An Identity Authentication Protocol for Acknowledgment in IEEE 802.15.4 Network

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

School of Electronics and Information, Kyung Hee University
1 Seocheon, Giheung, Yongin, Gyeonggi, 449-701 KOREA
heojoon@khu.ac.kr[1] ,*cshong@khu.ac.kr*[2]

.

Abstract. This paper proposes an identity authentication mechanism at the link layer for acknowledgment frame in IEEE 802.15.4 network. With the proposed mechanism there are only three bits for authentication, which can greatly reduce overhead. The encrypted bit stream for identity authentication will be transmitted to device by coordinator within association process. Statistical method indicates that our mechanism is successful in handling MAC layer attack.

1 Introduction

The IEEE 802.15.4 specification defines four frame types: beacon frames, data frames, acknowledgment frames, and control frames for the media access control layer. The specification does not support security for acknowledgment frames; other frame types can optionally support integrity protection and confidentiality protection for the frame's data field.The lack of a MAC covering acknowledgments allows an adversary to forge an acknowledgment for any frame. An adversary need only create the forged acknowledgment with the appropriate sequence number from the original frame; this is not hard, since this sequence number is sent in the clear[1][2]. In this paper, we propose a lightweight identity authentication at the link layer for acknowledgment frame in IEEE 802.15.4 network. With the proposed mechanism there are only three bits for authentication, which can greatly reduce overhead. Also encrypted n-bits stream for identity authentication will be transmitted by coordinator within association process.

2 Proposed Mechanism

Unlike traditional authentication mechanism, the proposed mechanism determines the legitimacy of a sender by continuously checking a series of acknowledgment frames transmitted by the sender. Ideally, since the attacker does not have the shared key, the probability for the attacker to guess continuously k times of three bits is as small as 8^{-k}.

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

2.1 *Authbit set* and *Set number* of Acknowledgments

If the coordinator determines acceptance of device, encrypted n-bits *Authbit* stream will be transmitted to device by coordinator within association process. Key management between coordinator and devices may be provided by higher layer, but are out of scope of this paper. And then, the coordinator and the device create *Authbit sets* and *Set numbers* as shown in Figure 1. Finally, the *Authbit set* and the *Set number* will be used making the same chain for authentication of acknowledgment between the coordinator and the device as shown in Figure 2.

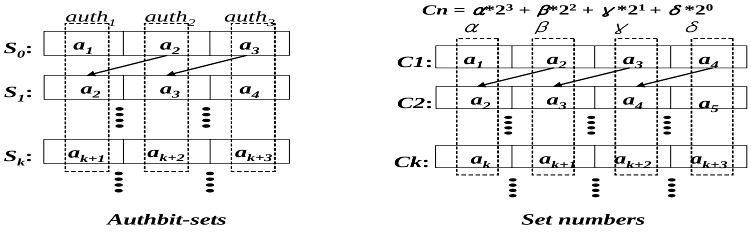


Fig.1. *Authbit sets* and *Set numbers* generation mechanism

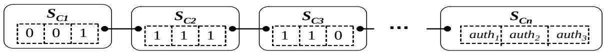
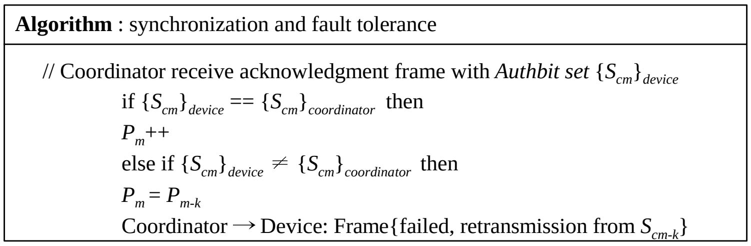


Fig.2. The authentication chain of *Authbit sets*

2.2 Synchronization and Fault tolerance using the *Set pointer*

Conceptually, both the coordinator and the device have a pointer pointing to the *Authbit set* for the next outgoing acknowledgment frame. Ideally, both the coordinator and the device will have their pointer pointing at exactly the same *Authbit set* and advance synchronously. Initially, the coordinator and the device pointers are synchronized. The device sends each acknowledgment frame with three additional bits and bits value is equal to the values of the *Set pointer* (P_n). When the coordinator receives a frame successfully, the coordinator checks the bits value of the acknowledgment frame. The synchronization and fault tolerance of *Set pointer* explained above can partially be described with the following Figure 3.



```
Algorithm : synchronization and fault tolerance

// Coordinator receive acknowledgment frame with Authbit set $\{S_{cm}\}_{device}$
        if $\{S_{cm}\}_{device} == \{S_{cm}\}_{coordinator}$ then
        $P_m$++
        else if $\{S_{cm}\}_{device} \neq \{S_{cm}\}_{coordinator}$ then
        $P_m = P_{m-k}$
        Coordinator → Device: Frame{failed, retransmission from $S_{cm-k}$}
```

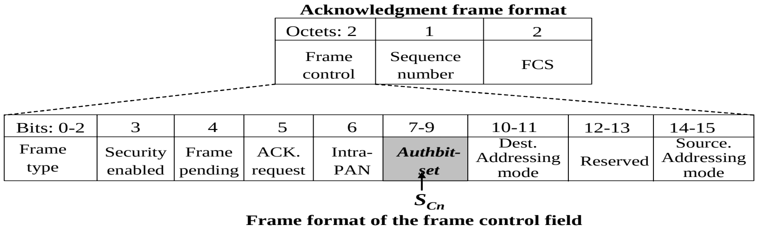
Fig.3. Pseudo code of synchronization algorithm

3 Statistical method and Implementation in LR-WPAN

The main objective of this authentication mechanism is to determine whether the sending device is an attacker or not. We have analyzed the proposed authentication mechanism and have devised a method to find out the authenticity of a device as a probability value. If the device's *Authbit set* doesn't match the coordinator's *Authbit set*, this means there are two possibilities either (a) there are no synchronization between the coordinator and the device *Set pointer* or (b) the sending device is an illegitimate device. In an error-prone wireless network, acknowledgment frames are 'frequently' lost due to wireless error. We use a statistical method to determine the authenticity of a device. We devise a statistical method to determine the probability of a station being an attacker. Let the number of acknowledgment frames from P_1 to P_n be n, let the number of synchronization done by device and coordinator be s, and let the acknowledgment frame loss rate be r, where r ($0 \leq r \leq 1$). We have the following theorem[3][4].
[Theorem]
For a sending device D, assume the a priori probability of device D to be an attacker is $\frac{1}{8}$, i.e., P(D=*attacker*) = $\frac{1}{8}$ and P(D=*legitimate*) = $\frac{7}{8}$, the probability of this device D being an attacker one when the number of synchronization is s, P(D=*attacker* | n, s), is given by

$$P(D = attacker|n, s) = \frac{2^{-n}}{2^{-n} + 7 * r^s(1 - r)^{n-s}} \tag{1}$$

Also, we describe how to implement the proposed mechanism with the existing IEEE 802.15.4 protocol. Although an extra bit is needed in our proposed mechanism, 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 which do not use the authentication mechanism. Figure 4 shows the common acknowledgment frame and frame control field of IEEE 802.15.4 protocol. We have used three bits reserved field of frame control field to authenticate of acknowledgment frame between coordinator and device. Figure 5 shows a frame sequence chart between coordinator and device by using the *Authbit set* chain to authenticate each other.



Acknowledgment frame format

Octets: 2	1	2
Frame control	Sequence number	FCS

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

Frame format of the frame control field

Fig.4. Frame format in the IEEE 802.15.4 Standard

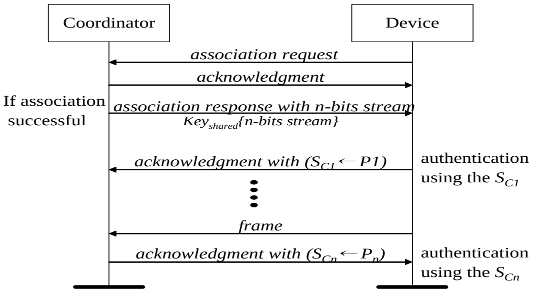

Coordinator
Device
association request
acknowledgment
If association successful
association response with n-bits stream
Key_{shared}\{n-bits stream\}
acknowledgment with ($S_{C1} \leftarrow P1$)
authentication using the S_{C1}
frame
acknowledgment with ($S_{Cn} \leftarrow P_n$)
authentication using the S_{Cn}

Fig.5. Frame sequence chart with *Authbit set* chain

4 Conclusion

In this paper, a lightweight identity authentication protocol for acknowledgment frame in IEEE 802.15.4 network has been presented. The proposed mechanism inserts identity authentication bits from an acknowledgment frame known only to the two communicating stations. With the proposed mechanism there are only three bits for identity authentication, which can greatly reduce overhead and thus preserves the scarce wireless bandwidth resource.

References

1. "Wireless Medium Access Control and Physical Layer Specification for Low-Rate Wireless Personal Area Networks", IEEE Standard, 802.15.4-2003, May 2003.
2. N. Sastry, D. Wagner, "Security Consideration for IEEE 802.15.4 Networks", WiSe'04, Proceeding, pp.32-42, 2004.
3. Henric Johnson, Arne Nilsson, Judy Fu, S.Felix Wu, Albert Chen and He Huang, "SOLA: A One-bit Identity Authentication Protocol for Access Control in IEEE 802.11", In Proceedings of IEEE GLOBECOM 2002.
4. Haoli Wang, Aravind Velayuthan, Yong Guan, "A Lightweight Authentication Protocol for Access Control in IEEE 802.11", In Proceedings of IEEE GLOBECOM 2003.