IJCES International Journal of Computer Engineering Science , Volume1 Issue2, November 2011
ISSN : 2250:3439
https://sites.google.com/site/ijcesjournal
http://www.ijces.com/

SECURED TRANSFER OF MESSAGES AGAINST MALICIOUS ATTACKS USING EFFICIENT ALGORITHM

F. EMILY MANOZ PRIYA
Department of Computer Science and Engineering
SASTRA University
Thanjavur, India-613402
sweetemblika@gmail.com

P.S. RAMESH
Asstt. Prof., Department of Information Technology
SASTRA University
Thanjavur, India-613402
ramesh@cse.sastra.edu

B. SANTHI
Prof., Department of Information and Communication Technology
SASTRA University
Thanjavur, India-613402
shanthi@cse.sastra.edu

Abstract**- Wireless Sensor Network (WSN) is a new class of networking technology .When we use sensor network in brutal environment, security is most important concern. The technology may face against various attacks. These attacks produce vulnerability against authentication, confidentiality and trustworthiness. This paper introduces an adaptive method for securing the transformation of messages in wireless sensor networks in the harsh environment. The light weight protocols are highly suitable for achieving authentication. The efficient matching algorithm will be used for performing packet matching and also it detects the malicious attack efficiently within the transformation of data. Finally, the encryption/decryption algorithm secures our original data.**

Keywords: ***wireless sensor network, security, light weight protocol, attack***.

I. INTRODUCTION

Wireless Sensor Network (WSN) are a fascinating and challenging area of research and a key enabler for new applications involving smart objects interacting with the physical environment. A wireless sensor network is a self-configuring network of small sensor nodes communicating among themselves using radio signals and deployed in large quantity to sends, monitor and understand the physical world. It contains nodes, where each node is connected to one sensor. The wireless sensor nodes are often called as Motes. Each motes has several fields: a radio transceiver (a transmitter and a receiver) with an antenna, a micro controller and a battery [1]. The main characteristics of WSN include low power consumption, ability to withstand hostile environmental conditions, mobility and scalability of nodes etc. Sensor nodes are specified in terms of their interface and components. A sensor network is composed of a gateway and a base station [2].

Sensor messages flow from the wireless sensors to the gateway where it is processed on the base station. Sensor controls the message flow from base station to gateway. Sensor nodes are normally low power and low cost devices. Therefore, we have to allow the nodes to use the available power carefully. The general architecture of the wireless sensor network [12] is shown in figure 1

.

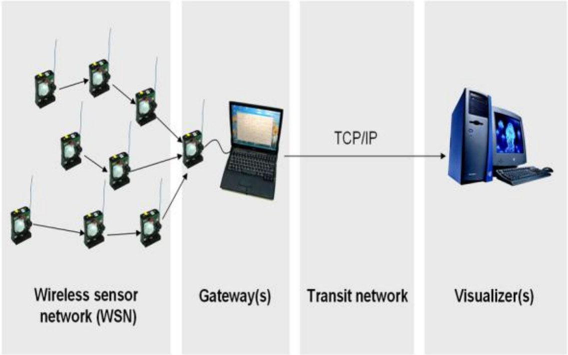

FIGURE 1: General structure of Wireless sensor network

In this diagram they show how the information is transferred from the sensor network to the gateway and then transferred to visualizer. For the message transaction within the wireless sensor network cryptography plays a vital role. It provides authenticity, confidentiality, and replay protection of exchanged messages.
Authenticity is very important in wireless sensor network to get reliable information. Confidentiality is to prevent the revelation of exchanged data for unauthorized parties. Replay protection prevents the attackers to record messages for replay attack. This paper introduces an adaptive method for securing our original data in the harsh environment. They achieve authentication, confidentiality and security. The paper is organized into four sections as follows: Section two discusses about security analysis. In that we identified various attacks and the requirements to overcome. In section three we describe the proposed adaptive method. In section four, we described the implementation of this adaptive method and section five concludes the paper with future direction.

II. SECURITY ANALYSIS

Generally, in real-time environment the network faces lot of attacks every day. The attacks are based on authentication, confidentiality and security. Here we see the important requirements for security in wireless sensor network [3, 4, 5]

Confidentiality

This can be achieved by encrypting the data. It means to assure that information contained in the data is only disclosed to users for which the data was intended.

Replay protection

To assure that an attacker is not able to record the message and use it successfully. Replay protection is achieved by adding unique information to each message. For example, add number of counters to the message and increment it.

1 Authenticity

Authentication is an important for many applications in sensor network [4].These are the first step to achieve the secured transformation of data. Adversary can easily inject the message, so a receiver of data able to conform that the data originates from the claimed sender.

1.1 Light weight protocol

The light weight protocol is a communication protocol that is designed with less complexity in order to reduce overhead in terms of more computations.

1.1.1 HB protocol

Over the past few years several protocols have been analyzed.
In 2001, Hopper and Blum are the two authors proposed a protocol called HB protocol [6].
The working of HB protocol as follows: The reader computes and sends the query to tag. Tag performs dot operation with query and secret key then XOR the result with noise value and computes result r and sends it to reader. Reader compares the values as r'= r and if so accept the process otherwise reject it.
This works well against passive attack but an active attack breaks its secureness. Hence an efficient protocol is needed to address this problem.

1.1.2 HB+ protocol

Juels and Weis (2005) modified HB against active attack from adversaries. The working of HB+ protocol is different from HB in two regards:

1. In HB+ the tag uses two secret keys instead of one.
2. The tag can produce a blinding vector and the remaining process is similar to HB.

This protocol is susceptible to active attack but it's not well secure against man- in-the-middle attack.

1.1.3 HB++ protocol

In 2006, Bringer modified HB+ protocol to secure against man-in-the-middle attack from adversaries in Gilbert (2005). It is called as HB++protocol. The working of HB++ is as follows:

The tag can initiate the process .It has four secret keys, and computes the value of z and z' and send it to reader. The reader recalculate the value of z and z' and check against the value which it was received. This protocol is also not highly suitable for man-in-the-middle attack in the harsh environment. The above algorithms much of the time fails in authentication. By considering that we are forced to go for a new authentication scheme.

1.2 Matching algorithm

Packet matching can be performed using Matching algorithm. In previous papers the authors revealed several methods like first match, Recursive Flow Classification (RFC), decision tree classifier[11] etc.

The main drawbacks in the previous approaches are time complexity, poor search time and space complexity. Apart from these basic drawbacks the malicious attack is also to be vulnerable to our original data.

The adaptive method deals with an efficient matching algorithm which will be used for detecting the malicious attack and transfer the message securely.

1.3 Encryption/Decryption

It's the process of transforming information (plain text) by using an algorithm and makes it unreadable (cipher text) to unauthorized users. In decryption side, it is the reverse process of encryption to make the encrypted information readable again. The conventional algorithm will be used for securing our original message.

III. PROPOSED METHOD

The data flow of the proposed method is shown below.

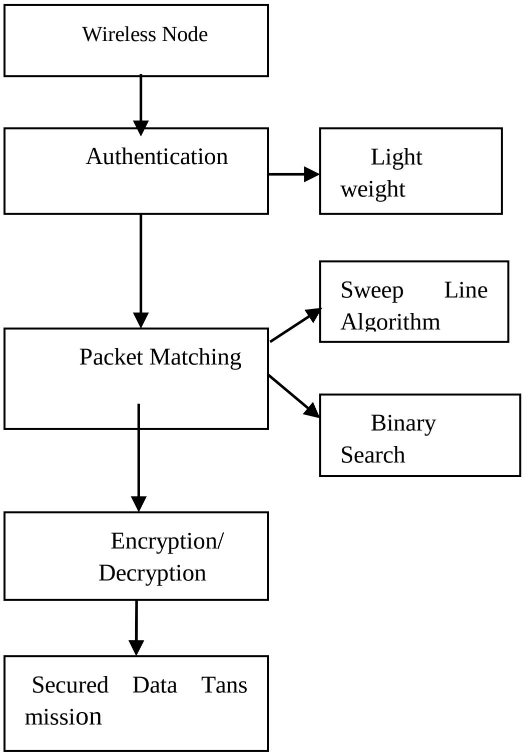

FIGURE 2: Proposed work flow

3.1 Authentication protocol

Wireless sensor networks are performed in low power energy sources, and having limited buffers for memory [8]. So we are using a Light weight protocol which provides more flexibility and high performance rate. In this paper the light weight protocol provides an authentication for efficient transaction. A modified HB++ protocol is an authentication protocol used it here which overcomes the man in middle attack and eliminates the vulnerability of the existing protocols. To achieve this, the protocol uses mutual authentication in both the sides.

3.2 Matching algorithm

The matching algorithm will be developed for performing packet matching efficiently. By providing an efficient rule sets the algorithm will detect the malicious attack easily and prevent the packet transaction.

By using this algorithm we will compute all intersecting pairs. They perform several operations[11] ,[7]like calculating the intersection points between two curves and list out the curves participating at each intersection point, also find whether an intersection point between any two curves exist or not.

Basically every packet has fields like source address, destination address, source port, destination port, PAN id etc.

Packets can be examined as per the prescribed rules by using Binary Search algorithm to detect the malicious attacks and to avoid unauthorized users access. The data structure of the packets having the fields to perform matching algorithm is shown below

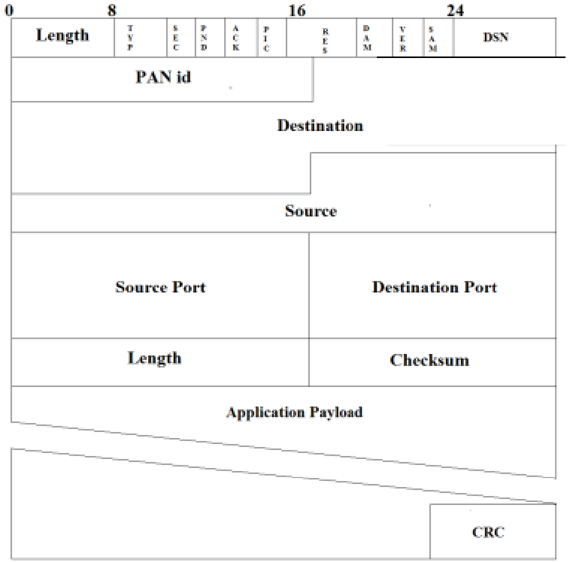

FIGURE 3: Packets data structure

3.3 Encryption/decryption algorithm

The algorithm for encryption/decryption process utilizes the conventional encryption algorithm. Here we considered Play fair cipher, because the algorithm has limited computing capability. But it produces cipher text that is more secure.

IV. PROPOSED ALGORITHM

The Architecture of the proposed method is shown below.

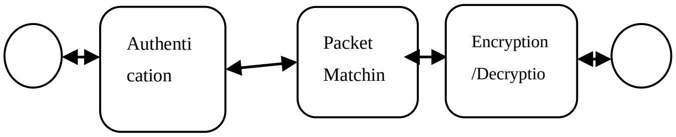

FIGURE 4: Architecture of Adaptive method

Step 1: The data will be transferred from the wireless node.
Step 2: By using the Light weight protocol the authentication for the transferred data will be checked out.
Step 3: Packet matching can be performed using matching algorithm and detect the malicious attack.
Step 4: If the data is efficient against malicious attack it will then encrypted using conventional algorithm
Finally secured data will be reached to another node.

V.CONCLUSION

In this paper, we presented a new approach for secured transformation of messages against various attacks. Our technique provides a modified version of authentication protocol has been developed for achieving authentication. Packet matching using efficient matching algorithm is to detect the malicious attacks for every transaction. The information is then subjected to encryption algorithm for physical transmission.

In future by implementing the proposed algorithm we have to perform the comparison of this algorithm with the existing algorithms in terms of high performance, power consumption, time complexity and space complexity.

REFERENCES

[1] Pawan Kumar Goel, Vinit Kumar Sharma "Wireless sensor network: a security model", IJSTM Vol. 2, Issue 2, April 2011

[2] Brian Carter and Ram Mohan Ragade "Message transformation services for wireless sensor network" (MTS-WSN)computer engineering and computer science, University of Louisville.

[3] Mohammed Mana, Mohammed Feham and Boucif Amar Ben saber "A Light weight protocol to provide location privacy in wireless body area networks" IJNSA,vol.3,No.2,March 2011.

[4] Xiuli Ren and Haibin Yu" Security mechanisms for wireless sensor networks", IJCSNS, Vol.6, No.3, March 2006.

[5] Mayank Saraogi "Security for wireless sensor networks "Department of Computer science, University of Tennessee, Knoxville.

[6] Julien Bringer, Herv´e Chabanne and Emmanuelle Dottax" HB++: a Lightweight Authentication Protocol Secure against Some Attacks" Sagem Defense Securite Avenue du Gros Chene 95610 Eragny sur Oise, France.

[7] www.cgal.org : 2Dsweep line of planar curves.

[8] Prashant Agarwal, Tan sun teck andAnandaA.L"A light weight protocol for wireless sensor networks", Center for internet research, school of computing. National university of Singapore,Singapore.

[9] Xuefei Leng, Mayes and Markantonkis "An improvement on HB-MP protocol", Dept of math's, university of London, May 2008.

[10] Roi Saltzman Adi Sharabani" Active man in middle attacks" A security advisory, A white paper from IBM Rtional application security group,febuary 2009.

[11] Dmitry Rovniagin and Avishai Wool,"The Geometric Efficient Packet Matching for Firewalls",IEEE transaction on dependable and secure computing,Vol.8,No.1,Jan-Feb 2011.

[12] Carsten Buschmann, Dennis Pfisterer and Stefan Fischer, "Spyglass: A Wireless sensor Networkvisualizer",Institute for Telematics, University of Lubeck.

[13]http://openwsn.berkeley.edu