CSMA/CF Protocol for IEEE 802.15.4 WPANs

Shiann-Tsong Sheu, *Member, IEEE*, Yun-Yen Shih, *Student Member, IEEE*, and Wei-Tsong Lee, *Member, IEEE*

***Abstract*—Different emerging IEEE 802.15.4 wireless personal area networks (WPANs) are one solution for wireless sensor networks (WSNs), where applications are restricted by low data rate, short transmission distance, and low power consumption. The frame transmission mechanism of the IEEE 802.15.4 standard, which adopts the blind random backoff mechanism, was designed to minimize power consumption. However, it cannot provide satisfactory performance in a realistic hidden-node environment, because it may incur a hidden-node collision chain situation and unexpectedly limit the overall network capacity. For each successful data transmission, any inefficient transmission mechanism will incur prolonged access delay and will consume too much power. Moreover, the current design becomes inefficient as the number of devices significantly increases. As a solution, we propose a new multiple access protocol with improved efficiency at the sublayer between the media access control layer and the physical layer, i.e., a carrier sense multiple access with collision freeze (CSMA/CF) protocol, which comprises a collision resolving scheme and a P-frozen contention strategy. The CSMA/CF protocol can quickly alleviate aggravated collision situations in a hidden-node environment. Such a particular collision phenomenon is denoted as a collision chain problem (CCP). The impact from CCP is thoroughly discussed and analyzed. As confirmed by the results of analysis and performance evaluations, the proposed CSMA/CF protocol can achieve significant performance improvement in energy conservation, access delay reduction, and transmission reliability enhancement.**

***Index Terms*—Collision chain, hidden node, IEEE 802.15.4, wireless sensor network (WSN).**

I. Introduction

A TYPICAL wireless sensor network (WSN) [1] comprises a number of low-power nodes with diversiform sensors and one central sink that collects information from the nodes that are scattered either one hop or multiple hops away from it. WSN was developed to provide specific services, e.g., ecological detection [2], health monitoring [3], and home automation [4], [5]. Regardless whether the communication is in a distributed control or a centralized coordinated manner, both the design of the channel access protocol to support efficient data transmission and battery longevity are crucial in achieving an effective WSN.

Manuscript received February 6, 2008; revised June 8, 2008 and June 15, 2008. First published July 16, 2008; current version published March 17, 2009. This work was supported in part by the National Science Council under Contract NSC 96-2221-E-008-032 and Contract NSC 96-2628-E-008-003. The review of this paper was coordinated by Dr. J. Misic.

S.-T. Sheu is with the Department of Communication Engineering, National Central University, Taoyuan 32001, Taiwan.

Y.-Y. Shih and W.-T. Lee are with the Department of Electrical Engineering, Tamkang University, Taipei 25137, Taiwan.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2008.928634

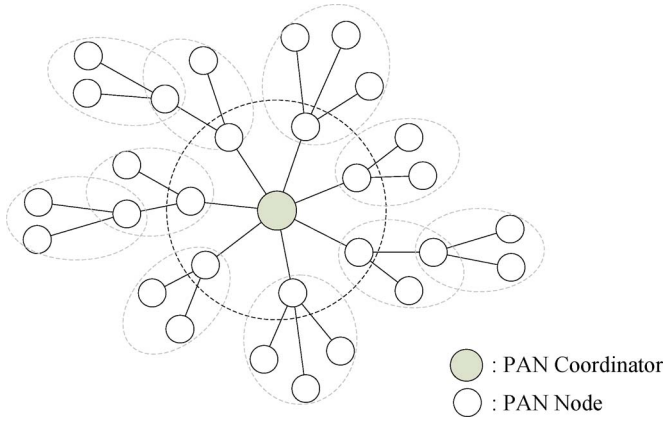


Fig. 1. Last-hop communication between nodes and the coordinator in a WPAN with multiple clusters.

The IEEE 802.15.4 wireless personal area network (WPAN) [6], which has been designed to have the properties of low cost, low data rate, short transmission distance, and low power consumption, is a strong candidate for a WSN. The standard type has three defined types of WPAN topology: 1) the *star topology* (also known as the *infrastructure topology*); 2) the *peer-to-peer topology* (also known as the *ad hoc topology*); and 3) the *cluster-tree topology*. Each WPAN demands that one coordinator function as the central controller to organize the WPAN and coordinate the other components of the WPAN [6]. The coordinator in any kind of network topology often plays the role of the sink, whereas the other nodes report environmental information to the coordinator after they have retrieved useful information from the sensors. Star, cluster-tree, and peer-to-peer networks may coexist and connect with other networks for a data collection job, as shown in Fig. 1. In such a network system, information is relayed toward the network sink by intermediate nodes. These intermediate nodes are sometimes coordinators of other WPANs, referred to as bridges [7]. For brevity, we use "node" to represent a node that is controlled by the coordinator and "device" to represent a node or the coordinator.

The WPAN network load is usually affected by two factors: 1) the number of active devices and 2) the traffic load of each device. Based on the usage model perspective, the node density of WSNs should be higher than the mobile ad hoc wireless networks, and the aggregated uplink traffic load at the last hop toward the coordinator should be heavier than the hop that is distant from the coordinator, as shown in Fig. 1. The probability of more than one device picking the same slot for either carrier sense or transmission is proportional to the number of devices [6], [9]; therefore, the last hop will become the bottleneck in a WSN, regardless of the network topology. To evaluate the performance bottleneck and to simplify performance analysis,

0018-9545/$25.00 © 2008 IEEE

Authorized licensed use limited to: Tamkang University. Downloaded on June 04,2010 at 03:49:35 UTC from IEEE Xplore. Restrictions apply.

we study the last-hop communication, which is modeled as a star network, where each node transmits aggregated information from its subordinators to the coordinator. For brevity, all ensuing discussion applies to communications that occur only at the last hop, unless otherwise noted.

Optionally, the IEEE 802.15.4 divides the timeline into contiguous superframes, each of which further consists of an active period and an inactive period. Superframes are bounded by beacon frames, and their timing is controlled by two essential system parameters, called *beacon order* (BO) and *superframe order* (SO), which control the length of each active and inactive period in the superframe. The values of BO (denoted as BO) and SO (denoted as SO) control the beacon interval (BI) and the length of the active period [denoted as the superframe duration (SD)], respectively. The BO must be larger than or equal to SO $(BO \geq SO)$. The inactive period of the superframe, which starts from the end of the active period and stops at the next beacon frame, is nonexistent if the BO is equal to the SO $(BO = SO)$. To efficiently describe superframe structures, both BI and SD are equally divided into 16 slots, and the slot sizes of BI and SD are $3 \cdot 2^{BO}$ and $3 \cdot 2^{SO}$ unit backoff periods (UBPs), respectively, where the UBP is the basic time unit that was used during the backoff process in the *carrier sense multiple access with collision avoidance* (CSMA/CA) protocol. For instance, one UBP takes 320 μs if the WPAN operates in the 2.4-GHz band.

The entire active period of a superframe further comprises a *contention access period* (CAP) and an *optional contention-free period* (CFP). The CAP starts from the end of the beacon frame and may stop at the beginning of the CFP (if there is one), the end of the active period (if $SO < BO$), or the beginning of the next beacon frame. Devices apply a modified CSMA/CA protocol to transmit frames during the CAP; however, because nodes are usually equipped with a battery as the power source, they always turn the transceiver off whenever there is no data frame to be sent. Direct communication between a pair of nodes is not allowed in a star network, and therefore, the coordinator is responsible for relaying the data from one node to another.

The key concept in an IEEE 802.15.4 modified CSMA/CA protocol is *blind backoff*, which modifies the IEEE 802.11 CSMA/CA protocol to shut down the transceiver during any random backoff period (BP) to preserve power. In fact, according to [6], a node shall turn on its transceiver to guarantee that the transceiver can twice perform clear channel assessments (CCAs) after the backoff process is completed, where each CCA takes one UBP. The basic time unit for a random BP is a UBP, and the number of UBPs within a BP is randomly selected from the range of the contention window (CW). If the result of two consecutive CCAs reveals an idle channel after a BP, the node transmits a data frame right away; otherwise, it gives up transmission and again performs random blind backoff but using a doubled CW. To control access delay, the CW is bounded by a specified maximal CW value. Due to this blind backoff, the media access control (MAC) protocol naturally omits a hidden-node protection scheme, e.g., a request-to-send/clear-to-send (RTS/CTS) handshake scheme. In the current design, channels are accessed by nodes on a random basis, and all the nodes, more or less, equally share resources if there is no hidden-node situation. This design is sensible for a low-power oriented network but, by no means, is it the most efficient one. It has already been shown in [16] that, as the number of nodes increases, the overhead that results from hidden-node collision (HNC) can cost more than 10% in MAC efficiency degradation.

The IEEE 802.15.4 has a defined reserved channel bandwidth called *guaranteed time slots* (GTSs), where real-time traffic can safely be transmitted in either an uplink or a downlink direction. GTS allocations are controlled by the coordinator, and information that is related to GTS assignments is carried in the GTS field of the beacon frame. The node that is allocated with a GTS must stay "awake" during the GTS subperiod that was allocated to it.

With regard to power-saving behavior, downlink transmission (i.e., traffic from the coordinator to a node) becomes more complicated than uplink transmission (i.e., traffic from a node to the coordinator), because nodes are not always ready for frame receptions. However, nodes are requested to periodically wake up to listen to beacon frames to receive time synchronization information and system information. As downlink frames are buffered in the coordinator, the corresponding nodes are notified via a beacon frame and triggered to contend the channel to issue a data request command frame (DATA-REQ) to the coordinator during CAP. Once the coordinator receives the DATA-REQ frame, an acknowledgement frame (ACK) is sent back to the sender node to acknowledge the receipt of the DATA-REQ frame and to inform it to stay awake for subsequent receptions. Thereafter, the coordinator contends the channel for transmitting downlink data frames that belong to acknowledged nodes.

Usually, a WPAN node is equipped with an omnidirectional antenna to achieve random deployment, because the actual sensing environment is very hard to predict. Although the radius of an antenna's radio coverage is a few meters, radio propagation still may incur a hidden-node situation [8], which has highly been emphasized in wireless local area networks [9]. The aforementioned hidden-node problem is exacerbated when the IEEE 802.15.4 CSMA/CA protocol is applied in a dense WPAN, as a significant number of nodes will be deployed therein, and a significant number of uplink data frames will be aggregated in the last hop. Based on our observations, the duration of a hidden node collision is appreciably extended if the other hidden node(s), with respect to nodes that collided, initiate transmission before the termination of the preceding collision. This design becomes cumbersome and inefficient as the number of nodes significantly increases.

Although the transmission performance of the IEEE 802.15.4 MAC protocol is not satisfactory [10], it may still be applicable to a WSN, as it produces an ultralow data rate. However, the drawbacks of the MAC protocol include diminished information reliability and greater consumption of power resources for each successful transmission. The authors in [11]–[13] proposed various management schemes to control sensing periods, depending on either quality-of-service requirements or the remaining power. Proper proportions are measured for the periods of monitoring, channel accessing, and sleep, but they ignore the inefficient contentions and overheads of the standard protocol. To curb the power losses and improve

Authorized licensed use limited to: Tamkang University. Downloaded on June 04,2010 at 03:49:35 UTC from IEEE Xplore. Restrictions apply.

the performance of the current IEEE 802.15.4 protocol on WSNs, we propose a smart *carrier sense multiple access with collision freeze* (CSMA/CF) protocol. The major concept behind CSMA/CF in resolving collisions is that it identifies collided nodes by retrieving useful information from damaged signals. Analyses and simulation results show that CSMA/CF indeed improves the IEEE 802.15.4 MAC protocol so that it can be a more appropriate candidate for WSNs, all the while retaining interoperability with the standard protocol.

The rest of this paper is organized as follows. A brief description of the current IEEE 802.15.4 protocol [6] and its deficiencies in handling collision chain situations is provided in Section II, which aims at supplying necessary background. The CSMA/CF protocol is elaborated upon in Section III. Analyses of the influence of collision chains on the standard protocol and on the performance of the CSMA/CF protocol are also provided. Performance evaluation results are presented in Section V. Concluding remarks are given in Section VI.

II. Collision Chain Problem (CCP) in IEEE 802.15.4 WPAN

The hidden-node problem [8] is one of the crucial problems in wireless networks, regardless of the communication range. Typically, two or more nodes in a wireless network are unaware of signals from the others; therefore, collisions occur at the receiver side (i.e., WPAN coordinator) if their transmissions fully or partially overlap in the time domain. Depending on the collision starting point, collisions can be categorized as one of the following two types: 1) *HNCs* and 2) *contention collisions* (CCs). HNC is a collision in which the transmission starting points for a number of hidden nodes are different, whereas their transmission periods are partially overlapped in the time domain. On the other hand, whenever two or more devices (including the coordinator) start transmission in the same time slot, a CC occurs among those nonhidden nodes. In addition, the CC covers the collision situation in which a number of hidden nodes simultaneously start transmissions.

Although HNC and CC could be resolved using a handshake scheme, the RTS/CTS scheme that was adopted in the 802.11 variant of the CSMA/CA protocol [6], [9] cannot be applied to the IEEE 802.15.4 standard, because a duration broadcast is meaningless to sleeping nodes in the IEEE 802.15.4 standard, which adopts the blind-backoff scheme. The lack of RTS/CTS support will prolong the mean HNC period if the rear part of the collided frames also collides with the frames that were sent from nodes that are hidden from prior transmitters. A collision chain frequently happens, because [14] has shown that the probability of two randomly distributed nodes in the radio coverage of a coordinator that cannot hear each other is as high as 41%. As confirmed by the ensuing analytic results and performance evaluations, HNC frequency is, indeed, higher than CC frequency, and the entailed overhead can result in a more appreciable degradation in MAC efficiency than CC.

Based on the aforementioned HNC phenomenon, we can see that the point of collision may happen at any time during frame reception. By monitoring all received signals, the coordinator can recognize an HNC if the physical (PHY) header

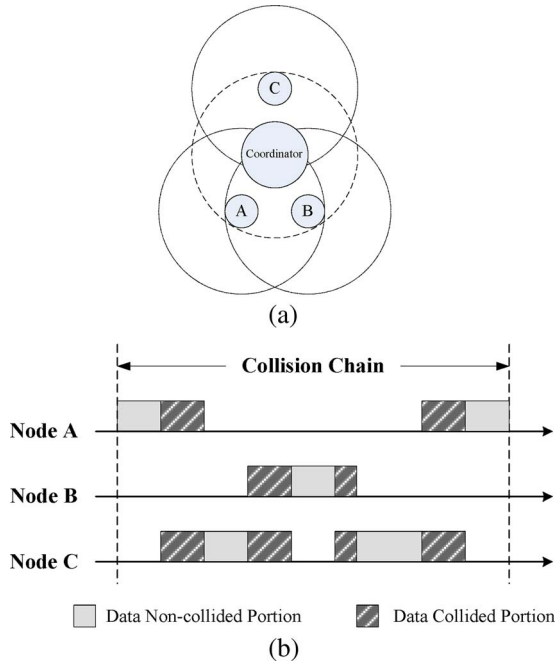


Fig. 2. Example illustrating the CCP. (a) Network topology, where nodes A and B are hidden from node C. (b) Instance of the collision chain situation in topology (a).

and part of the MAC header of the first received frame are successfully decoded and demodulated [15], because the direct-sequence spread spectrum (DSSS) technique provides precise correlated results. An elaboration of this point will follow in Section III.

Assume that three nodes A, B, and C are located in a WPAN, where nodes A and B can hear each other, but they are hidden from node C [see Fig. 2(a)]. Consider the situation where node A first transmits a frame, and its frame collides with the frame from node C at the coordinator. The frames that were sent from nodes B and C will again collide, because node B is allowed to transmit a frame as soon as node A finishes its transmission, as depicted in Fig. 2(b). The prolonged collision period due to subsequent collisions exhausts the system bandwidth and wastes considerable power. We refer to such phenomena as a *collision chain problem* (CCP), particularly in the IEEE 802.15.4 WPAN, where the hidden-node protection mechanism is omitted and further intentionally adopts the blind-backoff scheme.

The authors in [16] proposed a grouping strategy for the IEEE 802.15.4 standard to solve the CCP. First, the coordinator collects hidden-node relationships between any pair of nodes. Then, the coordinator partitions all nodes into an appropriate number of groups. No node in the same group is hidden from each other. Thereafter, the coordinator divides the entire CAP into a number of nonoverlapping subperiods according to the number of nodal groups. Although the grouping strategy provides an ideal nonhidden-node environment, the overheads of collecting hidden-node relationship and maintaining these groups are appreciable drawbacks. Another shortcoming of the grouping strategy is the weak support for mobile WSNs. Nevertheless, the simulation results of [16] illustrate that the transmission performance in a nonhidden-node environment is almost twice that in a hidden-node environment. This

Authorized licensed use limited to: Tamkang University. Downloaded on June 04,2010 at 03:49:35 UTC from IEEE Xplore. Restrictions apply.

encouraged us to alleviate the CCP influence by adopting a smarter strategy with less overhead.

The authors in [10] pointed out other potential problems that may restrict transmission performance. There are two major issues: 1) low superframe utilization and 2) congestion between data frames and DATA-REQ frames. The authors suggested controlling the number of pending addresses that were announced in the beacon frame to alleviate congestion in the DATA-REQ frames and improve superframe utilization. Obviously, this strategy improves downlink transmission performance; however, it is worthless in terms of improving uplink transmission performance, as uplink traffic tends to aggregate in the last hop. In our opinion, the WSN design principle is intended to solve the problem of uplink transmission inefficiency.

The IEEE 802.15.4 standard has defined the GTS scheme, where real-time services are prioritized and served in either an uplink or a downlink direction. The coordinator may dynamically allocate a number of GTSs to nodes that access channels during the CAP to alleviate collisions in the CAP. For GTSs that are allocated to unsuitable nodes, the dedicated channel resource serves no purpose. As a solution, we propose a new CSMA/CF protocol to precisely identify nodes from collided signals and automatically allocate a GTS of adequate time length for data transmission to those nodes. As a result, the CSMA/CF protocol avoids the aggravated collision phenomenon caused by HNC.

III. CSMA/CF

In this section, we propose a new efficiency improvement multiple access protocol at the sublayer between the MAC layer and the PHY layer, i.e., the CSMA/CF) protocol, which comprises a *collision resolving scheme* (CRS) and a *P-frozen contention strategy* (PFCS). The CRS is designed to recognize the collided node and prevent two anterior collided nodes from colliding again, whereas the PFCS is designed to control the access behavior of collided nodes that are successfully identified by the coordinator.

A. CRS

In wireless networks, both collision and noise will interfere with frame reception at the receiver, and it is an open issue for the receiver to differentiate between them. The authors in [15] proposed a technique for detecting collisions and further recover data by exploiting the *capture effect*. Such a collision detection scheme has three important properties: 1) It can differentiate between packet collision and packet loss; 2) it can detect collisions that occur at the receiver; and 3) it is possible to identify the transmitter(s) that are involved in the collision. The proposed technique [15] is applicable to all kinds of slot-based contention protocols. For an HNC, partial prefix data that do not overlap with subsequent frames should correctly be decoded as in a successful situation. For example, the commercialized IEEE 802.15.4 solution can detect, decode, and output undamaged signals [17]. Using the aforementioned techniques to process received signals, an HNC can now be identified if the essential header information is valid, even when the entire frame is corrupted. Note that the DSSS-based IEEE 802.15.4

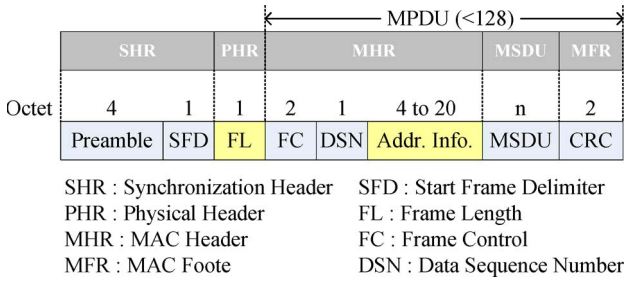


Fig. 3. Frame format for the IEEE 802.15.4 MAC frame.

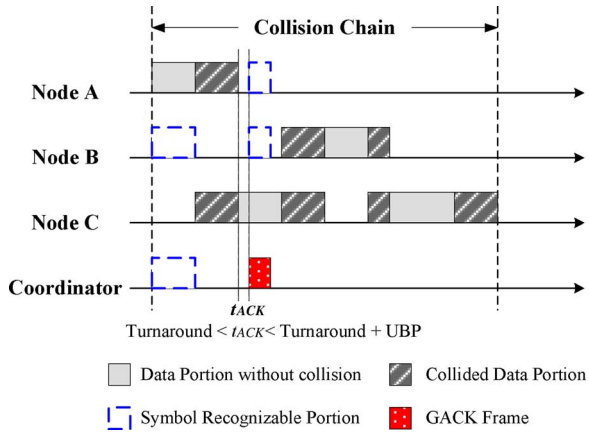


Fig. 4. Example that illustrates that one of the nodes (e.g., node A) has successfully been recognized by the coordinator and is removed from the contention group using GTS.

transmission technique [18] does not interleave binary data. Therefore, the survivable portion of the consecutive binary data can successfully be recognized. Regardless of CRC verification, the essential information that is carried in the prefix header field is already sufficient for identifying the transmitter of the frame, the rear part of which is corrupted by subsequent frame(s). The same result might be obtained if the channel noise makes consecutive *error vector magnitudes* of received symbols that exceed the threshold. The assumption that the transmitter can be identified by collided signals is true if and only if collision or channel noise appears just after the header field of the received frame. The receiver can recognize the transmitter of the collided frame without any change in the frame format but with a little change in the receiving process between the PHY and MAC layers.

Fig. 3 portrays the IEEE 802.15.4 MAC frame format. Whenever the frame length (FL) and source address (SA) fields of the frontal frame in collision are recognizable, the coordinator can move the corresponding node from CAP to CFP (using GTS) in the next superframe. This is how the CRS effortlessly lessens the contentions. According to the 802.15.4 standard, these two essential fields are always transmitted during the first two UBPs of the entire frame transmission period, as the link rate is 250 kb/s (under 2.4-GHz operation mode). Once the coordinator detects a collision, in which the collision starting point is two UBPs behind the beginning of the anterior frame, a special GTS ACK (GACK) is sent from the coordinator to the recognized transmitter, and the GACK is used to notify the transmitter of the collision's occurrence and the bandwidth

Authorized licensed use limited to: Tamkang University. Downloaded on June 04,2010 at 03:49:35 UTC from IEEE Xplore. Restrictions apply.

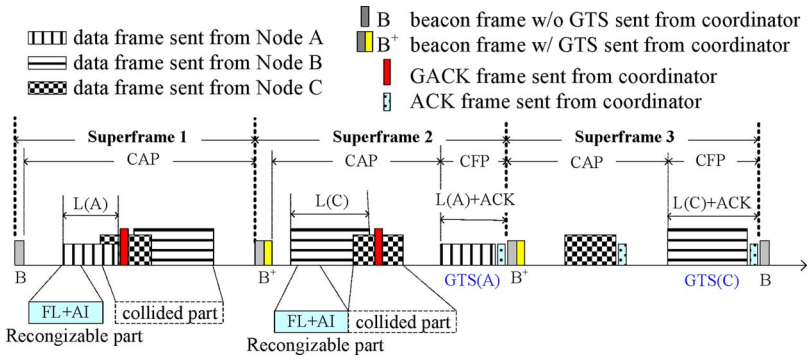


Fig. 5. Example that illustrates how the collision chain is smoothly resolved using the CRS.

reservation. An additional bit in the frame-type field is required to differentiate the GACK from the standard ACK. Based on the decoded FL, the coordinator can determine the time instance of sending GACK and the time length of GTS, which requires covering the time periods of data frame transmission, ACK frame transmission, and the gap between them. To comply with the standard, either the ACK or the GACK must reply before ACK timeout (i.e., turnaround time + UBP), as depicted in Fig. 4. Note that the coordinator is required to switch the transceiver from the receiving mode to the transmission mode to send the GACK to the recognized node, regardless of whether any node is still transmitting data to the coordinator. Thereafter, modification of original firmware or hardware design is required for such procedure.

The node that first transmits the frame and is disturbed by the other node(s) may receive the GACK, which notifies it of not only the occurrence of the HNC but also the GTS permission from the coordinator. Let "G-node" denote the node that received the GACK and is waiting for GTS. For subsequent collisions, the G-node should cease transmissions until its GTS is allocated in the following frame. Referring back to the network topology shown in Fig. 2, Fig. 4 illustrates the scenario of using CRS in a hidden-node situation to shorten collision chain duration as Node A is removed from the contention group.

Fig. 5 further depicts the instance in which collision chains are smoothly resolved by the proposed scheme under the network topology shown in Fig. 2(a). This example assumes that each node desires to transmit one frame and that there is no inactive period in the superframe. In the first superframe, the frontal corrupted frame that was sent from node A is first recognized by the coordinator, and a GACK is subsequently sent in reply to node A. Then, the coordinator allocates one GTS of an appropriate length (i.e., $FL + IFS + L_{ACK}$, where IFS is the interframe space between the data frame and ACK frame, and L_{ACK} is the transmission time of the ACK frame to node A in the second superframe). Nodes B and C failed to receive the GACK or ACK frames in the first superframe reselect random BPs, and their transmissions are assumed to collide again in the second superframe. As usual, node C is identified by the coordinator and receives one GTS period in the third superframe. Finally, node B successfully transmits the data frame in CAP, because the other hidden nodes have already been serviced. Through this example, we conclude that the proposed CRS can resolve the CCP step by step.

B. PFCS

The CRS demands that the G-node stop contention and wait for the dedicated GTS in the next superframe. It sacrifices transmission opportunity and prolongs access delay to avoid collisions. One interesting issue is raised, because the bandwidth that was allocated for CAP could unexpectedly be wasted when most of the nodes become G-nodes. This paper proposes the PFCS to provide G-nodes with another opportunity to access CAP, regardless of the acquirement of GTSs. The P-persistent scheme, as a simple technique applied in a wide variety of contention-based protocols, is used to control the transmission opportunity of the G-node. The retry count of the frame to be transmitted is the key parameter in determining the probability of transmission. Whenever a node detects that a channel is busy or fails to receive the ACK frame after transmission, the retry counter is increased by one. On the other hand, the retry counter is reset to zero whenever the node successfully transmits a frame or whenever the frame is discarded due to the retry count threshold. Let probability $P_F(k)$, which is linearly proportional to the number of retries in the data frame, be the parameter for deciding whether the G-node should freeze its transmission in CAP or not. The larger the value of the retry counter, the higher the probability of a ceased transmission. $P_F(k)$ is determined by the following equation:

$$P_F(k) = \begin{cases} K/RTH, & \text{if } 0 \le k < RTH \\ 1.0, & \text{otherwise} \end{cases} \quad (1)$$

where k is the number of retries in the present frame, and RTH is the retry threshold for retransmissions. Notably, the maximal number of retransmissions should be set to $RTH + 1$. For instance, if $RTH = 5$, each failed transmission attempt will increase $P_F(k)$ by 0.2. When the retry count k is equal to 5, this indicates that the network load is high and that channel accesses from the G-nodes should be prohibited. Accordingly, this G-node ceases transmission and waits for the GTS to conserve power. Thus, we name the proposed protocol CSMA/CF.

There is another interesting situation where a G-node with a second access opportunity successfully transmits its frame in the current CAP but retains the capacity to access GTS in the coming frame. To eliminate unfairness and/or inconsequential GTS allocation, the coordinator only allocates GTS periods to those G-nodes whose frames are still waiting to be transmitted.

Authorized licensed use limited to: Tamkang University. Downloaded on June 04,2010 at 03:49:35 UTC from IEEE Xplore. Restrictions apply.

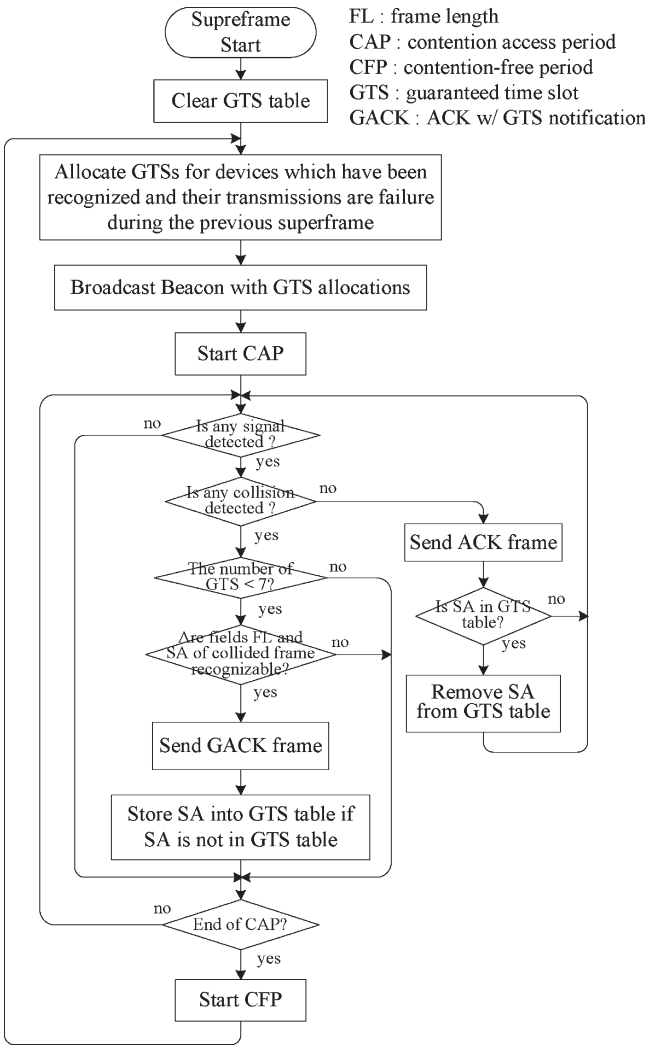


Fig. 6. Flowchart of the coordinator with CSMA/CF.

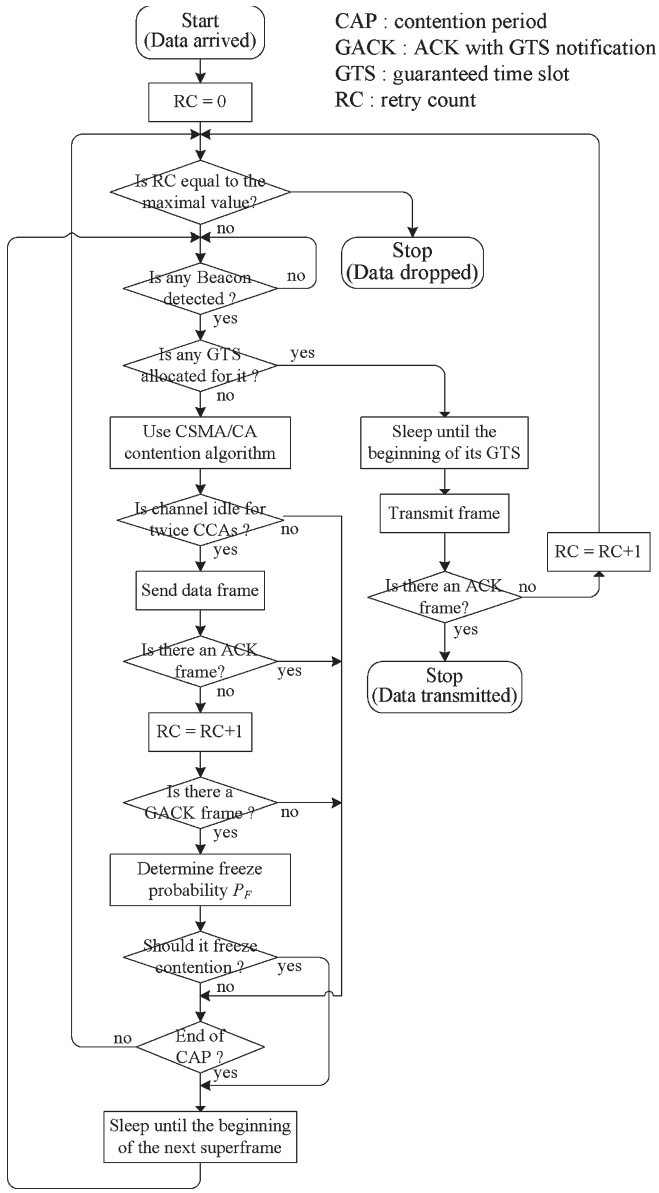


Fig. 7. Flowchart of the node with CSMA/CF.

In other words, once the coordinator perceives a successful transmission from a G-node during CAP by checking the transmitter of the received frame, it automatically countermands it from the GTS allocation list.

A GTS is measured in time slots, and the time slot size is linearly proportional to the system parameter S; therefore, the remaining period could be used to carry other data transmissions from the same source node if the allocated GTS period is longer than the required period $FL + IFS + L_{ACK}$. If transmission during the GTS period is unsuccessful, the coordinator will not allocate another GTS to that node, because such a failure is caused neither from the CC nor the HNC. That is, the GTS owner will transit back to the contention state after CFP.

Figs. 6 and 7 depict the flowcharts for the coordinator and the nodes with the proposed CSMA/CF protocol, respectively. For brevity, these two flowcharts do not consider the mechanism of regular GTS allocation. Note that the coordinator must ensure that the number of GTS allocations in one superframe is not greater than seven. Therefore, if there is no more room for accommodating a new G-node, the coordinator must stop replying with GACK frames, and the network will operate as a standard network.

By taking backward compatibility into account, the CSMA/CF can fully coexist with the standard protocol. From the MAC protocol aspect, the message formats of the proposed CSMA/CF protocol comply with the standard specification. The additional functions that are required for the CSMA/CF firmware/hardware in a coordinator are given as follows: 1) extracting the SA from a corrupted frame and 2) replying the GACK frame. On the other hand, the additional functions required for ordinary nodes are given as follows: 1) parsing the GACK frame; 2) performing PFCS; and 3) freezing contentions. By slightly modifying the association handshake messages, the coordinator can easily differentiate between CSMA/CF capable and standard nodes during the network entry procedure. As we have previously mentioned, when the coordinator detects a HNC, it tries to identify the sender address from the collided frame. The coordinator will not return the GACK if the address is unidentifiable or if the node is a standard node. In other words, the CSMA/CF capable nodes and the

Authorized licensed use limited to: Tamkang University. Downloaded on June 04,2010 at 03:49:35 UTC from IEEE Xplore. Restrictions apply.

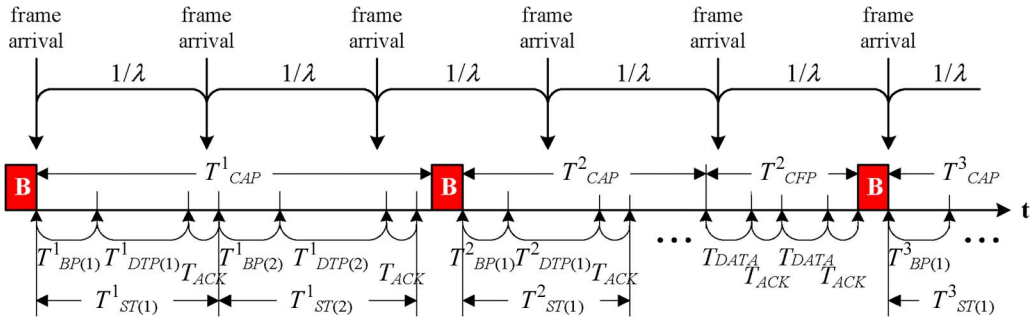


Fig. 8. Statistical model of the proposed CSMA/CF protocol.

standard nodes follow the same contention procedure most of the time. The difference between them lies in how they deal with HNCs.

IV. Performance Analysis

In this section, we analyze the performance of the CSMA/CF protocol. To concentrate on the proposed protocol, an error-free channel condition is assumed. Furthermore, we assume that the frame arrival rate of each node follows a Poisson distribution. The probability $P(k,t)$ that exactly k frames arrive at a node during the time interval t is given by

$$P(k,t) = \frac{(\lambda t)^k}{k!} e^{-\lambda t} \tag{2}$$

where the time unit of interval t is the UBP, λ is the payload arrival rate of a node in interval t, and $k = 0, 1, 2, \ldots, \infty$. According to the queuing theory, the total traffic load (TL) of a network that consists of M nodes can be derived by $TL = M \cdot \lambda \cdot L$, where L is the mean length of data payload, excluding the header and CRC trailer. From the perspective of the network, the probability $P(0,t)$ that no frame arrives at the network within interval t is given by

$$P(0,t) = e^{-M \cdot \lambda \cdot t}. \tag{3}$$

The total amount of data for one UBP($= 320\ \mu$s) is 10 B when the link rate is 250 kb/s. In this paper, the original link rate is transformed as a new metric $D_{UBP}(= 10$ B/UBP), because UBP is used as the basic time unit throughout analyzes and simulations. For performance evaluation purposes, the active period in each superframe is assumed to be equal to the superframe period ($SD = 48 \times 2^{SO}$ UBPs), and every superframe comprises the CAP and the CFP, as shown in Fig. 8. The time periods for the CAP and CFP of the nth superframe are denoted as T^n_{CAP} and T^n_{CFP}, respectively.

CSMA/CF utilizes both CAP and CFP to maximize transmission performance; therefore, we first analyze the average time cost that is required for a successful transmission in the CAP and then analyze the average number of GTSs that are allocated in the CFP according to previous contention results. Then, the expected system *goodput* can be derived from the ratio of the amount of transmitted payload and the total time cost. With the modified slotted CSMA/CA MAC protocol, each successful frame transmission in the CAP is required to experience three states: 1) the backoff state; 2) the data frame transmission state; and 3) the ACK reception state. For the ith successful data frame transmission in the nth superframe, the intervals for the BP, data frame transmission period (DTP), and ACK reception period are denoted as $T^n_{BP(i)}$, $T^n_{DTP(i)}$, and T_{ACK}, respectively. For brevity, the first successful transmission in each superframe is indexed by one (i.e., $i = 1$). Intuitively, $T^n_{BP(i)}$ and $T^n_{DTP(i)}$ are affected by the factors of network loading and frame size, but T_{ACK} is fixed and equal to the transmission time of the standard ACK frame plus an interframe space (τ_{ACK}), i.e., $T_{ACK} = L_{ACK}/D_{UBP} + \tau_{ACK}$, where L_{ACK} is the fixed length of the ACK frame ($= 11$ B). The total time cost of the ith successful transmission in the nth superframe (denoted as $T^n_{ST(i)}$) is the summation of these three periods. Therefore, we have

$$T^n_{ST(i)} = T^n_{BP(i)} + T^n_{DTP(i)} + T_{ACK}. \tag{4}$$

Evidently, both $T^n_{BP(i)}$ and $T^n_{DTP(i)}$ need to derive the expected value of $T^n_{ST(i)}$. The period $T^n_{DTP(i)}$ that is required for the ith successful data frame transmission is the summation of all the time lengths that were wasted for unsuccessful attempts (denoted as $T^n_{FT(i)}$) prior to the successful transmission plus the time length of the successful transmission. That is, $T^n_{DTP(i)} = T^n_{FT(i)} + T_{DATA}$, where T_{DATA} is the average time length for one data frame transmission. Recall that the BP might be lengthened, as the previous contention was unsuccessful. Failed contention is caused either by a node that senses that the channel is busy or its transmission is corrupted by other frame or channel noise. As we have previously mentioned, the channel noise factor is simply ignored throughout the analysis. Intuitively, the probability that a node encounters a busy channel in the hidden-node environment should be less than that in a nonhidden-node environment.

If the number of contending nodes changes from one superframe to another, then the network traffic arrival rate during the superframe period will also change. Therefore, the traffic arrival rate that was defined in (2) is rewritten as

$$P(k,N,t) = \frac{(N \cdot \lambda \cdot t)^k}{k!} e^{-N \cdot \lambda \cdot t} \tag{5}$$

where N is the number of active nodes.

Let T_{CCA} be the time cost of processing two CCAs. We have $T_{CCA} = 2$ UBPs, because each CCA takes one UBP. Upon the completion of the backoff process, the node turns on its transceiver and starts to sense channels. The node is

Authorized licensed use limited to: Tamkang University. Downloaded on June 04,2010 at 03:49:35 UTC from IEEE Xplore. Restrictions apply.

well aware of busy channels if there is a nonhidden node that starts transmission in the period $T_{DATA} + T_{ACK} + T_{CCA} - 1$ ahead of the end of its carrier sensing. According to the discrete time events of successful transmissions in the CAP of a superframe, the entire CAP of the nth superframe is logically partitioned as a number of subperiods, where the first subperiod (denoted as SP_1^n) is the subperiod in front of the first successful transmission, the second subperiod (denoted as SP_2^n) is the time period between the first and the second successful transmissions, and so on. Consequently, the generalized notation SP_i^n represents the subperiod between the ith and the $(i+1)$th successful transmission. Let $P_{CLR(i)}^n$ be the probability that a node detects an idle channel during the subperiod SP_i^n. We then have

$$P_{CLR(i)}^n = P\Big(0, (N_{CN(i)}^n - 1) \cdot (1 - P_{HD}) \cdot T_{DATA} + T_{ACK} + T_{CCA} - 1\Big) \quad (6)$$

where $N_{CN(i)}^n$ is the total number of nodes that desire to transmit data frames during SP_i^n, and P_{HD} is the probability that any two nodes are hidden from each other. According to [14], the value of P_{HD} is equal to 41%.

Although sensing carriers before transmission are used to minimize the probability of collision, frame transmission can still fail due to CC and HNC. Let $P_{CC(i)}^n$ denote the probability of CC occurrence. We then have

$$P_{CC(i)}^n = 1 - P\left(0, N_{CN(i)}^n - 1, 1\right). \quad (7)$$

The probability of HNC occurrence (denoted as $P_{HC(i)}^n$) is the probability that more than one node transmits a frame during the period of two consecutive data frame transmissions (i.e., $2 \cdot T_{DATA}$). Thus, we have

$$P_{HC(i)}^n = 1 - P\left(0, \left(N_{CN(i)}^n 1\right) \cdot P_{HD}, 2 \cdot T_{DATA} - 1\right). \quad (8)$$

Notice that T_{DATA} is equal to $(L_{DATA} + O_{DATA})/D_{UBP}$ (in UBPs), where L_{DATA} is the payload length, and O_{DATA} is the minimum overhead of the data frame ($= 15$ B). For any node that is involved in the contending group during SP_i^n, the probabilities for a successful transmission ($P_{S(i)}^n$), CC ($P_{C(i)}^n$) and HNC ($P_{H(i)}^n$) can be derived from the following:

$$P_{S(i)}^n = \left(1 - P_{CC(i)}^n\right) \cdot \left(1 - P_{HC(i)}^n\right) \quad (9.1)$$

$$P_{C(i)}^n = P_{CC(i)}^n \quad (9.2)$$

$$P_{H(i)}^n = \left(1 - P_{CC(i)}^n\right) \cdot P_{HC(i)}^n. \quad (9.3)$$

The probability $P_{C(i)}^n$ includes the probability of CC occurrence and the probability of simultaneously encountering both CC and HNC. Once any collision occurs, the probability that the coordinator fails to distinguish which device was involved in the collision is $P_{C(i)}^n$. On the other hand, the probability that the coordinator succeeds in telling which device was involved in collision is $P_{H(i)}^n$. The number of HNCs occurring during SP_i^n (denoted as $N_{HN(i)}^n$) is given by

$$N_{HN(i)}^n = \frac{P_{H(i)}^n}{P_{S(i)}^n}. \quad (10)$$

If the node that sends the frontal frame in HNC is recognizable by the coordinator, then it will become the G-node and probably cease contentions according to its freeze probability. The larger the value of the retry counter, the higher the probability of stopping contention. The expected retry count of the G-node (denoted as $N_{RC(i)}^n$) is derived using the following equation:

$$N_{RC(i)}^n = \sum_{j=1}^{RTH} \left\{ \prod_{k=1}^{j} \left[1 - P_{CLR(i)}^n + P_{CLR(i)}^n \cdot \left(P_{C(i)}^n + P_{H(i)}^n \cdot (1 - P_F(k))\right)\right] \right\}. \quad (11)$$

Consequently, the probability $P_{FRZ(i)}^n$ that a node freezes contentions during SP_i^n is given by

$$P_{FRZ(i)}^n = \frac{N_{RC(i)}^n}{RTH}. \quad (12)$$

For a single G-node, the PFCS stipulates that it receives one GTS in some superframe, despite numerous GACK receptions in previous frame(s). In fact, the coordinator may recognize a node from HNC, but that node has already been recorded in the GTS allocation list. Let $P_{UCGTS(i)}^n$ be the probability that the number of GTSs that are allocated for the next (i.e., the $(n+1)$th) superframe is unchanged. We have

$$P_{UCGTS(i)}^n = \frac{N_{GTS(i)}^n \cdot \left(1 - P_{FRZ(i)}^n\right)}{N_{CN(i)}^n} \quad (13)$$

where $N_{GTS(i)}^n$ is the number of GTSs that will be allocated in the $(n+1)$th superframe. Both parameters $P_{UCGTS(i)}^n$ and $N_{GTS(i)}^n$ affect the dedicated resources that are required for the $(n+1)$th superframe, so both must be determined at the end of the nth superframe. Based on these two parameters, the number of required GTSs for the next superframe that can be estimated prior to the $(i+1)$th successful transmission (i.e., $N_{GTS(i+1)}^n$) is derived by the following equation:

$$N_{GTS(i+1)}^n = \min\left(N_{GTS(i)}^n + N_{HN(i)}^n \cdot \left(1 - P_{UCGTS(i)}^n\right) 7\right). \quad (14)$$

Intuitively, parameter $N_{GTS(1)}^n$ is set to 0 at the beginning of the nth superframe. Now, we are going to estimate the parameter $N_{GTS(i)}^n$ in (13). The number of active nodes during SP_i^n (i.e., $N_{CN(i)}^n$) is affected by $P_{FRZ(i)}^n$ and can easily be derived using the following equation:

$$N_{CN(i)}^n = N_{CN(i-1)}^n - N_{HN(i-1)}^n \cdot \left(1 - P_{UCGTS(i-1)}^n\right) \cdot P_{FRZ(i-1)}^n. \quad (15)$$

Authorized licensed use limited to: Tamkang University. Downloaded on June 04,2010 at 03:49:35 UTC from IEEE Xplore. Restrictions apply.

The numbers of nodes that desire access to the channel at the end of one superframe and at the beginning of the next superframe should be the same when there is no inactive period (i.e. $BO = SO$) or no data frame that arrives during the inactive period. Let $N^{n+1}_{CN(1)}$ denote the number of nodes that desire channel access at the beginning of the $(n+1)$th superframe. We have $N^{n+1}_{CN(1)} = N^{n}_{CN(I_n)}$, where notation I_n denotes the index of the last successful transmission in the nth superframe. Moreover, we suppose that the initial number of active nodes at the beginning of the first superframe is equal to the total number of nodes (M) in WPAN, i.e., $N^{1}_{CN(1)} = M$.

Next, we calculate the expected time cost of a collision chain. Let $T^n_{H(i)}$ denote the average time cost that was caused by collision chains that occur during SP^n_i. We have

$$T^n_{H(i)} = f_L(0) + f_L(1) + \sum_{k=2}^{\infty} \cdot \left[f_L(k) \cdot \prod_{j=2}^{n} \left[1 - P\left(0, \left(N^n_{CN(i)} - 1\right) \cdot P^n_{HD(i)}, f_L(j)\right)\right]\right]$$

where

$$f_L(k) = \begin{cases} T_{DATA}, & \text{if k = 0} \\ T_{DATA} - f_L(k-1)/2, & \text{otherwise.} \end{cases} \quad (16)$$

In (16), $f_L(k)$ is a recursive function for obtaining the mean time cost of a collision chain. From a statistical viewpoint, each collided frame in the collision chain is transmitted behind half the preceding frame. The expected time cost $T^n_{FT(i)}$ for all failed transmissions during SP^n_i is obtained as follows:

$$T^n_{FT(i)} = \frac{P^n_{C(i)}}{P^n_{S(i)}} \cdot T^n_{C(i)} + \frac{P^n_{H(i)}}{P^n_{S(i)}} \cdot T^n_{H(i)} \quad (17)$$

where $T^n_{C(i)}$ is the mean time period that was wasted by CCs, and $T^n_{C(i)} = T_{DATA}$. Let $P^n_{FC(i)}$ be the probability that a failed contention that was caused by a channel or collision is busy. We have

$$P^n_{FC(i)} = 1 - P^n_{CLR(i)} + P^n_{CLR(i)} \cdot \left(P^n_{C(i)} + P^n_{H(i)} \cdot \left(1 - P^n_{FRZ(i)}\right)\right). \quad (18)$$

Now, the total time cost $(T^n_{BP(i)})$ of repeatedly performing backoff processes and sensing the channel status during SP^n_i is derived by the following equation:

$$T^n_{BP(i)} = \sum_{j=0}^{RTH} \left[\left(P^n_{FC(i)}\right)^j \cdot \left(\frac{\min(2^n \cdot CW_{\min}, CW_{\max})}{2} + T_{CCA} \right) \right] \quad (19)$$

where $CW_{\min}$ and $CW_{\max}$ are the initial and the maximal CWs that were used for the backoff process, respectively. Therefore, the total time cost that was required for the ith successful transmission (i.e., $T^n_{ST(i)}$) in (4) has been resolved, and the performance of CAP can accordingly be derived.

We then turn the focus of our analyses to the average number of GTSs in the CFP of a superframe. Let $N_{GTS}(n)$ denote the number of GTSs that are allocated in the nth superframe. The coordinator always allocates GTSs in the $(n+1)$th superframe; therefore, we can have $N_{GTS}(n+1) = N^n_{GTS(I_n)}$, according to the value of parameter $N^n_{GTS(I_n)}$ that was derived at the end of the nth superframe. If any node in the GTS list successfully transmits a frame in the CAP, then the coordinator automatically deletes it from the GTS allocation list and decreases the value of $N_{GTS}(n+1)$ by one. $N_{GTS}(n+1)$ is derived from the following equation:

$$N_{GTS}(n+1) = N^n_{GTS(I_n)} \cdot \left(P^n_{FRZ(I_n)} + \left(1 - P^n_{FRZ(I_n)}\right) \cdot \left(1 - P^n_{S(I_n)}\right)\right). \quad (20)$$

Let $X^{(n)}$ denote the total number of data frames that are serviced during the CAP of the nth superframe. Evidently, in the nth superframe, $X^{(n)}$ is affected by two factors: 1) the time length of CAP (T^n_{CAP}) and 2) the time cost for each successful transmission (i.e., $T^n_{ST(i)}$, $1 \le i \le I_n$). Moreover, the total number of active nodes also bounds $X^{(n)}$. Therefore, we have $X^{(n)} = f_N(n, x)$, where $f_N(n, x)$ is a recursive function for deriving the number of successful transmissions that were accumulated after the xth successful transmission during the CAP of the nth superframe. It is defined in (21), shown at the bottom of the page, where T^n_{BCN} is the time cost for beacon frame broadcasting at the beginning of the nth superframe. Index I_n of the last successful transmission in the nth superframe is the same as $X^{(n)}$.

The precise time cost of the beacon frame in the nth superframe is derived by $T^n_{BCN} = L^n_{BCN}/D_{UBP}$, where L^n_{BCN} is the length of the beacon frame for the nth superframe. Note that the value of L^n_{BCN} increases as the number of GTS entries increases. Moreover, it can be derived by $L^n_{BCN} = O_{BCN} + N^n_{GTS} \cdot O_{GTS}$, where O_{BCN} is the fixed beacon overhead, and O_{GTS} is the default length of a GTS information element. Referring to the 802.15.4 standard, O_{BCN} and O_{GTS} are 20 and 3 B, respectively. Now, the CFP period in the next superframe (T^{n+1}_{CFP}) can be estimated by $T^{n+1}_{CFP} = N^{n+1}_{GTS} \cdot T_{GTS}$, where T_{GTS} is the constant time length that was required to accommodate the transmission period of the maximal data FL and the replied ACK frame. We then have

$$T_{GTS} = \left\lceil \frac{T_{MDATA} + T_{ACK}}{T_{SLT}} \right\rceil \cdot T_{SLT} \quad (22)$$

$$f_N(n, x) = \begin{cases} f_N(n, x+1) + 1, & \text{if } \sum_{j=1}^{x} T^n_{ST(j)} < (T^n_{CAP} - T^n_{BCN}) \text{ and } x < N^n_{CN(j+1)} \\ 0, & \text{otherwise} \end{cases} \quad (21)$$

Authorized licensed use limited to: Tamkang University. Downloaded on June 04,2010 at 03:49:35 UTC from IEEE Xplore. Restrictions apply.

where T_{MDATA} is the transmission time of the data frame of the maximal payload length ($= 14$ UBPs), and T_{SLT} is the unit time slot ($T_{SLT} = 3 \cdot 2^{SO}$ UBPs) of the active period. Let $Y^{(n)}$ denote the total number of data frames that were transmitted during the CFP of the nth superframe. We have

$$Y^{(n)} = N_{GTS}(n) \cdot \left(P_{FRZ(I_n)}^{n-1} + \left(1 - P_{FRZ(I_n)}^{n-1}\right) \cdot P_{FC(I_n)}^{n-1} \cdot \frac{T_{GTS}}{T_{DATA} + T_{ACK}} \right). \quad (23)$$

As with the aforementioned explanation, the number of active nodes at the beginning of each superframe (i.e., $N_{CN(1)}^{n}$) is set to $N_{CN(I_n)}^{n-1}$. Then, the total number of active nodes at the beginning of the $(n+1)$th superframe ($N_{CN(1)}^{n+1}$) is

$$N_{CN(1)}^{n+1} = N_{CN(I_n)}^{n} + N_{GTS}(n) \cdot P_{FRZ(I_n)}^{n}. \quad (24)$$

Based on the above analyses, the goodput (G), which is the ratio of the total amount of transmitted payload to the observed time period, can be expressed using the following equation:

$$G = \frac{L \cdot \sum_{n=1}^{K} \left(X^{(n)} + Y^{(n)}\right)}{K \cdot D_{UBP} \cdot SD} \quad (25)$$

where K is the number of observed superframes.

Table I lists all the parameters that were used in the goodput analysis.

TABLE I
NOTATIONS THAT WERE USED DURING GOODPUT ANALYSIS

G	The ratio of the amount of transmitted payload to the observed period
I_n	The index of the last successful transmission in CAP of the *n*-th superframe
L	The mean length of data payload excluding header and CRC trailer
M	The number of nodes in the WPAN
$N_{CN(i)}^{n}$	The number of nodes desiring channel access between the (*i*-1)-th and the *i*-th successful transmission in the *n*-th superframe
$N_{GTS(i)}^{n}$	The expected number of GTSs for the (n+1)-th superframe prior to the *i*-th successful transmission in the *n*-th superframe
$N_{GTS}(n)$	The number of GTSs allocated to nodes in the *n*-th superframe
$N_{RC(i)}^{n}$	The expected number of retry attempts between the (*i*-1)-th and the *i*-th successful transmissions in the *n*-th superframe
$P_{C(i)}^{n}$	The probability of contention collision occurring between the (*i*-1)-th and the *i*-th successful transmissions in the *n*-th superframe under the condition that channel is sensed clear by the node
$P_{CC(i)}^{n}$	The probability of contention collision occurring between the (*i*-1)-th and the *i*-th successful transmissions in the *n*-th superframe
$P_{CLR(i)}^{n}$	The probability of a node perceiving clear channel between the (*i*-1)-th and the *i*-th successful transmissions in the *n*-th superframe
$P_{F(i)}^{n}$	The probability of failed contention caused by busy channel assessment or collisions between the (*i*-1)-th and the *i*-th successful transmissions in the *n*-th superframe
$P_{FRZ(i)}^{n}$	The probability of a node freezing contention between the (*i*-1)-th and the *i*-th successful transmissions in the *n*-th superframe
$P_{H(i)}^{n}$	The probability of hidden-node collision between the (*i*-1)-th and the *i*-th successful transmissions in the *n*-th superframe under the condition that channel is sensed clear by node
$P_{HC(i)}$	The probability of hidden-node collision between the (*i*-1)-th and the *i*-th successful transmission in the *n*-th superframe
P_{HD}	The probability that any two nodes are hidden from each other
$P(k,t)$	The probability of exactly *k* frames arriving at a node during the time interval *t*
$P(k,N,t)$	The probability of exactly *k* frames arriving during the time interval *t* when the number of active nodes is *N*
$P_{UCGTS(i)}^{n}$	The probability of unchanging the number of reserved GTS slots in the next superframe calculated between the (*i*-1)-th and the *i*-th successful transmissions in the *n*-th superframe
$P_{S(i)}^{n}$	The probabilities of transmitting successfully after sensing channel clear between the (*i*-1)-th and the *i*-th successful transmissions in the *n*-th superframe
RTH	The maximum retry count of a data frame
T_{ACK}	The transmission time length of ACK frame plus an inter-frame spacing period
T_{BCN}^{n}	The transmission time length of beacon frame broadcasting in the *n*-th superframe
$T_{BP(i)}^{n}$	The time cost of couple times of backoff and channel sensing between the (*i*-1)-th and the *i*-th successful transmissions in the *n*-th superframe
T_{CCA}	The period of twice clear channel assessments (CCAs)
T_{CFP}^{n}	The period of CFP in the *n*-th superframe
T_{DATA}	The mean transmission period of data frame
$T_{DTP(i)}^{n}$	The data transmission period including failed transmitting periods and the *i*-th successful transmission period in *n*-th superframe
$T_{FT(i)}^{n}$	The wasted time period of all failed transmission periods between the (*i*-1)-th and the *i*-th successful transmissions in the *n*-th superframe
T_{GTS}	The total required transmission period for a data frame of the maximum payload length plus the replied ACK frame
$T_{H(i)}^{n}$	The average time cost caused from a hidden-node collision and the subsequent collision chain(s) between the (*i*-1)-th and the *i*-th successful transmissions in the *n*-th superframe
T_{MDATA}	The transmission period of a data frame of the maximum payload length
T_{SLT}	The time length of one slot
$T_{ST(i)}^{n}$	The time length of the *i*-th successful transmission in the *n*-th superframe
$X^{(n)}$	The total number of data frames served during CAP of the *n*-th superframe
$Y^{(n)}$	The total number of data frames served during CFP of the *n*-th superframe
λ	The mean payload arrival rate of a node in one UBP

V. SIMULATIONS

To focus on the proposed protocol, an error-free channel condition and a WPAN with hidden-node situation are assumed. The network under investigation only includes one coordinator and ten static nodes (i.e., $M = 10$), which are randomly distributed in the WPAN, and any pair of nodes has a 41% probability of a hidden-node relationship. Suppose that the frame arrival rate of a node follows a Poisson distribution with a mean of λ frame(s) and that the FL has an exponential distribution with a mean of L B. Moreover, each node can store at most 20 data frames so that it will drop arrival frames when the buffer is full. The network load is normalized as $(M \cdot \lambda \cdot L)/B$, where B is the channel bandwidth, which is set as $B = 250$ kb/s $= 31.25$ kB/s. Moreover, we consider two kinds of mean FL: 1) $L = 20$ B and 2) $L = 40$ B.

Other simulation parameters, e.g., (SO) and (BO), are set based on hypothetical applications in WSNs [1]. Using a small BO setting will multiply the frequency of beacon transmissions. Conversely, a larger BO setting will incur time synchronization issues. Two values of BO setting are applied in simulations: 1) 2 (about 16 superframes per second) and 2) 3 (about eight superframes per second). Moreover, we set $SO = BO$ for all simulations. The maximal number of retries (i.e., RTH) is set to 5 in both protocols. The probability P that was used in the PFCS entity of the CSMA/CF protocol is set to C/RTH, where C is the retry count $(0 \leq C \leq RTH)$ of the frame. In the following figures, the proposed CSMA/CF and legacy standard protocols are denoted as CSMA/CF and Standard, respectively.

Authorized licensed use limited to: Tamkang University. Downloaded on June 04,2010 at 03:49:35 UTC from IEEE Xplore. Restrictions apply.

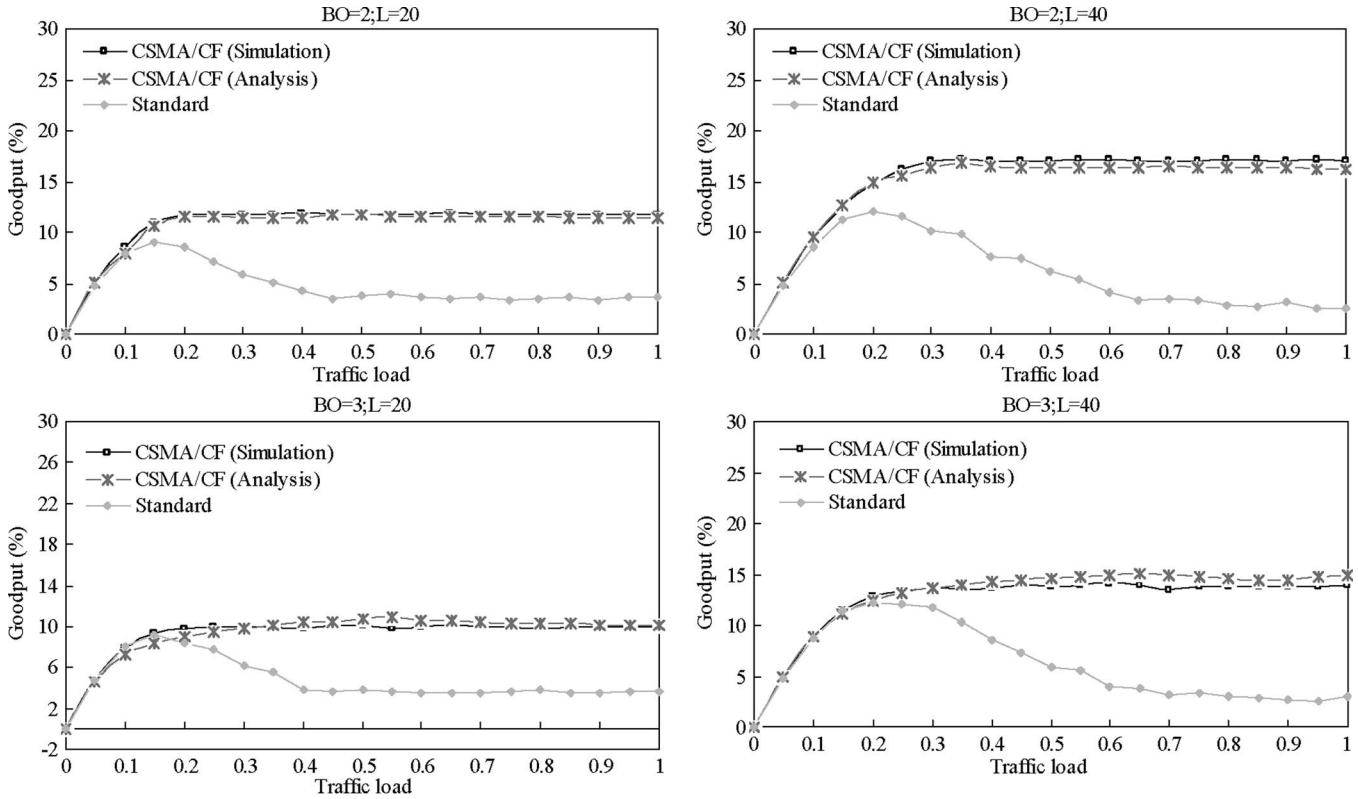


Fig. 9. Comparisons of goodputs between the CSMA/CF and standard protocols under different settings of BO, FL, and traffic load.

To compare the results of the analyses and the simulations, the goodput in (25) is used as the primary metric. First, the goodput is depicted in Fig. 9 as a function of the normalized network load for both the legacy IEEE 802.15.4 and the proposed CSMA/CF protocol. Evidently, the simulation results of the CSMA/CF protocol are very close to the analytical results in Section IV. In addition, the adoption of the CSMA/CF protocol always results in a higher system goodput relative to the legacy protocol, regardless of the simulation environment. It can be observed in Fig. 9 that the legacy blind-backoff scheme, in conjunction with the CRS and PFCS, can sustain a stable goodput, whereas the legacy protocol yields a sharp decrease in efficiency as the network load increases. One simple comparison between these four figures, as grouped in Fig. 9, indicates that the goodput improvement that the proposed CSMA/CF enabled heavily relies on the frame size. Given a network load, a larger mean frame size will result in fewer data frames and a longer mean collision chain period. In addition, the goodput improvement becomes more pronounced as the network load increases. For example, the improvement that was achieved can reach as high as 500% when the normalized network load is larger than or equal to 0.5, as plotted in cases with $L = 40$.

Fig. 10 further illustrates the relationship between link utilization and network load. Intuitively, link utilization is proportional to traffic load when the network load is light. One closer examination of the link utilization results that was derived using the standard protocol reveals that, as the traffic load slightly increases, it will more likely occupy most of the channel bandwidth by retransmitting frames, thus increasing the waste-causing collision inefficiency to an appreciable level. Note that the steep rise in link utilization makes the standard protocol waste not only the channel bandwidth but the power source as well. In other words, both characteristics, i.e., high link utilization and low goodput, explicitly indicate that the channel inefficiency in the standard protocol is the result of collisions. This highly desirable feature of insensibility is particularly indispensable for an 802.15.4 network, as the last hop will experience a magnitude of increase in the number of nodes.

Surprisingly, the CSMA/CF protocol provides sustainable goodputs in all cases when the link utilization is well controlled below a certain level. Moreover, both CRS and PFCS avoid hidden-node collisions to accommodate more successful transmissions; therefore, the reduction in link utilization that CSMA/CF can accomplish is clearly lower than the standard protocol. We can see that, under the saturation cases, the link utilization improvement that was reaped by the CSMA/CF protocol is, on the average, 20%. Reducing link utilization naturally results in the advantages of low power consumption and a high probability of successful transmission. However, it is only tenable if the contention does not become violent and disordered after the link utilization saturates.

To determine whether the CSMA/CF protocol can also provide better delay control than the standard protocol, the average access delays that were achieved by both the legacy 802.15.4 protocol and the CSMA/CF protocol are compared and plotted in Fig. 11. Frame access delay is measured from the time that the frame arrives at the node to the time that the same frame is successfully transmitted. During simulations, frames that are dropped, because the buffer is full or approaches the retry threshold, are not accumulated. As expected,

Authorized licensed use limited to: Tamkang University. Downloaded on June 04,2010 at 03:49:35 UTC from IEEE Xplore. Restrictions apply.

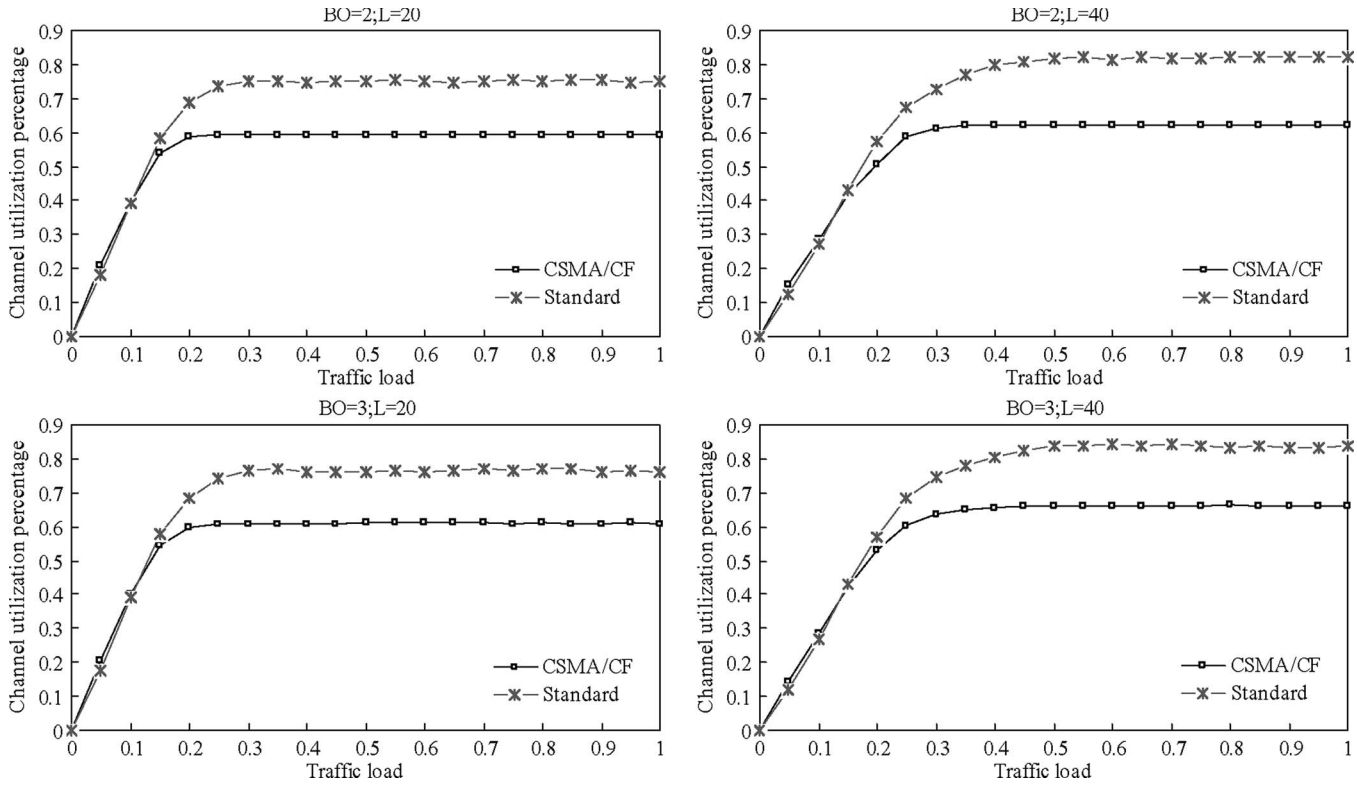


Fig. 10. Comparisons of the channel utilization percentage between the proposed CSMA/CF and standard protocols under different settings of BO, FL (L), and traffic load.

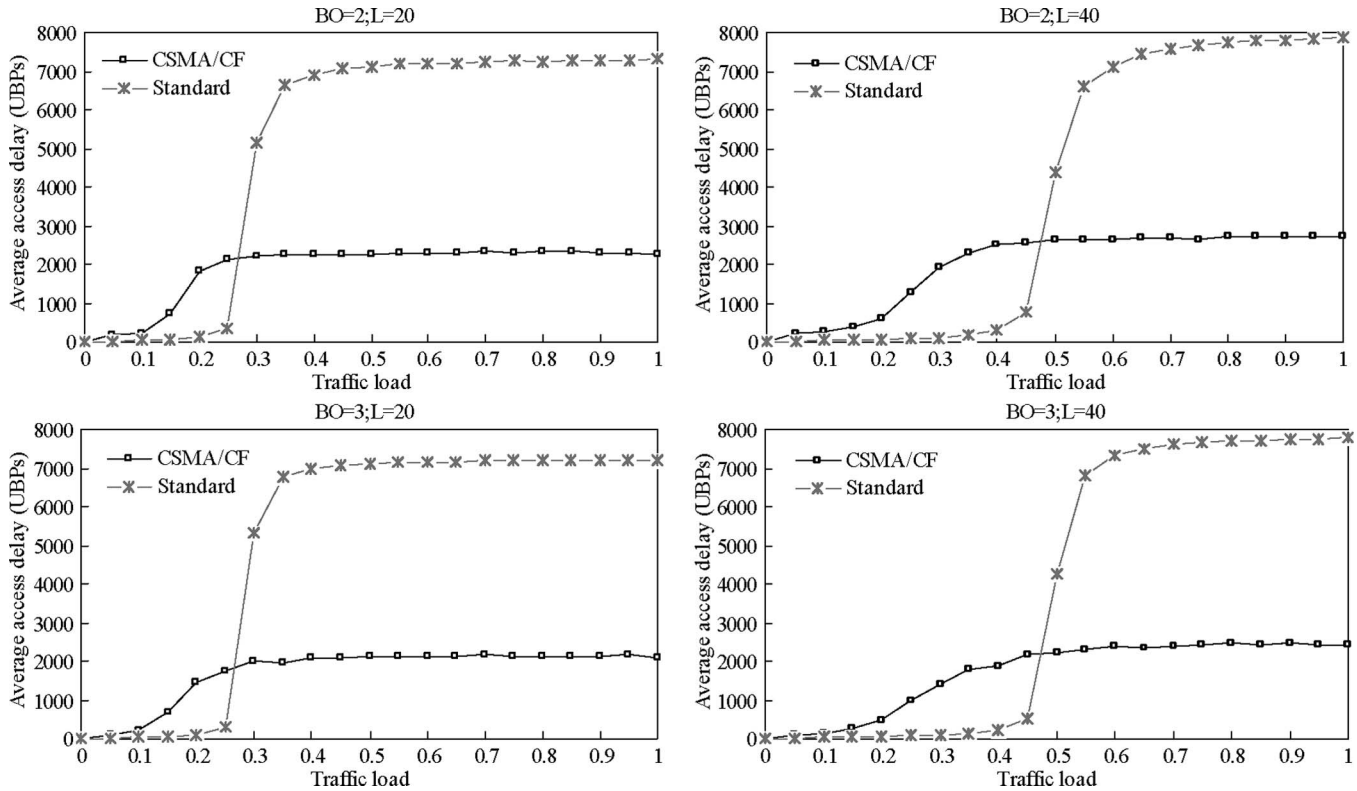


Fig. 11. Comparisons of the average access delays that were derived from the CSMA/CF and legacy standard protocols under different settings of BO, FL(L), and traffic load.

the simulation results demonstrate that the access delay for the legacy 802.15.4 protocol is significantly lower than for the CSMA/CF protocol when the link utilization is unsaturated, because the CSMA/CF protocol uses probability P to detain transmissions of G-nodes until GTSs in the next superframe or a later one. However, under most circumstances, CSMA/CF

Authorized licensed use limited to: Tamkang University. Downloaded on June 04,2010 at 03:49:35 UTC from IEEE Xplore. Restrictions apply.

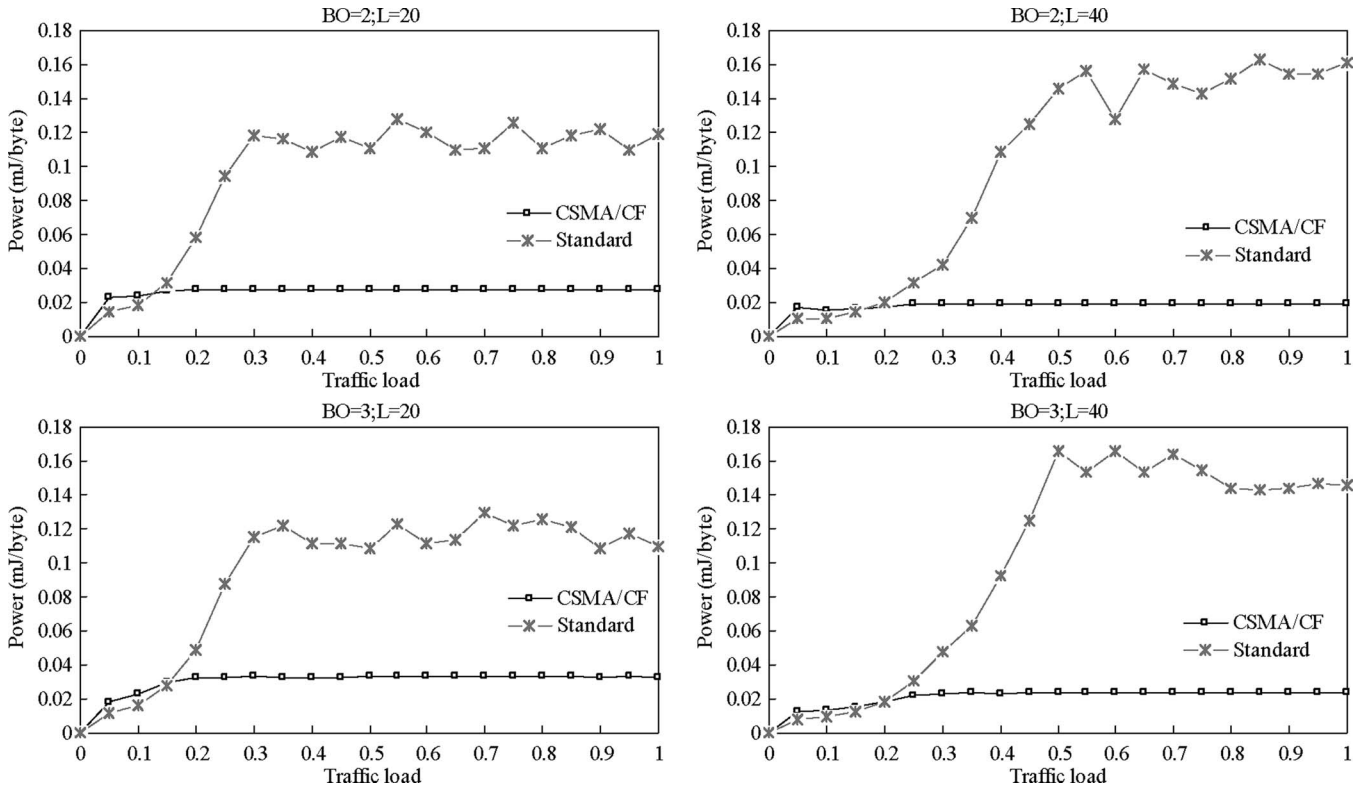


Fig. 12. Comparisons of the power consumption of the CSMA/CF and standard protocols with different settings of BO, FL(L), and traffic load.

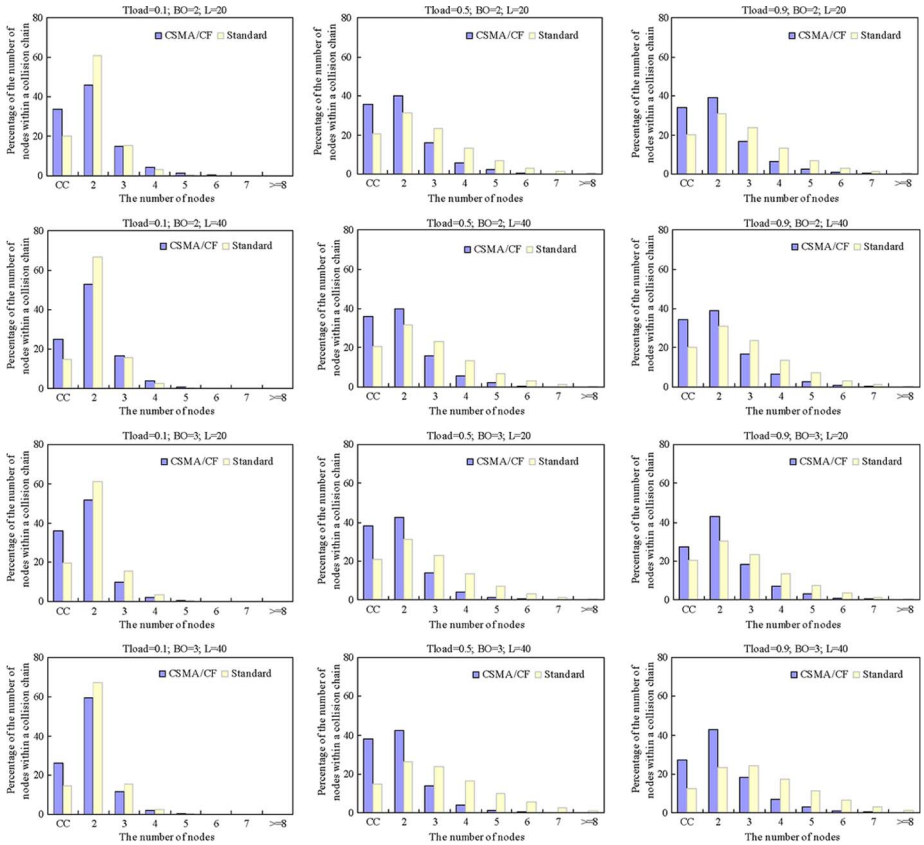
can achieve significantly fewer access delays than the legacy protocol. In particular, when the network load increases beyond 0.3 (in the case of $L = 20$ B) or 0.5 (in the case of $L = 40$ B), the access delay for the legacy 802.15.4 protocol rapidly increases to approximately 7500 UBPs due to excessive HNCs. On the other hand, the average access delay that CSMA/CF achieved increases to approximately 2500 UBPs as the network load increases. At that point, the CSMA/CF access delay plateaus at approximately 2500 UBPs. This highly desirable feature of CSMA/CF is attributed to the fact that, as the network load increases, the likelihood of a node in the collision chain being marked as a G-node also increases. In other words, the growing availability of G-nodes not only cancels the goodput degradation caused by increased collisions but also results in a substantial improvement in the average access delay. This instance demonstrates that CSMA/CF is more suitable for handling time-critical applications than the legacy 802.15.4 protocol.

To reveal energy costs, the power consumption parameters of the Chipcon CC2420 transceiver, which operates at 2.4 GHz [19], are adopted to observe the actual power that was consumed for the successful transmission of 1 B by both the CSMA/CF and legacy protocols. The current costs in the reception and transmission modes of the CC2420 RF transceiver are 19.7 and 17.4 mA, respectively, and the chip is powered by 3.3V. Therefore, the reception and transmission of 1 B will consume 2.08 and 1.77 μJ, respectively. In simulations, power consumption is accumulated only when the transceiver operates at a working mode (i.e., the reception mode or the transmission mode). Fig. 12 compares the energy cost that the CSMA/CF and legacy protocols achieved and shows that the CSMA/CF protocol is most effective under heavy network load conditions, which is consistent with the results shown in Fig. 10. At the saturation point, the CSMA/CF energy cost plateaus at approximately 20 μJ $\sim$ 30 μJ/B, which is significantly lower than the energy cost of 120 μJ $\sim$ 160 μJ/B that was achieved with the legacy 802.15.4 protocol.

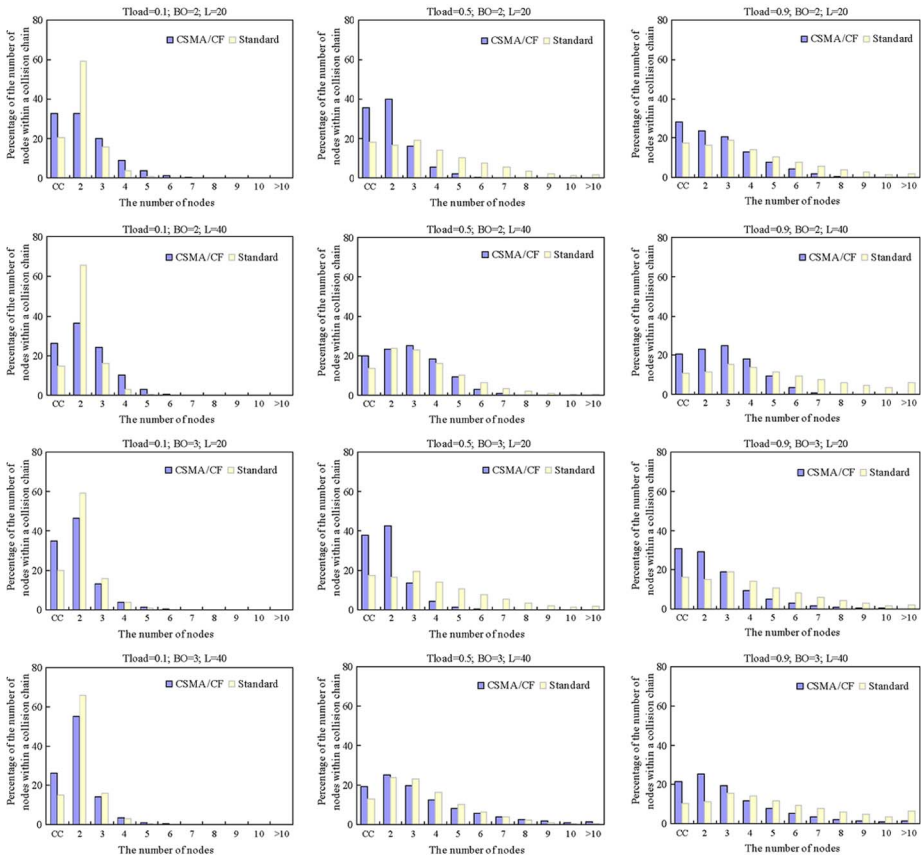
To understand the effect of CCPs in an 802.1.5.4 WPAN, we look at the average number of nodes that are involved in collision chains and the average duration of the collision chains. The distribution of the number of nodes that are involved in collision chains, under conditions of a network with ten nodes ($(M = 10)$), are plotted in Fig. 13(a). For comparison, the corresponding percentage of CCs is attached to every subfigure in Fig. 13. In Fig. 13(a), we can see that the HNC type dominates collisions that occur in WPANs. More specifically, the overall HNC ratio for the legacy 802.15.4 protocol is as high as 80% $\sim$ 90%. On the other hand, the overall HNC ratio that CSMA/CF achieved reduces this to approximately 60% $\sim$ 70% in all circumstances. A closer examination of the distribution results reveals that, as traffic load decreases, it will more likely have two-node HNCs; thus, CSMA/CF can efficiently avoid subsequent hidden-node collisions by moving one node from the CAP to the CFP. In addition, the comparisons also show that the CSMA/CF protocol always produces more CCs than the legacy standard protocol. Therefore, CSMA/CF can, indeed, limit the prolongation of collision chains; consequently, the probability of an HNC that comprises a number of nodes is further reduced.

As shown in Fig. 14, both the standard and CSMA/CF protocols contribute similar time overheads when the network load is low. On the other hand, the average collision chain

Authorized licensed use limited to: Tamkang University. Downloaded on June 04,2010 at 03:49:35 UTC from IEEE Xplore. Restrictions apply.



(a)



(b)

Fig. 13. Distributions of numbers of collided nodes in CC and HNC with different settings of BO, FL(L), network size (M), and traffic load. (a) $M = 10$. (b) $M = 20$.

Authorized licensed use limited to: Tamkang University. Downloaded on June 04,2010 at 03:49:35 UTC from IEEE Xplore. Restrictions apply.

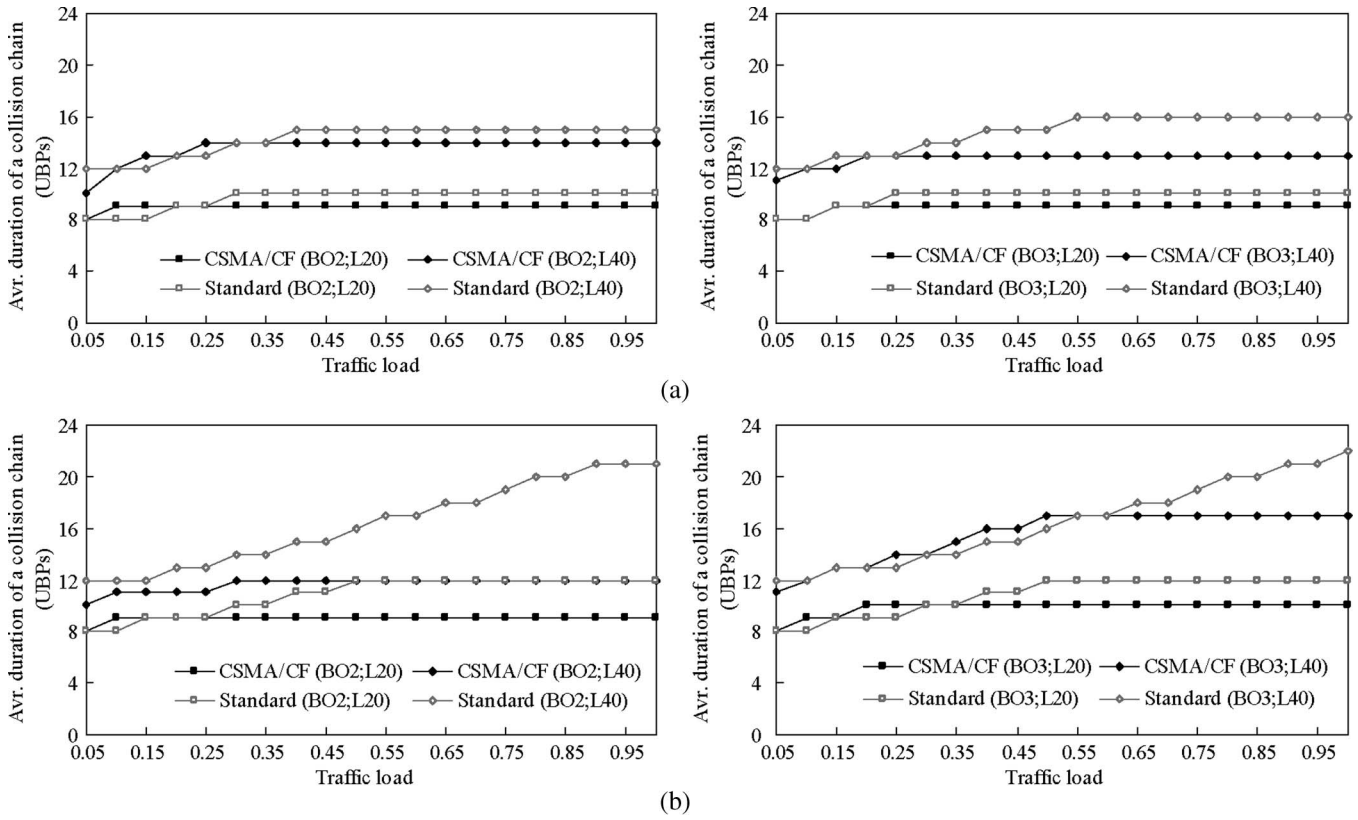


Fig. 14. Average collision chain duration for different settings of BO, FL(L), and traffic load. (a) $M = 10$. (b) $M = 20$.

duration is obviously prolonged by the standard protocol as the network load increases. Fig. 14(b) shows that the curves (BO $= 2$ and BO $= 3$) that were derived using the CSMA/CF protocol are different. We note that the CSMA/CF protocol does not ideally perform when the beacon interval is extended in a heavily loaded network, because G-nodes are somehow permitted the opportunity to stay in the contention mode, participate in normal contentions, and, thus, cause prolonged HNCs. However, based on Fig. 13, CSMA/CF can reduce the collision chains and, therefore, lower the overall cost of collision chains.

Based on the above performance results, we conclude that the CSMA/CF protocol is superior to the legacy 802.15.4 protocol for four reasons: 1) reduced contending nodes; 2) support of guaranteed transmission opportunities for contending nodes; 3) the capability for HNC avoidance; and 4) the shortening of collision chains. In conclusion, the CSMA/CF protocol, which consists of a CRS and a PFCS, indeed possesses the following superior capacities: 1) Resolve the CCP; 2) alleviate potentially excessive collisions; 3) decrease frame access delays; 4) improve network goodput; and 5) diminish power consumption.

VI. Conclusion

In this paper, we have proposed the CSMA/CF protocol, which comprises two efficiency-improvement schemes—the CRS and the PFCS—to leverage the legacy IEEE 802.15.4 CSMA/CA protocol and improve the readiness of the IEEE 802.15.4 protocol for adoption in a WSN. The CRS was originally designed for a coordinator to determine which node is involved in each hidden node collision. Then, the PFCS extends the applicability of GTSs from regular real-time data to asynchronous data from those recognized nodes while delivering an improvement in efficiency. In addition, the PFCS provides alternative contention opportunities for recognized nodes to shorten access delays. The performance analysis and evaluation results confirm that the CSMA/CF protocol can sustain protocol efficiency and, thus, limit the performance degradation that CCPs causes. Finally, the CRS and PFCS work together to provide a comprehensive efficiency-improving solution for application in IEEE 802.15.4 networks.

References

[1] B. Sinopoli, C. Sharp, L. Schenato, S. Schaffert, and S. S. Sastry, "Distributed control applications within sensor networks," *Proc. IEEE—Special Issue on Sensor Networks Applications*, vol. 91, no. 8, pp. 1235–1246, Aug. 2003.

[2] R. Szewczyk, E. Osterweil, J. Polastre, M. Hamilton, A. Mainwaring, and D. Estrin, "Habitat monitoring with sensor networks," *Commun. ACM*, vol. 47, no. 6, pp. 34–40, Jun. 2004.

[3] E. Hanada, Y. Hoshino, and T. Kudou, "Safe introduction of in-hospital wireless LAN," in *Proc. Int. Medinfo.*, Sep. 2004, pp. 1426–1429.

[4] J. H. Lee and H. Hashimoto, "Controlling mobile robots in distributed intelligent sensor network," *IEEE Trans. Ind. Electron.*, vol. 50, no. 5, pp. 890–902, Oct. 2001.

[5] S. Ray, D. Starobinski, A. Trachtenberg, and R. Ungrangsi, "Robust location detection with sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 22, no. 6, pp. 1016–1025, Aug. 2004.

[6] IEEE 802 Working Group, *Standard for Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*, ANSI/IEEE Std. 802.15.4, Sep. 2006.

Authorized licensed use limited to: Tamkang University. Downloaded on June 04,2010 at 03:49:35 UTC from IEEE Xplore. Restrictions apply.

[7] J. Mišić, C. J. Fung, and V. B. Mišić, "On node population in a multilevel 802.15.4 sensor network," in *Proc. GLOBECOM*, Nov. 2006, pp. 1–6.
[8] F. A. Tobagi 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. Commun.*, vol. COM-23, no. 12, pp. 1417–1433, Dec. 1975.
[9] IEEE 802.11 Working Group, *Information Technology Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirement. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, ANSI/IEEE Std. 802.11b-1999/Cor. 1-2001-7, Nov. 2001.
[10] J. Mišić, S. Shafi, and V. B. Mišić, "Avoiding the bottlenecks in the MAC layer in 802.15.4 low-rate WPAN," in *Proc. Parallel Distrib. Syst.*, Jul. 2005, vol. 2, pp. 363–367.
[11] R. Iyer and L. Kleinrock, "QoS control for sensor networks," in *Proc. ICC*, May 2003, vol. 1, pp. 517–521.
[12] Y. Sankarasubramaniam, O. B. Akan, and I. F. Akyildiz, "ESRT: Event to sink reliable transport in wireless sensor networks," in *Proc. 4th ACM MobiHoc*, Jun. 2003, pp. 177–188.
[13] J. Mišić, S. Shafi, and V. B. Mišić, "Maintaining reliability through activity management in an 802.15.4 sensor cluster," *IEEE Trans. Veh. Technol.*, vol. 55, no. 3, pp. 779–788, May 2006.
[14] Y. C. Tseng, S. Y. Ni, and E. Y. Shih, "Adaptive approaches to relieving broadcast storms in a wireless multihop mobile ad hoc network," *IEEE Trans. Comput.*, vol. 52, no. 5, pp. 545–557, May 2003.
[15] K. Whitehouse, A. Woo, F. Jiang, J. Polastre, and D. Culler, "Exploiting the capture effect for collision detection and recovery," in *Proc. 2nd IEEE Workshop EmNetS-II*, May 2005, pp. 45–52.
[16] L. J. Hwang, S. T. Sheu, Y. Y. Shih, and Y. C. Chen, "Grouping strategy for solving hidden device problem in IEEE 802.15.4 LR-WPAN," in *Proc. WICON*, Jul. 2005, pp. 26–32.
[17] *Data sheet for UZ2400 low power 2.4 GHz transceiver for IEEE 802.15.4 standard*. [Online]. Available: http://www.ubec.com.tw/product/downfiles/uz2400/DS-2400-02_v1_3_RN.pdf
[18] IEEE 802.11 Working Group, *Information Technology Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirement. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 4: Further Higher Data Rate. Extension in the 2.4 GHz Band*, ANSI/IEEE Std. 802.11g-2003, Jun. 2003.
[19] *Data Sheet for CC2420 2.4GHz IEEE 802.15.4/Zigbee RF Transceiver*. [Online]. Available: http://www.chipcon.com/files/CC2420_Data_Sheet_1_4.pdf

Shiann-Tsong Sheu (M'03) received the B.S. degree in applied mathematics from the National Chung Hsing University, Taichung, Taiwan, in 1990 and the Ph.D. degree in computer science from the National Tsing Hua University, Hsinchu, Taiwan, in 1995.

He was an Associate Professor with the Department of Electrical Engineering, Tamkang University, Taipei, Taiwan, from 1995 to 2002 and became a Professor in February 2002. In August 2005, he joined the faculty of the Department of Communication Engineering, National Central University, Taoyuan, Taiwan. His research interests include next-generation wireless communication, optical networks, protocol designs, and intelligent control algorithms.

Dr. Sheu received the Outstanding Young Researcher Award from the IEEE Communications Society Asia Pacific Board in 2002.

Yun-Yen Shih (S'03) received the B.S. degree in electrical engineering in 2002 from Tamkang University, Taipei, Taiwan. He is currently working toward the Ph.D. degree in electrical engineering with the Department of Electrical Engineering, Tamkang University.

His research interests include various wire/wireless communication network protocols.

Wei-Tsong Lee (M'07) received the B.E.E.E., M.S., and Ph.D. degrees in electrical engineering from the National Cheng Kung University, Tainan, Taiwan, in 1984, 1986, and 1995, respectively.

He is currently an Associate Professor with the Department of Electrical Engineering, Tamkang University, Taipei, Taiwan. His research interests include high-speed networks, cable modems, embedded systems, and stochastic ordering.

Dr. Lee is a member of the Institute of Electrical, Information, and Communication Engineers.

Authorized licensed use limited to: Tamkang University. Downloaded on June 04,2010 at 03:49:35 UTC from IEEE Xplore. Restrictions apply.