a continuous random variable $w'$, exponentially distributed with rate $1/E_w$, i.e. $w' \sim \text{EXP}(1/E_w)$. Figure 5 shows that $w'$ is a good approximation of $w$ for different $\alpha$ values.

### 6.4. The Life Cycle of an Active Period

Consider $m$ regular active nodes competing for channel access at a certain time. Suppose all regular active nodes are performing their CSMA waits initially. Suppose node $X$ is the first such node to finish its CSMA wait. We
mark this event as the beginning of an active period. In other words, node $X$ triggers an active period. Node $X$ would find the channel idle and proceed with its packet transmission. Thus, node $X$ would have zero probability of CCA failure. The active period ends when node $X$, and any other node that begins its transmission during the active period, have finished their transmissions.

If another node, say node $Y$, finishes its CSMA wait during the active period, its CCA would fail unless node $Y$’s CSMA wait ends during one of the collision windows (as identified in Sect. 5) associated with node $X$’s transmission. Figure 6 shows different states during the life time of an active period under the following assumptions:

- Both regular and hidden nodes send 133 byte long packets (including the 6 byte IEEE 802.15.4 PHY header);

- In case of a collision, the last colliding node finishes its CSMA wait just before the end of the collision window.

The sojourn times in various states could be explained as follows. State $S0$ corresponds to the beginning of the active period as well as that of the first collision window and has a sojourn time equal to 12 symbols. These 12 symbols consist of 8 symbols of CCA by node $X$ and the first 4 symbols of node $X$’s RX-to-TX turnaround. If at least one regular active node finishes its CSMA wait during the first collision window, which happens with probability $1 - e^{-12(m-1)/E_w}$, a collision is guaranteed. In this case, there
is a transition to the collision state, $S_4$. For simplicity, we assume that the last colliding node finishes its CSMA wait just before the end of the collision window and completes its transmission over next 286 symbols (8 symbols of CCA + 12 symbols of turnaround + 266 symbols of packet transmission), which constitute the sojourn time in state $S_4$. The completion of sojourn in state $S_4$ concludes the active period. On the other hand, if no regular active node finishes its CSMA wait during the first collision window, which happens with probability $e^{-12(m-1)/E_w}$, node $X$ would complete its turnaround (additional 8 symbols) and transmit the packet (266 symbols). These 274 symbols correspond to the sojourn in state $S_1$.

If a transmission by a hidden node collides with node $X$'s transmission, the destination will ignore node $X$'s transmission and the active period gets over. Assuming that the hidden node’s transmission also lasts for 266 symbols, it will collide with transmission by node $X$ if it starts during state $S_1$ or state $S_0$ or 245 symbols preceding state $S_0$ (a total time duration of $274 + 12 + 245 = 531$ symbols). Since the time interval between two consecutive transmissions by the hidden nodes is exponentially distributed with rate $1/H$, the probability that a hidden node transmission collides with that of node $X$ is $1 - e^{(-531/H)}$. Note that we take the possibility of collision with a hidden node into account only if no collision takes place with a regular active node during the first collision window.

If there is no collision with a regular active node or a hidden node, the destination receives the transmission successfully and starts its RX-to-TX turnaround to send the ACK. This marks the beginning of the second collision window, which is 4 symbols long and corresponds to state $S_2$. If at least one regular active node finishes its CSMA wait during the second collision window, which happens with probability $1 - e^{-4(m-1)/E_w}$, there is a transition to the collision state, $S_4$. Otherwise, following the completion of 4 symbol long collision window, there is a transition to state $S_3$. The sojourn time in state $S_3$ is 30 symbols during which the destination node completes its RX-to-TX turnaround that started in state $S_2$ (8 symbols) and transmits the 11 byte long ACK (22 symbols). The completion of the ACK transmission completes the active period.

Note that the hidden node transmissions can not affect the successful transmission or receipt of the ACK. Once the destination node successfully receives node $X$’s transmission, it begins its RX-to-TX turnaround and ignores all transmissions (including those by hidden nodes) until it finishes the ACK transmission and completes the subsequent TX-to-RX turnaround.
Since node $X$ is outside the radio range of the hidden nodes, any transmissions by hidden nodes never reach node $X$.

6.5. The Probability of CCA Failure

Next, we determine the probability of CCA failure for a regular active node, $\alpha(m)$. For this purpose, we first enumerate different possible durations of an active period, the probability of occurrence for each duration, the probability that a regular active node finishes its CSMA wait during the active period of a particular duration and the probability of CCA failure for such a node:

- If one or more regular active nodes finish their CSMA waits during the first collision window, which happens with probability $p_1 = 1 - \frac{e^{-12(m-1)/E_w}}{E_w}$, the active period would sojourn over state sequence $S0-S4$ and last for 298 symbols. The probability that a regular active node finishes its CSMA wait during such an active period is $q_1 = 1 - \frac{e^{-298/E_w}}{E_w}$. Since, the CCA would not fail during the collision window, the probability of CCA failure for such a node would be $\alpha_1 = \frac{298 - 12}{298} = 286/298$.

- If no regular active node finishes its CSMA wait during the first collision window but there is a collision with a hidden node’s transmission, which happens with probability $p_2 = \frac{e^{-12(m-1)/E_w} \times (1 - e^{-531/H})}{E_w}$, the active period would sojourn over state sequence $S0-S1$ and last for 286 symbols. Given that no node finishes its CSMA wait during the first collision window ($= 12$ symbols), the probability that an active node finishes its CSMA wait during such an active period is $q_2 = 1 - \frac{e^{-274/E_w}}{E_w}$. Since, the CCA does not take place during the first collision window, the probability of CCA failure for such a node would be $\alpha_2 = 274/274 = 1$.

- The probability that no regular active node finishes its CSMA wait during the first collision window and there is no collision with a hidden node’s transmission but one or more regular active nodes finish their CSMA waits during the second collision window is $p_3 = \frac{e^{-12(m-1)/E_w} \times e^{-531/H} \times (1 - e^{-4(m-1)/E_w})}{E_w}$. Such an active period would sojourn over state sequence $S0-S1-S2-S4$ and last for 576 symbols. Given that no node finishes its CSMA wait during the first collision window ($= 12$ symbols), the probability that an active node finishes its CSMA wait during the second collision window is $q_3 = 1 - \frac{e^{-4(m-1)/E_w}}{E_w}$. Since, the CCA does not take place during the second collision window, the probability of CCA failure for such a node would be $\alpha_3 = 4(m-1)/E_w$.
during such an active period is $q_3 = 1 - e^{-564/E_w}$. Since, the CCA does not take place during the first collision window but may take place during the second collision window, the probability of CCA failure for such a node would be $\alpha_3 = (564 - 4)/564 = 560/564$.

- The probability that no regular active node finishes its CSMA wait during the two collision windows and there is no collision with a hidden node either is $p_4 = e^{-12(m-1)/E_w} \times e^{-531/H} \times e^{-4(m-1)/E_w}$. Such an active period would sojourn over state sequence $S0-S1-S2-S3$ and last for 320 symbols. Given that no node finishes its CSMA wait during the two collision windows ($= 12 + 4 = 16$ symbols), the probability that an active node finishes its CSMA wait during such an active period is $q_4 = 1 - e^{-304/E_w}$ and the probability of CCA failure for such a node would be $\alpha_4 = 1$.

Clearly, an active node may finish its CSMA wait either by triggering a new active period or inside an ongoing active period. However, it is not necessary that all $m-1$ active nodes (excluding the one that triggered an active period) would finish their CSMA waits during an ongoing active period. Suppose $q_i$ is the probability that a node finishes its CSMA wait during an ongoing active period, i.e. $q_i \in \{q_1, q_2, q_3, q_4\}$. Then the expected number of nodes that would finish their CSMA waits during an active period (including the node that triggers the active period) is $1 + (m-1)q_i$. Therefore, the probability that a regular active node triggers an active period is $1/(1 + (m-1)q_i)$ and the probability that a regular active node finishes its CSMA wait during an ongoing active period is $(m-1)q_i/(1 + (m-1)q_i)$. Since the node triggering an active period has zero probability of CCA failure, the overall probability of CCA failure can be expressed as a function of $m$, the number of regular active nodes, $E_w$, the average CSMA wait duration, and $H$, the expected time interval between two consecutive transmissions by hidden nodes, as follows:

$$\alpha(m, E_w, H) = \sum_{i=1}^{4} p_i \frac{(m-1)q_i}{1 + (m-1)q_i} \alpha_i$$

Note that, for a given values of $\{m, H\}$, $\alpha$ is a continuous function of $E_w$, which in turn is a continuous, monotone increasing function of $\alpha$ (Equation 5). This relationship can be exploited to determine the unique value of $\alpha$ for the given values of $\{m, H\}$. Let $\alpha*$ be the function expressing $\alpha$ in terms
of $E_w$, obtained after inverting Equation 5. Figure 7 plots $\alpha$ values against $E_w$ (in terms of backoff periods) for different values of $m$ (with $H$ set to infinity) using Equation 6 as well as $\alpha^*$ values using Equation 5. The point of intersection between $\alpha$ and $\alpha^*$ curves gives the unique value of $\alpha$ for the given values of $m$ and $H$. Note that $H$ itself has a negligible impact on the value of $\alpha$ as shown in Figure 8, which plots $\alpha$ values against $E_w$ for different values of $H$ with $m$ set to 5.

6.6. The Probability of Collision for a Transmission

Out of $m-1$ regular active nodes still in the middle of their CSMA waits when an active period starts, the probability that $i$ ($0 \leq i \leq m-1$) nodes finish their CSMA wait during the first collision window and hence transmit during this active period is $p_{\text{coll1}}(i) = \binom{m-1}{i}(1 - e^{-12/E_w})^i (e^{-12/E_w})^{m-1-i}$.

If no regular active node finishes its CSMA wait during the first collision window, the transmission that triggers the active period may still collide with a transmission from a hidden node with probability $p_{\text{hidden}} = 1 - e^{-531/H}$.

The second collision window comes into picture if no active node finishes its CSMA wait during the first collision window and there is no collision with a hidden node. The probability that $i$ ($0 \leq i \leq m-1$) nodes finish their CSMA wait during the second collision window and hence transmit during this active period is $p_{\text{coll2}}(i) = \binom{m-1}{i}(1 - e^{-4/E_w})^i (e^{-4/E_w})^{m-1-i}$.

An active period would consist of just one packet transmission, the one that triggers the active period, if:

- No regular active node finishes its CSMA wait during the first collision window AND there is a collision with a hidden node; OR

- No regular active node finishes its CSMA wait during the first collision window AND there is no collision with a hidden node AND no regular active node finishes its CSMA wait during the second collision window.

Similarly, an active period would consist of $i > 1$ transmissions, including the one that triggers the active period, if:

- $(i - 1)$ regular active nodes wake up during the first collision window; OR

- No regular active node wakes up during the first collision window AND there is no collision with a hidden node AND $(i - 1)$ regular active nodes wake up during the second collision window.
Thus, the probability that $i$ transmissions take place during an active period, including the one that triggers the active period, is given by:

$$p_{\text{trans}}(i) = \begin{cases} p_{\text{coll1}}(0)(p_{\text{hidden}} + (1 - p_{\text{hidden}})p_{\text{coll2}}(0)) & i = 1 \\ p_{\text{coll1}}(i - 1) + p_{\text{coll1}}(0)(1 - p_{\text{hidden}})p_{\text{coll2}}(i - 1) & 2 \leq i \leq m \end{cases}$$

Thus, the expected number of transmissions during an active period is $\sum_{i=1}^{m} i \times p_{\text{trans}}(i)$. Clearly, two or more transmissions during an active period imply collision for all these transmissions. Also, a single transmission during an active period may be involved in a collision with transmission from a hidden node. Thus, the expected number of transmissions during an active period that witnesses a collision is $p_{\text{coll1}}(0)p_{\text{hidden}} + \sum_{i=2}^{m} i \times p_{\text{trans}}(i)$. Thus, the fraction of transmissions that experience a collision, or in other words the probability of collision for a transmission, can be described as follows:

$$\beta(m, E_w, H) = \frac{p_{\text{coll1}}(0)p_{\text{hidden}} + \sum_{i=2}^{m} i \times p_{\text{trans}}(i)}{\sum_{i=1}^{m} i \times p_{\text{trans}}(i)}$$  \hfill (7)

As mentioned earlier, the cyclic relationship between $\alpha$ and $E_w$ (Equations 6 and 5) can be used to determine the unique value of $\alpha$, and hence $E_w$, for given $m$ and $H$ values. Then, we can use Equation 7 to determine the corresponding $\beta$ value. Clearly, $\alpha$ and $\beta$ are functions of $m$ and $H$. Figure 9 shows the $\alpha(m, H)$ and $\beta(m, H)$ values, as well as the predicted probability of packet loss $\lambda(m, H)$ (to be discussed in Sect. 6.7), for different values of $m$ and $H$. We observed $\alpha$, $\beta$ and $\lambda$ to be monotone increasing functions of $m$ for a given value of $H$. Figure 9 shows that the $\alpha$ values are largely unaffected by $H$, whereas $\beta$ increases as $H$ decreases (i.e., hidden node transmissions become more frequent).

6.7. The Probability of Packet Loss in IEEE 802.15.4 MAC

As discussed earlier, the IEEE 802.15.4 MAC layer declares failure in sending a packet if it fails to receive the acknowledgement for the packet even after $1+\text{macMaxFrameRetries}$ (i.e. 4, by default) transmission attempts. The failure could be declared sooner if, during a transmission attempt, the MAC layer suffers a channel access failure, which happens when $1+\text{macMaxCSMABackoffs}$ (i.e. 5, by default) back-to-back CCA failures take place. Let $\alpha$ be the probability of CCA failure and $\beta$ be the probability of collision
Figure 7: Determining unique $\alpha$ for a given $m$ value ($H$ set to infinity). $E_w$ in backoff periods ($=20$ symbols).

Figure 8: Impact of $H$ value on $\alpha$ (with $m$ set to 5). $E_w$ and $H$ in backoff periods ($=20$ symbols).

Figure 9: The predicted $\alpha, \beta$ and $\lambda$ values for different values of $m$ and $H$. 

28
for a packet transmission (or its acknowledgement). Thus, the probability of a channel access failure is $\alpha^5$. Figure 10 shows a state diagram for the packet transmission process followed by IEEE 802.15.4 MAC layer. Clearly, the probability of packet loss, $\lambda$, is given by:

$$\lambda(\alpha, \beta) = \frac{\alpha^5 + (1 - \alpha^5)\beta}{\alpha^5 + (1 - \alpha^5)\beta\left(\frac{\alpha^5 + (1 - \alpha^5)\beta}{\alpha^5 + (1 - \alpha^5)\beta}\right)}$$  \hspace{1cm} (8)$$

Since $\alpha$ and $\beta$ are functions of $m$ and $H$, the probability of packet loss $\lambda$ is a function of $m$ and $H$ as well and can be represented as $\lambda(m, H)$. Figure 9 shows the predicted probability of packet loss $\lambda(m, H)$ for different values of $m$ and $H$. These values were calculated by first obtaining $\alpha$ and $\beta$ values for given $m$ and $H$ values and then using Eq. 8 to obtain the corresponding $\lambda(m, H)$ value.

6.8. The Packet Latency

Next, we determine the packet latency as a function of the probabilities $\{\alpha, \beta\}$. The packet latency refers to the time required by IEEE 802.15.4 MAC layer to report back the fate of a packet to the upper layer. As discussed earlier, IEEE 802.15.4 MAC layer performs up to $1+macMaxCSMABackoffs$ (5 by default) CCAs to find the channel idle during a transmission attempt. Each CCA is preceded by a CSMA wait. With default values for
macMinBE and macMaxBE (3 and 5 respectively), the average duration of the five CSMA waits are 3.5, 7.5, 15.5, 15.5, 15.5 backoff periods (=20 symbols) respectively. Each CSMA wait is followed by 8 symbols of CCA. Thus, after including the CCA duration, the average durations of five CSMA waits are 78, 158, 318, 318 and 318 symbols respectively. If $\alpha$ is the probability of CCA failure, the probability that a transmission attempt involves exactly $i$, $1 \leq i \leq 4$, CSMA waits is $\alpha^{i-1}(1 - \alpha)$. The probability that a transmission attempt involves 5 CSMA waits with success in the 5th CCA is $\alpha^4(1 - \alpha)$. The probability that a transmission attempt involves 5 CSMA waits, all of which end in CCA failures (i.e. there is a channel access failure), is $\alpha^5$. Thus, total time spent (in symbols) in CSMA waits and CCAs during a transmission attempt can be described as follows:

\[
\begin{align*}
    d_{\text{CSMA}} &= \begin{cases} 
        78 & \text{w. p. } 1 - \alpha \\
        78 + 158 & \text{w. p. } \alpha(1 - \alpha) \\
        78 + 158 + 318 & \text{w. p. } \alpha^2(1 - \alpha) \\
        78 + 158 + 2 \times 318 & \text{w. p. } \alpha^3(1 - \alpha) \\
        78 + 158 + 3 \times 318 & \text{w. p. } \alpha^4(1 - \alpha) + \alpha^5
    \end{cases}
\end{align*}
\]

Clearly, the expected duration of a transmission attempt that ends in a channel access failure is $d_{\text{CAF}} = 78 + 158 + 318 + 318 + 318 = 1190$ symbols (or 19.04ms) and the expected duration in symbols, if the transmission attempt does not end in a channel access failure, is $d_{\text{noCAF}} = \frac{1 - \alpha}{1 - \alpha^5}(78 + 236\alpha + 554\alpha^2 + 872\alpha^3 + 1190\alpha^4)$.

If a CCA is successful, the node would proceed with RX-to-TX turnaround ($d_{TA} = 12$ symbols) and transmit the packet ($d_T = 266$ symbols for a 133 byte packet) and wait for the acknowledgement. The acknowledgement should be received in $d_A = 34$ symbols (12 symbols RX-to-TX turnaround for destination + 22 symbols to transmit 11 byte acknowledgement) unless the packet (or acknowledgement) transmission ends up in collision, in which case the node waits for $d_W = 54$ symbols for acknowledgement and then proceeds with next transmission attempt. Let $d' = d_{\text{noCAF}} + d_{TA} + d_T + d_A$. Following the state diagram for the packet transmission process (Fig. 10), the packet latency, $\delta$, in symbols can be expressed as a function of $\alpha$ and $\beta$ as follows:
\[\delta(\alpha, \beta) = \alpha^5d_{CAF} + (1 - \alpha^5)(d' + \beta(d_W - d_A) + \alpha^5d_{CAF} + (1 - \alpha^5)(d' + \beta(d_W - d_A) + \alpha^5d_{CAF} + (1 - \alpha^5)(d' + \beta(d_W - d_A)))))\] (9)

Since \(\alpha\) and \(\beta\) are functions of \(m\) and \(H\), the packet latency \(\delta\) is a function of \(m\) and \(H\) as well and can be referred to as \(\delta(m, H)\). Figure 11 shows the predicted values of packet latency \(\delta(m, H)\) in milliseconds for different values of \(m\) and \(H\). These values were calculated by first obtaining \(\alpha\) and \(\beta\) values for given \(m\) and \(H\) values and then using Equation 9 to obtain the corresponding \(\delta(m, H)\) value. As Fig. 11 shows, for a particular value of \(H\), the packet latency initially increases with \(m\). Once \(m\) value reaches a certain threshold, any further increase in \(m\) causes the packet latency to decrease. This happens because increase in \(m\) causes the probability of CCA failure, \(\alpha\), to increase, which in turn increases the likelihood of channel access failures and thus reduces the likelihood of retransmissions. Note that the initial surge in latency with increase in \(m\) is higher with more frequent hidden node transmissions (i.e. lower \(H\)). This is because more frequent hidden node transmissions lead to more collisions and hence more retransmissions by regular active nodes, which results in higher latency. Also, it is clear that the threshold value of \(m\) after which the latency starts to decrease gets smaller with more frequent hidden node transmissions. This happens because the increase in retransmissions by regular active nodes also causes a quicker rise in the probability of CCA failure.

6.9. Tying It All Together

Since the inter-packet generation (or arrival) interval at each regular node is exponentially distributed with rate \(1/T\), the packet arrivals at each regular node can be modeled as a Poisson process with rate \(1/T\).

Suppose \(D(n, T, H)\) represent the expected packet latency for the regular nodes. For the given values of \(m\) and \(H\), the corresponding packet latency, \(\delta(m, H)\), can be calculated by first calculating \(\alpha\) and \(\beta\) and then using these values in Eq. 9. We assume that, for given values of \(n\), \(T\) and \(H\), \(m\) is in turn a function of \(D(n, T, H)\) as described below. This relationship between \(\delta(m, H)\) and \(D(n, T, H)\) can be exploited to determine \(D(n, T, H)\).
Suppose node $X$ is in the process of sending a packet. During the service time of this packet, some regular active nodes would finish sending their packets (and thus become inactive) while other regular inactive nodes would get a new packet to send (and thus become active). We assume that the probability that $m$ regular nodes are active is same as the probability that $m - 1$ inactive regular nodes get a new packet to send during the time node $X$ is servicing its packet (equal to the expected packet latency $D(n, T, H)$). Since the number of regular active nodes at any given time is small and an active node is unlikely to receive another packet while it is servicing one, we calculate the probability that $m$ regular nodes are active simply as the probability that $m - 1$ regular nodes, out of a total of $n - 1$ nodes, get a new packet to send during time interval $D(n, T, H)$.

Since the combined packet arrivals across $n - 1$ regular nodes can be modeled as a Poisson process with rate $(n - 1)/T$, the probability that $m$ regular nodes are active, i.e. $m - 1$ regular nodes get a new packet to send during time interval $D(n, T, H)$, is given by:

$$p(m) = \frac{(\frac{n - 1}{T} D(n, T, H))^{m-1} e^{-\frac{n - 1}{T} D(n, T, H)}}{(m - 1)!}$$  \hspace{1cm} (10)$$

Thus, for given $n$, $T$ and $H$ values, the expected packet latency, $D(n, T, H)$,
can be obtained by solving the following recursive equation:

\[ D(n, T, H) = \sum_{m=1}^{n} \delta(m) \times p(m) \]  \hspace{1cm} (11)

Once we have determined the expected packet latency \( D(n, T, H) \) for given \( n, T \) and \( H \) values, we can determine the probability, \( p(m) \), that \( m \) regular nodes are active at any given time using Eq. 10 and hence the expected values of the probability of CCA failure, \( A(n, T, H) \), the probability of collision for a transmission, \( B(n, T, H) \), and the probability of packet loss, \( L(n, T, H) \), as follows:

\[ A(n, T, H) = \sum_{m=1}^{n} \alpha(m) \times p(m) \]  \hspace{1cm} (12)

\[ B(n, T, H) = \sum_{m=1}^{n} \beta(m) \times p(m) \]  \hspace{1cm} (13)

\[ L(n, T, H) = \sum_{m=1}^{n} \lambda(m) \times p(m) \]  \hspace{1cm} (14)

Also, the expected number of regular active nodes at any given time is simply

\[ E_{\text{m}}(n, T, H) = 1 + \frac{(n-1) \times D(n, T, H)}{T} \]  \hspace{1cm} (15)


In Section 6.1, we described the topological arrangement of regular and hidden nodes for which the stochastic model developed in this paper is applicable. In this section, we describe how to estimate the frequency of hidden node transmissions in these scenarios.

Suppose the time interval between consecutive packet send events at a node is exponentially distributed with rate \( 1/T \) and the probabilities of CCA failure and collision for a transmission are \( \alpha \) and \( \beta \) respectively. Then, \( \alpha^5 \) represents the probability of channel access failure. The probability that the packet send event involves no transmission is \( \alpha^5 \), i.e. the node encounters a channel access failure in the first transmission attempt. The first transmission takes place with probability \( 1 - \alpha^5 \). The probability that exactly one transmissions take place for this packet send event is \( (1 - \alpha^5)(1 - \beta + \beta \alpha^5) \), where \( (1 - \beta + \beta \alpha^5) \) term is the probability that the transmission does not
encounter a collision or it does experience a collision but the next transmission attempt ends in channel access failure. The probability that exactly two transmissions take place is \((1 - \alpha^5)^2 \beta (1 - \beta + \beta \alpha^5)\), where \((1 - \alpha^5)^2\) term is the probability that channel access failure does not take place in both transmission attempts and \(\beta\) term is the probability that the first transmission encounters a collision. Similarly, the probability that exactly three transmissions take place is \((1 - \alpha^5)^3 \beta^2 (1 - \beta + \beta \alpha^5)\). The probability that exactly four transmissions take place is simply \((1 - \alpha^5)^4 \beta^3\) since the node does not make the 5th transmission attempt (assuming default value 3 for macMaxFrameRetries). Thus, the expected number of transmissions by the node for each packet send event is given by:

\[
E_{\text{trans}}(\alpha, \beta) = 4(1 - \alpha^5)^4 \beta^3 + \sum_{i=1}^{3} i \times (1 - \alpha^5)^i \beta^{i-1} (1 - \beta + \beta \alpha^5)
\]  

Given \(\{T, \alpha, \beta\}\) values for a hidden node, we assume that the time interval between successive transmissions by this node is exponentially distributed with rate \(E_{\text{trans}}(\alpha, \beta) / T\).

Consider the scenario illustrated in Figure 4. Suppose there are \(g\) groups of hidden nodes, with \(n_i, 1 \leq i \leq g\), nodes in the \(i\)th group, and the time interval between consecutive packet send events at each node in the \(i\)th group is exponentially distributed with rate \(1/T_i\). As mentioned earlier in Section 6.1, we assume that these hidden nodes themselves do not have any hidden nodes, i.e. \(H\) for each group can be considered to be infinity. Thus, we can use Eq. 12 and 13 to determine the probability of CCA failure, \(\alpha_i\), and the probability of collision for a transmission, \(\beta_i\), for the hidden nodes in the \(i\)th group and hence the rate, \(E_{\text{trans}}(\alpha_i, \beta_i) / T_i\) for the exponentially distributed time interval between successive transmissions by one node in this group. Thus, the time interval between successive transmissions by hidden nodes in all \(g\) groups can be assumed to be exponentially distributed with rate \(\sum_{i=1}^{g} n_i E_{\text{trans}}(\alpha_i, \beta_i) / T_i\), the inverse of which gives us \(H\) for the regular nodes.

7. Evaluating the Model’s Accuracy

To verify the accuracy of the stochastic model developed above, we performed simulations with a significantly improved version [31] of IEEE 802.15.4 protocol implementation in NS2 simulator [32]. The simulated network scenarios satisfied the conditions listed in Sec. 6.1. IEEE 802.15.4 MAC layer
operated in beaconless mode while IEEE 802.15.4 PHY layer operated in 2450 MHz range. All the IEEE 802.15.4 MAC and PHY parameters had their default values as listed in IEEE 802.15.4 specification [1]. Particularly, the \textit{macMinBE}, \textit{macMaxBE}, \textit{macMaxFrameRetries} and \textit{macMaxCSMABackoffs} parameters had values 3, 5, 3 and 4 respectively. The CCA duration was 8 symbols. In this paper, we report two sets of simulation results and corresponding model predictions. The first set compares simulation results and model predictions for a group of regular nodes in the absence of any hidden nodes, whereas the second set does the comparison when one group of 50 hidden nodes affect transmissions by the regular nodes. As per the stochastic model’s assumptions, the hidden nodes themselves do not have any hidden nodes, i.e., the regular and hidden nodes are arranged as shown in Figure 4. Although the simulations reported in this paper were performed using 133 bytes as the packet size (including 6 bytes of IEEE 802.15.4 PHY header), we did simulations with other packet sizes as well and found similar match between the simulation results and the model predictions.

We first discuss simulations in the first set (i.e. no hidden nodes). Each simulation begins with a certain number of source nodes, \( n \in \{10, 20, 30, \ldots, 100\} \), coming up in a randomly determined sequence within first 100 seconds of the simulation. Since association with a coordinator is not required for beaconless operation, the simulated nodes skip the association procedure and directly embark on generating packets for a common destination with the time interval between two packet send events at each node being exponentially distributed with average \( T \in \{0.2s, 1s, 5s\} \). A successful packet delivery requires the receipt of MAC-level acknowledgement from the destination. All the nodes, including the common destination node, are always in each other’s radio range and hence no multi-hop routing is required and there are no hidden nodes. The simulation time is set such that each node sends more than 10000 packets to the common destination during the simulation. Each node keeps track of the average values of the following measures: 1) the probability of CCA failure, i.e., the fraction of CCA attempts ending in failure; 2) the probability of collision for a transmission, i.e. the fraction of packet transmissions involved in a collision; 3) the probability of packet loss, i.e. the fraction of packets the MAC layer reports as lost due to channel access or collision failures; and 4) the packet latency, i.e. the time difference between the instants when a packet is sent to the MAC layer for transmission and when the MAC layer reports the fate of the packet (successfully delivered or lost) back to the higher layer. The node-level values are then used to calculate the
average values of the performance measures, and their confidence intervals, across all the nodes in the simulation. The 95% confidence intervals were always observed to be within a small range around the average value.

Figure 12 shows the comparison between the average values of the performance measures, calculated across all the nodes, from the simulations and the model predictions when no hidden nodes are present. Although the model underestimates the probability of CCA failure (Fig. 12(a)), there is quite a good match between the model predictions and simulation results for the probability of collision for a transmission (Fig. 12(b)), the overall probability of packet loss (Fig. 12(c)) and the packet latency (Fig. 12(d)) for all simulated \((n, T)\) scenarios. The discrepancies between the simulation results and model predictions can be attributed to various modeling assumptions listed in Sec. 6.2.

The simulations in the second set involved a group of \(n\) regular nodes \((n \in \{10, 20, 30, ..., 100\})\) and one group of 50 hidden nodes. Each regular node sent one packet per second on average with the time interval between two packet send events being exponentially distributed. Each hidden node sent 1 or 3 packets per second on average with the time interval between two packet send events being exponentially distributed. The simulations in the second set ran in the same manner as the simulations in the first set with each regular node in a simulation sending more than 10000 packets and keeping track of its probability of CCA failure, the probability of collision for a transmission, the probability of packet loss and the packet latency. Figure 13 shows the comparison between the average values of these performance measures, calculated across all the nodes, from the simulations and the model predictions. As in the absence of hidden nodes, the model underestimates the probability of CCA failure (Fig. 13(a)). The model also slightly underestimates the probability of collision for a transmission in the presence of hidden nodes (Fig. 13(b)). This may be due to the fact that the model disregards the impact of ACK transmissions by the destinations of regular nodes on the transmissions by hidden nodes. These transmissions increase the probability of CCA failure for the hidden nodes and ultimately result in more frequent transmissions by hidden nodes than what is predicted by the model. The underestimate of the probability of CCA failure and the probability of collision for the regular nodes causes the model to underestimate the packet loss probability (Fig. 13(c)) and the packet latency (Fig. 13(d)) for the regular nodes. However, the model can clearly predict the "ball park" values for these performance measures. We performed a number of additional
Figure 12: Comparing the model predictions for regular nodes with NS2 simulation results when no hidden nodes are present.

Simulations with varying number of hidden nodes and their packet generation rates and found similar level of match between the model predictions and the simulation results.

In addition to NS2 simulations, we also evaluated the model predictions against the observed performance in a wireless sensor network made of commercial IEEE 802.15.4 hardware. The IEEE 802.15.4 operation in real hardware typically includes extra implementation-specific delays [28] that may significantly affect the performance. We observed that it was relatively straightforward to adjust the model presented in this paper to account for such delays and obtain a very good match between the model predictions and actual performance.
Figure 13: Comparing the model predictions for regular nodes with NS2 simulation results when one group of 50 hidden nodes is present (as shown in Figure 4). The $T$ value for regular nodes is 1s, whereas that for hidden nodes is listed in the figures as $T_h$. 
8. Conclusion

IEEE 802.15.4 enabled wireless sensor networks are finding increasing acceptance in various monitoring and control applications that hitherto depended on wired communication. The existing and planned deployments may consist of thousands of nodes with each node possibly competing with hundreds of other nodes for access to the transmission channel. Being a CSMA-based protocol, the IEEE 802.15.4 performance strongly depends on the number of nodes competing for channel access, their packet generation rates as well as the presence of any hidden nodes.

In this paper, we presented a stochastic model for the popular beaconless operation of IEEE 802.15.4 MAC protocol. Given the number of nodes competing for channel access and their packet generation rates, the model can very accurately predict the packet loss rate and latency. The model can also predict the impact of hidden nodes in certain deployments. This model is useful in several different ways. It can be used as a tool in designing the topology of an IEEE 802.15.4 based wireless network as well as to determine the values of various configuration parameters (macMinBE, macMaxBE, macMaxCSMABackoffs, macMaxFrameRetries etc.). The model can also be used to evaluate the impact of various modifications in the protocol to improve its performance.

References


