International Journal for Modern Trends in Science and Technology
Volume: 02, Issue No: 12, December 2016
ISSN: 2455-3778
http://www.ijmtst.com

An Encrypted MAC for the Authentication Process in WSN

Pavan A C

PG Student, Department of CS&E, P.E.S. College of Engineering, Mandya, Karnataka, India.

To Cite this Article
Pavan A C , "An Encrypted MAC for the Authentication Process in WSN", *International Journal for Modern Trends in Science and Technology*, Vol. 02, Issue 12, 2016, pp. 30-32.

ABSTRACT

Security infringement and energy consumption issues are vital in WSN (wireless sensor networks). Looking at the attacks like Denial-of-Sleep, Man-in-the-Middle, Correlation attack, etc, are affecting the transfer of any data. It might be the data loss or the modification where in the third party access the information to one self. This paper explains how to authenticate the data transfer using the encryption standards in MAC algorithm in a riskless technique.

KEYWORDS: *WSN, Denial-of sleep, MAC, Encryption Standards, Transport Layer Security, Cryptography.*

I. INTRODUCTION

Wireless sensor networks are in continual need where the physical environment requirements are to be converted to readable data. Be it the area of monitoring, heath care or earth sensing like air pollution, WSN [2]-[5] sensors are in major use in all such applications. When considering duty-cycle based WSN MAC protocols, the sensor nodes are either in one of the two states namely awake/active and sleep state. These states are switched periodically and they enter sleep mode after certain idle period hence, reducing energy consumption.WSN often encounters various security attacks, one such attacks is DOS (denial-of-service). In a DOS attack the legitimate user node is sent certain unwanted data to process sent by the attackers. This leads to not providing the actual service required to the user who requested the service.

Denial of sleep is a special type of DOS attack. In denial of sleep attack the sensor nodes are kept awake to consume more energy. An anti-node can send fake data packets to other nodes of WSNs. If the receiver is unable to judge among the real and the fake node, the receiver will receive and process the data from the anti-node. This keeps the receiver awake as long as the data transmission sustains, thus exhausting the battery of nodes rapid manner. This might lead the legitimate user node to provide all the services to fake node repeatedly. Hence the security is an issue and more power consumed unnecessarily.

The data to be transmitted is sent with a MAC signature which is generated by MAC algorithm. This data while matching the signature the energy may drain off or if the algorithm is hacked then the message may be modified before reaching to the destination. In order to overcome these problems a fast authentication scheme is required that if integrated with Encrypted MAC protocol it could counter the Denial-of-Sleep attack.

The design principles and features of the proposed secure scheme are:

- Energy conservation
- Low complexity
- Mutual authentication

- Capability to counter the Denial-of-Sleep attack
- Integrating the Encrypted MAC protocol

The paper structure is as follows. Firstly, a literature survey upon the existing system is being specified in "EXISTING SCHEME" section which also mentions the various types of encryption in brief. Secondly, the proposed system in the "ENHANCED SCHEME", briefs about how encrypted MAC is being integrated and the un-authorization is reduced.

II. EXISTING SCHEME

A message authentication code [1] (MAC) is a short signature that is used to authenticate a message. A MAC algorithm, accepts as input a secret key and an arbitrary-length of message from the actual message that has to be sent and outputs a MAC. The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content. In MAC protocol, all the nodes will be having the MAC algorithm. Here, the sender node will have a key (k) and uses the message to run in the MAC algorithm to get the MAC tag. The message and the MAC signature are then sent to the receiver node. The receiver node in turn runs the message portion of the transmission through the same MAC algorithm using the same key, producing another MAC signature. The receiver then compares the MAC signature. If they are matched, the message was not altered during transmission and it is not an anti-node. If the MAC function is not matched then the message will be discarded.

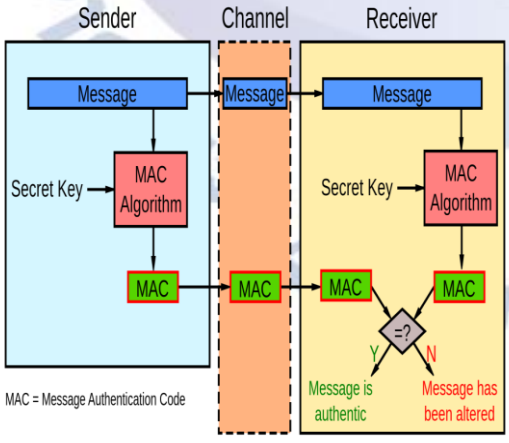

Fig-1 :- Message Authentication Code (MAC)

MAC protocol [6]-[7] uses the hashing function so that the authentication process takes places at a faster rate, so that the system wake-up time will be less and the energy will not be drained soon. Therefore the normal nodes are kept as it is and the anti-nodes are labeled malicious and are neglected for further transmission.

MAC protocol is safe and authenticated process where in no data is lost or modified at the time of transfer of message. But even at some point of time if the pre-installed MAC algorithm is hacked then the message that is transfer can be accessed or modified and this will effect in draining of energy in the node. Therefore, to reduce the energy consumption, to counter the power exhausting attacks, and enhance the performance of sensor nodes, a transport layer security design of secure scheme which integrates the MAC protocol along with encryption can be used.

III. ENHANCED SCHEME

In order to overcome the drawbacks of the above discussed scheme, the enhanced scheme that is the MAC-then-Encrypt (MtE) process is being used in which Transport Layer Security (TLS) is being utilized.

A MAC [8]-[9] is produced based on the plaintext, and then the plaintext and MAC are together encrypted to produce a ciphertext based on both. The ciphertext (containing an encrypted MAC) is sent. Even though the MtE approach has not been proven to be strongly unforgettable in it, the SSL/TLS [10]-[11] implementation has been proven to be strongly unforgeable by Krawczyk who showed that SSL/TLS was in fact secure because of the encoding used alongside the MtE mechanism.Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communications security over a cluster of nodes.

The Transport Layer Security protocol aims primarily to provide privacy and data integrity between two communicating nodes.

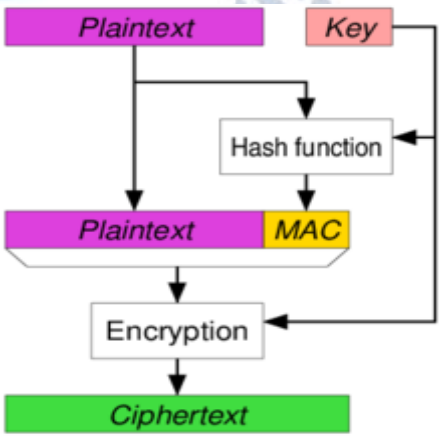

Fig-2:- MAC with Encryption

When secured by TLS, connections between two nodes have one or more of the following properties:

- The connection is *secure* because symmetric cryptography is used to encrypt the data transmitted. The keys for this symmetric encryption are generated uniquely for each connection and are based on a shared secret negotiated at the start of the session. The nodes negotiate the details of which encryption algorithm and cryptographic keys to use before the first byte of data is transmitted. The negotiation of a shared secret is both secure (the secret is unavailable and cannot be obtained, even by an attacker who places themselves in the middle of the connection) and reliable (no attacker can modify the communications during the transfer without being detected).
- The identity of the communicating nodes can be *authenticated* using public-key cryptography. This authentication can be made optional, but is generally required for at least one of the nodes.

IV. CONCLUSION

In this paper, an enhancement of Encrypted MAC protocol has been proposed to secure authentication, confidentiality and save the energy in the nodes in a wireless sensor network. The involvement of MAC signature with every message encrypted while transfer gives more authenticity and also reduces wakeup time of the node. Hence the proposed Encryption MAC protocol helps to uphold the secure authentication and energy efficiency of the wireless sensor networks.

REFERENCES

[1] Pavan A C and P. Prasanna, "Secure & Energy Efficient Scheme against Denial-of-Sleep Attack in WSN", IJMTST | Volume: 2 | Issue: 05 | May 2016.

[2] Zheng, Jun, and Abbas Jamalipour. Wireless sensor networks: a networking perspective. Wiley. com, 2009.

[3] Kaur, Simerpreet, MdAtaullah, and Monika Garg. "Security from Denial of Sleep Attack in Wireless Sensor Network." INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY 4.2 (2013): 419-425.

[4] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, "Analyzing and modeling encryption overhead for sensor network nodes," in Proc. ACM 2nd ACM Int. Conf. Wireless Sensor Netw. Appl. (WSNA), San Diego, CA, USA, 2003, pp. 151–159.

[5] W. Liu, R. Luo, and H. Yang, "Cryptography overhead evaluation and analysis for wireless sensor networks," in Proc. WRI Int. Conf. Commun. Mobile Comput. (CMC), Kunming, China, Jan. 2009, pp. 496–501.

[6] A. Bachir, M. Dohler, T. Watteyne, and K. K. Leung, "MAC essentials for wireless sensor networks," IEEE Commun. Surv. Tuts., vol. 12, no. 2, pp. 222–248, Second Quarter 2010.

[7] J. Kabara and M. Calle, "MAC protocols used by wirelesssensor networks and a general method of performance evaluation," Int. J. Distrib. Sensor Netw., vol. 2012, pp. 1–11, 2012, Art. ID 834784.

[8] P. Huang, L. Xiao, S. Soltani, M.W. Mutka, and N. Xi, "The evolution of MAC protocols in wireless sensor networks: A survey," IEEE commun. Surv. Tuts., vol. 15, no. 1, pp. 101–120, First Quarter 2013.

[9] W. Ye, J. Heidemann, and D. Estrin, "An energy-efficient MAC protocol for wireless sensor networks," in Proc. 21st Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), Los Angeles, CA, USA, 2002, vol. 3, pp. 1567–1576.

[10] T. Dierks; E. Rescorla (August 2008). "The Transport Layer Security (TLS) Protocol, Version 1.2" SSL: Intercepted today, decrypted tomorrow, Netcraft, 2013-06-25.

[11] A. Freier; P. Karlton; P. Kocher (August 2011). "The Secure Sockets Layer (SSL) Protocol Version 3.0".