Perspectives in Communication, Embedded-Systems and Signal-Processing (PiCES)
ISSN: 2566-932X, Vol. 2, Issue 4, July 2018
Proceedings of National Conference on Emerging Trends in VLSI, Embedded and Networking (NC-EVEN 18), April 2018

Authenticated Encryption for Wireless Sensor Network

Padmini R[1], Pavithra A B[1], Manjunath B E[2], Manjunath M[2]

[1.] UG Scholars, Dept. Of ECE, Brindavan College of Engineering

[2.] Assistant Professor, Dept. Of ECE, Brindavan College of Engineering

Abstract: Wireless Sensor Networks (WSNs) are becoming popular day by day. Security issues on WSN thus draw much attention.To receive trusted information from these sensor nodes they have to send authenticated messages. Encryption is alone not enough to ensure the confidentiality, authenticity and integrity of communicated data. AES encryption algorithm is adopted by many WSN standards such as IEEE 802.15.4 and IEEE 802.15.6. AES algorithm which provides data encryption, also provides additional security services such as data authentication, integrity when it is combined with appropriate functionality.In this paper we have discussed different modes of operation of block ciphers which gives authenticated encryption. AES-CCM (Advanced Encryption Standard –Counter Mode with Cipher Block Chaining Mode) is a security standard that gives highest level of security. Software implementation of the algorithm is done in java and the obtained results show that it is a good solution for wireless sensor network Security.

Keywords: Security, Authentication, Block ciphers

I. INTRODUCTION

Selection of suitable security scheme is critical in wireless sensor networks (WSNs) due to wireless media communication and limited resources of sensor nodes.Because of the communication channel and the trust less environment, security issues have been a big problem on WSN node research. IEEE 802.15.4 is one of the standards defining radio and media access control for a low rate, low power WSN[1].IEEE 802.15.4 investigates low data rate WSN solutions with a battery life ranging from few months to several years. The IEEE 802.15.4 standard is intended to operate in unlicensed and international frequency band.802.15.4 specifies cryptographic procedures for protecting communications at medium access control layer.The MAC layer of 802.15.4 uses the AES-CCM protocol as security mechanism, it uses the AES algorithm as the core, uses CTR mode to ensure confidentiality of data, uses CBC-MAC mode to authenticate the public information of the header in MAC frame [1].

In this paper we use java cryptographic library functions to implement generic AES algorithm in CCM mode.

The paper is organized as follows. Section II presents the Authenticated Encryption and modes of operation. Section III gives the security protocol suite of IEEE 802.15.4. Section IV gives the result of implementation and limitations. Section V is conclusion.

II. AUTHENTICATED ENCRYPTION

Block ciphers are only able to encrypt short messages. For example AES is able to encrypt only 16 bytes of messages and blowfish is able to encrypt 8 bytes long messages. Longer messages are split into blocks. Each block is combined with previously encrypted blocks and passed to the block cipher. Block combining is called an operation mode and there are multiple secure ways how to do it. Mode of operation is a technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application. These modes of operation (ECB, CBC, CFB, OFB, CTR) are intended to use with any block ciphers including triple DES and AES. These modes of operation can provide confidentiality or authenticity, but are not able to provide both simultaneously.

Authenticated Encryption (AE) is a term used to describe encryption systems which simultaneously protect confidentiality, authenticity and integrity of communications.AE rejects any modified ciphertext as invalid. It is not possible to take encrypted data, modify them and end up with valid ciphertext. This property is also called ciphertext integrity. Any cipher that does not provide ciphertext integrity or authenticated encryption is probably vulnerable to some active attack.

Basic components of AE are Message authentication Code and Symmetric encryption. Composition methods are:

- Encrypt-and –MAC
- MAC-then-Encrypt
- Encrypt-then-MAC

Encrypt-then-MAC provides the most secure solution for authenticated encryption. Authenticated encryptions are secure against active attackers. Most common operation modes that provide also authentication are:

- GCM(Galois Counter Mode)
- CCM(Counter Mode with Cipher Block Chaining Mode)
- OCB(Offset Code Book Mode)
- CWC(Cater-Wegman Counter Mode)

These AE modes extend the advantages of the known modes and improve them by the carefully chosen algorithm to provide confidentiality and authenticity [3].

A. Message Authentication Code

To ensure message authentication and integrity, a message authentication code (MAC) is appended to each message sent. This MAC is viewed as a cryptographically secure checksum of the message. Computing the MAC requires senders and receivers share a secret key. Depending upon the secret key, the sender computes a MAC and adds it to the message it sends. On the other end, the receiver sharing the secret key recalculates the MAC and accepts the message if and only if the received and the computed MACs are the same. The success of this idea heavily relies on the strength of MAC which is generally difficult to forge without a secret key. This security measure prevents the adversary from modifying a valid message and making it acceptable to a receiver without the knowledge of a shared secret key [3].

B. Symmetric Encryption

AES is cryptographic algorithm which has become the basic choice of encryption for a wide range of application. AES is a symmetric-key block cipher with a Plaintext length of 128 bits and a flexible Key length of 128, 192 or 256 bits. The output of the AES algorithm is also 128 bits and it is called Ciphertext. In most wireless standards such as IEEE 802.15.4, the key length is 128 bits.

The AES algorithm contains encryption and key Expansion processes.

- Encryption process consists of 10 rounds and in each round it does SubBytes(), ShiftRows() ,MixColums() and AddRoundKeys() operations.
- Key Expansion process is done by a function called ScheduleKey() which in turn consists of two operations namely SubWord() and Rotword().

AES provides various security services based on 7 modes of operations [4].

C. Galois/Counter Mode

The Galois/Counter Mode (GCM) is a block cipher mode of operation which is used to provide authenticated encryption. As the name suggests, the GCM mode combines the well-known counter mode with the new Galois mode. The GCM mode can be applied to 64-bit block cipher. GCM has two functions, authenticated encryption and authenticated decryption. The two outputs of the authenticated encryption function are:

● A ciphertext, denoted C, which has the same length as that of the plaintext.

● An authentication tag, denoted T, which has any bit length between 64 and 128.

The GCM mode uses a variation of the Counter mode with an incrementing function to ensure the confidentiality. And the authentication is ensured by using a hash function over a binary Galois field, this hash function is called GHASH. The encryption and authentication of GCM are secure against the chosen-plaintext attack. The implementation of GCM can be done in both hardware and software [4].

D. Counter mode with Cipher Block Chaining Mode

The CCM mode is a combination of the Counter (CTR) mode and the Cipher Block Channing (CBC) mode, where the Counter mode and the CBC mode are applied respectively to provide confidentiality and authenticity with using a single key. The CCM mode is only defined to support the 128-bit block cipher algorithm, such as AES-128. The CCM mode accepts a variable-length authentication tags (from 32-bits to 128-bits), thus allowing varying degrees of protection against unauthorized modifications. The CCM mode has two functions, namely encryption-authentication function and decryption-verification function. Because the CCM mode uses single key, the key does not allow to be accessed without evidence. The value of the nonce should be unique for each key in encryption [4].

E. Offset Code Book Mode

The Offset Code Book (OCB) mode is another AE mode, which provides the confidentiality and the authenticity simultaneously. Before appearing of the AE modes, the confidentiality and the authenticity are provided separately by two systems: block cipher for the confidentiality and MAC for the authenticity. However, the OCB mode combines appropriately block cipher and MAC, and the computational cost is lower as the two separate systems. The OCB mode accepts the block cipher, which has the size of 128, 192 and 256 [5].

F. Cater Wegman Counter Mode

The Cater-Wegman Counter (CWC) mode is an AE mode, which uses the Counter mode and the Carter-Wegman universal hash function to provide confidentiality and authenticity respectively. The outstanding point is that this mode has five important properties: provable security, parallelizable, high performance in hardware, high performance in software, and free from intellectual property concerns [5].

III. SECURITY MODEL FOR WSN

The IEEE 802.15.4 standard is designed for low-rate wireless personal area networks (LR-WPANs).Unlike wireless local area networks (WLANs), connections effected via WPANs involve little or no infrastructure. This is set to become the standard communications protocol for use in wireless sensor networks. Features allow small, power efficient, inexpensive solutions to be implemented for an expansive range of devices. The main objectives of an LR-WPAN are ease of installation, reliable data transfer, short-range operation, and extremely low cost and reasonable battery life, whilst maintaining a simple and flexible protocol. The standard itself defines the physical (PHY) and MAC layers, component devices and supported network topologies. There are number of security suites specified in this standard [6].

A. IEEE 802.15.4 Security

There are many security suites that can be implemented under IEEE 802.15.4 standard. A link layer protocol provides the four basic security services. These include access control, message integrity, and message confidentiality and replay protection [6].

Table 1. Security Suites defined by IEEE 802.15.4

Name	**Description**
Null	No security
AES-CTR	Encryption only
AES-CBC-MAC-128 AES-CBC-MAC-64 AES-CBC-MAC-32	Authentication only
AES-CCM-128 AES-CCM-64 AES-CCM-32	Authenticated Encryption

Adding a MAC to messages enables data authenticity and integrity. Corresponding to IEEE 802.15.4 an application chooses different lengths of MAC. According to low power requirement for sensor nodes one prefers shorter messages which needs less transmission time and thus less power. But in contrast, better authenticity and integrity requires longer MAC [7].

The CCM mode authentication mechanism described in 802.15.4 takes a message as input and gives a MAC of variable length as output [7]. See figure 1.

The CCM mode confidentiality mechanism described in IEEE 802.15.4 takes payload/MAC of a message as input and gives encrypted payload/MAC as output [7]. See figure 2.

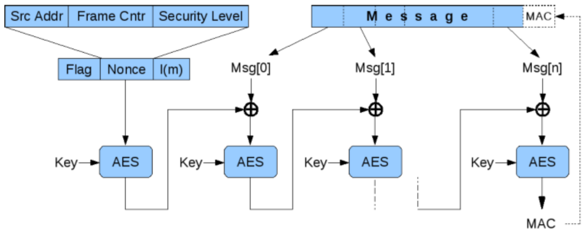

Fig 1. Authentication of a message according to CCM with AES

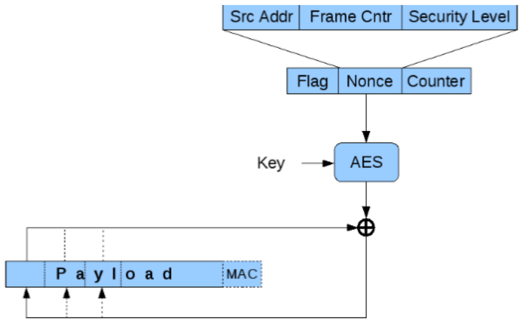

Fig 2. Encryption of a message according CCM with AES

There are other alternative security implementations are possible with IEEE 802.15.4 addition to CCM mode.

No Security

Len	IEEE 802.15.4 Header	Payload	CRC

Authentication

Len	IEEE 802.15.4 Header	Auxiliary Security Header	Payload	PAD	MAC	CRC

Encryption

Len	IEEE 802.15.4 Header	Auxiliary Security Header	Encryption Payload	PAD	CRC

Encryption and Authentication

Len	IEEE 802.15.4 Header	Auxiliary Security Header	Encr Payload	PAD	PAD	MAC	CRC

REFERENCES

[1] D.-y. Q. . H. H. Bin Feng, "Parallel and multiplex architecture of aes-ccm coprocessor implementation for ieee 802.15.4," Emerging Intelligent Data and Web Technologies, pp. 149 – 153, Sept. 2013.

[2] W. S.. X. W. Islam, K., "Wireless sensor network reliability and security in factory automation: A survey," Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 42, no. 6, pp. 1243 – 1256, Nov. 2012.

[3] G. . H. J. . C. F. . H. J. .d. G. H. . G. C. Tsekoura, I. Selimis, "Exploration of cryptographic asip designs for wireless sensor nodes," Electronics, Circuits, and Systems, pp. 827 – 830, Dec. 2010.

[4] T. N. David Boyle, "Securing wireless sensor networks: Security architectures," Journal Of Networks, vol. 3, no. 1, pp. 65–77, Jan 2008.

[5] H. Chen, "Authentication mode of block ciphers," [Online]. Available:https://www.emsec.rub.de/media /crypto/attachments/files/2011/03/chen.pdf.[Accessed: Feb. 22, 2015].