An Efficient and Secured Media Access Mechanism Using the Intelligent Coordinator in Low-Rate WPAN Environment*

Joon Heo[1] and Choong Seon Hong[2]

School of Electronics and Information, Kyung Hee University
1 Seocheon Giheung Yongin Gyeonggi 449-701 Korea
{heojoon,cshong}@khu.ac.kr

Abstract. The convenience of IEEE 802.15.4 (Low-rate Wireless Personal Area Network) based wireless access network will lead to widespread deployment in the evolutionary computing and adaptive systems. However, this use is predicated on an implicit assumption of confidentiality and availability. In this environment, malicious device may obtain an unfair share of the channel bandwidth. For example, IEEE 802.15.4 requires nodes competing for getting access to the channel to wait for a 'backoff' interval, randomly selected from a specified range, before initiating a transmission. Malicious devices may wait for smaller 'backoff' intervals than well-behaved devices, thereby obtaining an unfair advantage. Such misbehavior can seriously degrade the throughput of well-behaved devices. In this paper, we proposed an intelligent coordinator, a modification to IEEE 802.15.4 specification to simplify the prevention of such malicious devices. Proposed coordinator is able to ascertain whether to apply PTP (Priority Time Period). Simulation results indicate that our prevention mechanism is successful in handling MAC layer misbehavior. We plan to foster our solution in the evolutionary computing systems through further development.

1 Introduction

The growing importance of small and cheap wireless devices demands a common platform so that the device can communicate with each other. The IEEE 802.15.4 (Low-Rate WPAN) describes wireless and media access protocols for personal area networking devices. This standard specifies the physical (PHY) layer and Medium access control (MAC) sub-layer of a low cost, low power consumption and ad hoc wireless network. The MAC layer provides services that higher layers can use to access the physical radio. MAC layer protocols provide a means for reliable, single-hop communication links between devices [1][5][6]. This specification is meant to support a variety of applications, many of which are security sensitive. Wireless Medium Access Control (MAC) protocols such

* This work was supported by University ITRC Project of MIC. Dr. C.S.Hong is the corresponding author.

R. Khosla et al. (Eds.): KES 2005, LNAI 3682, pp. 470–476, 2005.

as IEEE 802.15.4 and IEEE 802.11 use distributed contention resolution mechanisms for sharing the wireless channel. The contention resolution is typically based on cooperative mechanisms (e.g., random backoff before transmission) that ensure a reasonably fair share of the channel for all the participating nodes. In this environment, some malicious devices in the network may misbehave by failing to adhere to the network protocols, with the intent of obtaining an unfair share of the channel. The presence of malicious devices that deviate from the contention resolution protocol can reduce the throughput share received by conforming devices. A misbehaving node may obtain more than its fair share of the bandwidth by

- Selecting backoff values from a different distribution with smaller average backoff value (e.g., by selecting backoff values from range $[0,\frac{CW}{4}]$ instead of $[0,\ CW]$, where $CW(ContentionWindow)$ is variable maintained by each node.
- Using a different retransmission strategy that does not double the CW value after collision.

Such malicious misbehavior can seriously degrade the throughput of well-behaved devices [2][3]. In this paper, we propose modification to IEEE 802.15.4, for simplifying the prevention of such misbehaving devices. This paper is organized as follows. Section 2 includes characters of IEEE 802.15.4 MAC specification for channel access. Section 3 describes the proposed mechanism for prevention against attacks. Also, we describe how to implement the proposed mechanism with the existing IEEE 802.15.4 protocol. We can use reserved bits in the frame without violating the IEEE 802.15.4 MAC frame format. This means the proposed mechanism does not modify the frame structure and is compatible with legacy devices. Performance results of proposed mechanism are presented in section 4. Finally, we give some concluding remarks.

2 Media Access of IEEE 802.15.4

In this section we explain some defined functions of IEEE 802.15.4 MAC specification for channel access. In this specification, the device uses CSMA-CA for resolving contention among multiple nodes accessing the channel. A device (sender) with data to transmit on the channel selects a random backoff value from range [0, 2^{BE}-1]. BE is the backoff exponent, which is related to how many backoff periods a device shall wait before attempting to assess a channel. Each time device wishes to transmit data frames during the CAP (Contention Access Period), it shall locate the boundary of the next backoff slot and then wait for a random number of backoff slots. If the channel is busy, following this random backoff, the device shall wait for another random number of backoff slots before trying to access the channel again. If the channel is idle, the device can transmit on the next available backoff slot boundary. Acknowledgment and beacon frames shall be sent without using a CSMA-CA mechanism [1]. Also, the MAC sub-layer needs a finite amount of time to process data received by the PHY. To allow

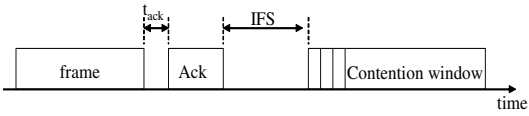


Fig. 1. Interframe Space

this, transmitted frames shall be followed by an IFS period; if the transmission requires an acknowledgment, the IFS shall follow the acknowledgment frame [1][8]. These concepts are illustrated in Figure 1. The IEEE 802.11 specification uses four different interframe spaces. Varying interframe spacings create different priority levels for different type of traffic. The logic behind this is simple: high-priority traffic doesn't have to wait as long after the medium has become idle. Therefore, if there is any high-priority traffic waiting, it grabs the network before low-priority frames have a chance to try. To assist with interoperability between different data rates, the interframe space is a fixed amount of time, independent of the transmission speed [8][9].

3 Media Access Mechanism Using Priority Time Period

The proposed mechanism is designed to require minimal modifications to IEEE 802.15.4 MAC specification. As mentioned above, a malicious device selects backoff values from a different distribution with smaller average backoff value, than the distribution specified by standard (e.g., by selecting backoff values from [0, $\frac{2^{BE}-1}{3}$], instead of [0, 2^{BE}-1]). Such misbehavior of malicious device can seriously degrade the performance of well-behaved devices. Also well-behaved devices should consume the energy to acquire channel. The proposed mechanism is designed to prevent misbehavior of malicious device using the PTP (Priority Time Period) which is decided by coordinator. If well-behaved device repeatedly can't access the channel, device uses the PTP to transmit the frame; this frame should be authenticated by coordinator. The start of PTP (Priority Time Period) can locate in IFS (Interframe Space) as shown in Figure 2. The $time_{start}$ is the time to start PTP after acknowledgment frame and the *length* is the maintenance duration of PTP; both $time_{start}$ and *length* are decided by coordinator. The coordinator transmits these values to well-behaved devices using the encryption algorithm to protect these values. Key management between coordinator and devices may be provided by the higher layer, but are out of scope of this paper. Generally well-behaved device uses the CSMA-CA algorithm to acquire the channel. If the value of NB is more than 3, the device can use the PTP. In IEEE 802.15.4 specification, NB is the number of times the CSMA-CA algorithm was required to backoff while attempting the current transmission; this value shall be initialized to 0 before each new transmission attempt and the maximum value is 6. At first, the coordinator decides whether apply the PTP as shown in Figure 3. Priority Time Period is 1 bit in length and shall be set to 1 if coordinator applys the PTP. Otherwise, Priority Time Period subfield shall be set to 0.

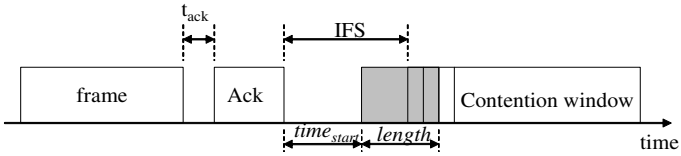


Fig. 2. Proposed Priority Time Period

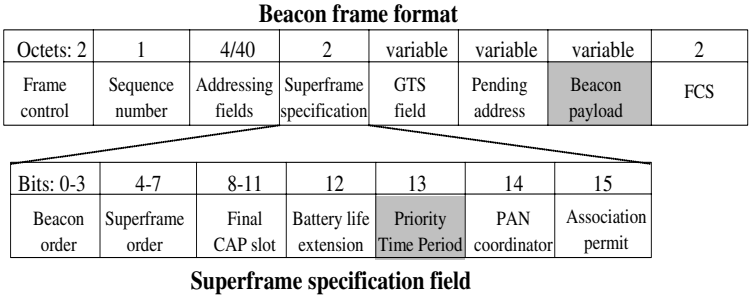


Fig. 3. Beacon frame format for PTP

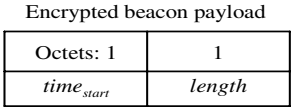


Fig. 4. Encrypted information to use PTP

As shown in Figure 4, The accurate information to use PTP (the $time_{start}$ and the $length$) are encrypted by shared key between coordinator and well-behaved devices. These values are included in beacon payload field.

- encrypted beacon payload: $E_{key}\{time_{start}\ ,length\}$

A malicious device can't know these values, because it has not shared key. Beacon enabled network use a slotted CSMA-CA channel access mechanism, where the backoff slots are aligned with the start of the beacon transmission. Each time a device wishes to transmit data frames during the CAP, it shall locate the boundary of the next backoff slot and then wait for a random number of backoff slots. If the channel is busy, following this random backoff, the device shall wait for another number of backoff slots before trying to access the channel again. If the value of NB is more than to 3, the device can use the PTP. As mentioned above, NB is the number of times the CSMA-CA algorithm was required to backoff while attempting the current transmission. Also, the device includes hash value for authentication as shown in Figure 5. The coordinator can authenticate using this hash value whether the device is well-behaved or not. If malicious

Format of the frame control field

Bits: 0-2	3	4	5	6	7-9	10-11	12-13	14-15
Frame type	Security enable	Frame pending	Ack. request	Intra-PAN	Reserved	Dest. Addressing mode	Reserved	Source Addressing mode

$Hash_{key}\{time_{start}\}$

Fig. 5. Hash value for authentication

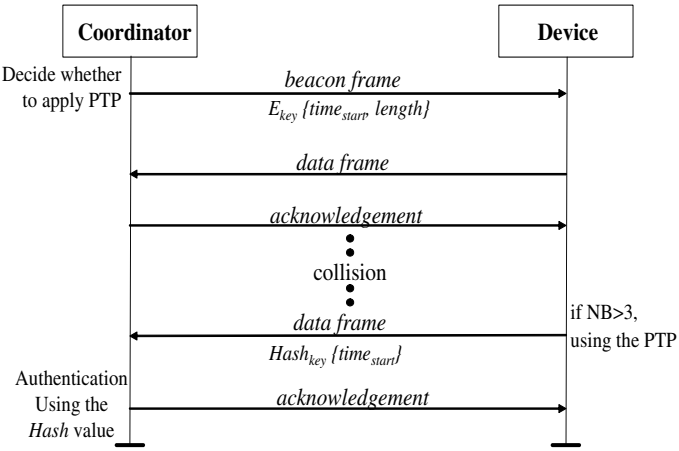


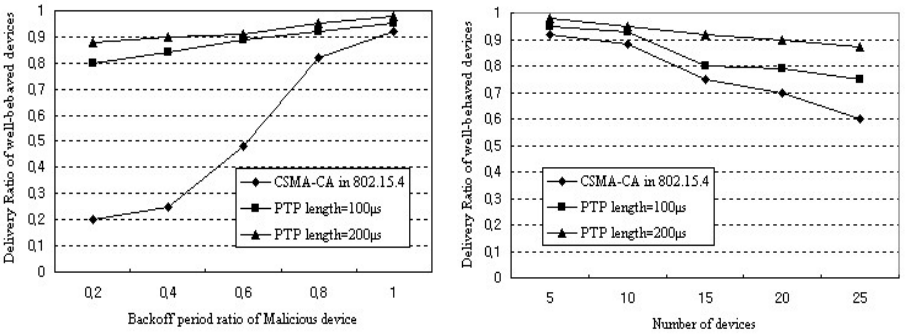
Fig. 6. Process for channel acquirement

device is detected, the coordinator can disconnect with that device. Figure 6 shows an entire process between coordinator and device.

4 Performance Analysis

In this section, simulation results are presented to demonstrate the effectiveness of the proposed mechanism. The performance metrics we use include 'Delivery Ratio of data frames of well-behaved devices', which is the ratio of well-behaved device's frame throughput over their sending rate. All the simulation results are based on a modified version of ns-2 network simulator. The traffic sources are chosen to be constant bit rate (CBR) source using packet-size of 20 bytes. Figure 7(a) shows the delivery ratio of well-behaved devices depending on the backoff range ratio of malicious device (for example, if malicious device select backoff value from $[0, \frac{2^{BE}-1}{4}]$, backoff range ratio is 0.25).

Also, Figure 7(b) shows the delivery ratio of well-behaved devices depending on the number of devices. The simulation results demonstrate that severe contention among frames of devices will cause significant performance degradation without PTP (Priority Time Period).



(a) Delivery ratio vs. backoff period ratio of malicious device

(b) Delivery ratio vs. number of devices

Fig. 7. Delivery Ratio Performance Comparison

5 Conclusion and Future Works

Preventing MAC layer misbehavior is an important requirement in ensuring a reasonable throughput share for well-behaved nodes in the presence of misbehaving devices. In this paper, we have presented modification of IEEE 802.15.4 MAC protocol to use PTP. Also, we have described how to implement the proposed mechanism with the existing IEEE 802.15.4 protocol. We can use reserved bits in the frame without violating the IEEE 802.15.4 MAC frame format. Simulation results indicate that our prevention mechanism is successful in handling MAC layer misbehavior. We plan to foster our solution in the evolutionary computing systems through further development.

References

1. IEEE Standard for Wireless Medium Access Control and Physical Layer Specification for Low-Rate Wireless Personal Area Networks, P802.15.4, 2003.
2. Pradeep Kyasanur, Nitin H. Vaidya, "Detection and handling of MAC layer misbehavior in wireless networks", Dependable Systems and Networks 2003, pp.173 - 182, June 2003.
3. V. Gupta, S. Krishnamurthy, M. Faloutsos, "Denial of service attacks at the MAC layer in wireless ad hoc networks", MILCOM 2002 Proceedings, pp.1118 - 1123, vol.2, Oct 2002.
4. G. Noubir, G. Lin, "Low-Power DoS Attacks in Data Wireless LANs and Countermeasures", ACM MobiHoc, Poster Session, 2003.
5. TS Messerges, J Cukier, et al, "A security design for a general purpose, self-organizing, multihop ad hoc wireless network", Proceedings of the 1st ACM workshop Security of Ad Hoc and Sensor Network, 2003.
6. N. Sastry, D. Wagner, "Security Consideration for IEEE 802.15.4 Networks", WiSe'04 Proceeding, pp.32-42, 2004.
7. Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, Lixia Zhang, "Security in Mobile Ad Hoc Networks: Challenges and solutions", Wireless Communications, Volume 11, Issue: 1, pp 38-47, Feb 2004.

8. Imad Aad, Claude Castelluccia, "Differentiation mechanisms for IEEE 802.11", IEEE INFOCOM, April 2001.
9. Michael Barry, Andrew T. Campbell, Andras Veres, "Distributed Control Algorithms for Service Differentiation in Wireless Packet Networks", IEEE INFOCOM, April 2001.
10. V. Kanodia, C. Li, A. Sabharwal, B. Sadeghi, E. Knightly, "Distributed Multi-Hop Scheduling and Medium Access with Delay and Throughput Constraints", MOBICOM, August 2001.