

Research and Implementation of CSMA-CA Back-off Algorithm based on Embedded System and ADF7025

Hualin Zhan^{1,a}, Xiaochun Lai^{2,b}, Pengfei Zuo^{1,c}, Sixia Yang^{1,d}

¹Communication and Electronic College, JiangXi Science & Technology Normal University, NanChang, China

²Science and Technology Development Office, JiangXi Provincial Higher Education Institutions, NanChang, China

^ae-mail:james392@sohu.com, ^be-mail:laixiaochun@163.com, ^ce-mail: PengfeiZ@sohu.com, ^de-mail: SixiaY@163.com

Keywords: embedded; ADF7025; CSMA-CA; Back-off

Abstract. CSMA-CA back-off algorithm is the most important link for wireless sensor network(WSN) MAC protocol, distributes the limited wireless communication resource among all WSNs, is the key to ensure the efficient communication for WSN. ADF7025 is a single chip wireless transceiver with a low rate, low power consumption and lost cost. This paper describes the implementation of CSMA-CA back-off algorithm in embedded system and ADF7025 wireless transceiver. This paper describes platform, by adjusting the parameters and test, results show that the embedded ADF7025 platform based on improving the transmission node back-off success rate, decrease the packet collision probability and the retransmission probability, so as to improve the success rate of the receive node.

Introduction

Based on OSI model and combined with its own characteristics, WSN protocol will be divided into client application layer(Demo), application support sublayer(ASS), network layer(NWK), media access control(MAC), the physical layer(PHY), as shown in figure 1.

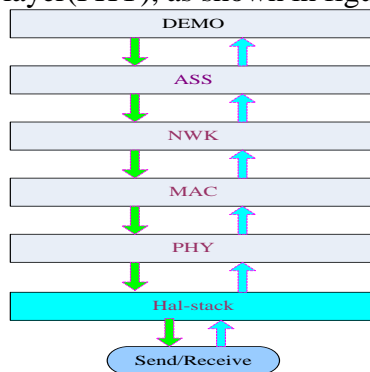


Figure 1 WSN hierarchy diagram

The hardware abstraction layer does not belong to the wireless sensor protocol, but it provides the interface function between physical layer and hardware transceiver. This layer is mainly convenient transplanted between different platform transceiver. WSN protocol can be network and run on the embedded platform and ADF7025 because of transplanting the MAC layer protocol and modifying the hardware abstraction layer protocol. Therefore, this focuses on the CSMA-CA back-off algorithm research and implementation on the embedded platform.

Design Timer

WSN protocol can orderly operate by one reasons of depending on timing counter service for each layer of the protocol, since the wireless transceiver ADF7025 do not design special timing counter, referring to IEEE 802.15.4 protocol and CC2430 timing principle, using software realize the timing and counting function for CSMA-CA back-off algorithm.

Table 1 is ADF7025 software timing referring to CC2430 relevant timing principle.

Table I Timing Parameter

platform item	CC2430	ADF7025
implementation	TIMER2	Greenwich mean time
timing unit	each sending 4 bit count one, that is a symbol period TICK	each sending 4 bit count one, that is a symbol period TICK
the timing unit size	$(4 * 1000000) / (250 * 1000) = 16\mu s$	$(4 * 1000000) / (173 * 1000) = 23\mu s$
timing method	TIMER2 count register will increase 1 when every symbol period of time	the time difference from the start to the end of time divided by the period time

Note: 1. TIMER2 is a special timer in CC2430.

2. $(4 * 1000000) / (250 * 1000) = 16\mu s$, 250kbps means CC2430 transmission rate.

3. $(4 * 1000000) / (173 * 1000) = 23\mu s$, 173kbps means ADF7025 transmission rate.

Energy threshold

A. Principle of Energy Threshold

The nodes in WSN randomly send data, interception channel is idle or not and idle interval is greater than the inter frame spacing before a node wants to send data, if it is, data is immediately sent, otherwise not sent and continue listening. Listening on a channel is the physical carrier sense and virtual carrier sense, this paper uses the former because the ADF7025 platform provides the relevant support. Using physical carrier sense has common three ways to estimate the channel is idle or not, energy detection(ED), carrier detection(CD), energy carrier hybrid detection. This paper uses ED, the channel is idle or not depending on the energy through the node, this way has strong operability and easy implement. The channel is occupied when the energy through the node exceeds a energy threshold. Node energy threshold provides an important basis for CSMA-CA back-off algorithm.

B. Algorithm Flow Chart

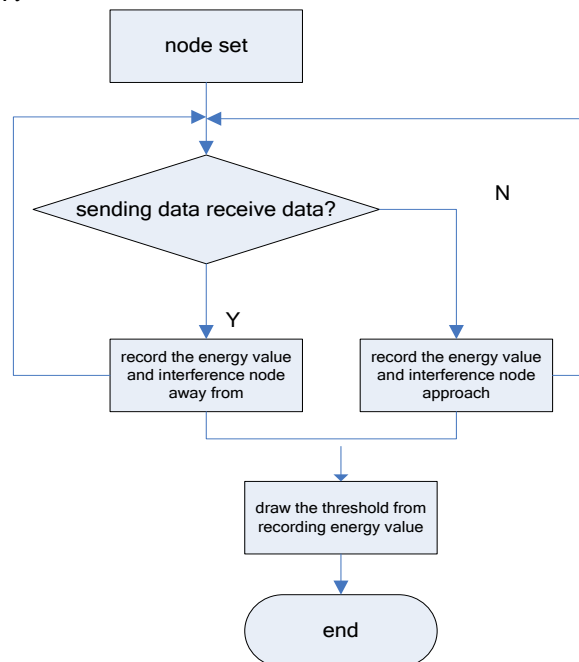


Figure 2 the energy threshold debugging flow chart

The energy threshold is a two dimension function about transmitting power and distance, will be integrated into the power and distance. Interfering nodes transmission power set to a fixed value (-15dbm), the mobile transmit node use the successive approximation method for testing energy threshold. Interference nodes without any delay send data, sending node is defined according to the

whole network logic function, here is actually running receive test procedure, also do not make any delay.

C. Debugging Experiment Environment

1. hardware required: BF533 development board, network card, ADF7025 wireless transceiver module.

2. software required: receive test-program temprecv.c with read input energy threshold and temprecv.c is running on the sending node, sending test-program tempsend.c is running on the interference node, u-boot bootloader and uClinux2007 operate system with embedded ADF7025 driver.

3. connected graph: interference node and the sending node as shown in Figure 3.

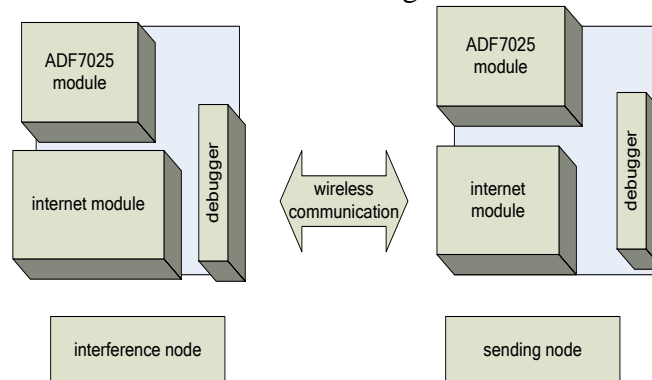


Figure 3 connected diagram between interference and send node

D. Debugging Result Analysis

1. Debugging Result

Setting the ADF7025 transmitting power is -15dbm, measure values of input energy in the critical reception condition. The following list data is input energy in the critical condition which transmitting node receives data or not.

79 83 82 72 81 79 83 81 84 85 75 80 85 82 85 83 83 83 84 82 67 68 66 67 75 76 75 69 69 67 69
 69 64 65 63 68 64 62 61 65 68 66 63 68 67 64 66 68 69 64 67 65 68 67 66 63 65 68 66 65 67 64 68
 abcdefghijklivoprstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
 66 67 67 66 68 65 66 70 66 68 66 66 65 67 67 65 66 67 65 65 67 66 67 68 67 65 66 67 66 66 67
 67 67 67 66 65 67 66 66 67 67 66 64 87 81 80 86 85 82 81 82 82 84 80 77 84 79.

2. Result Analysis

According to the input energy of recorded values, it is certain that the interfering nodes will affect the sending node to receiving data, so setting the input energy threshold should be larger than the input energy average value, but will be less than input energy value of sending data. After several test and analysis under the different environment, finally, the energy absolute threshold is set at 70.

CSMA-CA back-off Algorithm Parameters Determination

A. CSMA-CA back-off Algorithm Process

In order to minimize the number of data transmission collision and retransmissions, the media access control method in this paper is Carrier Sensor Multiple Access with Collision Avoidance(CSMA-CA) based on the binary exponential back-off(BEB). CSMA-CA can effectively prevent each sending node from disorderly contending channel and avoid a collision probability by random delay so the signal conflict is reduced to minimum value.

Figure 4 is a flow chart of the CSMA-CA algorithm.

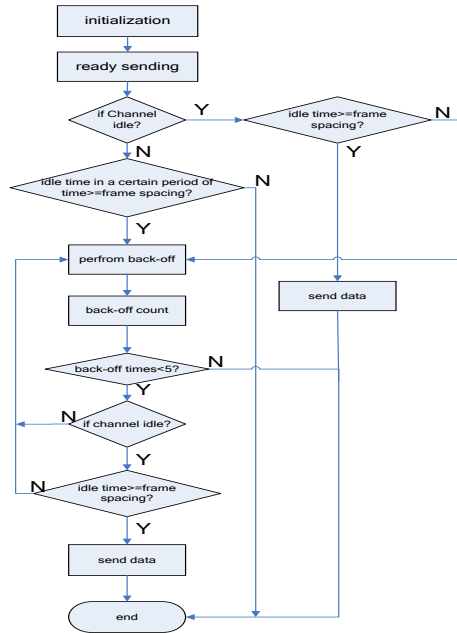


Figure 4 CSMA-CA Algorithm Diagram

B. The experimental environment

1. hardware required: BF533 development board, network card, ADF7025 wireless transceiver module.
2. software required: adf7025sendtest, adf7025recvtest, interferencetest, u-boot and uClinux2007 operate system with embedded ADF7025 driver.
3. connected graph: the sending node and the receiving node and interference node as shown in Figure 5.
4. constraints: setting energy input threshold 70, power and the distance is set to ensure that the three nodes are in the one hop communication range.

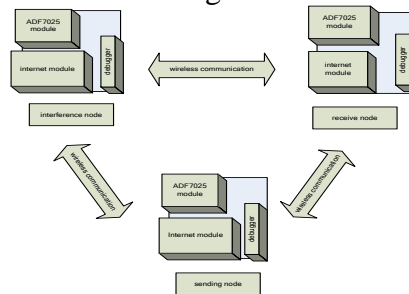


Figure 5 the three node connected diagrams

C. CSMA-CA Parameter Explain

Using CSMA-CA described in section 4.2 intercept the current media state. If the media is busy, the sending nodes will be delayed until the medium idle time is greater than the inter frame space DIFS(distribute coordination function interframe spacing), DIFS is necessary condition that a node successfully send data, it has close contact with hardware platform. After DIFS success, node will generate a random back-off time to postpone sending before sending, perform a back-off algorithm. A back-off time is determined by the following formula.

$$\text{Back-off Time} = \text{Random}(CW) \times \text{aSlotTime} \quad (1)$$

$$CW = 2^{BE}, \text{ BE is the back-off exponent} \quad (2)$$

1. Pseudo random integer Random (): it is uniformly distributed pseudorandom integers in the contention window $[0, CW]$, CW is a random integer, and $CW_{\min} = 2$, $CW_{\max} = 31$, BE is the back-off exponent and generally $0 \sim 5$.
2. Slot time aSlotTime: considering emission startup time and data transmission time and detection time of channel in addition to the node itself time factors, time for sending once data and slottime should be in the same order of magnitude, otherwise even execution of the longest back-off delay, other the node still sends data. So the slottime time and hardware platform have high correlation.

3. Number of back-off time(NB): the initial value of NB is 0, if a node want to send data, it should intercept channel state. If the channel is busy performing a back-off counter, NB will be plus 1 at the same time. The maximum value of NB is defined 4 in this paper, if the channel is still busying after four back-off counters, the node will give up the delivery in order to avoid excessive expenses.

DIFS and aSlotTime are two parameters associated with the hardware platform. DIFS must be greater than required time which the node sends client application data, otherwise the node cannot find space time to send a complete data, so the back-off algorithm is a complete failure. aSlotTime, namely a recession period, generally set in the tens to hundreds of symbol period (symbol period is 23us in this paper).

D. Relevant Parameter Setting

1. aSlotTime: aSlotTime unit is TICK, however a TICK is set to transmit half a byte, namely $(4 * 1000000) / (173 * 1000) = 23\text{us}$. Given that other nodes in the network spend 5ms level sending once a data, so aSlotTime preset 250TICKS.

2. DIFS: a transmit data length is approximately 20 to 50 bytes, ADF7025 send 50 bytes for $8 * 50 * 1000000 / (173 * 1000 * 23) = 100 \text{ TICKS}$, adding transmission delay 10ms in the drive, so DIFS is set to $10 * 1000 / 23 + 100 = 500 \text{ TICKS}$.

3. communication time interval: a node randomly sends data in the project. In order to improve the reliability of the algorithm, delay time of interference node obeys the Poisson distribution, the unit is ms. Sending node transmit data with a certain delay time because the sending function is a block type, however receiving node transmit without delay since the receiving function is non blocking type.

Results

Debugging CSMA-CA back-off algorithm according to the parameter value of theory analysis, the sending node transmit data 5000 times every time, then automatically end the sending program, and the sending program recorded the number of the back-off success for the first time and the second time and the third time and the last time.

A. Debugging Results

Table 2 is the only test results of aSlotTime and DIFS typical combined conditions.

Table II Testing Results

NO	aSlotTime	DIFS	col1	col2	col3	col4	col5	col6	col7
1	150	500	94.4	4436	34	18	6	4	94.2
2	200	500	95.1	4435	35	15	7	3	94.1
3	250	500	98.9	4424	40	21	8	5	98.4
4	300	500	98.4	4439	38	18	6	3	98.4
5	350	500	97.5	4438	36	19	7	4	97.2
6	150	550	94.6	4430	34	18	6	4	94.2
7	200	550	98.4	4431	35	15	7	3	95.4
8	250	550	98.7	4439	38	18	6	3	98.5
9	300	550	99.8	4422	43	19	9	5	99.5
10	350	550	97.9	4434	35	17	8	3	97.1

Note: col1-the success rate of back-off

col2-direct successfully sent

col3-numbers of the first success back-off

col4-numbers of the second success back-off

col5-numbers of the third success back-off

col6-numbers of the last success back-off

col7-the success rate of receiving

B. The Results Analysis

The first, we should see how much is the rate of success back-off, if it is very small, shows that the disturbance nodes transmit frequency is very high, the transmitting node fail to back-off due to not seize channel, therefore should reduce sending frequency of the interference node, adjust aSlotTime and DIFS after the rate of success back-off at least reach to above 80%. The second, we should see how much is the rate of success receiving, this is can verify whether the data is subject to interference of the disturbance nodes, if it is very small, shows that the sending node can not completely send data in the channel's idle time, therefore should increase the interval time of the interfering nodes for sending data, adjust aSlotTime and DIFS after the rate of success receiving at least reach to above 85%.

Through multiple testing and analysis in the different combinations of parameter aSlotTime and parameter DIFS, finally, parameter aSlotTime and parameter DIFS respectively set 300TICKS and 550TICKS.

References

- [1] Analog Devices, ADF7025 Datasheet.
- [2] T.R.Park, T.H.Kim, J.Y.Choi, S.Choi, W.H.Kwon. "Throughput and energy consumption analysis of IEEE 802.15.4 slotted CSMA/CA". *Electronics Letters* . 2005.
- [3] J.He, Z.Tang, H.-H.Chen, S.Wang. "An Accurate Markov Model for Slotted CSMA/CA Algorithm in IEEE 802.15.4 Networks". *IEEE Communications Letters* . 2008.
- [4] J.Misic, S.Shafi, V.B.Misic. "Performance of a beacon enabled 802.15.4 cluster with downlink & uplink traffic". *IEEE Trans. Parallel Distrib. Syst* . 2006.
- [5] Y.Zhang, P.Xu, Z.Zhang, G.Bi. "Comments on Throughput Analysis of IEEE 802.15.4 Slotted CSMA/CA Considering Timeout Period". *IEEE Electronics Letters*. 2006.
- [6] T.Park et al. "Throughput and energy consumption analysis of IEEE 802.15.4 slotted CSMA/CA". *Electronics Letters* . 2005.
- [7] J.Zheng, M.J. Lee. "Will IEEE 802.15.4 Make Ubiquitous Networking a Reality?: A Discussion on a Potential Low Power Low Bit Rate Standard". *IEEE Communications Magazine*.
- [8] Ramachandran et al. "Analysis of the contention access period of IEEE 802.15.4 MAC". *ACM Trans. Sensor Networks*. 2007.
- [9] T.Kim, S.Choi. Priority-based delay mitigation for event-monitoring IEEE 802.15.4 LR-WPANs. *IEEE Communications Letters*. 2005.