Available online at: http://www.ijmtst.com/vol3issue11.html

International Journal for Modern Trends in Science and Technology

ISSN: 2455-3778 :: Volume: 03, Issue No: 11, November 2017

A Cross - Layered MAC Approach against Denial-of-Sleep attack in WSN

Pavan A C

Department of Computer Science, KLE's S. Nijalingappa College, Bangalore, Karnataka, India

To Cite this Article

Pavan A C, "A Cross-Layered MAC Approach against Denial-of-Sleep attack in WSN", *International Journal for Modern Trends in Science and Technology* , Vol. 03, Issue 11, November 2017, pp.-131-134.

ABSTRACT

Security contravention and energy consumption issues are vital in WSN (wireless sensor networks). Along with that the attacks like Denial-of-Sleep, Blackmail Attack, Wormhole Attack, etc., are affecting in the energy efficiency of the nodes in WSN. The transfer of data without any security might end-up in loss of data or data integrity. This paper untangles the security authentication provided for the message transfer at both source and destination ends using the cross-layered approach along with MAC algorithm and also symmetric encryption standards.

KEYWORDS: *Cross-Layer, MAC Algorithm, Denial-of-Sleep, Cryptography, Network Layer Security*

I. INTRODUCTION

A Wireless sensor network can be defined as a network of devices that can communicate the information gathered from a monitored field through wireless links. The data is forwarded through multiple nodes, and with a gateway, the data is connected to other networks like wireless Ethernet.

WSN is a wireless network (Fig 1) that consists of base stations and numbers of nodes (wireless sensors).These networks are used to monitor physical or environmental conditions like sound, pressure, temperature and co-operatively pass data through the network to a main location as shown in the figure below.

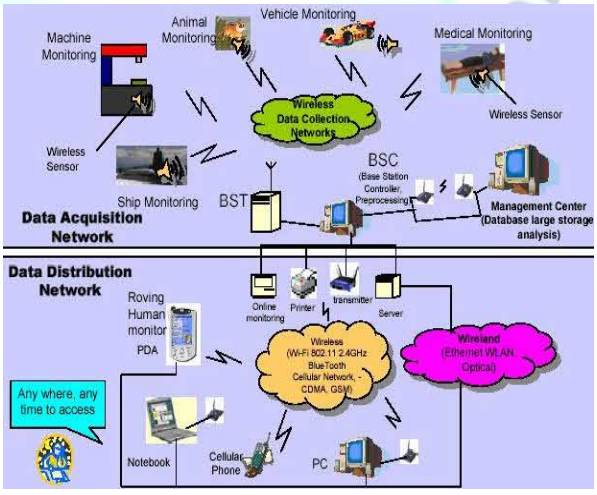

Fig 1 - Wireless Sensor Network

Characteristics of a WSN

The main characteristics of a WSN [2] include:

- Power consumption constraints for nodes using batteries or energy harvesting.
- Ability to cope with node failures and Ability to withstand harsh environmental conditions
- Scalability to large scale of deployment
- Ease of use
- Cross-layer design

Attacks in WSN

A classification of the attacks consists in distinguishing the passive attacks from the active attacks.

The passive attack is limited to listening and analyzes exchanged traffic. This type of attacks is easier to realize, and it is difficult to detect. Since, the attacker does not make any modification on exchanged information. The intention of the attacker can be the knowledge of confidential information or the knowledge of the significant nodes in the network, by analyzing routing information, to prepare an active attack.

In the active attacks, an attacker tries to remove or modify the messages transmitted on the network. He can also inject his own traffic or replay of old messages to disturb the operation of the network or to cause a denial of service. Among the most known active attacks, I can quote:

Tampering: It is the result of physical access to the node by an attacker; the purpose will be to recover cryptographic material like the keys used for ciphering.

Black Hole: A node falsifies routing information to force the passage of the data by itself, later on; its only mission is then, nothing to transfer, creating a sink or black hole in the network.

Selective Forwarding: A node play the role of router, in a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them.

Sybil Attack: "A malevolent device, taking multiple identities in an illegitimate way", attacker can use the identities of the others nodes in order to take part in distributed algorithms such as the election.

Blackmail Attack: A malicious node makes announce that another legitimate node is malicious to eliminate this last from the network. If the malicious node manages to tackle a significant number of nodes, it will be able to disturb the operation of the network.

Wormhole Attack: Attackers here are strategically placed at different ends of a network. They can receive messages and replays them in different parts by means of a tunnel.

Denial-of-Sleep: 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.

II. Existing System

Review A MAC [7]-[8] is produced based on the plaintext, and then the plaintext and MAC are together encrypted to produce a ciphertext based on both (Fig 2). 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 implementation has been proven to be strongly unforgettable by Krawczyk who showed that SSL/TLS was in fact secure because of the encoding used alongside the MtE mechanism [5].

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.

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 and reliable.

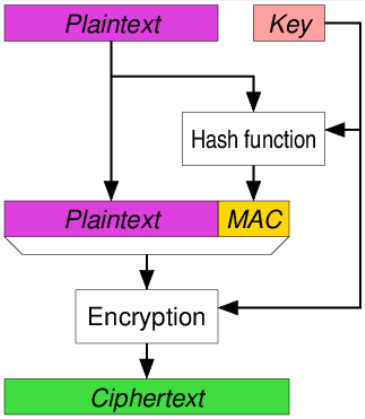

Fig 2 - MAC with Encryption

- 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.

III. Enhanced System

Use In order to improve the performance and to decrease the denial-of-sleep attack [1][3] of the above discussed scheme, the enhanced scheme that is a cross-layered MAC[9]-[10] encryption process is being used in which difficulty in decrypting or decoding the MAC is assured and in which even the techniques of network layer (OSI) is used for the interconnection purposes.

The cross-layer design stands as the most promising alternative to inefficient traditional layered protocol architectures. The message P (Fig 3) which is to be transferred from source node will be divided into equal blocks (P1, P2,.., Pn), if the last block (Pn) is lesser than the other equal blocks then to make it equal some random bogus text will be added. These blocks of message will be individually encrypted [4] [6] with the symmetric encryption key. After encryption, the whole encrypted message will be considered and a MAC will be created using the arbitrary length of message, MAC – algorithm and secret key. This MAC will be attached it to the encrypted message and a Cipher Text will be produced.

At the destination node, if the MAC is matched at the first level then the security check proceeds to decryption level else the message will be discarded and the destination node goes back to sleep. If MAC is matched then the process uses the symmetric key and decrypts. After decryption the blocks of message can be combined to form the original message.

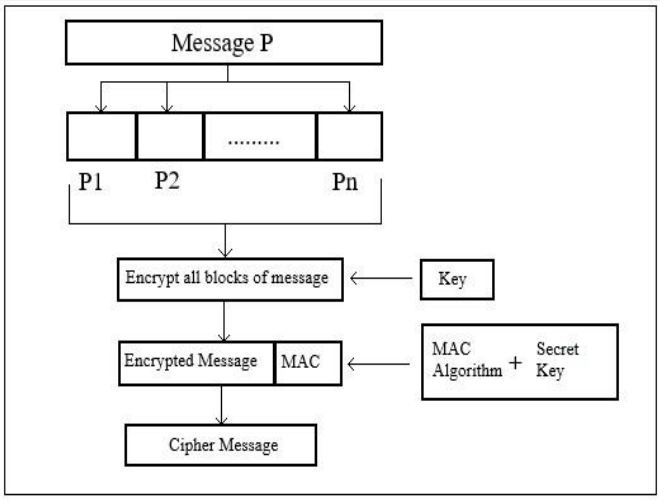

Fig 3 - Cross-Layered MAC

The duration of sleep time of the node will be increased and the energy of the node will not drain soon.

IV. Conclusion

In this paper, a cross-layered MAC protocol has been proposed to secure authentication, confidentiality and to save the energy in the nodes in a wireless sensor network. The involvement of cross-layered MAC with every message being divided into blocks then encrypt them and finally attach MAC gives more authenticity and also reduces wakeup time of the node. Hence the proposed cross-layered MAC protocol helps in improvement of 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]Pavan A C, "An Encrypted MAC for Authentication Process in WSN", IJMIST |Volume: 2 |Issue: 12 |December 2016.

[6] 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.

[7] 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.

[8] 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.

[9] Jun Yu and Xueying Zhang, "A Cross-Layer Wireless Sensor Network Energy-Efficient Communication Protocol for Real-Time Monitoring of the Long-Distance Electric Transmission Lines", Volume 2015 (2015), Article ID 515247.

[10]S. Jagadeesan and V. Parthasarathy," Cross-Layer Design in Wireless Sensor Networks", Department of Computer Science and Engineering, Chettinad College of Engineering & Technology, Karur, Tamilnadu, India