MODELING HIDDEN NODES COLLISIONS IN WIRELESS SENSOR NETWORKS: ANALYSIS APPROACH

A. Sjamsjiar Rachman [1,2]   **Wirawan [1]**   **Gamantyo Hendrantoro [1]**

[1]Department of Electrical Engineering, Institut Teknologi Sepuluh Nopember (ITS), Surabaya, 60111, Indonesia
[2]Department of Electrical Engineering, Universitas Mataram, Mataram, 83125, Indonesia
Email: sjamsjiar@elect-eng.its.ac.id   wirawan@ee.its.ac.id   gamantyo@ee.its.ac.id

This paper studied both types of collisions. In this paper, we show that advocated solutions for coping with hidden node collisions are unsuitable for sensor networks. We model both types of collisions and derive closed-form formula giving the probability of hidden and visible node collisions. To reduce these collisions, we propose two solutions. The first one based on tuning the carrier sense threshold saves a substantial amount of collisions by reducing the number of hidden nodes. The second one based on adjusting the contention window size is complementary to the first one. It reduces the probability of overlapping transmissions, which reduces both collisions due to hidden and visible nodes. We validate and evaluate the performance of these solutions through simulations.

Keywords: hidden nodes, wireless sensor network, collisions, avoidance

Collisions stem from simultaneous multiple access to a shared communication medium. In wireless networks, they occur when nodes use a contention-based medium access method. Specifically, a collision may happen when a receiver is within the transmission range of two or more nodes that are transmitting simultaneously so that it does not capture any frame. Each collision represents unnecessary energy dissipation. Therefore, reducing collisions should be one of the main design objectives of an access method for wireless sensor networks. Although there are schedule-based TDMA-like methods [1, 2] that collision-free, contention based methods [3, 4, 5, 6] are still widely used in sensor networks, because they are less complex, they adapt well to traffic changes and network dynamics, and they don't require tight synchronization between nodes. Moreover, contention-based methods are more suitable for unlicensed radio bands.

In contention-based methods with carrier sensing before transmission, collisions may be caused by two types of nodes: visible nodes and hidden nodes [7]. A collision caused by a visible node occurs when two nodes perform carrier sensing at the same time, detect that the channel is free and transmit at the same time. A collision caused by a hidden node occurs when a node performs a carrier sense and does not detect the ongoing transmissions with which it may interfere, because their signal strength is below its carrier sense threshold. As the node does not detect these signals, it falsely assesses the channel as free and transmits, causing a collision.

RELATED WORK

The problem of hidden node collisions has been extensively treated in the literature, however there is no sufficently efficient for sensor networks. The main solution to the problem of hidden nodes when assuming a single channel is the RTS/CTS handshake proposed in MACA [14]. The RTS/CTS exchange reserves the channel both around the sender and around the receiver to protect a transmission from being corrupted by hidden nodes. Although the use of RTS/CTS lowers hidden node collisions in wireless networks, it is ineïñĂective in multihop sensor networks for the following reasons.

1) RTS/CTS are control frames, therefore their transmissions is considered as an extra overhead. The RTC/CTS exchange may generate high overhead: about 40% to 75% of the channel capacity [3, 8]. Moreover, as RTS/CTS are broadcast, the energy drained by their transmissions may be considerable in preamble sampling protocols [3, 6, 9, 10, 11, 12, 13]. 2) Data frames in sensor networks are usually small; therefore, they have nearly the same size as RTS/CTS frames. In this case, the collision probability is nearly the same for data frames as for RTS/CTS. Thus, the probability that a communication is successful is higher when RTS/CTS are not used–when CTS/RTS are used, the communication is successful only if all RTS, CTS, and data frames are not corrupted, which is lower than the probability that the data frame alone is not corrupted. 3) RTS and CTS are broadcast frames. For some protocols, a unicast costs less energy than a broadcast [6, 9, 12, 13, 11, 10]. Thus, sending unicast data without RTS/CTS is much more beneficial. 4) RTS/CTS exchange does not avoid collisions in multi-hop networks [14]. 5) RTS/CTS exchange may lower the network capacity due to the exposed node problem [15]. 6) RTS/CTS exchange cannot be used for protecting broadcast frames.

As the use of RTS/CTS is unsuitable for multihop sensor networks, we to model the collisions and provide solutions, which are described in the next section.

HIDDEN NODES MODELING

We consider a sensor network in which node A wants to transmit a frame to node B (see Figure 1). We assume the following propagation model:

$$P_{rx}(B) = \frac{P_{tx}(A)}{a.d(A,B)^b} \tag{1}$$

This generic expression covers in fact two common models 1) Free space:

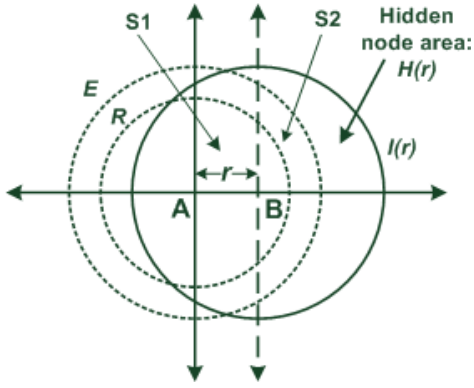$$a = \frac{(4p)_2}{l_2 G_t G_r} \quad b = 2 \tag{2}$$

Figure 1: Transmission, reception, and interference ranges.

and 2) Two Ray Ground Reflection:

$$a = \frac{1}{G_t G_r H_t^2 H_r^2} \qquad b = 4 \qquad (3)$$

where $G_t\,G_r$ is the antenna gain at the transmitter (resp. at the receiver) and $H_t\,(H_r)$ is the antenna height at the transmitter and (resp. at the receiver).

We define the following sets of nodes:

$N_{tx}(A)$: the set of nodes able to detect transmissions of node A:

$$N_{tx}(A) = \{x | d(x, A) \pounds E\} \qquad (4)$$

where E is the transmission range defined as:

$$E = \sqrt[b]{\frac{P_{tx}(A)}{a \times TR_{CS}}} \qquad (5)$$

The nodes are inside the dotted circle in Figure 1.

$N_{rx}(A)$: the set of nodes able to correctly receive frames sent by A in the absence of interference:

$$N_{rx}(A) = \{x | d(x, A) \pounds R\} \qquad (6)$$

where R is the reception range defined as:

$$R = \sqrt[b]{\frac{P_{tx}(A)}{a \times TR_{RX}}} \qquad (7)$$

A node outside this set cannot correctly decode the frames because of insufficient signal strength. This set is delimited by the dashed circle in Figure 1.

$N_i(A, B)$: the set of nodes that may interfere with a transmission and corrupt a frame sent by A to $B (r = d(A, B))$:

$$N_i(A, B) = \{x | d(x, A) \pounds I(r)\} \qquad (8)$$

Table 1: Notation	
$d(x, y)$	distance between nodes x and y
$P_{tx}(x)$	Transmission power of node x (Watt)
$P_{rx}(x)$	Received power at node x (Watt)
l	Wavelength (m)
a	Channel gain, assumed constant ($m^{-}\beta$)
b	Path loss exponent
E	Signal detection range
R	Signal reception range
$I(r)$	Signal interference range
TR_{CS}	Carrier sense threshold (Watt)
TR_{RX}	Reception threshold (sensitivity) (Watt)
TR_{CP}	Threshold of capture ratio

where $I(r)$ is the interference range. As a frame may be corrupted if,

$$\frac{\frac{P_{tx}(A)}{a \times r^b}}{\frac{P_{tx}(A)}{a \times d(x,A)^b}} < TR_{CP} \qquad (9)$$

and

$$d(x, A) \pounds r \sqrt[b]{TR_{CP}} \qquad (10)$$

the interference range is the following:

$$I(r) = r \sqrt[b]{TR_{CP}} \qquad (11)$$

Note that the cardinality of this set depends on the distance between A and B.

$N_v(A, B)$: the set of nodes for which A is visible:

$$N_v(A, B) = N_{tx}(A, B) \varsigma N_i(A, B) \qquad (12)$$

A visible node may corrupt a frame sent by A to B, but before transmitting its frame, the node will sense the carrier and defer until the end of the current transmission.

$N_h(A, B)$: the set of nodes for which A is hidden:

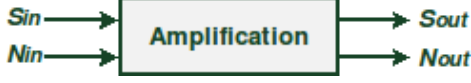$$N_h(A, B) = N_i(A, B) \setminus N_v(A, B) \qquad (13)$$

A hidden node may corrupt a frame sent by A to B, because it does not receive the signal of A, so its transmission will result in a collision.

Let us denote by $n_h(r)$ the number of hidden nodes (resp. $n_v(r)$ the number of visible nodes). If we assume that nodes are distributed over a surface with a homogeneous density D (number of nodes per m^2), $n_h(r)$ is proportional to the area of the zone in which hidden nodes may appear.

Let $S(r)$ be the common area of the zones corresponding to $N_{tx}(A)$ and $N_i(A, B)$. The circles of radius E and $I(r)$ intersect at two points, they are $(u, -\sqrt{E^2 - u^2})$ and $(u, \sqrt{E^2 - u^2})$ where $u = \frac{E^2 + r^2 - I(r)^2}{2r}$

Thus,

$$S(r) = 2 \times [S_1(r) + S_2(r)] \qquad (14)$$

Figure 2: Reception System.

Figure 3: Free Space Model.

$$S_1(r) = \int_{I(r)+r}^{u} \sqrt{I(r)^2 - t^2} dt$$

$$= I(r)^2 \left(\frac{p - a_2}{2} + \frac{sin2a_2}{4} \right)$$

$$S_2(r) = \int_{u}^{E} \sqrt{E^2 - t^2} dt$$

$$= E^2 \left(\frac{a_3}{2} + \frac{sin2a_3}{4} \right)$$

$$\tag{15}$$

where $a_2 = arccos\frac{u-r}{I(r)}$ and $a_3 = arccos\frac{u}{E}$. Finally, we obtain the following results.

Proposition 1: The number of hidden nodes is:

$$n_h(r) = \begin{cases} 0 & E^3 I(r) + r \\ p \times (l(r)^2 - E^2) \times D & E \pounds I(r) - r \\ p \times (I(r)^2 - S(r)) \times D & otherwise \end{cases} \tag{16}$$

where:
$E^3 I(r) + r$, interference $(B)I$ listening (A)
$E \pounds I(r) - r$, interference $(B)E$ listening (A)
$I(r) - r \pounds E \pounds I(r) + r$, intersection calculate u

In third case, there is an intersection. Therefore, refer to $X(x, y)$ as the positive point of this intersection, i.e. $x > 0$ and $y > 0$.

We have the equations of the circles of transmission range and interference range as follows:

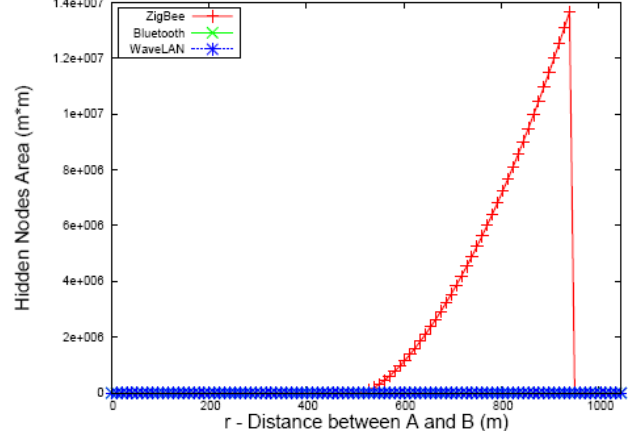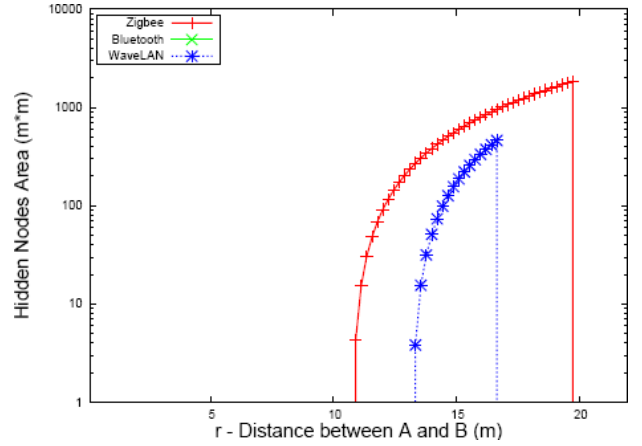$$x^2 + y^2 = E^2 \tag{17}$$

$$(x - r) + y^2 = I^2(r) \tag{18}$$

Solving these equations gives:

$$x = \frac{E^2 + r^2 - I^2(r)}{2r} \tag{19}$$

$$y = \pm\sqrt{E^2 - x^2} \tag{20}$$

Proposition 2: The number of visible nodes is:

$$n_v(r) = p \times I(r)^2 \times D - n_h(r) \tag{21}$$

Figure 4: Two Ray Ground Reflection Model, antenna height = 0.1m.

Numerical results for ZigBee, Bluetooth, WaveLAN

We consider three radio technologies: Bluetooth, Zig-Bee (IEEE 802.15.4), and WaveLAN (IEEE 802.11). Table 2 presents their parameters that come from the specifications of industrial products or IEEE standards.

The system described in Figure 2 has the following characteristics: $S_i n$ is the strength of the received signal. $N_i n$ is the strength of the noise of the system. $S_o ut$ is the strength of the signal after amplification. $N_o ut$ is the strength of the noise after amplification.

The noise factor F of this system is defined as:

$$F = \frac{SNR_{in}}{SNR_{out}} = \frac{\frac{S_{in}}{N_{in}}}{\frac{S_{out}}{N_{out}}} \tag{22}$$

The Noise Figure (NF) is of this system is the Noise Factor converted to dB, i.e. $NF = 10log(F)$. We have,

$$NF = (SNR_{in})_{dB} - (SNR_{out})_{db} \tag{23}$$

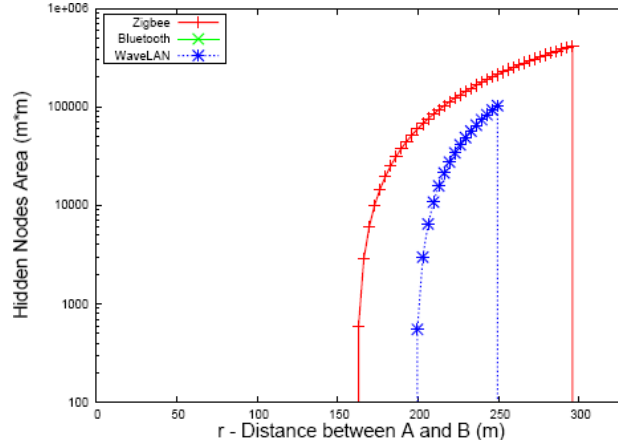$$= (S_{in})_{dB} - (N_{in})_{db} - (SNR_{out})_{db} \tag{24}$$

3

Figure 5: Two Ray Ground Reflection Model, antenna height = 1.5m.

Table 2: Radio Parameters

	Bluetooth (IEEE 802.15.1)	ZigBee (IEEE 802.15.4)	WaveLAN (IEEE 802.11)
$P_{tx}(x)$	0 dBm	0 dBm	24.5 dBm
TR_{RX}	-80 dBm	-92 dBm	-64.4 dBm
TR_{CP}	11 dB	10 dB	10 dB
TR_{CS}	-102 dBm	-99 dBm	-78 dBm

Then,

$$(S_{in})_{dB} = NF + (N_{in})_{db} + (SNR_{out})_{db} \qquad (25)$$

We have,

$$N_{in} = KTBw \qquad (26)$$

where K is the constant of Boltzman, Bw is the bandwidth, and T is the temperature. At 25, we have $KT = -174dBm$. If we have a channel of $1MHz(Bw = 106)$, then:

$$\begin{aligned} (N_i n)_d B &= KT + 10 log_{10}(10^6) \\ &= -174 + 60 = -114 \qquad (27) \end{aligned}$$

In the systems currently in use, NF is approximately Fig. 5. Free Space Model equal to 6 dB. In computation of $S_i n$, referred to as TR_{CS}, we have taken $(SNR_{out})_d B$ equal to 6 dB. Therefore, we have the following values of TR_{CS}: For Bluetooth, we have TR_{CS} = -174 + 10 $log_{10}(106)$ + 6 + 6 = -102dBm. For Zigbee, we have TR_{CS} = -174 + 10 $log_{10}(2.106)$ + 6 + 6 = -99dBm.

For $TR_R X$, the IEEE 802.15.4 standard recommends the value of -85dBm, whereas the ZigBee compatible Freescale MC13192 transceiver uses -92dBm. For 802.11, we use the values encoded in ns2 corresponding to the physical specifications of 914MHz Lucent WaveLAN DSSS. We theoretically calculate the carrier sense threshold $TR_C S$ for the ZigBee and Bluetooth radios.

The antenna gain for transmission and reception is the same for all nodes and fixed to 1 (Gr = Gt = 1). Figure 3 shows the area that contains hidden nodes in function of the distance between the sender and the receiver for the Free Space model. Even if this model is purely theoretical, we can observe that there are no hidden nodes for Bluetooth and WaveLAN. ZigBee presents an important hidden nodes area for the distance range between 500m and 1000m.

Figures 4 and 5 show the hidden nodes area when assuming the Two Ray Ground Reflection model. The scale is logarithmic (the linear scale of the previous figure was needed to show the zero area for Bluetooth and WaveLAN). There are hidden nodes areas only for WaveLAN and ZigBee whereas they are absent for Bluetooth.

HIDDEN NOISE AVOIDANCE

Hidden nodes may limit the performance of multihop sensor networks, because their transmissions result in collisions. Once we have quantified the problem by deriving the number of hidden nodes, we can consider various solutions for avoiding this limitation. We consider below an existing approach the Carrier Sense Tuning [16, 17] and propose another solution.

Carrier Sense Tuning

In this approach, the carrier sense threshold TR_{CS} is tunable. This means that the signal detection range (Eq. 4) becomes ETR_{CS}. We can analyze the area of the hidden nodes zone for different values of TR_{CS}.

There will be no collisions due to hidden nodes, if the area of the hidden nodes zone becomes null, i.e. when $E(TR_{CS})I(r)+r, r$ being the distance between the sender A and the receiver B. We thus have:

$$\sqrt[b]{\frac{P_{tx}(A)}{a \times TR_{CS}(r)}} = r \times \sqrt[b]{TR_{CP}} + r \qquad (28)$$

Then,

$$TR_{CS}(r) = \frac{P_{tx}(A)}{a(r \times \sqrt[b]{TR_{CP}} + r)^b} \qquad (29)$$

If we set r to the maximum reception range R, there will be no hidden nodes. Although this prevents collisions due to hidden nodes, it forces nodes to behave in a conservative way. Many transmissions may be delayed because a receiver will often detect the carrier due to the large radio carrier sense range. In addition to that, increasing the carrier sense range may be not possible for physical reasons. Another problem with Carrier Sense Tuning is the presence of physical obstacles between nodes. In this case, increasing the radio carrier sense range does not solve the problem of hidden nodes.

Adjusting Contention Window

In this section, we propose a solution to the hidden nodes problem based on adjusting the contention window. As the access method during active periods basically behaves as the 802.11 DCF, the probability that a node transmits in a slot is given by [18]:

$$t = \frac{2}{CW + 1} \qquad (30)$$

This expression is based on the following assumptions: nodes are greedy, i.e. nodes have always frames to send during the active period, there is no exponential backoff, nodes do not decrement their contention counter when the channel is not idle. It is only decremented once when the channel is sensed busy (which is not the case in 802.11, in fact).

The first assumption is justified if we consider that in many sensor network applications, communications tend to synchronize the network, e.g. sensors decide to send their data at the same time such as during the route request operation or gathering sensor information.

Then, we may compute probability p_c that a transmission attempt in a given slot ends up as a collision involving either a visible node or a hidden node. We consider that each slot is composed of two phases (which is different from the standard 802.11 DCF): a node first performs CCA of duration t_{CCA} to sense the channel state and then transmits if the channel is free. Only the visible nodes that start their slots at the same instant as the transmission may cause a collision: it can be seen from Figure 1 that only if stations X and A perform CCA at the same instant, they will both observe the channel free and eventually collide. This mechanism marginally extends the backoff between transmissions, but we neglect its impact on the transmission probability used bellow.

We call p_s the fraction of the visible nodes that may cause a collision. Assuming that the nodes have independently distributed time references and that a transmission needs to last the entire t_{CCA} interval for a station to detect an ongoing transmission, $p_s = 2' \frac{t_{CCA}}{t_{SLOT}}$. A transmission is successful if: 1) no node, among $n_v(r)$ nodes, transmits in the same slot. This implies that it did not overhear the transmission in the channel assessment phase,

$$P_v = (1 - t)_{n_v(r)'p_s}$$

no node, among $n_h(r)$ nodes, transmits in the same slot,

$$P_H = (1 - t)_{n_h(r)}$$

Thus p_c is the probability that, in a time slot, at least one of the visible and hidden nodes (relatively to the transmitting node), transmits. That is:

$$p_c = 1 - P_H P_V = 1 - (1 - t)^{n_h(r) + n_v(r)'p_s} \qquad (31)$$

which can be represented as:

$$\left(\frac{CW - 1}{CW + 1}\right)^{n_h(r) + n_v(r)'p_s} = 1 - p_c \qquad (32)$$

and finally we obtain:

$$CW(r) = \frac{1 + \sqrt[n_h(r)+n_v(r)'p_s]{1 - p_c}}{1 - \sqrt[n_h(r)+n_v(r)'p_s]{1 - p_c}} \qquad (33)$$

We could use this expression to dynamically adjust CW so that collision probability p_c stays under a given value. However, notice that the contention window CW depends on r, the distance between the sender and the receiver - applying this result for controlling CW is quite difficult, because all the nodes in the network should know the distance between nodes willing to communicate. To avoid this problem, we can use a static value of CW by taking $r = R$, which corresponds to the worst case when the distance between nodes is equal to the signal reception range R. In this case, the contention window becomes:

$$CW(r) = \frac{1 + \sqrt[n]{1 - p_c}}{1 - \sqrt[n]{1 - p_c}} \qquad (34)$$

where $n_h(r) + n_v(r)'p_s$.

Figure 6 shows the required value of CW to obtain a given collision probability (ZigBee radio parameters).

SIMULATION

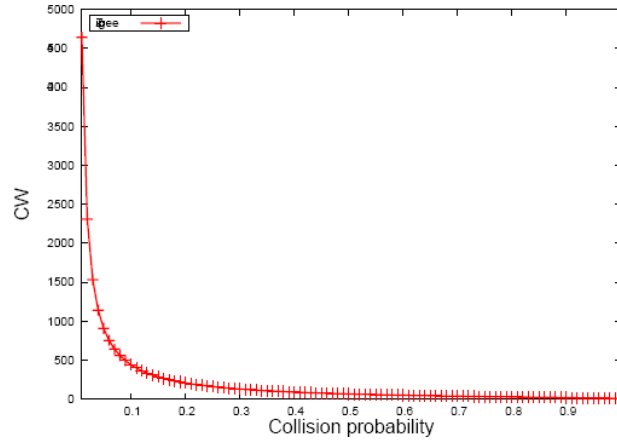We have used NS2 to evaluate the performance of the proposed method for avoiding the hidden nodes problem.

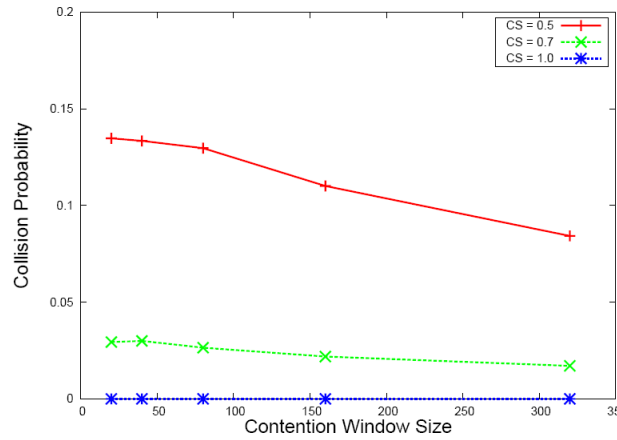**Figure 6:** Contention Window in function of collision probability for ZigBee.

Figure 7: Collision probability due to hidden nodes, slot of 32 μs.

We compare Adjusting Contention Window with Carrier Sense Tuning. We have set up the following simulation experiment: 30 nodes are uniformly distributed in a 40mx40m square, we use the parameters of the Chipcon's CC2420 radio transceiver with a bandwidth of 250Kbps and a radio transmission range of about 20m (resulting from the Two Ray Ground propagation model with antenna height of 0.1m), we randomly pick two nodes, a source and a destination, and make sure that they are not reachable in one hop, the source node broadcasts 50 frames of 60 bytes at a constant bit rate (the inter-frame interval is set to 2ms), each node re-broadcasts only once the frame it receives, we use the MAC protocol with two different values of a slot ($32\mu s$ and $3840\mu s$, twice the transmission of a maximum sized frame), we set three different values for the carrier sense threshold: $TR_{CS}(0.5R)$, $TR_{CS}(0.7R)$, and $TR_{CS}(R)$, which correspond to CS = 0.5, 0.7 and 1 according to (Eq. 19) each point in the figures represents the average of 10 values.

We can distinguish two types of collisions: those due to contention when a visible node tries to access the channel during the same slot and collisions due to hidden nodes. A collision with a hidden node occurs if the distance between two transmitters is larger that the signal transmission range, otherwise it is a collision due to channel contention.

Figures 7 and 8 show the observed collision probability due to hidden nodes. We can notice that it strongly depends on the carrier sense range the case $CS = 1(TR_{CS}(R))$ shows that Carrier Sense Tuning eliminates collisions that caused by hidden nodes.

However, as previously stated, such increase of the carrier sense range may be not possible or not effective due to obstacles. A reasonable value of the carrier sense threshold corresponds to $CS = 0.5(TR_{CS}(0.5R))$, for which we can see that the collision probability decreases with the increase of the contention window. If we choose a threshold of an acceptable collision probability, we can find the contention window for which the collisions will be negligible. We also notice that the collision probability is significantly smaller when the slot time is large (3840 μs).

Figure 9 show an inverse phenomenon the collision probability due to contention increases with the radio carrier sense range (we only show the graph for the short slot of 32 μs. The graph is almost the same for the long slot of 3840 μs). This means that even if Carrier Sense Tuning has a beneficial effect on collisions due to hidden nodes, it increases other collisions. We can also see that when choosing a sufficiently large contention window, we can
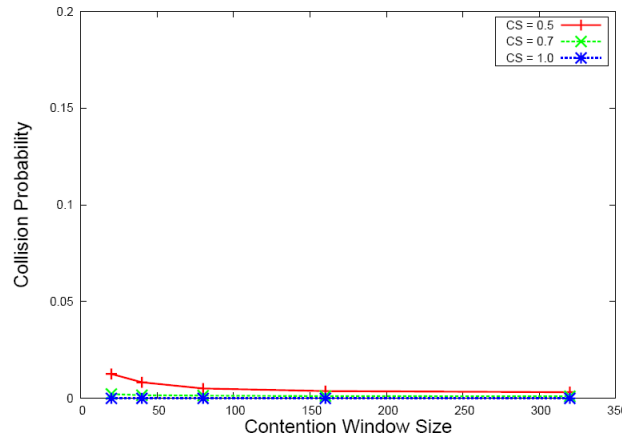
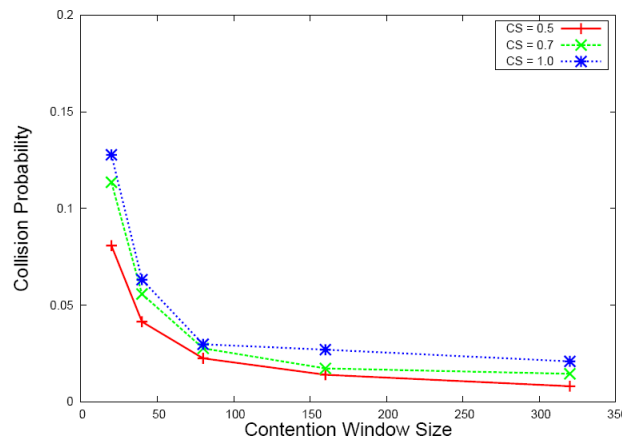**Figure 8:** Collision probability due to hidden nodes, slot of 3840 μs.

Figure 9: Collision probability due to contention.

keep this type of collisions acceptably low.

CONCLUSIONS

In this paper, we have analyzed the hidden node problem and found expressions for the number of hidden nodes and the probability of collisions. We have proposed to use a sufficiently large value of the contention window to guarantee an acceptably low collision probability due to hidden nodes: based on the characteristics of a given sensor networks (area, node density, antenna height etc.) we estimate the number of hidden nodes and then fix the contention window in function of the number of hidden nodes so that the probability of collisions stays under some threshold.

As we use the transmission range as the worst case estimate for the collision probability, the actual number of collisions should be even smaller. We have simulated an example sensor network based on ZigBee radios and shown that our access method can lower the collision probability in the desired way.

REFERENCES

[1] Rajendran, V., Obraczka, K., Garcia-Luna-Aceves, J.: *Energy-Efficient, Collision Free Medium Access Control for Wireless Sensor Networks*. In: Proceedings of ACM Sensys, Los Angeles, CA (November 2003) 181–92

[2] Rhee, I., et al: *DRAND: Distributed Randomized TDMA Scheduling ForWireless Adhoc Networks*. In: Proceedings of ACM MobiHoc, Florence, Italy (May 2006)

[3] Polastre, J., Hill, J., Culler, D.: *Versatile Low Power Media Access forWireless Sensor Networks*. In: Proceedings of ACM SenSys. (2004)

[4] Ye, W., Heidemann, J., Estrin, D.: *An Energy-Efficient MAC Protocol for Wireless Sensor Networks*. In: Proceedings of IEEE Infocom, New York, NY (July 2002) 1567–76

[5] van Dam, T., Langendoen, K.: *An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks*. In: Proceedings of ACM Sensys, Los Angeles, CA (November 2003) 171–80

[6] Enz, C., El-Hoiydi, A., Decotignie, J., Peiris, V.: *WiseNET: An Ultralow-Power Wireless Sensor Network Solution*. IEEE Computer **37**(8) (August 2004) 62–70

[7] Tobagi, F., Kleinrock, L.: *Packet Switching in Radio Channels: Part II The Hidden Terminal Problem in Carrier Sense Multiple-Access and the Busy-Tone Solution*. IEEE Trans. On Comm. **23**(12) (December 1975) 1417–33

[8] Woo, A., Culler, D.: *A Transmission Control Scheme for Media Access in Sensor Networks*. In: Proceedings of ACM Mobicom, Rome, Italy (July 2001)

[9] Ye, W., Silva, F., Heidemann, J.: *Ultra-Low Duty CycleMAC with Scheduled Channel Polling*. In: Proceedings of ACM SenSys, Boulder, CO (November 2006)

[10] Chipcon Corporation: *CC2500 Single Chip Low Cost Low Power RF Transceiver, Data Sheet*. Technical report (2005)

[11] Schurgers, C., et al: *Optimizing Sensor Networks in the Energy-Latency-Density Design Space*. IEEE Transactions on Mobile Computing **1**(1) (January-March 2002) 70–80

[12] Buettner, M., et al: *X-MAC: A Short Preamble MAC Protocol For Duty-Cycled Wireless Networks*. In: Proceedings of ACM SenSys, Boulder, CO (November 2006)

[13] Mahlknecht, S., Boeck, M.: *CSMA-MPS: A Minimum Preamble Sampling MACProtocol for Low Power Wireless Sensor Networks*. In: Proceedings of IEEE Workshop on Factory Communication Systems, Vienna, Austria (September 2004)

[14] Xu, S., Saadawi, T.: *Does the IEEE 802.11 MAC Protocol Work Well in Multihop Ad Hoc Networks?* IEEE Communications Magazine (June 2001) 130–137

[15] Sobrinho, J., de Haan, R., Brazio, J.: *Why RTS-CTS is not your Ideal Wireless LAN Multiple Access Protocol*. In: Proceedings of IEEE WCNC, New Orleans, LA (March 2005)

[16] Enz, C., El-Hoiydi, A., Decotignie, J., Peiris, V.: *WiseNET: An Ultralow-Power Wireless Sensor Network Solution*. IEEE Computer **37**(8) (August 2004) 62–70

[17] Deng, J., Liang, B., Varshney, P.K.: *Tuning the Carrier Sensing Range of IEEE 802.11 MAC*. In: Proceedings of the IEEE Globecom, Dallas, TX (Nov-Dec 2004)

[18] Bianchi, G.: *Performance Analysis of the IEEE 802.11 Distributed Coordination Function*. IEEE JSAC **13**(3) (March 2000) 535–47