Grouping Strategy for Solving Hidden Node Problem in IEEE 802.15.4 LR-WPAN

Lain-Jinn Hwang†, Shiann-Tsong Sheu‡, Yun-Yen Shih‡ and Yen-Chieh Cheng‡

†Department of Information Engineering,
‡Department of Electrical Engineering,
Tamkang University, Tamsui, Taipei Hsien, Taiwan 251, R.O.C.
E-mail:micro@mail.tku.edu.tw; stsheu@ee.tku.edu.tw

Abstract **—** The medium access control (MAC) protocol defined in IEEE 802.15.4 standard is able to achieve low-power transmissions in low-rate and short-distance wireless personal area networks (WPANs). The modified CSMA/CA protocol used to minimize power consumption does not have the hidden-node protection mechanism, such as RST/CTS mechanism, for the sake of reducing the control overheads. Referring to previous research results, which proved that the probability of any two nodes in infrastructure network unheard each other is about 41%, the hidden-node problem (HNP) could result in inefficient data transmission in WPAN and quick power consumption. In this paper, we propose a simple and efficient grouping strategy to solve the IEEE 802.15.4 HNP without needing extra control overheads in data transmissions. The proposed strategy groups nodes according to their hidden-node relationships and then separates the periodic transmission period into several non-overlapping sub-periods, one for each group. The WPAN coordinator is responsible for detecting the hidden-node situation and performing the grouping procedure if necessary. In this paper, we also prove that the maximal number of groups in a WPAN is five. Simulation results demonstrate that the proposed strategy is able to improve the standard transmission efficiency and to conserve energy by eliminating the unnecessary collisions.

I. INTRODUCTION

Recently, many fancy applications are developed in the low-rate, short-distance, and low-cost wireless sensor networks (WSNs) [1]. The WSN typically consists of a gateway and a number of sensor nodes. The WSN node combining wireless transmission and various sensors now is able to provide specific services such as ecological detection, health monitoring, digital home, and so on. The sensor nodes are allocated randomly or artificially for retrieving specific environmental information and then return results via wireless communication to the gateway. However, wireless sensor nodes made by different enterprises and academic laboratories cannot interoperate to each other because there is lack of a wireless transmission standard protocol for them.

The IEEE 802.15.4 low-rate wireless personal area networks (LR-WPAN) standard [2] is the potential one of standard candidates of WSN. This standard specifies two physical (PHY) layers: an 868/915 MHz direct sequence spread spectrum (DSSS) PHY and a 2450 MHz DSSS PHY. The 2450 MHz PHY supports data rate of 250 kb/s and the 868/915 MHz PHY supports data rates of 20 kb/s and 40 kb/s. The transmission distance varies from 10 to 100 meters depending on the transmission power level. There are two kinds of WPAN topologies: the star (infrastructure) and the peer-to-peer (ad-hoc) topologies. In this paper, we focus on the star-based network topology where one of WPAN nodes is the coordinator.

The IEEE 802.15.4 devices are categorized as full -function devices (FFD) and reduced-function devices (RFD). In an infrastructure mode, the first active FFD will establish the WPAN and of course becomes the WPAN coordinator. The coordinator broadcasts beacon frames periodically not only to inform neighboring devices its existence but also to synchronize the members already anticipate in the network. Devices belonging to WPAN are denoted as ‘nodes’ in this paper. Similar to the master/slave relationship, nodes are informed the system operation parameters by the coordinator. The coordinator and nodes have two kinds of transmission manners. One is to contend channel in the contention access period (CAP), and the other is to access channel in a collision-free manner during a contention-free period (CFP).

The channel access in CAP is based on a modified CSMA/CA protocol, which is modified from the IEEE 802.11 DCF protocol and is particularly suitable for low-power WPANs. When a node has frame(s) in the transmission buffer, it first selects a random backoff value from the initial contention window (CW) and then enters the backoff mode. Different from the standard CSMA/CA, this node starts sensing channel only when the backoff countdown process is complete. During the sensing period, if node perceives the channel idle for two consecutive unit backoff periods (UBPs), it will transmit the frame. (Notice that the UBP is the basic time unit in the backoff process.) Contrarily, if node detects that the channel is busy during

This work is supported by NSC under contracts 93-2213-E-032-021, 93-2213-E-032-022 and 93-2622-E-032-002-CC3.

carrier sensing period, it stops listening and selects another random backoff value from the doubled CW for the next attempt. Then the node turns off its transceiver and starts to countdown the new chosen backoff time. Due to the characteristic of blinding countdown, the channel utilization could be very low and the access delay could be very long.

Oppositely to the channel contention period, standard provides the contention-free period (CFP) for real-time applications. The CFP is composed of several guaranteed time slots (GTSs) for providing nodes to have their own transmission periods. For real-time downlink/uplink services, at most seven FFD nodes are able to demand the coordinator to allot GTS. The GTS allocation information is attached in the beacon frames. In the periodical and dedicated GTS period, the GTS owner can transmit and receive frames under the rule that transmissions cannot interference other GTS(s) or the next beacon frame transmission.

The WPAN coordinator performs synchronization by using the superframe structure. A superframe is bounded by beacon frame transmission, and has an active portion and an inactive portion. The active portion consists of CAP and CFP, and begins at the beacon frame broadcasting. The interval of active portion in a WPAN is decided by a system parameter, which is denoted as superframe order (SO) in standard. The interval of beacon frames appearance (which equals to the interval of a superframe) is decided by another parameter named as beacon order (BO). An active period and a superframe interval both consist of 16 equal size time slots but these two kinds of slots are different from each other. One slot of the active period and the superframe interval equals to 3×2^{SO} UBPs and 3×2^{BO} UBPs respectively. The values of SO and BO, denoted as *SO* and *BO* respectively, can be set from 0 to 14. Notably, the *BO* must be larger than or equal to *SO*. Thus, the interval of inactive portion is equal to $16\times3\times(2^{BO}-2^{SO})$ UBPs. Notably, the inactive period does not exist whilst *SO* equals to *BO*. In an inactive period, devices including the coordinator may turn off their transceivers to save the power. The values of two system parameters SO and BO are carried on the beacon frame broadcasting from the coordinator to nodes.

In WPAN, although transmission region of the coordinator is able to cover all nodes, nodes are not guaranteed to hear the signals from all the other nodes. If signals transmitted from node A to coordinator cannot be sensed by any other listening node B, then node B will recognize the channel is clear and transmit data to the coordinator at the same time. The coordinator will fail to recognize the overlapping signals. This scenario is called hidden node (or hidden terminal) problem (HNP) in the wireless networks [3]. In an infrastructure wireless network, assume that nodes having the same transmission radius are randomly spread, in the coverage area of coordinator, the probability of any two nodes having hidden node relationship is up to 41% [4]. Through out this paper, we call the collision caused by hidden node problem as hidden node collision (HNC). We note that the HNC is quite different from the contention collision (CC) caused by several nodes with some contention resolution algorithm selecting the same time slot to access the channel. The shortcoming of consecutive CCs can be solved by the truncated binary exponential backoff (TBEB) mechanism used in IEEE 802.11 CSMA/CA protocol [5]. Only using TBEB is insufficient to solve the HNCs, therefore, the IEEE 802.11 standard uses RTS/CTS handshake mechanism to eliminate the HNC situation. Furthermore, a particular field, named 'Duration/ID' field, of MAC frame is allocated to indicate the precise time period of each transmission to avoid unnecessary HNC [5]. Unfortunately, the IEEE 802.15.4 MAC does not have any protection mechanism to against the HNP. Besides, for the sake of power conservation, a node with the modified CSMA/CA cannot sense the channel when it stays in backoff mode and this action makes either the RTS/CTS handshake protocol or the duration notification protocol useless.

This article will propose a new grouping strategy to enhance the IEEE 802.15.4 protocol to solve the HNP. The proposed strategy consists of four phases. The first phase is hidden node situation discovery, the second phase is hidden relationship collection, the third phase is nodes grouping, and the final phase is bandwidth allocation. That is, the coordinator monitors whether the corrupted signal is caused from HNC. If the HNC is found, the coordinator begins to collect the connectivity among nodes. The approaches of precisely finding HNC and collect the hidden relationships among nodes are proposed in this paper. The coordinator exploits the polling to request every node to reply the corresponding acknowledge (ACK) frame to coordinator and every node can find its hidden nodes according to the received acknowledge frames. After the polling period, the coordinator asks all nodes to report their observed results about the information of hidden nodes. Then, the coordinator groups nodes into a number of groups according to collected information. Nodes in a same group have the property that they can hear all the signals sent from the others. Finally, coordinator notifies the grouping result to all nodes. After grouping, the coordinator periodically allocates each group the bandwidth according to the group size among all groups. The reserved channel period for grouping access is named as hidden avoidance guaranteed time slots (HA-GTS) and nodes access their own HA-GTS by applying the standard modified CSMA/CA. By controlling the transmissions of nodes, the grouping strategy can significantly relieve the contentions and improve the network performance.

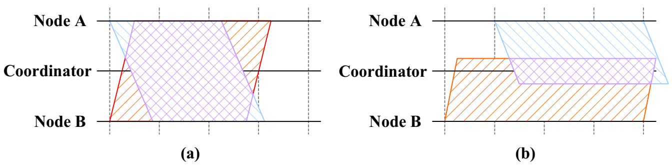

Figure 1. Two possible collision cases in WPAN.

The rest of the paper is organized as following. Section II describes how the grouping strategy builds non-hidden-node WPANs. Section III proves that at maximal five groups are needed for any kinds of wireless network topology. Section IV describes the simulation model and results for evaluating the efficiency of proposed grouping strategy. Simulation results obviously reveal that the hidden node problem has been solved by proposed strategy and, moreover, the energy conservation has been reduced at the same time. Finally, some conclusion remarks are given in Section V.

II. THE GROUPING STRATEGY

The grouping strategy basically consists of four phases: hidden node situation discovery phase, hidden relationship collection phase, nodes grouping phase, and bandwidth allocation phase. The following subsections will describe each phase in detail.

A. The Hidden Node Situation Discovery

In CSMA/CA based protocol, contention collision always occurs when two or more devices select the same UBP to transmit frames. In such condition, transmitted signals will be interfered from the beginning of the transmissions (i.e. it happens at the UBP boundary). On the contrary, hidden node collision (HNC) only occurs when two or more nodes unhearing to the others transmit frames simultaneously and, in the receiver, the corrupted signals could appear at any time during frame transmission. We note that the farthest transmission distance of IEEE 802.15.4 PHY is about 100 meters; therefore, the maximum propagation delay between transmitter and receiver is about 0.5us. If the synchronization is perfectly achieved by beacon broadcastings, then the propagation delay is much smaller than the interval of an UBP (= 320us) and that these two cases of collisions can be precisely distinguished. Figure 1(a) illustrates the coordinator cannot recognize most of signals of frame when the contended collision (CC) happens. On the other hand, in HNC case, the coordinator is able to successfully recognize part of signals of one frame before the HNC happens, as shown in Fig. 1(b). Therefore, when the coordinator successfully receives consecutive signals for one UBP before detecting the corrupted signals, it is conscious of theoccurrence of hidden node situation. We also note that the DSSS technology used in standard is able to against the channel noise in most kinds of environments and this also means that the considered PHY is capable of distinguishing two collision cases. In a word, the CC and HNC are distinguishable by observing the timing of occurring corrupt signals and the functionality of hidden node situation discovery needed in proposed approach is accomplished.

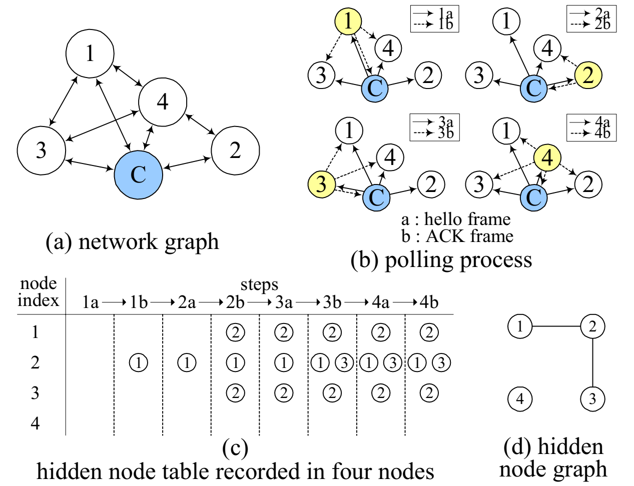

Figure 2. An example illustrates how the coordinator builds the hidden node graph.

B. The Hidden Node Information Collection

Once the coordinator finds the hidden node situation, it needs to collect the hidden relationships among nodes. For readability, we use a WPAN, which contains one coordinator and four nodes, as an example, as shown in Fig. 2(a). In this example, a two-way link between two nodes means that the connected two nodes can hear each other. There exists hidden node situation in this topology because Node 2 is unconnected with Nodes 1 and 3. After being aware of hidden node situation, the coordinator transmits an awaking request message, which is attached on beacon frame, to command every node to enter active mode in the current superframe and wait the following polling message(s) sent from coordinator. Then, the coordinator starts transmitting one data frame with empty payload (we denote it as polling frame in this paper) to each node in turn and waits the ACK response, as shown in Fig. 2(b). Nodes who receive the polling frame but failing in receiving the acknowledgement (ACK) frame will record the correspondent node polled by coordinator as their hidden node.

As the polling process has finished, every node should have the information about its hidden nodes. At that time, the coordinator broadcasts the reporting request frame to all nodes to command them to return the hidden-node information. Nodes replying results to coordinator can use either polling-based approach or contention-based approach. The coordinator then transforms collected hidden node information into a hidden node graph, as shown in Fig. 2(d). In the hidden node graph, the edge between two nodes indicates they have the hidden relationship. For simplicity, we assume the transmission link between transceivers is symmetric and the links in hidden node graph are bi-directional. In the next subsection, we will describe how the coordinator forms groups according to the hidden node graph.

C. The Group Assignation

Once the hidden node graph has been built, the coordinator starts to perform grouping procedure for separating nodes into a number of groups as described before. By the grouping strategy, nodes that are connected in hidden node graph cannot be assigned to the same group. This constraint makes sure no hidden node situation exists in every group. It is obvious that the simple way to avoid HNC is to allow each node to form its own group. Owing to the whole active period will be divided into a number of exclusive subperiods, one subperiod for one group, the channel utilization must be taken into considerations. In other words, if too many groups are formed, the advantage of frames multiplexing in multiple access protocol is missing and consequently the channel utilization is not acceptable. Therefore, we have to control 1) the number of groups as smaller as possible and 2) the numbers of nodes of groups (also denoted as group sizes in this paper) as equal as possible.

Solutions to minimize the number of groups seem like the well known problem — partition into Hamiltonian subgraphs problem (or coloring problem) [6] and this problem can be reduced into a 3SAT problem [6] which has been proved as a NP-complete problem. Therefore, for the sake of minimizing the complexity of proposed grouping algorithm, this paper proposes a simple heuristic algorithm to find out the proper number of groups for nodes.

Let V denote the set of nodes excluding the coordinator in WPAN. The proposed algorithm first selects the node with the maximal degree in set V to form the first group and then removes this node from set V. Then, the node with the second maximal degree in set V is investigated whether it can join into the first formed group according to the hidden relationship between this node and all the nodes in this group. If there is no edge between them, this node is successfully grouped into the considered group and it is removed from set V. Otherwise, the algorithm passes and marked this node, and then it investigates the other unmarked nodes one by one according to the degree factor from high to low. When the nodes in set V are all marked, the algorithm starts to form the second group following the steps described above. This group forming process is repeated until set V becomes empty. The complexity of the proposed algorithm is $O(N^2)$ where N is the number of nodes excluding the coordinator in WPAN. The grouping algorithm is listed as following.

Grouping Algorithm

Input: Given a hidden node graph $G = (V,E)$;
Output: The group sets $S_1, S_2, \ldots, S_g$; $(g \leq 5)$
$k = 1$; // the group index

```
while |V| > 0 do
    pick a node v from V of the largest degree;
    construct group set S_k = {v};
    V = V - {v};
    construct temporary set W = V;
    while |W| > 0 do
        pick a node w from W of the highest degree;
        W = W - {w};
        if node w has no edge to any nodes in S_k then
            S_k = S_k + {w};    // join into group k
            V = V - {w};
        end if
    end
    k++;
end;
```

D. The Grouping Result and Access Period Notification

The grouping result is broadcast by using the beacon frames and an additional grouping information field (GIF) is needed to carry the grouping results. Due to the pages limitation, we do not describe the detailed format of the GIF. Following the GIF is the GTS information field, which indicates the precise period reserved for real-time nodes or the formed groups. Each group is assigned only one period for transmissions. The method of period notification is the same as the GTS notification in the IEEE 802.15.4 protocol [2]. Because the allocated periods (GTSs) for groups are accessed following the modified CSMA/CA contention protocol but the contention-free manner, so we name the particular GTS as the hidden avoidance GTS (HA-GTS). Moreover, the whole period of HA-GTSs are called as group access period (GAP) in this paper. A superframe now is separated into three disjoint periods except the beacon transmission and inactive portion: CAP, CFP and GAP. We notice that standard needs to reserve at least 22 UBPs for CAP and this minimal period is just sufficient for a new coming device to send the joining management frame. Standard GTS period is still reserved for real-time nodes to transmit periodic and urgent data frames. In the GAP, the access period of one group is linearly proportional to the number of nodes in it. Assume the active period excluding the minimal CAP and original GTS is L (in UBP) and the total number of nodes is n. A group with m nodes will be allocated a period of mL/n UBPs.

In GAP, nodes access the channel following the modified CSMA/CA protocol. If one node desires to access channel and the correspondent HA-GTS period expires, then it has to wait until the next period. Although nodes are not guaranteed to have the transmission opportunity in every GAP, the decreased number of contending nodes in every subperiod certainly increases the successful accessing ratio. On the other hand, since the coordinator is the central node of WPAN, it is allowed to transmit data frames in the whole active period. For each data frame, the coordinator transmits it in the correspondent HA-GTS according to the destination node and grouping result. If the data frame cannot be successfully transmitted in the specified HA-GTS, this frame will be delayed to the next super-frame.

We also note that if some of nodes are mobile nodes, the hidden relationship among nodes may change from time to time. In this case, the coordinator has to keep monitoring all collision cases even after the grouping has done.

III. Mathematical Analysis

In this section, we will prove that using at most five groups is enough to cover all nodes in a WPAN.

Based on the grouping constrain, nodes in the same group must hear signals from the others. The transmission coverage of any one of group members could be treated as the transmission coverage of this group. Therefore, the theory proof of that five groups can cover all nodes in network is transformed to prove that the area covered by the transmission ranges of five selected nodes is able to cover the whole network.

Assume that the coordinator of the network locates at the center O of circle and the radius of the circle is the transmission distance. Then, all nodes must locate within the circle. Before proving this theory, we first denote some useful parameters listed as following:

- N: denotes the number of nodes excluding the coordinator in the WPAN.
- r: denotes the transmission distance.
- $\overline{N_iN_j}$: denotes the line connecting two nodes N_i and N_j.
- $|\overline{N_iN_j}|$: the Euclidean distance of the line $\overline{N_iN_j}$.
- $\theta(i,j)$: denotes the angle between lines $\overline{N_iO}$ and $\overline{N_jO}$ ($0<\theta(i,j)\le\pi$).
- $\alpha(i,j)$: denotes the angle between lines $\overline{N_jO}$ and $\overline{N_iN_j}$ ($0<\alpha(i,j)\le\pi/2$).

Now, we will use the following cases with different network sizes N to prove that the transmission area covered by the transmission areas of at most five selected nodes can cover all nodes no matter how many nodes N in the network:

Case *1*: (N=1)

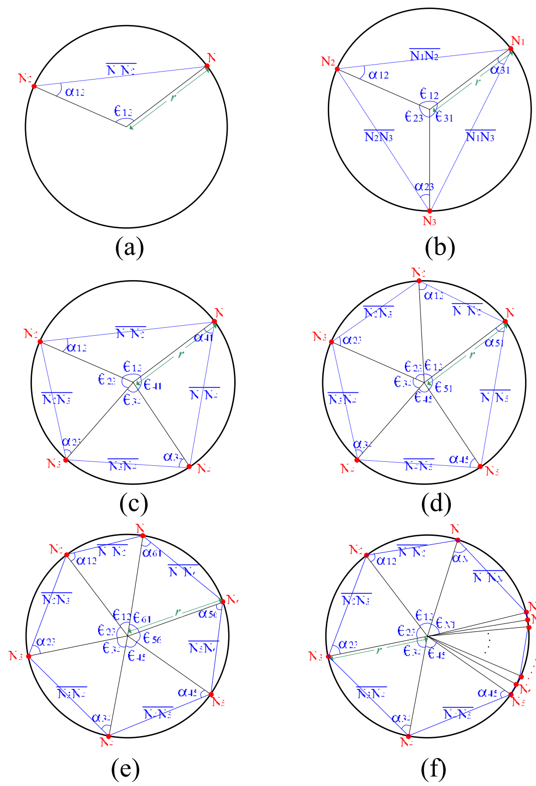

Figure 4. The network topologies with different numbers of nodes N are considered for analyzing the maximal number of groups.

While the network consists of the coordinator and one node, none of other nodes needs to be covered by this node. In this case, one node (i.e. one group) is sufficient to cover the whole network. In fact, the grouping procedure will not be executed in this case.

Case *2*: (N=2)

There are a coordinator and two nodes in WPAN as shown in Fig. 4(a). According to the trigonometric function, the relationship between $|\overline{N_iN_j}|$ and r is

$$\frac{\operatorname{Sin}\theta(1,2)}{|\overline{N_1N_2}|}=\frac{\operatorname{Sin}\alpha(1,2)}{r}. \qquad (1)$$

Because ΔN_1N_2O is an isosceles triangle and the angle summation of a triangle is equal to π, we have

$$\alpha(1,2)=\frac{\pi-\theta(1,2)}{2}. \qquad (2)$$

Combining equations (1) and (2), we derive that

$$\frac{\operatorname{Sin}\theta(1,2)}{|\overline{N_1N_2}|}=\frac{\operatorname{Sin}\left(\pi-\frac{\theta(1,2)}{2}\right)}{r}=\frac{\operatorname{Sin}\pi\operatorname{Cos}\frac{\theta(1,2)}{2}-\operatorname{Cos}\frac{\pi}{2}\operatorname{Sin}\frac{\theta(1,2)}{2}}{r}=\frac{\operatorname{Cos}\frac{\theta(1,2)}{2}}{r},$$

$$|\overline{N_1N_2}|=\frac{\operatorname{Sin}\theta(1,2)}{\operatorname{Cos}\frac{\theta(1,2)}{2}}\times r \qquad (3)$$

Proceedings of the First International Conference on Wireless Internet (WICON'05)
0-7695-2382-X/05 $20.00 **IEEE**

Applying double angle formula on equation (3), we get

$$\left|\overline{N_1N_2}\right| = \frac{2\mathrm{Sin}\frac{\theta(1,2)}{2}\mathrm{Cos}\frac{\theta(1,2)}{2}}{\mathrm{Cos}\frac{\theta(1,2)}{2}} \times r = 2r\mathrm{Sin}\frac{\theta(1,2)}{2} \quad (4)$$

Therefore, in the case of $\theta(1,2)>\pi/3$, the Euclidean distance between nodes N_1 and N_2 is longer than the radius (i.e., $|\overline{N_iN_j}| > r$) and the network needs two groups to cover all nodes. Otherwise, one group is enough.

Case *3*: ($3\leq N\leq 5$)

As shown in Figures 4(b) to 4(d), we can see that the similar results of forming groups as presented in case 2. If $\theta(i,i+1)>\pi/3$, nodes N_i and N_{i+1} will separately join two different groups. Since the summation of all angels must be less than or equal to 2π, there are at most five angels whose degrees are larger than $\pi/3$. Therefore, in this case where $3\leq N\leq 5$, the maximal number of groups is less than or equal to N.

Case 4: ($N \geq 6$)

From Figures 4(e) and 4(f), the summation of N angles $\{\theta(1,2), \theta(2,3), \theta(3,4),\ldots, \theta(N,1)\}$ is equal to 2π. Therefore, it is impossible that all the angels are larger than $\pi/3$. In fact, the maximal number of angels larger than $\pi/3$ is five as described in case 3. In other words, at least N-5 links are shorter than radius r and those correspondent nodes will be grouped into appropriate groups. So, we conclude that the maximal number of groups in network is no more than five.

IV. SIMULTAION RESULTS

In this section, we will compare the performance of the proposed grouping strategy and the standard IEEE 802.15.4 protocol under the hidden-node environment. Nodes are randomly distributed and any two nodes of them have 41% probability unheard each other. In the simulation model, we assume the WPAN contains one coordinator and twenty static nodes (N=20). The channel bandwidth is B bytes/s and the wireless channel is assumed noiseless and error-free. Frame arrival rate of any node follows the Poisson distribution with a mean of λ (frames/s) and the frame length is an exponential distribution with a mean of L bytes. The normalized network load is equal to $(N\times\lambda\times L)/B$. In the simulations, we set B=250Kbit/s=31.25Kbytes/s.

In order to show the influence caused from hidden node collisions, we additionally observe the performance of the standard IEEE 802.15.4 protocol operating in the non-hidden-node environment. Nodes in the non-hidden-node environment are assumed to be capable of hearing all signals in WPAN. For readability, the proposed grouping strategy, the standard protocol operating with hidden-node environment, and non-hidden-node environment are respectively denoted as terms ‘Grouping’, ‘Standard-H’, and ’Standard-NH’ in the following figures.

The simulation parameters such as frame mean length (L), superframe order (SO) and beacon order (BO) are set based on the normal applications in sensor networks. A data frame is produced only when a node has sensed some environmental information such as the degree of lightness, temperature, movement, magnetism, and so on. Therefore, we consider two kinds of mean frame lengths: L=10 bytes and L=20 bytes. The setting of BO is an important factor to the system performance. As a smaller BO is applied, a higher frequency of beacon transmission and a much faster speed of power consumption will be resulted. Contrarily, using a higher BO value will result in a more difficulty on synchronization. Thus, in our opinions, the values of BO considered in simulations are 3 (about 8 superframes per second when BO=3) and 4 (about 4 superframes per second when BO=4). Assume the sensing process in the simulations to be operated continuously and we set SO=BO. In the simulations with grouping strategy, the CAP always occupies 22 UBPs (=440 symbols) as explained in Section II and we also assume there is no CFP requirement in WPAN.

Fig. 5 illustrates the derived goodputs measured in percentage of the total channel bandwidth. We emphasize that the curves of Grouping strategy and Standard-H are the highest curve and the worst curve respectively. From observing the goodput differential between Standard-NH and Standard-H, we find an interesting result that the interference time of hidden node situation is delayed while the mean frame length L becomes larger. However, as L increasing, more hidden node collisions are caused. This is because longer frames have a higher probability to be interfered by hidden nodes than shorter frames. On the other hand, the goodput curves of Standard-NH and Standard-H are degraded a lot caused by violent contentions when the traffic load becomes heavy. The proposed grouping strategy separates nodes into isolated access intervals to alleviate the degree of contentions. Note that the goodput curves of grouping strategy are a little worse than Standard-NH when the traffic load is less than 0.4. The weakness of grouping strategy is that channel bandwidth might be wasted under light traffic load due to the access period restriction on nodes which transmissions in active parts of subperiods cannot overlap inactive parts. We verify that the grouping strategy under light traffic load is able to provide high performance as good as the IEEE 802.15.4 protocol in the non-hidden-node situation and is able to keep its best performance under heavy traffic load.

For the sake of revealing the power saving capability of proposed grouping strategy, in our simulations, we adopt the power consumption parameters of the 8MHz 8-bit Atmel ATmega128L microprocessor [7] and the Chipcon CC2420 transceiver [8] to observe how long the battery longevity can be extended in our grouping strategy. Note that the ATmega128L microprocessor is particularly designed for power-saved applications and it consumes 5mA and 2mA in the active mode and idle mode respectively. The CC2420 RF transceiver operates at 2.4GHz and it provides 250 Kb/s data rate. The power consumptions in reception mode, transmission mode, and idle mode are 19.7mA, 17.4mA, and 20uA, respectively. The device is powered by two AA batteries, which provide approximately 2850mA/h. Following these settings, the average lifetimes (in days) of nodes are displayed in the Fig. 6. We can find that, when the traffic load is higher than 0.3, the nodes with grouping strategy can survive at least 7 days and 18 days longer than the nodes with Standard-NH and the nodes with Standard-H respectively. The reason is that the grouping strategy can not only reduce the wakeful time but also eliminate energy waste caused by hidden node collisions. From simulation results, the grouping strategy indeed possesses the superior abilities of 1) resolving the hidden node problem, 2) alleviating the violent contentions 3) improving the network performance, and 4) reducing the power consumptions, as desired.

V. CONCLUSIONS

A novel grouping strategy has been proposed in this paper to effectively solve the hidden node problem in IEEE 802.15.4 WPANs. The way of coordinator detecting the collisions caused from hidden node situation was proposed and the heuristic grouping algorithm also was proposed to form groups. We also prove that the maximal number of formed groups is five in any WPAN. Simulation results demonstrated that, in the hidden node situation, the proposed grouping strategy with a relatively longer superframe interval can provide the goodput as high as the standard protocol operating in the non-hidden-node situation. Moreover, with the proposed strategy, the battery longevity could be even doubled related to that in standard protocol. From these simulation results, we conclude the proposed grouping strategy is a simple, efficient approach to enhance the IEEE 802.15.4 protocol while applying in wireless sensor networks.

REFERENCES

[1] Bruno Sinopoli, Courtney Sharp, Luca Schenato, Shawn Schaffert and S. Shankar Sastry, "Distributed control applications within sensor networks," *Proceedings of IEEE*, vol. 91, Issue 8, pp. 1235-1246, Aug. 2003.

[2] 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 802.15.4*, Oct. 2003.

[3] Fouad A. Tobagi and Leonard Kleinrock, "Packet Switching in Radio Channels: Part II-The Hidden Terminal Problem in Carrier Sense Multiple-Access and the Busy-Tone Solution," *IEEE Transaction on Communication*, vol. 23, Issue 12, pp. 1417-1433, Dec. 1975.

[4] Yu-Chee Tseng, Sze-Yao Ni and En-Yu Shih, "Adaptive Approaches to Relieving Broadcast Storms in a Wireless Multihop Mobile Ad Hoc Network," *IEEE Transactions on Computers*, vol. 52, Issue 5, pp. 545-557, May 2003.

[5] 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.

[6] M.R. Garey and D.S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-completeness,* W.H.Freeman and Company, Jun. 1979.

[7] Data Sheet for 8-bit Microcontroller with 128K Bytes In-System Programmable Flash, available online at http://www.atmel.com/dyn/resources/prod_documents /doc2467.pdf.

[8] Data Sheet for CC2420 2.4GHz IEEE 802.15.4/Zigbee RF Transceiver, available online at http://www.chipcon.com/ files/CC2420_Data_Sheet_1_2.pdf.

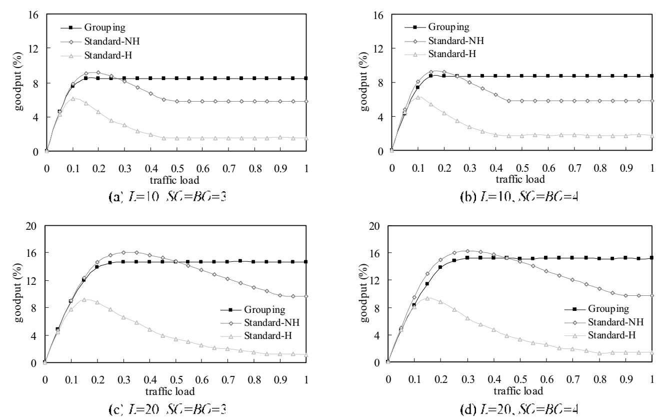

Figure 5. Comparisons of derived goodputs of three protocols under different environments.

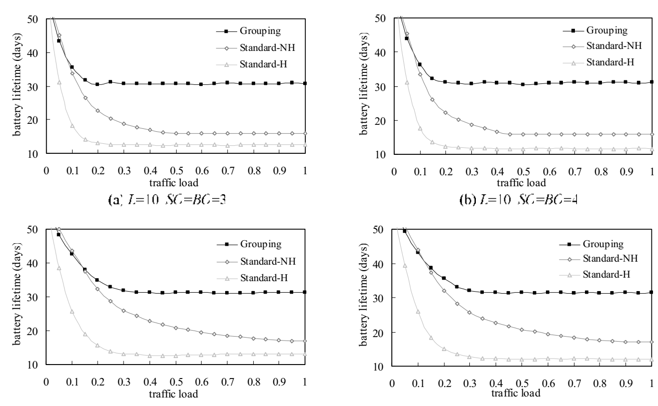

Figure 6. Comparisons of the average battery lifetime of nodes with three protocols under different environments.