Hidden Nodes Avoidance in Wireless Sensor Networks

Abdelmalik Bachir and Dominique Barthel
France Telecom R&D
Meylan, France
{Abdelmalik.Bachir, Dominique.Barthel}@francetelecom.com

Martin Heusse and Andrzej Duda
LSR-IMAG Laboratory
Grenoble, France
{Martin.Heusse, Andrzej.Duda}@imag.fr

***Abstract*— We propose a new access method for wireless multi-hop sensor networks. It reduces collisions due to hidden nodes, a source of significant energy dissipation. Our access method operates similarly to SMAC by alternating sleeping and active periods, but it does not use RTS/CTS. Instead, it adjusts the contention window so that the probability of collisions due to hidden nodes becomes negligible. We analyze the hidden node problem to derive expressions for the number of hidden nodes and the probability of collisions. We show the numerical results for different low power radios and validate our access method through simulation.**

I. Introduction

We consider wireless sensor networks composed of a large number of battery operated nodes. Nodes share a common radio channel and are organized as a multi-hop network—communication between nodes requires relaying packets by intermediate nodes. The medium access control (MAC) sets up rules for using the common channel. The first goal of a good MAC protocol is the energy efficiency, because sensor networks should be long-lived without battery recharge or replacement. Performance indices like throughput, delay, and fairness are much less important since sensor networks usually support only one application with limited communication requirements.

Radio communication is one of the main sources of energy dissipation because of: idle listening, frame collisions, traffic overhearing, and control packet overhead [1], [2]. We follow the same approach to reduce energy consumption in idle listening as SMAC [1], which defines sleeping and active periods. The radio transceiver is switched on only during an active period. SMAC manages contention between nodes in a similar way to the IEEE 802.11 DCF [3].

The second source of energy dissipation, namely frame collisions, arises in CSMA-based access methods. Although there exists collision-free access methods such as schedule-based TDMA or FDMA, CSMA-based methods are the most widely used techniques for multi-hop wireless networks, because of their simplicity and ability to work in a decentralized environment. We can cite SMAC [1] and WiseMAC [4] as examples of such access methods.

A wireless multi-hop sensor network should be *dense* to ensure that all nodes can communicate with each other via intermediate nodes. When a CSMA-based method is used in such a network, collisions may happen when a receiver is within the transmission range of two transmitters that are transmitting simultaneously so that the receiver captures neither frame. As each collision represents unnecessary energy dissipation, reducing collisions should be the main design objective of a CSMA-based access method. There are two main reasons for collisions: two nodes choose the same slot in a contention window or the hidden node problem [5] (a hidden node may corrupt a frame being transmitted, because it does not receive the signal of the transmitter). A significant part of collisions is due to this last problem.

In this paper, we propose a new access method that reduces collisions due to hidden nodes. It is similar to SMAC, but uses a different approach to avoid collisions caused by hidden nodes. We analyze the hidden nodes problem and show that it is possible to reduce the probability of collisions by setting correctly the contention window.

II. Related work

Several authors dealt with the problem of hidden nodes, however there is no satisfactory solution that does not rely on out of band channels: BTMA (Busy Tone Multiple Access) provides a solution in a centralized system with a base station [5], whereas DBTMA (Dual Busy Tone Multiple Access) offers a distributed solution for ad hoc networks [6]. Other solutions such as RTS/CTS proposed in MACA [7] only alleviates the problem by degenerating to ALOHA when hidden terminals are present [6].

The hidden nodes problem in wireless multi-hop sensor networks was mainly addressed with two techniques: RTS/CTS [1] and Carrier Sense Tuning [4], [8].

RTS/CTS was basically designed to reduce the number of collisions due to hidden nodes by reserving the channel around both the sender and the receiver to protect frame transmission from being corrupted by hidden nodes. However, this method presents several problems when used in wireless multi-hop sensor networks:

- the energy consumption related to a RTS/CTS exchange is significant,
- as data frames are usually small, the collision probability is the same for data frames as for RTS/CTS, so it does not make any difference if the technique is used or not,
- it does not avoid collisions in multi-hop networks [9],

- it may lower the network capacity due to the exposed node problem,
- it cannot be used for broadcast frames.

Several MAC protocols have proposed to use Carrier Sense Tuning to cope with the hidden node problem [4], [8]. The key idea comes from the observation that hidden nodes cause collisions, because their radio carrier sense range is not large enough to sense on going transmissions they may collide with. Hence, a node should tune its radio carrier sense range to make sure that when it transmits, there is no another transmission. Although this method allows a node to detect ongoing transmissions, it is not suitable for all situations. For example, it assumes a homogeneous radio channel for all nodes, which is not always possible because of obstacles, different antenna height, etc. Even if the channel is homogeneous, it is not possible to increase the carrier sense range of radio transceivers indefinitely due to physical limitations.

III. MAC Access Method

We assume that our access method operates similarly to SMAC by alternating sleeping and active periods. It is not required for nodes to be synchronized. When a node wakes up and has a frame to send, it chooses a backoff b, an integer distributed uniformly in the contention window $[0, CW[$ and waits for b time slots before attempting to transmit. The node decrements the counter each time it senses the medium free for a duration of a slot time. When the counter expires, the node sends a frame. We consider two different definitions of a slot:

- a slot can be short, as in 802.11, corresponding to the minimum time required for CCA (Clear Channel Assessment) to sense the channel state (idle or busy). This time takes into account the propagation delay, the delay for switching from reception to transmission, and channel sensing itself. When a node starts to transmit at a given slot, any other node that has chosen a different slot will learn about the transmission and defer.
- a slot can be long, for example up to the duration of a maximum sized frame or even twice this duration. A node performs CCA at the beginning of a slot (cf. Figure 1) and defer if the slot is sensed busy, otherwise it transmits its frame. When nodes are not synchronized, if the slot is twice the transmission time, they may collide only if they choose the same backoff interval (cf. Figure 2). With such a long slot, we make the effect of hidden nodes equivalent to the one of visible nodes in the short slot case, because a collision occurs only if a hidden node transmits at the same slot as the current transmission.

In the rest of the paper, we will analyze the hidden node problem so that for a given density of the sensor network we will be able to estimate the probability of collisions due to hidden nodes. Then, we set the contention window CW so that the probability of collisions due to hidden nodes becomes negligible.

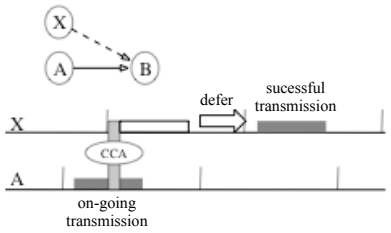

Fig. 1. Large slots allow channel sensing before transmission.

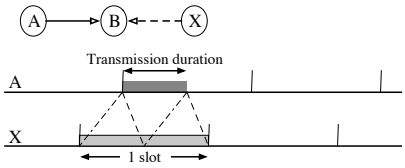

Fig. 2. Collision in the case of a long slot.

IV. Analysis of the Hidden Nodes Problem

We consider a sensor network in which node A wants to transmit a frame to node B (cf. Figure 3). We assume the following propagation model:

$$P_{rx}(B) = \frac{P_{tx}(A)}{\alpha \cdot d(A,B)^{\beta}} \tag{1}$$

This generic expression covers in fact two common models:

Free Space	*Two Ray Ground Reflection*
$\alpha = \frac{(4\pi)^2}{\lambda^2 G_t G_r}$	$\alpha = \frac{1}{G_t G_r H_t^2 H_r^2}$
$\beta = 2$	$\beta = 4$

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:

$$N_{tx}(A) = \{x | d(x,A) \leq E\}, \tag{2}$$

where E is the transmission range defined as:

$$E = \sqrt[\beta]{\frac{P_{tx}(A)}{\alpha \cdot TR_{CS}}}. \tag{3}$$

The nodes are inside the dotted circle in Figure 3.

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

$$N_{rx}(A) = \{x | d(x,A) \leq R\}, \tag{4}$$

where R is the reception range defined as:

$$R = \sqrt[\beta]{\frac{P_{tx}(A)}{\alpha \cdot TR_{RX}}}. \tag{5}$$

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 3.

TABLE I

NOTATION FOR THE ANALYSIS

$d(x,y)$	distance between nodes x and y
$P_{tx}(x)$	Transmission power of node x (Watt)
$P_{rx}(x)$	Received power at node x (Watt)
λ	Wavelength (m)
α	Channel gain, assumed constant ($m^{-\beta}$)
β	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

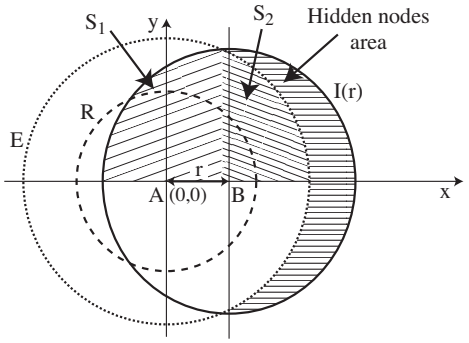

Fig. 3. Transmission, reception, and interference ranges.

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

$$N_i(A,B) = \{x | d(x,A) \leq I(r)\}, \tag{6}$$

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

$$\frac{\frac{P_{tx}(A)}{\alpha \cdot r^{\beta}}}{\frac{P_{tx}(A)}{\alpha \cdot d(x,A)^{\beta}}} < TR_{CP} \tag{7}$$

and

$$d(x,A) \leq r \sqrt[\beta]{TR_{CP}}, \tag{8}$$

the interference range is the following:

$$I(r) = r \sqrt[\beta]{TR_{CP}}. \tag{9}$$

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*:

$$N_v(A,B) = N_{tx}(A,B) \cap N_i(A,B) \tag{10}$$

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*:

$$N_h(A,B) = N_i(A,B) \backslash N_v(A,B) \tag{11}$$

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: $(u, -\sqrt{E^2-u^2})$ and $(u, \sqrt{E^2-u^2})$, where $u = \frac{E^2+r^2-I(r)^2}{2r}$. Thus,

$$S(r) = 2 \cdot [S_1(r) + S_2(r)], \tag{12}$$

where

$$S_1(r) = \int_{-I(r)+r}^{u} \sqrt{I(r)^2 - t^2}dt = I(r)^2 \left[\frac{\pi - a_2}{2} + \frac{\sin 2a_2}{4}\right],$$

$$S_2(r) = \int_{u}^{E} \sqrt{E^2 - t^2}dt = E^2 \left[\frac{a_3}{2} + \frac{\sin 2a_3}{4}\right], \tag{13}$$

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:

$$n_h(r) = \begin{cases} 0 & \text{if } E \geq I(r) + r, \\ \pi \cdot [I(r)^2 - E^2] \cdot D & \text{if } E \leq I(r) - r, \\ [\pi \cdot I(r)^2 - S(r)] \cdot D & \text{otherwise} \end{cases} \tag{14}$$

Proposition 2: The number of visible nodes is:

$$n_v(r) = \pi \cdot I(r)^2 \cdot D - n_h(r). \tag{15}$$

A. Numerical results for Bluetooth, ZigBee, WaveLAN

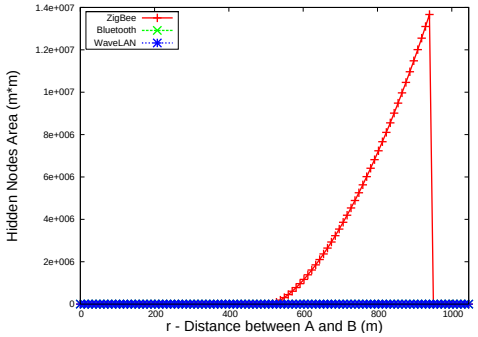

Fig. 4. Hidden nodes area, Free Space model

We consider three radio technologies: Bluetooth, ZigBee (IEEE 802.15.4), and WaveLAN (IEEE 802.11). Table II presents their parameters that come from the specifications of industrial products or IEEE standards. [1]

[1]for TR_{RX}, 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_{CS} for the ZigBee and Bluetooth radios.

TABLE II
RADIO PARAMETERS

	Bluetooth (802.15.1)	ZigBee (802.15.4)	WaveLAN 914 MHz (802.11)
P_{tx}	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
Antenna height: $H_t = H_r$	0.1 m or 1.5 m	0.1 m or 1.5	0.1 m or 1.5 m

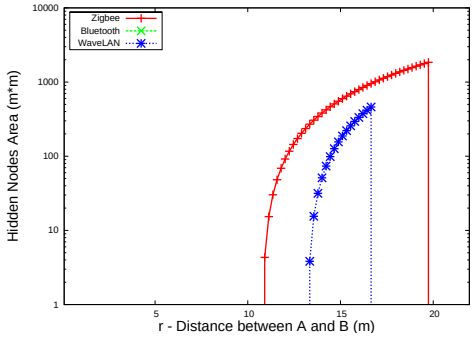

Fig. 5. Hidden nodes area, Two Ray Ground Reflection model, antenna height 0.1m.

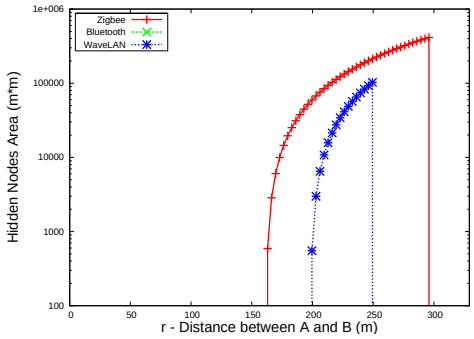

Fig. 6. Hidden nodes area, Two Ray Ground Reflection model, antenna height 1.5m.

The antenna gain for transmission and reception is the same for all nodes and fixed to 1 ($G_r = G_t = 1$).

Figure 4 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 5 and 6 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.

V. AVOIDING HIDDEN NODES PROBLEM

Hidden nodes may limit the performance of multi-hop 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 [4], [8], and propose another solution.

A. Carrier Sense Tuning

In this approach, the carrier sense threshold TR_{CS} is tunable. This means that the signal detection range (Eq. 2) becomes $E(TR_{CS})$. 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 $E(TR_{CS}) \geq I(r) + r$, r being the distance between the sender A and the receiver B. We thus have:

$$\sqrt[\beta]{\frac{P_{tx}(A)}{\alpha TR_{CS}(r)}} = r \cdot \sqrt[\beta]{TR_{CP}} + r \tag{16}$$

Then,

$$TR_{CS}(r) = \frac{P_{tx}(A)}{\alpha \left(r \cdot \sqrt[\beta]{TR_{CP}} + r\right)^{\beta}} \tag{17}$$

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.

B. 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 [10]:

$$\tau = \frac{2}{CW + 1} \tag{18}$$

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[2].

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[3]. 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, $p_s = 2 \times \frac{t_{\mathrm{CCA}}}{t_{\mathrm{SLOT}}}$.

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. $P_V = (1-\tau)^{n_v(r)\times p_s}$.
2) no node, among $n_h(r)$ nodes, transmits in the same slot. $P_H = (1-\tau)^{n_h(r)}$

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:

$$p_c = 1 - P_H P_V = 1 - (1-\tau)^{n_h(r)+n_v(r)\times p_s}, \tag{19}$$

which can be represented as:

$$\left(\frac{CW-1}{CW+1}\right)^{n_h(r)+n_v(r)\times p_s} = 1 - p_c, \tag{20}$$

and finally we obtain:

$$CW(r) = \frac{1 + \sqrt[n_h(r)+n_v(r)\times p_s]{1-p_c}}{1 - \sqrt[n_h(r)+n_v(r)\times p_s]{1-p_c}}. \tag{21}$$

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:

$$CW(R) = \frac{1 + \sqrt[n]{1-p_c}}{1 - \sqrt[n]{1-p_c}}, \tag{22}$$

where $n = n_h(R) + n_v(R) \times p_s$.

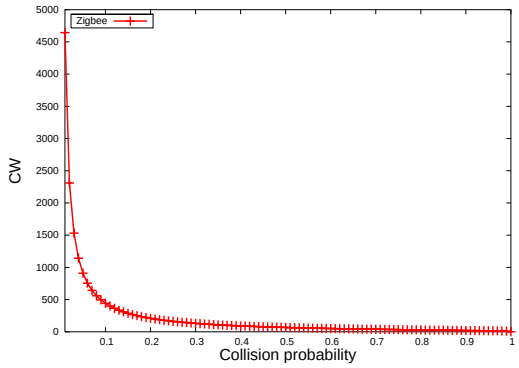

Fig. 7. Contention Window in function of collision probability for ZigBee.

Figure 7 shows the required value of CW to obtain a given collision probability (ZigBee radio parameters).

VI. Simulations

We have used `ns2` to evaluate the performance of the proposed method for avoiding the hidden nodes problem: 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 Freescale's MC13192 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 described in Section III with two different values of a slot (32μs and 3840μs, 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. 17)
- 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 8 and 9 show the observed collision probability due to hidden nodes. We can notice that it strongly depends on the

[2]it is only decremented once when the channel is sensed busy (which is not the case in 802.11, in fact).

[3]This mechanism marginally extends the backoff between transmissions, but we neglect its impact on the transmission probability used bellow.

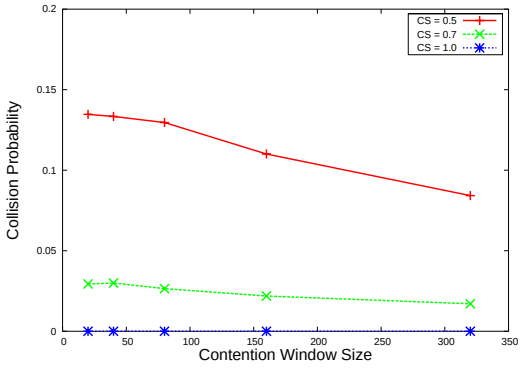

Fig. 8. Collision probability due to hidden nodes, slot of 32 μs.

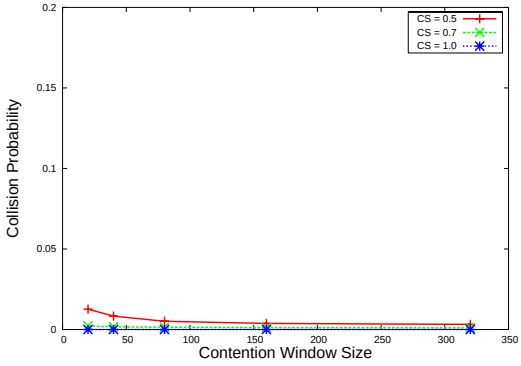

Fig. 9. Collision probability due to hidden nodes, slot of 3840 μs.

carrier sense range—the case $CS = 1$ ($TR_{CS}(R)$) shows that Carrier Sense Tuning eliminates collisions 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 (3840μs).

Figure 10 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 keep this type of collisions acceptably low.

VII. Conclusion

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

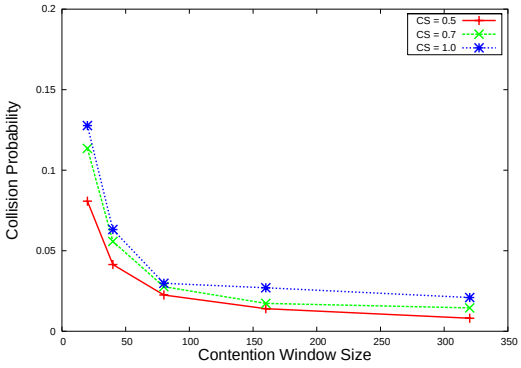

Fig. 10. Collision probability due to contention.

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] Wei Ye, John Heidemann, and Deborah Estrin, "An energy-efficient MAC protocol for wireless sensor networks," *Proceedings of the IEEE Infocom*, pp. 1567–76, New York, NY, July 2002.

[2] T. van Dam and K. Langendoen, "An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks," *Proceedings of the ACM Sensys*, pp. 171–80, Los Angeles, CA, November 2003.

[3] L. M. S. Committee, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Computer Society ed. IEEE Std. 802.11-1197, 1997.

[4] Enz, C.C.; El-Hoiydi, A.; Decotignie, J.; Peiris, V., "WiseNET: An Ultralow-Power Wireless Sensor Network Solution," *IEEE Computer*, vol. 37, no. 8, pp. 62–70, August 2004.

[5] Tobagi, F. and L. Kleinrock, "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.*, vol. 23, no. 12, pp. 1417–33, December 1975.

[6] J. Deng and Z. Haas, "Dual Busy Tone Multiple Access (DBTMA)- a Multiple Access Control Scheme for Ad Hoc Networks," *IEEE Transactions on Communications*, vol. 50, no. 6, 2002.

[7] P. Karn, "MACA- a new channel access method for packet radio," *in ARRL/CRRL Amateur Radio 9th Computer Networking*, pp. 134–40, 1990.

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

[9] S. Xu and T. Saadawi, "Does the IEEE 802.11 MAC Protocol Work Well in Multihop Ad Hoc Networks?" *IEEE Communications Magazine*, pp. 130–137, June 2001.

[10] G. Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," *IEEE JSAC*, vol. 13, no. 3, pp. 535–47, March 2000.