Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/090457

Practical Techniques for ACK Authentication in IEEE 802.15.4 Networks

Eun-Kyung Ryu and Kee-Young Yoo**

The School of Computer Science and Engineering, Kyungpook National University, Daegu 702-701, South Korea

Received: 26 Nov. 2014, Revised: 26 Feb. 2015, Accepted: 28 Feb. 2015
Published online: 1 Jul. 2015

Abstract: A secure acknowledgement (ACK) mechanism is essential to ensure reliable data transfer in wireless communication networks. However, because efficiency is the highest priority for resource-constrained settings, existing wireless security protocols tend to exclude integrity or confidentiality protection for ACK messages. This limits the use of ACK mechanisms for reliable communication. In this paper we describe our schemes for supporting ACK authentication in 802.15.4 networks. Our schemes do not require a pre-setup phase for the sharing of additional secrets and introduce no additional computation or communication overhead. They are practical for use and directly applicable to the 802.15.4 standard.

Keywords: IEEE 802.15.4, LR-WPAN, security, ACK authentication.

1 Introduction

The IEEE 802.15.4 standard [1] includes various security suites for supporting security services on incoming and outgoing packets over low-rate wireless personal area networks (LR-WPANs). These security suites can be classified into three categories based on the type of security properties of transmitted data: AES-CTR, AES-CBC-MAC, and AES-CCM. AES-CTR is for data protection, AES-CBC-MAC for data integrity, and AES-CCM for both data protection and integrity [2,3].

The 802.15.4 specification, however, does not include integrity or confidentiality protection for ACK packets. This allows an eavesdropper to forge an ACK for any packet. To forge an ACK for a given data packet, the attacker only needs to know the appropriate sequence number of the packet in the transmitted data. This is not difficult since the sequence number is sent in the clear. Furthermore, the problem of a forged ACK can worsen if it is combined with radio interference or jamming, which prevents delivery of selected packets [4]. These limit the use of ACK message as a means to ensure reliable data transfer over a wireless communication medium.

A common solution to address such problems is to append a message authentication code (MAC) to the end of each ACK message [5]. The fact, however, that the long ACK message runs down the power of network devices overwhelmingly faster makes it impractical to use existing secure MAC algorithms in highly resource-constrained settings. Devices that use the 802.15.4 standard employ low-power, low-data-rate, and low-complexity short-range radio frequency transmissions. In particular, low-energy consumption is a major design requirement, due to the nature of battery-operated devices [6]. Therefore, we require a new mechanism for ACK authentication that minimizes security overhead and simultaneously supports a reasonable security level.

This study introduces practical techniques for supporting ACK authentication in 802.15.4 LR-WPAN settings. Notable features of our techniques are described as follows. They support all required security properties, including data confidentiality, data authenticity, replay protection, and ACK integrity. They do not require a pre-setup phase for sharing additional secrets necessary for the ACK authentication, thus resulting in greater efficiency and ease of implementation. These techniques introduce practically no additional computation or communication overhead on resource-constrained devices. Hence, they are practical, and directly applicable to the 802.15.4 standard.

The remainder of this paper is structured as follows. In Section 2, we briefly review the 802.15.4 network and its security services relevant to our work. In Section 3, we

* Corresponding author e-mail: ekryu@knu.ac.kr, yook@knu.ac.kr

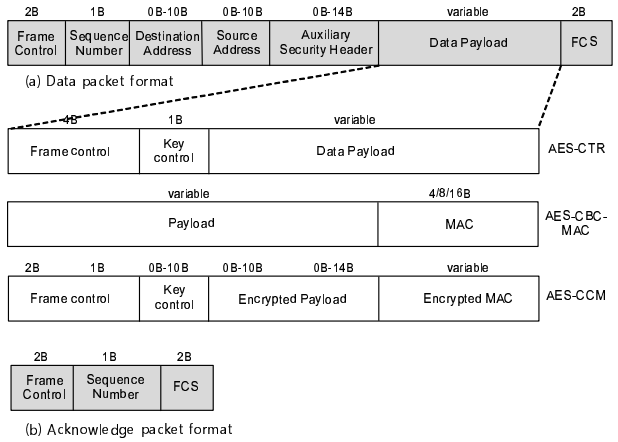

Fig. 1: Data and acknowledgement packet format

describe our solutions for supporting ACK authentication, which enable senders to confirm ACK integrity and authenticate the source of each ACK message. In Section 4, we analyze the security and efficiency of our constructions. In addition, we discuss the advantages of our schemes compared to those discussed in previous works. We conclude in Section 5.

2 IEEE 802.15.4 and its security services

An 802.15.4 LR-WPAN consists of two device types: a full-function device (FFD) and a reduced-function device (RFD). An FFD is a device that is able to act as a personal area network (PAN) coordinator. By contrast, an RFD, which is intended for applications that are extremely simple, such as a light switch or passive infrared sensor, is unable to act as a coordinator. An FFD can communicate with RFDs or other FFDs, whereas an RFD can communicate with only a single FFD at a time. The 802.15.4 networks work in either of two topologies: the star topology or the peer-to-peer topology. In a star topology, communication occurs only between devices and a single PAN coordinator, which manages the entire PAN. A peer-to-peer topology also has a PAN coordinator, but it differs from the star topology in that any of devices within a common communication range can arbitrarily communicate with one another.

From a security perspective, the networks are similar to any other wireless network in which the use of wireless links increases their vulnerability to various types of attack from passive eavesdropping to active interference. The 802.15.4 standard considers the following security services: data confidentiality, data authenticity, and replay protection. The security mechanism used in this standard is based on symmetric-key cryptography and uses keys that are provided by higher layer processes. Fig. 1 shows two important packet types, data and acknowledgment packets. Depending on application requirements, the payload of the data packet can have different security suites, AES-CTR, AES-CBC-MAC, or AES-CCM. The AES-CTR suite provides data confidentiality only using the AES block cipher [8]. The AES-CTR suite, however, is susceptible to denial-of-service attacks, as discussed in [4]. The AES-CBC-MAC suite provides data authenticity only using CBC-MAC [7], in which the MAC can have different sizes: 32, 64, and 128 bits. The AES-CCM provides both data confidentiality and authenticity using CBC-MAC and AES-CTR, and has the three MAC options of 32, 64, and 128 bits. Note that for acknowledgment packets, the 802.15.4 specification does not include any integrity or confidentiality protection. A one-byte length of a sequence number serves to identify the packet number for acknowledgments.

3 ACK Message Authentication

In this section, we introduce our constructions for supporting ACK message authentication. Our constructions employ a classical challenge-response mechanism. However, it is used in a practical manner for highly resource-constrained settings of a network.

Our design goal is to support all required security properties including data protection, data integrity, replay protection, and ACK integrity with the following features: low computation and communication overhead for generation and verification of authentication information, and direct application to the 802.15.4 standard. To achieve this goal we limit the choice of underlying cryptographic primitives to symmetric-key algorithms and use keys that are provided by higher layer process, as those in the standard.

3.1 The Scheme I: Using MAC Verifier

We assume that each pair of devices is associated with a unique n-bit secret key K_i. We also assume that a pair of keys for encrypting and signing (K_i^{enc}, K_i^{mac}) is derived from the key K_i in a predetermined manner. Table 1 lists the notations used throughout this paper to describe our scheme.

The scheme is comprised of three procedures, as indicated in Algorithm 1. These include message sending,

Table 1: Notations

Notation	Meaning
S, R	Sender and receiver
SID, RID	Identifiers of sender and receiver
SN	Sequence number
K_i^{enc}, K_i^{mac}	Secret keys for symmetric cryptosystems
$\{m\}_{K_i^{enc}}$	Symmetric encryption of "m" with the key K_i^{enc}
$\langle x,y \rangle$	Concatenation of x and y

ACK response, and verification. In message sending, a sender encrypts a message for a receiver and constructs an n-bit length of MAC over the contents of the header and message. The sender then sends the encrypted message and MAC value. The first $n-l$ bits of the MAC are used to validate the message that is sent, while the last l bits are used for ACK authentication. In the ACK response, the receiver confirms the received MAC value. If the MAC is correct, the receiver accepts it and replies with the corresponding last l bits of the MAC as an ACK response. In verification, the sender verifies whether the ACK message is from the intended receiver or not by comparing it with the stored MAC value. If the ACK message is correct, the sender is convinced that the transmission has been successfully completed. More details are given as follows.

1) Message sending: When a sender S sends a message m to a receiver R, the sender performs the followings: *i*) Encrypt the message m using the encryption key K_S^{enc} to obtain encrypted message $\{m\}_{K_S^{enc}}$. *ii*) Compute the MAC value of the header and encrypted message in the key K_S^{mac} as follows: MAC $=$ $\mathsf{MAC}_{K_S^{mac}}(SID, RID, SN, \{m\}_{K_S^{enc}})$. Then, split it into two parts: $\langle v_c, v_r\rangle \leftarrow$ MAC, where v_c and v_r denotes the first $n-l$ bits and the last l bits of MAC, respectively. *iii*) Send $\langle SID, RID, SN, \{m\}_{K_S^{enc}}, v_c\rangle$ to R.

2) ACK Response: Upon receiving $\langle SID, RID, SN, \{m\}_{K_S^{enc}}, v_c\rangle$ from sender S, receiver R verifies it, and then replies with an authenticated ACK message by performing the followings: *i*) Compute MAC$'$ $=$ $\mathsf{MAC}_{K_R^{mac}}(SID, RID, SN, \{m\}_{K_S^{enc}})$ in the key K_R^{mac}. Then, split the MAC value into two parts, $\langle v_c', v_r'\rangle \leftarrow$ MAC$'$, in the same manner as S. *ii*) If v_c' matches the received value v_c, then accept the message. Otherwise, it is rejected. *iii*) Reply with the value v_r' as an ACK message.

3) Verification: Sender S accepts the ACK message, if and only if $v_r' = v_r$. Otherwise, S discards it.

Algorithm 1 Using MAC Verifier

procedure SENDER_MESSAGE_TRANSMITTING
  local input: $SID, RID, K_S^{enc}, K_S^{mac}$
  choose SN
  $c \leftarrow E_{K_S^{enc}}(m)$
  $\langle v_c, v_r\rangle \leftarrow \mathsf{MAC}_{K_S^{mac}}(SID, RID, SN, c)$
  $t \leftarrow \langle SID, RID, SN, c, v_c\rangle$
  send t to R
end procedure
procedure RECEIVER_ACK_RESPONSE(t)
  local input: K_R^{enc}, K_R^{mac}
  $\langle SID, RID, SN, c, v_c\rangle \leftarrow t$
  $\langle v_c', v_r'\rangle \leftarrow \mathsf{MAC}_{K_R^{mac}}(SID, RID, SN, c)$
  if $v_c = v_c'$ **then**
    reply v_r' to S and accept c
  else
    return fail
  end if
end procedure
procedure SENDER_VERIFICATION(v_r')
  if $v_r = v_r'$ **then**
    return succ
  else
    return fail
  end if
end procedure

1.	$S \rightarrow R$:	SID, RID, SN, $\{m\}_{K_S^{enc}}$, v_c
2.	$S \leftarrow R$:	v_r'

Fig. 2: Message flows in MAC-verifier based ACK authentication

Fig. 2 shows the message flows in MAC-verifier based ACK authentication. The MAC-verifier based scheme supports ACK authentication in the following manner. If we receive an ACK message from a non-trusted device, the MAC verifier v_r', which represents the last l-bits generated for the sent message, will not correspond to that which would be generated using the secret key. This makes the scheme secure against an ACK forgery.

Note that the size of n and l may be determined depending on the levels of security required. If we assume that the size of l is 8 bits and the MAC is created using the 128-bit AES algorithm as in the standard, the value v_c in our scheme has slightly different options: 32, 64, and 120 bits.

3.2 The Scheme II: Using Encrypted Challenge

We now show how to obtain an alternative that uses an encrypted challenge. As before, we assume that each pair of devices is associated with a unique n-bit secret key K_i, and a pair of keys for encrypting and signing (K_i^{enc}, K_i^{mac}) is derived from the key K_i in a predetermined manner.

1) Message sending: A message sender S performs the following: *i*) Choose an l-bit random value r. *ii*) Encrypt the message m with the value r in the encryption key K_S^{enc} to obtain encrypted message $\{m, r\}_{K_S^{enc}}$. *iii*) Compute the message authentication code in the key K_S^{mac} as follows: MAC $=$ $\mathsf{MAC}_{K_S^{mac}}(SID, RID, SN, \{m, r\}_{K_S^{enc}})$ *iv*) Send $\langle SID, RID, SN, \{m, r\}_{K_S^{enc}}, \text{MAC}\rangle$ to receiver R.

2) ACK Response: Receiver R performs the following: *i*) Compute MAC$'$ $= \mathsf{MAC}_{K_R^{mac}}(SID, RID, SN, \{m, r\}_{K_S^{enc}})$ in the key K_R^{mac}. *ii*) If MAC$'$ $=$ MAC, then accept the received message. Otherwise, the message is rejected. *iii*) Decrypt $\{m, r\}_{K_S^{enc}}$ using the secret key K_R^{enc} to obtain the message $\langle m', r'\rangle$. Send the value r' to sender S as an ACK response.

3) Verification: Upon receiving message r', the sender confirms that it matches r. If it matches, the sender is convinced that the ACK message is from the intended receiver and transmission has been completed successfully. Otherwise, the sender discards it.

1.	$S \rightarrow R:$	SID, RID, SN, $\{m,r\}_{K_S^{enc}}$, MAC
2.	$S \leftarrow R:$	r'

Fig. 3: Message flows in encrypted-challenge based ACK authentication

Fig. 3 shows the message flows in encrypted-challenge based ACK authentication.

4 Analysis

4.1 Security

Our schemes are built on cryptographic primitives, MAC and encryption algorithms. The security of our schemes is analyzed in the following theorem.

Theorem 1. *If the underlying cryptographic primitives, MAC and encryption algorithms, are secure then the schemes described in the previous section provides the property of ACK authentication.*

Proof. First, consider the scheme that uses the MAC verifier. That the MAC-verifier based scheme provides the property of ACK authentication is clear. This is because only the legitimate receiver R who possesses the key K_R^{mac} can create a valid verifier. Specifically, let us suppose that for fraudulent purposes, an attacker tries to fabricate an ACK message for an honest sender. To accomplish this, the attacker must derive the MAC verifier v_r' such that $v_r' = v_r$, where v_r represents the last l bits of $\mathsf{MAC}_{K_S^{mac}}(SID, RID, SN, \{m\}_{K_S^{enc}})$. Note that since the MAC key is known only by the receiver, the only way for the attacker to achieve its goal is to guess the verifier v_r'. This implies that the security of the scheme relies on the security of the MAC algorithm. In other words, we can say that if the underlying MAC primitive is secure then the probability that an attacker succeeds in fabricating an ACK message is $1/2^l$. This ensures that the MAC-verifier based scheme prevents the problem of an fabricated ACK message with a probability of approximately $1/2^l$. Let us now consider the scheme that uses the encrypted random challenge. Similar to the previous scenario, suppose that an attacker attempts to fabricate an ACK message for an honest sender. To accomplish this, the attacker must derive r' from the transmitted message $\{m,r\}_{K_S^{enc}}$ such that $r' = r$. However, only the legitimate receiver R who possesses the key K_R^{enc} can decrypt the message. Therefore, the only way for the attacker to achieve its goal is to guess the random value r'. We hence say that if the underlying encryption algorithm is secure then the probability that an attacker succeeds in fabricating an ACK message against the scheme using the encrypted random challenge is the same as in the previous scenario. This leads us to conclude that the security of our schemes relies on the security of the underlying primitives, the MAC and encryption algorithms. □

For data packets, our scheme provides the following security properties: data confidentiality, data authenticity and replay protection. Specifically, in our scheme only authorized devices that share the secret key can decrypt the message $\{m\}_{K_S^{enc}}$ (or $\{m,r\}_{K_S^{enc}}$). The MAC of each data packet enables the following: if an attacker modifies a message from an authorized sender while the message is in transit, the receiver can detect this tampering. In addition, the MAC also prevents any replayed message from being accepted by the receiver and ensures that the packet that has arrived is the most recent and not a replayed packet. This is achieved by associating the sequence number SN with each data packet. The security proof can be done in a similar manner to as in Theorem 1, which we have omitted here for clarity.

4.2 Efficiency

We next consider the energy consumption required for supporting ACK authentication in highly resource-constrained settings. Low-energy consumption is an major design requirement for 802.15.4 networks, due to the nature of battery-operated devices. Most energy consumed when security protocols are added is caused by the transmission of additional data rather than by computational costs.

Our techniques do not require additional communication costs for sending or receiving authenticated ACK messages. This is because they use a MAC verifier (or an encrypted challenge) that has the same length as the sequence number in the plain ACK packet specified in the standard. In other words, the total size of the data payload and ACK packets is exactly the same as that of the security suite currently defined in the 802.15.4 standard. For computational costs, our schemes require only two cryptographic operations, one is for data encryption and another is for data integrity. No additional operation is required for the ACK authentication. The operations involve inexpensive symmetric-key algorithms, such as the AES block cipher and CBC-MAC, and are essential to ensuring basic security services specified in the 802.15.4 standard. Table 2 shows a comparison of 802.15.4 security suites and authenticated ACK schemes in terms of security features and other attributes.

4.3 Advantages

Here we focus on the discussion of authenticated ACK schemes. The advantages of our techniques compared to those examined in the recent work [9], which is the only work having the same objective as ours, are summarized

Table 2: Comparisons of 802.15.4 Security Suites and Authenticated ACK Schemes

Schemes	Data protection	Data authentication	Replay protection	ACK authentication	Key setup	Network model
AES-CTR [1]	√	-	√	-	Not required	Star, P2P
AES-CCM [1]	√	√	√	-	Not required	Star, P2P
AES-CBC-MAC [1]	-	√	√	-	Not required	Star, P2P
PSCM [9]	√	√	-	√	Required	Star
Our scheme I, II	√	√	√	√	Not required	Star, P2P

as follows: *i) No additional pre-setup requirement:* Our schemes do not require any pre-setup phase for sharing additional secrets for ACK authentication. This is in contrast to the PSCM scheme [9], which requires an initial setup phase for generating a Prime-Sequence Code Matrix (PSCM) [10] and then securely distributing a secret value to each device. These requirements limit the use of the scheme. *ii) Full-fledged security:* Our schemes support all required security services, including data confidentiality, data authenticity, replay protection, and ACK integrity. The PSCM scheme, however, does not support security against replay attacks on data payload packets. In our schemes, this problem is eliminated by the use of a sequence number for each payload packet. *iii) Practical:* Unlike PSCM, the fact that our schemes do not impose a pre-setup requirement means thy can be used not only in large-scale networks, but also in both peer-to-peer and star topology networks supported by the 802.15.4 standard. Furthermore, they introduce practically no additional computation or communication overhead, and are thus practical for use in LR-WPAN settings.

5 Conclusion

We have described practical techniques for supporting ACK authentication in 802.15.4 LR-WPAN settings. Our techniques have several major advantages. They achieve all required security properties including data protection, data authentication, replay protection, and ACK authentication. They do not require a pre-setup phase for sharing additional secrets for ACK authentication. This results for us in greater efficiency and ease of implementation. Our schemes are usable not only in large-scale networks, but also in both peer-to-peer and star topologies supported by the 802.15.4 standard. They introduce practically no additional computation or communication costs, and thus are practical for use in LR-WPAN settings. We believe that our schemes provide new building blocks for the construction of security services on 802.15.4 packets.

Acknowledgement

The second author acknowledges that this work was supported by the IT R&D program of MSIP/IITP [10041145, Self-Organized Software platform(SoSp) for Welfare Devices]. The authors would like to thank anonymous reviewers for a careful checking of the details and their helpful comments on the paper.

References

[1] IEEE Standard 802.15.4-2006, “Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Low Rate Wireless Personal Area Networks (WPANs),” June 2011.

[2] D. Gascon, “Security in 802.15.4 and ZigBee networks,” http://www.sensor-networks.org/index.php?page=0903503549.

[3] H. Li. B. Xue, and W. Song, “Application and analysis of IEEE 802.14.5 security services,” in *Proc. 2010 ICNDS*, vol.2, pp.139–142, May 2010.

[4] N. Sastry and D. Wagner, “Security considerations for IEEE 802.15.4 networks,” in *Proc. 2004 ACM WiSec*, pp. 32–42.

[5] Y. Xiao, S. Sethi, H.H. Chen, and B. Sun, “Security services and enhancements in the IEEE 802.15.4 wireless sensor networks,” in *Proc. 2005 IEEE GLOBECOM*, vol. 3, pp. 1796–1800.

[6] R. Daidone, “Experimental evaluations of security impact on IEEE 802.15.4 networks,” in *Proc. 2011 IEEE WoWMoM*, pp.20-24, June 2011.

[7] M. Bellare, J. Kilian, and P. Rogaway, “The security of the cipher block chaining message authentication code,” *Journal of Computer and System Sciences*, vol. 61, no. 3, pp. 362–399, Dec. 2000.

[8] J. Daemen and V. Rijmen, “The block cipher Rijndael,” In Proc. 2000 CARDIS, LNCS 1820, pp. 277–288.

[9] M.H. Park, “Challenge-response based ACK message authentication,” *Electronics Letters*, vol. 48, no. 16, pp. 1021–1023, Aug. 2012.

[10] W.C. Kwong and G.C. Yang, “Construction of 2n prime-sequence codes for optical code division multiple access,” *IEE Proceedings - Communications*, vol. 142, no. 3, pp. 141–150, June 1995.

Eun Kyung Ryu received the Ph.D. degree in Computer Engineering from Kyungpook National University (KNU) in 2005. She worked as a visiting professor in the Depart. of Mobile Content, Daegu Haany University in 2006. In 2007, she worked as a research fellow at School of Systems Information Science, Future University Hakodate, Japan. Currently, she is a contract professor at School of Computer Science and Engineering in KNU. Her research interests include applied cryptography, security Protocols, and network security.

Kee Young Yoo received the B.Sc. degree in Education of Mathematics from Kyungpook National University in 1976 and the M.Sc. degree in Computer Engineering from Korea Advanced Institute of Science and Technology in 1978, South Korea. He received the Ph.D. degree in Computer Science from Rensselaer Polytechnic Institute, New York, USA in 1992. He is currently a professor at School of Computer Science and Engineering, Kyungpook National University. His primary research interests include cryptography, smart card security, network security, DRM security, and steganography.