ENERGETIC KEY FOR PROTECTED COMMUNICATION IN WIRELESS SENSOR NETWORK

S.Selvi[1], G.Sankareeswari[2], Vidhyalakshmi[3]

[1, 2]Assistant Professor, CSE, [3]Assistant Professor, IT, Sri Vidya college of Engineering and Technology, Tamilnadu, India
sselvi201987@gmail.com, sankariram90@gmail.com, vidhyarajme@gmail.com

Abstract

The enormous world wide web and its application of sending data have caused a tremendous increase in stolen or attach the false data with the original data while sending from one node to another node through the intermediate nodes for that we have to securely send the data from source to destination. Virtual energy based encryption and keying has introduced an effective solution to the problem of detection of false data over the network. In the virtual energy based encryption and keying technique we introduced an concept is one time dynamic key (i.e.).The data which is to be send from source to destination is encrypted using the secret key and the encryption algorithm. The secret key is generated, one time dynamic key is employed for one packet only and different keys are used for the successive packets. Virtual energy based encryption and keying is a secure communication framework the data to be send is encrypted using the AES algorithm. The intermediate nodes are verified the incoming packets if the incoming packet is false packet injected in the network by the malicious outsiders those packets are detected and dropped otherwise the packet is forwarded to the next node. In the virtual energy based encryption and keying there are two modes of operations they are virtual energy based encryption and keying-I and virtual energy based encryption and keying- II. In the virtual energy based encryption and keying-I each node monitors their neighbor node and in the virtual energy based encryption and keying-II each nodes randomly choose the nodes and monitors those nodes. These two modes of operation monitor the nodes and detect the false packet and drop those false packets.

Keywords: *Wireless sensor networks, security, one time dynamic key*

----------***----------

1. OBJECTIVE

When the important data's are send from one node to another node through the wireless sensor networks some false packets are attached with the original data by malicious outsiders. For that we have to detect and drop those packets. Successful implementation of this project solves those above problems.

2. INTRODUCTION

The explosive growth of networks offers enormous benefits in terms of increased exchange of information. There are two basic key management schemes for WSNs: fixed and active. In fixed key management schemes, key management functions (i.e., key generation and distribution) are handled statically. That is, the sensors have a permanent number of keys loaded either prior to or shortly after network deployment. On the other hand, active key management schemes perform keying functions (rekeying) either periodically or on demand as needed by the network. The VEBEK structure based on the two types of operational modes. The VEBEK means Virtual Energy based encryption and key. They are VEBEK-I, VEBEK-II[1]. These modes are suitable for different scenarios. VEBEK-I nodes contain only one hop. VEBEK-II contains full of downstream nodes. We easily analyze the VEBEK's possibility and performance in two ways. They are 1.Analytic process 2.Simulations.These two processes based on the reception module and sink. Performance analysis also checks the routing path from source to sink. It also analyzes the performance of the nodes. During the rescue of the data the path is stable or fixed. VEBEK [1] is a secure process because the sensitive's data's are encoded using permutation code through AES encryption process. The same key never appears for the same data. It increases the packet size of the sending data and it avoids the unnecessary data in an efficient manner. Many encryption algorithms used to send only 40 bits of message, through wireless network. So the message is not fully secured that is the level of security is reduced. But the VEBEK[1] overcome these types of problems. It has the ability to transmit 64 bit data. It provides full security to the whole message. It encrypts the whole data. The key generation based on the 8 or 10 digits. Here sensor is used in between the process of the crypto module and packet transmission. The virtual energy of the sensor is dynamically changed through AES encryption mechanism.

3. WIRELESS SENSOR NETWORK (WSN)

A wireless sensor network (WSN) consists of spatially spread autonomous sensors to monitor physical or natural situation, such as temperature, sound, pressure, etc. and to freely pass their data through the network to a main location. The

expansion of wireless sensor networks was forced by military applications such as battleground observation; today such networks are used in many industrial and consumer applications.

The WSN is built of "nodes" – from a little to a number of hundreds or even thousands, where each node is related to one (or sometimes several) sensors. Each such sensor network node has usually several parts: a radio transceiver with an interior antenna or link to an outside antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy resource, usually a battery or an surrounded form of energy harvesting. Size and cost constraint on sensor nodes outcome in equivalent constraints on resources. The topology of the WSNs can differ from a easy star network to an superior multi-hop wireless mesh network. The transmission technique between the hops of the network can be routing or flooding.

3.1 Platforms

3.1.1 Software

Energy is the scarcest source of WSN nodes, and it determines the life span of WSNs. WSNs are proposed to deployed in vast number in a mixture of environments, jointly with distant and destructive regions, where ad hoc communications are a key component. For this basis, algorithms and protocols require to address the following issues:

- Lifetime maximization
- Robustness and fault tolerance
- Self-configuration

Lifetime maximization: Energy/Power utilization of the sensing device should be minimized and sensor nodes should be energy efficient since their partial energy resource determines their lifetime. To save power the node should shut off the radio power supply when not in use.

3.1.2 Hardware

One main challenge in a WSN is to generate low cost and small sensor nodes. There are an growing number of small companies producing WSN hardware and the commercial circumstances can be compared to home computing in the 1970s. Many of the nodes are still in the study and growth stage, mainly their software. Also natural to sensor network acceptance is the use of very low power methods for data achievement.

In many applications, a WSN communicates with a Local Area Network or Wide Area Network during a gateway. The access acts as a link between the WSN and the other network.

4. EXISTING SYSTEM

Some of the drawbacks occurred in the existing system. RC4 algorithm is used. In that security is low and only 40 bit is transmitted. It follows simple and ancient techniques. It will encrypt the stream of bytes using Stream-Cipher technology.

5. PROPOSED SYSTEM

The complete project deals with the key process of WSN's. WSN's is a technique to verify the data or message line by line and give up the fake packets. It also maintain the condition of the sensor. Here the proposed system uses AES algorithm instead of using the RC4 algorithm. The proposed system has some merits compared with the existing system. The proposed system uses the recent and superior encryption technique. The block of the data encrypted using the block-cipher technique. Using WSN 64 bits of data are transmitted. Based on the encryption technique the whole process is completely secured.

6. OPERATIONS

The VEBEK contains the following four operations:

1. Virtual energy based keying module.
2. Encryption.
3. Packet transmission and reception module.
4. Performance analysis module.

6.1. Virtual Energy Based Keying Module

The virtual energy-based keying process involves the creation of active keys. Opposite to other active keying schemes, it does not exchange extra messages to create keys. A sensor node computes keys based on its enduring virtual energy of the sensor. The key is then feed into the next module.

6.2. Encryption

The encryption module in VEBEK employs a simple encoding process, which is basically the process of variation of the bits in the packet according to dynamism created variation code generated via AES encryption technique. The encoding is a simple encryption mechanism adopted for VEBEK. However, VEBEK's elastic architecture allows for adoption of stronger encryption mechanisms.

6.3. Packet Transmission and Reception Module

The Packet transmission and reception module handles the process of sending or receiving of encoded packets along the path to the sink. And also get the acknowledgement from the receiver side to conform the delivery status of the node.

6.4. Performance Analysis Module

In the performance analysis module we are going to consider the false injection and eavesdropping of messages from an outside malicious node. And also check a routing path is established from the sources in the event region to the sink. We assume that the path is permanent during the delivery of the data and the route setup is secure. So the sensor network is thickly occupied generate reports for the same event. This module will help to analyze the performance of the nodes.

7. ARCHITECTURE

In our general architecture of implementation we use the concept of AES encryption algorithm.

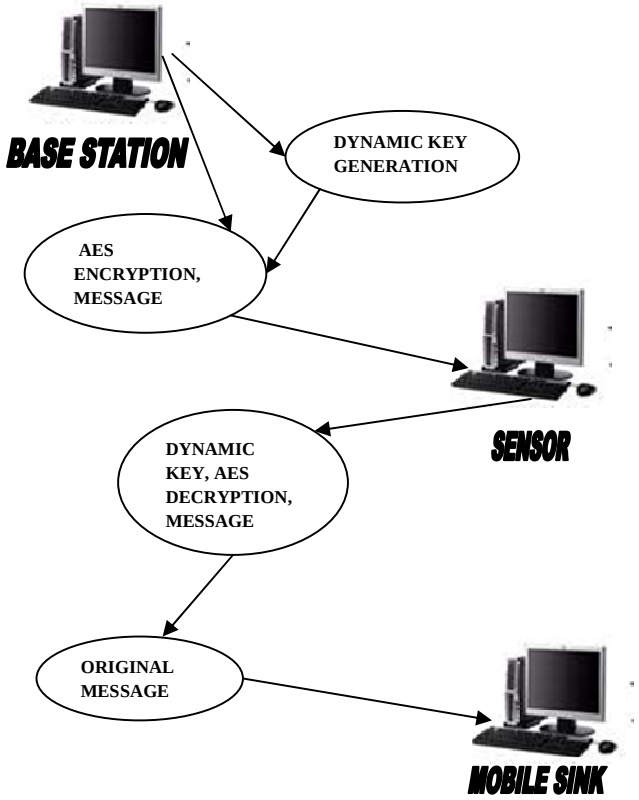

Fig 1. General architecture for Key management scheme for wireless sensor networks

The dynamic key is generated from the base station. (i.e.) one time dynamic key is employed for one packet only and different keys are used for the successive packets. The original message is encrypted using the AES encryption algorithm and with the secret key (dynamic key).Then the encrypted message is given to the sensor.

In the sensor, it will decrypt the message and verify the packets whether the message is came from correct source or it is send by the malicious outsider. If the message is send by the malicious outsider it is detected and dropped by the sensor. Otherwise it is forwarded to the mobile sink i.e. to the receiver.

8. ALGORITHM

```
1.  Cipher (byte in[4*Nb], byte out[4*Nb], word
    w[Nb*(Nr+1)])
2.  begin
3.  byte state[4,Nb]
4.  State = in
5.  AddRoundKey (state, w)
6.  for round = 1 step 1 to Nr-1
7.  SubBytes(state)
8.  ShiftRows(state)
9.  MixColumns(state)
10. AddRoundKey(state, w+round*Nb)
11. end for
12. SubBytes(state)
13. ShiftRows(state)
14. AddRoundKey(state, w+Nr*Nb)
15. out = state
16. end
```

AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. AES is a adjustment of Rijndael which has a preset block size of 128 bits, and an input size of 128, 192, or 256 bits. By difference, the Rijndael arrangement per se is specified with block and key sizes that may be any multiple of 32 bits, both with a least of 128 and a greatest of 256 bits.

AES operates on a 4×4 column matrix of bytes, termed the position, although some versions of Rijndael have a larger chunk size and have additional columns in the position. Most AES calculations are done in a special finite field.

The input size used for an AES cipher specifies the number of repetitions of change rounds that change the input, called the plaintext, into the last output, called the cipher text.

Each round consists of several processing steps, each containing four related but dissimilar stages, as well as one that depends on the encryption input itself. A set of reverse rounds are applied to convert cipher text back into the unique plaintext using the same encryption key.

High-level Description of the Algorithm

1. KeyExpansion—round keys are resulting from the cipher key using Rijndael's input plan. AES requires a separate 128-bit round key block for each round plus one more.

2. InitialRound
    1. AddRoundKey—each byte of the position is combined with a block of the round key using bitwise xor.
3. Rounds
    1. SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
    2. ShiftRows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
    3. MixColumns—a mixing operation which operates on the columns of the position, merge the four bytes in each column.
    4. AddRoundKey
4. Final Round (no MixColumns)
    1. SubBytes
    2. ShiftRows
    3. AddRoundKey.

CONCLUSIONS

This paper describes the concept of One time dynamic key structure used for only one packet and variant keys are used for the successive packets. It protects the entire data against the unauthorized users or hackers. It protects the data by generating different keys for each time and it shows the path and size of the file in the text box. It helps to send the message in highly secure manner.

REFERENCES

[1]. Arif Selcuk Uluagac, Student Member, IEEE, Raheem A. Beyah, Senior Member, IEEE,Yingshu Li, Member, IEEE, and John A. Copeland, Fellow, IEEE" VEBEK: Virtual Energy-Based Encryption and Keying for Wireless Sensor Networks" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 7, JULY 2010

[2]. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci,"Wireless Sensor Networks: A Survey," Computer Networks,vol. 38, no. 4, pp. 393-422, Mar. 2002.

[3]. C. Kraub, M. Schneider, K. Bayarou, and C. Eckert, "STEF: A Secure Ticket-Based En-Route Filtering Scheme for Wireless Sensor Networks," Proc. Second Int'l Conf. Availability, Reliability and Security (ARES '07), pp. 310-317, Apr. 2007.

[4]. Z. Yu and Y. Guan, "A Dynamic En-Route Scheme for Filtering False Data Injection in Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 1-12, Apr. 2006.

[5]. F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-Route Filtering of Injected False Data in Sensor Networks," IEEE J. Selected Areas in Comm., vol. 23, no. 4, pp. 839-850, Apr. 2005.

BIOGRAPHIES

Ms. S. Selvi Working as a assistant professor in Sri Vidya College of Engineering and Technology . She has completed Master of Engineering in computer science and Engineering at Coimbatore Institute of Engineering & Technology,Coimbatore. Her under graduation in computer science and Engineering at PSR Engineering College,Sivakasi.Her area of interest is Network Security.

Ms. G. Sankareeswari Working as a assistant professor in Sri Vidya College of Engineering and Technology . She has completed Master of Engineering in computer science and Engineering at Mohamed Sathak Engineering College at Kilakarai. Her under graduation in Information Technology at Raja College of Engineering Technology, Madurai. Her area of interest is Cloud Computing and Networks security.

Ms. R. Vidhyalakshmi Working as a assistant professor in Sri Vidya College of Engineering and Technology . She has completed Master of Engineering in computer science and Engineering at P.S.R Engineering College at Sivakasi. Her under graduation in Information Technology at P.S.R Engineering College at Sivakasi. Her area of interest is Cloud Computing and Networks security.