Journal of information and communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 10(3): 248-252, Sep. 2012 **Regular Paper**

Network and Data Link Layer Security for DASH7

Hwajeong Seo and Howon Kim*, *Member, KIICE*

Department of Computer Engineering, Pusan National University, Pusan 609-735, Korea

Abstract

The sensor network standard DASH7 was proposed to improve transmission quality and low power communication. Specifications for the standard are currently being developed, so the security specification has not been firmly implemented. However, without a security specification, a network cannot work due to threats from malicious users. Thus we must ensure confidentiality and authentication of data packets by using a cryptography method. To contribute to the DASH7 security specification, this paper shows the implementation results of network and data link layer security by using advanced encryption standard (AES) counter with CBC-MAC (CCM) over CC430 sensor nodes.

Index Terms: DASH7, Data link layer, Network layer, Security, AES-CCM, CC430

I. INTRODUCTION

Sensor networks are used for various applications including environmental monitoring systems, the smart grid, and vehicular networks. Recently, a sensor network standard, DASH7, was proposed to expand the market for low power wireless technologies [1]. The method achieves under 0.1 mA in average current and 50 mA in maximum current by transmitting packets through the low frequency range of 433 MHz. Due to the strengths of the DASH7 standard, the standard is being actively developed. The specification includes network protocols, architecture, and security. To implement the DASH7 specification, open source code, OpenTag, was released to debug the source code and test its performance [2]. A recent version, OpenTag beta 2, includes a security module, software-based advanced encryption standard (AES) cryptography for confidentiality of the data link. However, data authentication and network layer security was not implemented. To enhance security over the DASH7 standard, we applied AES-counter with CBC-MAC (CCM) to the data link and network layer.

The following are main contributions of the paper. We implemented data link and network layer security over OpenTag source code and applied AES-CCM mode to DASH7 standard for data confidentiality and authentication. Lastly a hardware-based AES module was efficiently used for AES-CCM mode.

This paper consists of five sections. In Section II, we introduce work related to DASH7 and the experimental setup. In Section III, we propose a security implementation, while Section IV includes an evaluation report. Finally, we conclude the paper in Section V.

II. RELATED WORK

In this section, we introduce DASH7, which is ultra-low power wireless data technology in the 433 MHz industrial, scientific and medical (ISM) band and explain the network layer and data link layer of DASH7 and the AES-CCM mode. The experimental setup is

Received 11 May 2012, **Revised** 11 June 2012, **Accepted** 18 June 2012
***Corresponding Author** E-mail: howonkim@pusan.ac.kr

Open Access **http://dx.doi.org/10.6109/jicce.2012.10.3.248** print ISSN:2234-8255 online ISSN:2234-8883

also described in this section.

A. DASH7 Standard

DASH7 is a wireless sensor networking standard which based on an ISO/IEC 18000-7 standard. ISO/IEC 18000-7 is a standard that specifies air interface communication on the 433 MHz ISM band and has a communication range of up to 1,000 m or more. This is six times greater than WiFi, Bluetooth, and ZigBee, which all operate in the 2.45 GHz band. The data rate is normally 28 kbps, with a maximum of 200 kbps. In addition, ISO/IEC 18000-7 devices can be used for 10 years. Thus, the standard has economic advantages and can be applied to areas such as smartphones, smart homes, and logistics.

However, ISO/IEC 18000-7 standard has a gray area that causes compatibility problems given that some aspects of the standard are not clearly defined and can be interpreted in several ways. The DASH7 alliance was founded in February 2009 and announced DASH7 to resolve the problems and preserve the compatibility of devices.

B. Data Link Layer

The data link layer is responsible for constructing frames and processing message authentication (MAC). To transmit frames, the data link layer constructs the frames in blocks that include the frame-length, headers, and cyclic redundancy check (CRC) block and also processes MAC based on carrier sense multiple access-collision avoidance (CSMA-CA).

There are two types of frames: background frames and foreground frames. Background frames are small and fixed-length frames for control between devices. Foreground frames are used to transfer actual messages. They have various types of headers and variable length.

C. Network Layer

The network layer is responsible for network routing and addressing, and thus provides background protocols and foreground protocols for the network.

Background network protocols are responsible for processing background frames, the advertising protocol, and the reservation protocol. The advertising protocol is used for ad-hoc group synchronization in broadcasting. The reservation protocol is used for reserving the channels by CSMA-CA.

The foreground network protocols are the data stream protocol and network protocol. The network protocol supports querying, and thus includes information on routing and addressing. The data stream protocol is a simple data encapsulation protocol. It does not include information on routing or addressing.

III. EXPERIMENTAL SETUP

A. AES-CCM

CCM is authenticate-and-encrypt block cipher mode [3]. By using 128-bit block cipher AES, CCM can be operated. To compute the authentication field, the CBC-MAC mode is used and to encrypt the message data, the counter (CTR) mode is used.

B. Target Board

The CC430 is equipped with MSP430X family microcontrollers, which provide various instruction sets and 12 general purpose registers which is 16 bit. The strong security feature of the target board is the AES accelerator module. The module computes AES cryptography by inputting setup parameters and a secret key and plain text. After 167 clock cycles, the result is available in defined memory. By accessing memory, we can easily obtain the result.

C. OpenTag

OpenTag is a full-featured communications stack for DASH7 mode 2 (ISO 18000-7.4). It is intended to run on embedded hardware. Currently four branches are available in [2].

IV. MAIN CONTRIBUTION: SPECIFICATION OF IMPLEMENTATION

This section includes detailed information on the packet specification and AES module for implementation.

A. Packet Specification

1) Data Link Layer Packet

In Fig. 1, Data link packet which is comprised of a frame header, data link layer security (DLLS) header, address header, and payload is depicted.

The frame header includes frame control attributes and setting parameters. The DLLS header defines the DLLS code for initialization data and authentication data footer. In the address header, the type of message transmission and address are described. The payload includes a network layer packet. A previous implementation provides encryption

from the address header to the network frame. In our implementation, we encrypt the data and in addition we authenticate whole packet using AES-CCM mode. As a result, we generate authentication data for the data link layer packet.

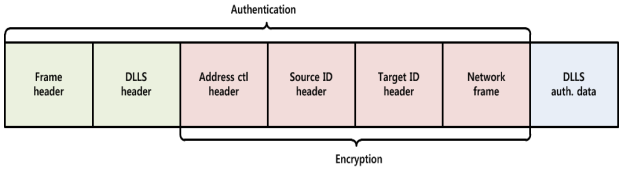

Fig. 1. Structure of data link layer packet. DLLS: data link layer security.

2) Network Layer Packet

In Fig. 2, Network layer packet which consists of a mode 2 network layer security header and routing header and payload is depicted. The M2NLS header defines the M2NLS code for initialization data and the authentication data footer. In the M2NP routing header, hop control information is described. The previous implementation does not provide security in the network model. In our implementation, we encrypt all of the data and generate authentication information which is defined in the DASH7 standard. Therefore, the implementation provides data confidentiality together with authentication.

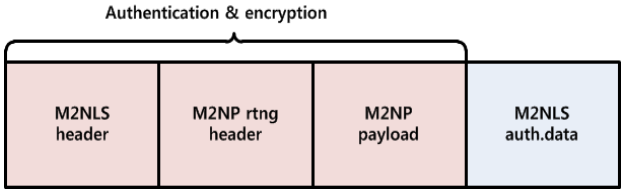

Fig. 2. Structure of network layer packet. M2NLS: mode 2 network layer security, M2NP: mode 2 network protocol.

The recent version of Open Tag provides a software AES module for encryption and decryption. However, the sensor node has little memory and low computation power. Therefore, implementing the DASH7 protocol together with an encryption module requires greater memory than the software's capacity. To reduce the required memory, we used an AES accelerator module. It performs encryption and decryption of 128-bit data with 128-bit keys according to the advanced encryption standard in hardware. As a result, software implementation can be replaced with a hardware version. The detailed process of AES using the accelerator is described in Table 1.

Table 1. Source code for AES accelerator

```
1: int i;
2: unsigned char result [16];
3: AESACTL0j = AESSWRST;
4: AESACTL0 & = NOT(AESSWRST);
5: AESACTL0 & = NOT(AESRDYIE);
6: AESACTL0 & = NOT(AESOP0jAESOP1);
7: while (AESASTAT & AESKEYWR);
8: i = 0;
9: while (i<16){
10: AESAKEY L = *(key+i++);
11: }
12: while (!(AESASTAT & AESKEYWR));
13: i = 0;
14: while (i<16){
15: AESADIN L = *(data+i++);
16: }
17: while (AESASTAT & AESBUSY);
18: i = 0;
19: while (i<16){
20: *(result+i++) = AESADOUT L;
21: }
22: for (i = 0; i < 16; i++){
23: data [i] = result [i];
24: }
```

```
AESSWRST: AES software reset
AESRDYIE: AES ready interrupt enable
AESOP0: AES operation bit: 0
AESOP1: AES operation bit: 1
AESKEYWR: AES all 16 bytes written to AESAKEY
AESBUSY: AES busy
AESAKEY L: Key address
AESASTAT: Status address
AESADOUT L: Output address
AESADIN L: Data address
```

AES: advanced encryption standard

3) Detailed Process of AES-CCM

Table 2 shows the process of AES-CCM. The AES-CCM mode consists of cipher block chaining (CBC) and counter (CNT) modes. First, the CBC mode is conducted for message integrity code (MIC). Initial vector (IV) is generated and encrypted and an exclusive-or operation is performed with the header and data. After final encryption, we can obtain MIC information. Secondly, to compute the CNT mode, IV is generated by increasing the counter encryption and an exclusive-or operation is conducted. In the last operation, MIC is generated and then through exclusive-or with the previous MIC, the complete MIC is generated.

Table 2. Source code of AES-CCM implementation on DASH7

CBC Mode: IV (initial vector) generation Out = Encryption (IV) Out = X or (Out, Header) Out = Encryption (Out) Out = X or (Out, Payload) Out = Encryption (Out) MIC = Out [0], Out [1]
CNT Mode: IV (initial vector) generation Out = IV j CNT Out = Encryption (Out) Out = X or (Out, Payload) Out = Out j CNT++ Out = Encryption (Out) MIC = X or (MIC, Out [0] j Out [1])

AES: advanced encryption standard, CCM: counter with CBC-MAC, CBC: cipher block chaining, CNT: counter, MIC: message integrity code.

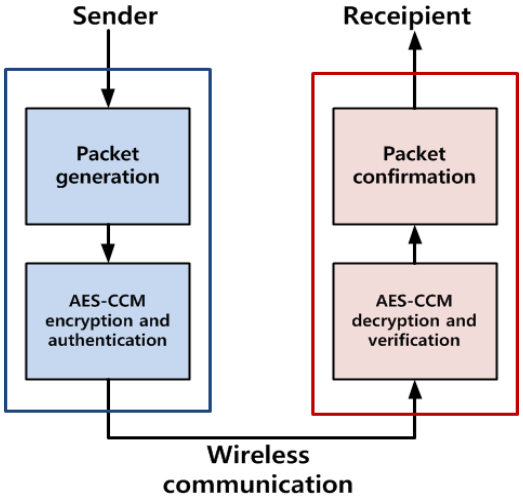

Fig. 3. Evaluation scenario: sender transmits packet after AES-CCM mode and recipient check the data. AES: advanced encryption standard, CCM: Counter with CBC-MAC, CBC: cipher block chaining, MAC: message authentication.

Table 3. Transmitted packet and AES-CCM parameter

Secret key	C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 CA CB CC CD CE CF
Plain text	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E
CBC IV	59 00 00 00 03 02 01 00 A0 A1 A2 A3 A4 A5 00 17
Cipher text & transmitted text	00 01 02 03 04 05 06 07 58 8C 97 9A 61 C6 63 D2 F0 66 D0 C2 C0 F9 89 80 6D 5F 6B 61 DA C3 84 17 E8 D1 2C FD F9 26 E0

AES: advanced encryption standard, CCM: Counter with CBC-MAC, CBC: cipher block chaining, MAC: message authentication.

V. EVALUATION

We have evaluated performance of a DASH7 security module by implementing the module. The target chip was a CC430-F5137 with a 20 MHz clock, 32 KB flash for the code, and 4 KB RAM. The compiler used was Code Composer Studio version 5.

The detailed scenario is described in Fig. 3. The first sender generates a transmission packet and during the network and data link layers, the packet is encrypted with a counter mode and authentication is conducted with CBC-MAC. After finishing the process, the packet is transmitted to the destination through the air. When the recipient receives the packet, the decryption and verification process are conducted. If the packet satisfies the message authentication information, the process continues.

We verified the success of transmission and packet encryption by printing data using a hyper terminal. The parameter used is described in Table 3.

VI. CONCLUSIONS

This paper implemented data link and network layer security in DASH7 by using the AES-CCM mode. The method provides authentication and confidentiality with efficient computation of the AES accelerator on embedded hardware. The implementation result shows that the DASH7 standard can configure a network and transmit data safely with a cryptography method. Future work will implement other cryptographic methods including HB2 [4], Letter-Soup [5], and Rabbit-MAC [6] and find the most efficient mode of operation over the DASH7 standard.

ACKNOWLEDGMENTS

This work was supported by the National Research Foundation (NRF) grant funded by the Korea government (Ministry of Education, Science and Technology; No. 2010-0026621).

REFERENCES

[1] J. P. Norair. Introduction to DASH7 technology [Internet]. DASH7 Alliance, Morgan Hill: CA, Whitepaper, 2009. Available: http://www.eetimes.com/electrical-engineers/education-training/tech-papers/4135414/Introduction-to-DASH7-Technologies.

[2] Sourceforge. OpenTag [Internet]. Available: http://sourceforge.net/projects/opentag/.

[3] D. Whiting, R. Housley, and N. Ferguson, “Counter with CBC-MAC,” The Internet Engineering Task Force, Fremont: CA, *RFC*

3610, 2003.

[4] D. Engels, M. J. O. Saarinen, P. Schweitzer, and E. M. Smith, "The hummingbird-2 lightweight authenticated encryption algorithm," *Proceedings of the 7th International Conference on RFID Security and Privacy*, Amherst, MA, pp. 19-31, 2011.

[5] M. A. Simplicio Jr, P. F. F. S. Barbuda, P. S. L. M. Barreto, T. C. M. B. Carvalho, and C. B. Margi, "The MARVIN message authentication code and the LETTERSOUP authenticated encryption scheme," *Security and Communication Networks*, vol. 2, no. 2, pp. 165-180, 2009.

[6] R. Tahir, M. Y. Javed, and A. R. Cheema, "Rabbit-MAC : lightweight authenticated encryption in wireless sensor networks," *Proceedings of International Conference on Information and Automation*, Changsha, China, pp. 573-577, 2008.

Hwajeong Seo

received the BSEE degree from Pusan National University, Pusan, Republic of Korea in 2010, and he is in the MS degree program in Computer Engineering at Pusan National University. His research interests include sensor networks, information security, elliptic curve cryptography, and RFID security. He is a member of IEEE.

Howon Kim

received the BSEE degree from Kyungpook National University, Daegu, Republic of Korea, in 1993 and the MS and PhD degrees in electronic and electrical engineering from the Pohang University of Science and Technology (POSTECH), Pohang, Republic of Korea, in 1995 and 1999, respectively. From July 2003 to June 2004, he studied with the COSY group at the Ruhr-University of Bochum, Germany. He was a senior member of the technical staff at the Electronics and Telecommunications Research Institute (ETRI), Daejeon, Republic of Korea. He is currently working as an associate professor with the Department of Computer Engineering, School of Computer Science and Engineering, Pusan National University, Busan, Republic of Korea. His research interests include RFID technology, sensor networks, information security, and computer architecture. Currently, his main research focus is on mobile RFID technology and sensor networks, public key cryptosystems, and their security issues. He is a member of the IEEE, and the International Association for Cryptologic Research (IACR).