A Lightweight Authentication Mechanism for Acknowledgment in LR-WPAN Environment

Joon Heo*, Choong Seon Hong*, Sang-Hyun Choi**
*Dept. of Electronics and Information, Kyung Hee University
**National Computerization Agency
e-mail : heojoon@khu.ac.kr, cshong@khu.ac.kr, csh@nca.or.kr

Abstract

In IEEE 802.15.4 (Low-Rate Wireless Personal Area Network) specification, a successful reception and validation of a data or MAC command frame can be confirmed with an acknowledgment. However, the specification does not support security for acknowledgment frame; the lack of a MAC covering acknowledgments allows an adversary to forge an acknowledgment for any frame. 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 is 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 (LR-WPAN) describes wireless and media access protocols for personal area networking devices. This standard specifies the physical (PHY) layer and Medium access control (MAC) sublayer of low cost, low power consumption and ad hoc wireless networks. The convenience of this specification based wireless access network will lead to wide-spread deployment in the evolutionary computing and mobility aware system. However, this use is predicated on an implicit assumption of confidentiality and availability [1][6]. 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 [1][2]. In this paper, we propose a lightweight identity authentication at the link layer for acknowledgment frame in IEEE 802.15.4 network. 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. With the proposed mechanism there is only three bits for authentication, which can greatly reduce overhead. Also encrypted bit stream for identity authentication will be transmitted by coordinator within association process. The major purpose of the proposed mechanism is to detect an attack in an error-prone wireless environment. When the coordinator detects an attack, some protection or anti-attack approaches for each type attack can be triggered. The goals of our lightweight authentication mechanism are the following [8][9]:

This work was supported by ITRC of MIC and by NCA

· ***Secure and Useful***: an attacker should with low probability be able to gain access to the network.

· ***Cheap***: by presenting an optimized *n*-bits identity authentication method for resource-constrained environments like wireless sensor networks, a cheap and efficient access control procedure is obtained.

· ***Robust***: due to loss channels in wireless communications a synchronization algorithm is required for the generated random authentication stream in the sink and the sensor node.

The proposed mechanism identifies the attack by using a statistical way and provides access control. This paper is organized as follows. Section 2 includes using the acknowledgment in LR-WPAN and association process between coordinator and device. Section 3 describes the proposed mechanism for identity authentication. Section 4 provides the statistical method and discusses the implementation in LR-WPAN. Finally, we give some concluding remarks.

2. Relates Works

2.1 Using the Acknowledgment and Weakness

In IEEE 802.15.4 specification, a successful reception and validation of a data or MAC command frame can be optionally confirmed with an acknowledgment. If the sender does not receive an acknowledgment after some period, it assumes that the transmission was unsuccessful and retries the frame transmission. If an acknowledgment is still not received after several retries, the sender can choose either to terminate the transaction or to try again [1][6]. The acknowledgment frame is sent by the receiver only if the corresponding data frame was not sent to a broadcast address and the sender requested an acknowledgment. Its format is simple: a 2 byte frame control field, the 1 byte sequence

number from the frame that it is acknowledging, and a 2 byte CRC. However, the IEEE 802.15.4 specification does not include any integrity or confidentiality protection for acknowledgment frames. 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. This weakness can be combined with targeted jamming to prevent delivery of selected frames [1][2].

2.2 Association Process in IEEE 802.15.4 Network

In IEEE 802.15.4 specification, all devices shall provide the function for the request and response association commands. If the device wishes to associate with a coordinator, the device generates an association request command and sends it to the coordinator with the specified PAN (Personal Area Network) identifier and address. If the device successfully transmits an association request command, the device will expect an acknowledgment in return. If this does not occur, the association request command frame will be retried. When the coordinator receives the association request command, the coordinator determines whether to accept or reject the unassociated device using an algorithm outside the scope of this paper. And then the coordinator generates an association response command; the command is sent to the device requesting association [1].

2.3 Security-Related Properties in WSNs

WSNs share several important properties with traditional wireless networks, most notably with mobile ad hoc networks. Both types of networks rely on wireless communication, ad hoc network deployment and setup, and constant changes in the network topology. Many security solutions proposed for wireless networks can be applied in WSNs; however, several unique characteristics of WSNs require new security mechanism. In this section two characteristics specific to WSNs are discussed [7].

· ***Limited resources***: Sensor network nodes are designed to be compact and therefore are limited by size, energy, computational power, and storage. The limited resources limit the types of security algorithms and protocols that can be implemented. Security solutions for WSNs operate in a solution space defined by the trade-off between resource spent on security and the achieved protection.

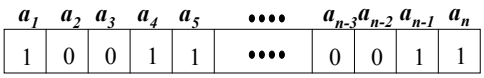
· ***In-network processing***: Communication between the nodes in a WSN consumes most of the available energy, much less than sensing and computation do. For that reason, WSNs perform localized processing and data aggregation. An optimal security architecture for this type of communication is one in which a group key is shared among the nodes in an immediate neighborhood. However, in an environment in which the nodes can be captured, the confidentiality offered by the shared symmetric keys is easily compromised.

3. Proposed Mechanism

The proposed security mechanism is designed to provide a lightweight identity authentication at the link layer for acknowledgment frame in IEEE 802.15.4 network. 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}. With the proposed mechanism there is only three bits for identity authentication, which can greatly reduce overhead and thus preserves the scarce wireless bandwidth resource.

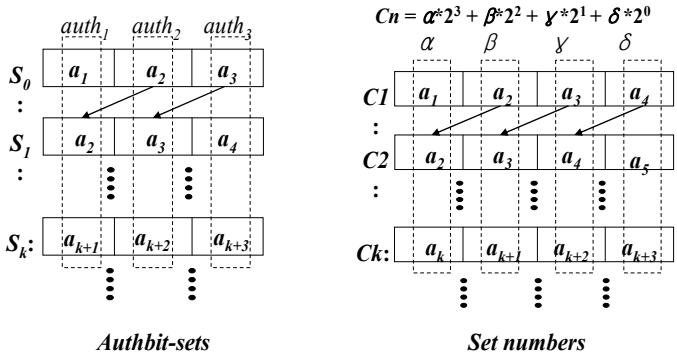
3.1 *Authbit set* and *Set number* of Acknowledgments

If the coordinator determines acceptance of device, encrypted n-bits *Authbit* stream (as shown in Figure 1) will be transmitted to device by coordinator within association process.



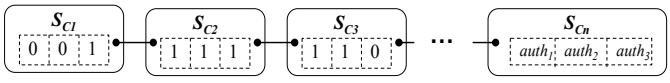
(Figure 1) n-bits *Authbit* stream

And then, the coordinator and the device create *Authbit sets* and *Set numbers* as shown in Figure 2. For example, if the coordinator and the device use the *Authbit* stream of Fiture 1, S_0={1,0,0}, S_1={0,0,1} and S_2={0,1,1}. Also, $C1=a_1*2^3+a_2*2^2+a_3*2^1+a_4*2^0=9$ and $C2=3$.



(Figure 2) *Authbit sets* and *Set numbers* generation mechanism

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 3.



(Figure 3) The authentication chain of *Authbit sets*

3.2 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 (Pn)*. 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 4 and Figure 5.

Algorithm : synchronization and fault tolerance

// Coordinator receive acknowledgment frame with *Authbit set* $\{S_{cm}\}_{device}$

if $\{S_{cm}\}_{device} == \{S_{cm}\}_{coordinator}$ then

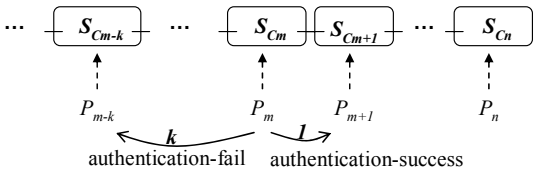
P_m++

else if $\{S_{cm}\}_{device} \neq \{S_{cm}\}_{coordinator}$ then

$P_m = P_{m-k}$

Coordinator → Device: Frame{failed, retransmission from S_{cm-k}}

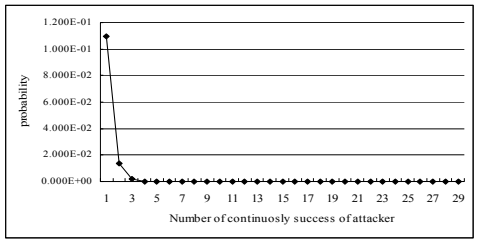
(Figure 4) Pseudo code of synchronization algorithm



(Figure 5) Synchronization and fault tolerance using the *Set pointer* (P_n)

4. 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. First let us assume that the sender is an attack i.e. it does not know the *Authbit set* chain. According to Geometric Random Variable, the probability of continuously success of attacks can be given as shown Figure 6.



$$P_X(n) = \begin{cases} p(1-p)^{n-1} & n=1,2,... \\ 0 & otherwise \end{cases}$$

Where the parameter n is the number of continuously success of attacker and the parameter p is 7/8

(Figure 6) Probability of continuously success of attacks

Also if the device's *Authbit set* doesn't match the coordinator's *Authbit set*, this means there are two possibilities either (a) there is 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 know that in a perfect channel, where there are no losses, a legitimate device will not have any synchronization with its receiver. However, in an error-prone wireless network, a receiver station cannot differentiate between non-synchronization due to attacker and non-synchronization due to wireless losses. Hence, 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 $(0 \le r \le 1)$. We have the following theorem.

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, $P(D=attacker \mid n, s)$, is given by

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

Proof

We know $P(D=legitimate \mid n, s) = 1 - P(D=attacker \mid n, s)$. According to Bayer's Formula, we have

$$P(D=attacker \mid n, s) = \frac{P(n,s|D=attacker)*P(D=attacker)}{P(n,s|D=attacker)*P(D=attacker)+P(n,s|D=legitimate)*P(D=legitimate)}$$

$$= \frac{P(n,s|D=attacker)}{P(n,s|D=attacker)+7*P(n,s|D=legitimate)} .(2)$$

First let us assume that the sending device is an attacker; also it does not know the authentication chain of *Authbit sets*. In this case, the probability of $P(n, s \mid D=attacker)$ can be given as follows:

$$P(n, s \mid D=attacker) = \binom{n}{s} * 2^{-n} .(3)$$

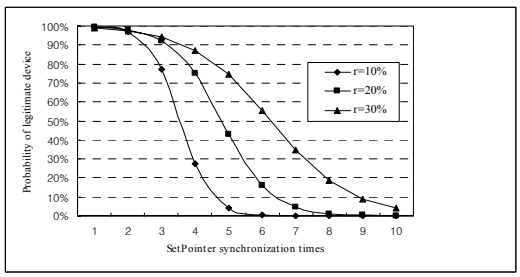
Now let us consider the case where the sending device is a legitimate device. We have the Probability of the number of synchronization s where the acknowledgment frame loss rate is r :

$$P(n, s \mid D=legitimate) = \binom{n}{s} * r^s (1-r)^{n-s} .(4)$$

Combing (2), (3) and (4), it is easy to derive (1), i.e.,

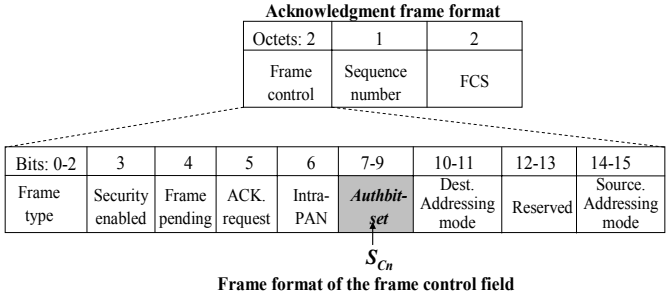
$$P\,(D=attacker \mid n, s) = \frac{2^{-n}}{2^{-n} + 7 * r^{s}(1-r)^{n-s}}$$

Figure 7 shows the probability of a sending device being a legitimate one. We have n=10. The analysis is for r=10%, 20% and 30%.

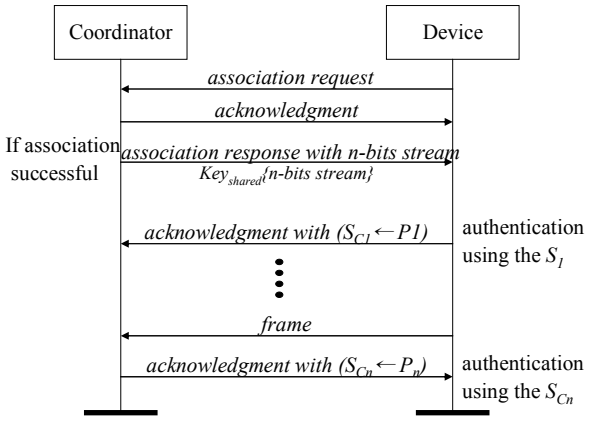


(Figure 7) Probability of legitimate sender

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 8 shows the common acknowledgment frame and frame control field of IEEE 802.15.4 protocol.



(Figure 8) Frame format in the IEEE 802.15.4 Standard



(Figure 9) Frame sequence chart with *Authbit set* chain

We have used three bits reserved field of frame control field to authenticate of acknowledgment frame between coordinator and device. Figure 9 shows a frame sequence chart between coordinator and device by using the *Authbit set* chain to authenticate each other.

5. 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 is only three bits for identity authentication, which can greatly reduce overhead and thus preserves the scarce wireless bandwidth resource. The major purpose of the proposed mechanism is to detect an attack in an error-prone wireless environment. When the coordinator detects an attack, some protection or anti-attack approaches for each type attack can be triggered. We plan to foster our solution in the evolutionary computing systems through further development.

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.

[5] Fan Zhao, Yongjoo Shin, S. Felix Wu, Henric Johnson, Arne Nilsson, "RBWA: An Efficient Random-Bit Window-based Authentication Protocol", In Proceedings of IEEE GLOBECOM 2003.

[6] Jose A. Gutierrez, Edgar H. Callaway Jr, Raymond L. Barrett Jr, "Low-Rate Wireless Personal Area Networks", IEEE Std 802.15.4.

[7] Mohammad Ilyas, Imad Mahgoub, "Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems" CRC PRESS, 2004.

[8] A. Menezes, P. Oorschot, S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1997.

[9] A. Perrig, R. Szewczyk, V. Wen, D. Culler, D. Tygar, "SPINS: Security Protocols for Sensor Networks", ACM MobiCom, pp. 189-199, July 2001.

[10] A. Perrig, J.D. Tygar, "Secure Broadcast Communication in Wired and Wireless Networks", Kluwer Academic Publisher, 2003.

[11] S. Capkun, L. Buttyan, J.P. Hubaux, "Self-Organized Public Key Management for Mobile Ad hoc Networks", MobiHoc 2002.