IJMTST | Volume: 2 | Issue: 05 | May 2016 | ISSN: 2455-3778

Secure & Energy Efficient Scheme against Denial-of-Sleep Attack in WSN

Mr. Pavan A C[1] | Mr. P Prasanna[2]

[1]PG Student, Department of CS&E, P.E.S College of Engineering, Mandya, Karnataka, India
[2]Assosiate Professor, Department of CS&E, P.E.S College of Engineering, Mandya, Karnataka, India

ABSTRACT

Security breaches and energy consumption issues are indispensable in WSN (wireless sensor networks). Considering attacks like Denial-of-Service (DoS) where not only the service is not provided but in addition to that unwanted power is also consumed."Denial-of-Sleep attack" (type of DoS attack) also results in unnecessary power exhaustion. This paper briefs about how energy consumption could be minimized in WSN by using MAC algorithm in a risk free manner.

KEYWORDS: *WSN, Key management in Network security, Denial-of-service attack, Denial-of-sleep attack, MAC protocol*

Copyright © 2015 International Journal for Modern Trends in Science and Technology
All rights reserved.

I. INTRODUCTION

Wireless sensor networks [1] 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 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 like:

- Wormhole attack
- Hello attack
- Sybil attacks
- Dos attacks

One such attacks thus being DOS (denial-of-service).In a DOS attack the legitimate user node is sent certain unwanted data to process sent by the attackers(in manner that data appears to be sent by a genuine user). This leads to not providing the actual service required to the user who requested the service.

Common DOS attacks:

- Buffer overflow
- Ping of death
- Smurf attack

Denial of sleep [2] is a special type of DOS attack. In denial of sleep attack the sensor nodes are kept awake to consume more energy. An attacker (anti-node) can send fake data packets to legitimate node of unprotected WSNs. Leading to unnecessary transmissions in a repeated manner. 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. Additionally, the fake node could also send fake ACK in order to give a mask of being genuine .This might lead the legitimate user node to provide all the services to fake node repeatedly. Hence more power consumed unnecessarily.

The data to be transmitted is basically encrypted either with keyed symmetric or asymmetric encryption algorithm. Symmetric algorithms are usually preferred in order to avoid the complicated computing and heavy energy consumption.

Encrypted data exhausts the battery. Additionally it becomes worse under Denial-of- Sleep attack. An anti-node can send the encrypted "gibberish" data to receiver. Receiver decrypts the data assuming it to be a genuine data. The power is being consumed as the receiver is decrypting the unwanted data until realizing the data is "gibberish". Also, the sensor node are awake while these process goes on.

In order to overcome these problems a simpler and fast mutual authentication scheme is required that if integrated with 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 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 when MAC is being integrated the energy consumption is reduced.

II. Existing Scheme

While setting up a network, a group of sensors are used and that sensors will be partition into clusters. Before the cluster formation is done the sensors should be authenticated and seen that the sensors are normal sensor nodes or the anti-nodes. The purpose of encryption is to ensure that only those nodes who are authorized to access data will be able to read it, using the decryption key. Some other nodes that are not authorized can be excluded, because they do not have the required key, without which it is impossible to read the encrypted information [3] [4].

A. Types of Encryption

a. Symmetric key encryption

In symmetric-key schemes, the encryption and decryption keys are the same. Communicating parties must have the same key before they can achieve secure communication.

b. Public key encryption

In public-key encryption schemes, the encryption key is published for anyone to use and encrypt messages. However, only the receiving party has access to the decryption key that enables messages to be read.

In this mechanism (Fig-1) of forming a cluster, a plaintext "*Hello*" message will be broadcasted. This text will be encrypted by the pre-distributed key. If the sensor cannot decrypt the received message successfully, the sender is said to be an anti-node and is it decrypts

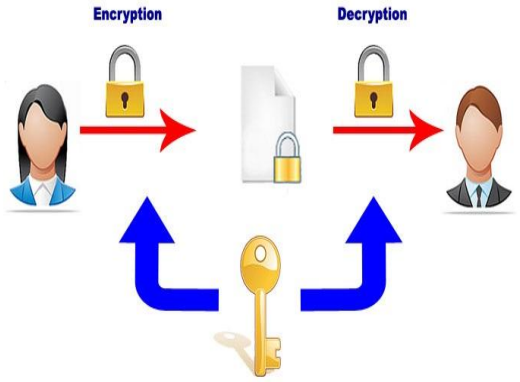

Fig-1: Encryption and Decryption Mechanism.

successfully, the sender is said to be a normal node. Thus, the normal nodes and the anti-nodes can be differentiated. Therefore, we keep on the network topology without anti-nodes in order to make the network safe.

This encryption and decryption is not much secure because the pre-distributed key can be successfully hacked at some point of time by the anti-node and it may start sending fake packets or it can edit the original message and send to the other nodes so that it will be awake for a longer duration and its battery will be drained soon. This process of keeping the sensor nodes awake for a long duration in known as Denial-of-Sleep.

Therefore, to reduce the energy consumption, to counter the power exhausting attacks, and enhance the performance of sensor nodes, a cross-layer design of secure scheme which integrates the MAC protocol can be used.

III. Enhanced Scheme

In order to overcome the drawbacks of the above discussed scheme, the enhanced scheme that is the MAC protocol is used.

A message authentication code (MAC) [5]-[9] is a short piece of information used to authenticate a message. A MAC algorithm, accepts as input a secret key and an arbitrary-length message to be authenticated, 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 tag 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 tag. The receiver then compares the first MAC tag received in the transmission to the second generated MAC tag. 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 (Fig-2).

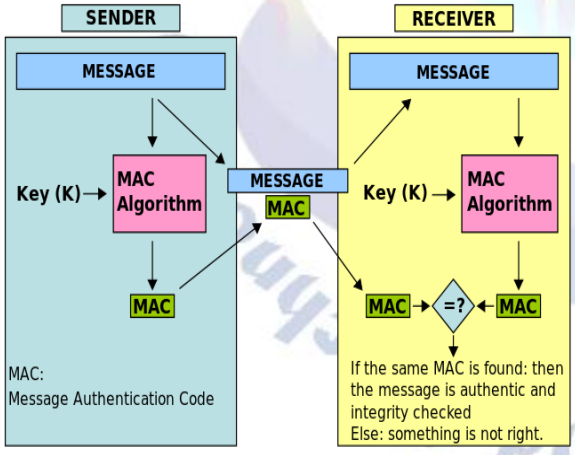

Fig-2: MAC functioning

MAC protocol 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.

IV. Conclusion

In this paper, an enhancement of MAC protocol has been proposed to save the energy in the nodes in a wireless sensor network. The main advantage of this protocol is less power exhaustion and usage of less energy. The involvement of MAC Algorithm and its tag in every message transfer gives more authenticity and also reduces wakeup time of the node. Hence the proposed MAC protocol helps to uphold the energy efficiency and power exhaustions of the wireless sensor networks

References

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

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

[3] 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.

[4] 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.

[5] 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.

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

[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] T. van Dam and K. Langendoen, "An adaptive energy-efficient MAC protocol for wireless sensor networks," in *Proc. 1st Int. Conf. embedded*