An Efficient users Authentication and Secure Data Transmission of Cluster Based Wireless Sensor Network

Korada Kishore Kumar[1], Konni Srinivasa Rao[2]
Final M.Tech Student[1], Asst.professor[2]
[1,2]Dept of CSE, Sarada Institute of Science, Technology and Management (SISTAM), Srikakulam, Andhra Pradesh

Abstract

The main goal of wireless sensor network is to transfer data in a secure manner. So that in the wireless sensor sharing of information from source node destination node in securely. By transferring information in securely by implementing cryptography techniques. To transfer data from source node to destination by using routing. In the generation of routing we are face the problem of time complexity for finding distance between source node to destination node. By overcome that problem we can implementing clustering on nodes in a wireless sensor network. In this paper we are implementing mainly three concepts for authentication of users, clustering of nodes in network, encryption and decryption of transferred message. By performing authentication process we are implementing polynomial key xor based signature algorithm. After completion of authentication process the server will performing clustering of nodes in network. By performing clustering process the server will use nodes distance clustering algorithm. Take those clustering nodes data and find out destination nodes for transferring information. Before transferring information from source node to destination node we are using binary sequence message integrity protocol. By implementing those concepts we can improve routing process and also provide more security of transferring data through wireless sensor network.

.

Keywords

cryptography techniques, hash function, security, encryption and decryption Signature, clustering process.

I. INTRODUCTION

Wireless sensor network (WSN) is widely considered as one of the most important technologies for the twenty-first century [1]. In the past decades, it has received tremendous attention from both academia and industry all over the world. A WSN typically consists of a large number of low-cost, low-power, and multifunctional wireless sensor nodes, with sensing, wireless communications and computation capabilities [2,3]. These sensor nodes communicate over short distance via a wireless medium and collaborate to accomplish a common task, for example, environment monitoring, military surveillance, and industrial process control [4]. The basic philosophy behind WSNs is that, while the capability of each individual sensor node is limited, the aggregate power of the entire network is sufficient for the required mission. In many WSN applications, the deployment of sensor nodes is performed in an ad hoc fashion without careful planning and engineering. Once deployed, the sensor nodes must be able to autonomously organize themselves into a wireless communication network. Sensor nodes are battery-powered and are expected to operate without attendance for a relatively long period of time. In most cases it is very difficult and even impossible to change or recharge batteries for the sensor nodes. WSNs are characterized with denser levels of sensor node deployment, higher unreliability of sensor nodes, and sever power, computation, and memory constraints. Thus, the unique characteristics and constraints present many new challenges for the development and application of WSNs.

Wireless sensor network consist of distributed autonomous devices, called sensors which monitor physical conditions of environment for support of different types of applications. As Sensors have the ability to sense data, process and forward data to neighbor sensor node. For these purpose sensors use their resources energy, storage and computation capacity [5]. The major concern of sensor network is network performance and scalability. Network performance is achieved by increasing network lifetime/optimizing energy. Scalability is measured such that network performance should be constant with increasing network nodes. Hence wireless sensor network works as one in association as a network towards achieves a frequent goal of sensing a physical parameter over a huge geographic region with energy optimization [6]. In wireless sensor networks sensor nodes sense data, process data then forward to the Base station. For efficient processing routing algorithms are responsible to select efficient path and forward data to base station and increase network lifetime also. Routing algorithms for sensor

network should be QoS efficient. These QoS requirements include end-to-end delay guarantee, bandwidth resource, energy consumption, loss packet ratio and the lifetime of network, etc. In wireless sensor networks field, there exist some algorithms to research the routing problem. But most of all routing algorithms try their best to consider the energy consumption because the energy is a scare resource to wireless sensor node.

The ability of Wireless Sensor Networks (WSN) to detect and observe any physical phenomenon has made them very popular in today's era. The low power devices called sensor nodes collaborate to perform any given task and constitute a network called a sensor network. The nodes are equipped with sensing and processing capabilities and they sense any physical phenomenon such as temperature, pressure etc. and send this data to a base station (BS) or sink using single hop or multi hop communication. Multi hop communication is preferred over single hop as it reduces energy consumption. WSN is quite different from traditional adhoc and wired networks in terms of low energy, limited resources and their applications. The protocols and algorithms developed for these networks cannot be directly applied to WSN. Researchers need to consider energy and resource constrained nature of WSN while designing protocols. Sensor networks work in a wide range of applications like military, surveillance, health monitoring etc. Depending upon the application, they can be deployed in deterministic or a random manner. Some applications are used in hostile environments and nodes are deployed in these environments in an uncontrolled manner and it is not possible to change the battery of nodes in these environments. So in case of random deployment nodes have to reconfigure themselves and large number of nodes may be deployed to overcome battery issues. In other applications where deterministic deployment is possible, position and placement of nodes is determined prior to deployment in a controlled manner. Node placement is a very important step and proper node placement can result in more energy efficient solutions. Different strategies for node placement are discussed in [7]. After deployment, coverage and connectivity are important issues to be considered, so proper coverage depending upon the application should be maximized and connectivity should be maintained. Different methods and issues related to coverage are discussed in [8, 9]. As a sensor network is used in hostile environment, energy conservation becomes an important issue and scalability problem also arises. Use of clustering overcomes these issues by incorporating network aggregation and processing which further reduces amount of data to be sent and overcomes several challenges related to resource constrained nature of WSN

II. RELATED WORK

A Survey on Clustering Routing Protocols in Wireless Sensor Networks has been presented by Xuxun Liu in [10]. Clustering attributes have been categorized into cluster characteristics, cluster-head characteristics, clustering process and entire proceeding of the algorithm. A more comprehensive and critical survey of prominent clustering routing protocols for WSNs compared with previous work is presented. Different clustering routing algorithms for WSN in detail based on the classification of different algorithmstages, and their characteristics with advantages and disadvantages has been discussed.

Many works investigate this problem under various metrics and assumptions [11]. Arora et al. defined the system models and examine the intrusion detection problem in the context of a security scenario called A Line in the Sand by quantitatively analyzing the effect of network unreliability on application performance, assuming that the nodes are deployed with uniform density and subject to some local variations. Wang et al. [11] provide a unifying approach in relating the intrusion detection probability with respect to various network settings. They assume a random WSN with uniform node density and disk sensing model. Given an intruder that moves on a straight line, they derived the probability of detecting the intruder within a predefined distance. Based on a Poisson approximation of uniform sensor distribution, Wang et al. [12] analytically compared its performance to that of a Gaussian distributed WSN. Dousse et al. analyze the delay in intrusion detection, which is defined as the first contact time when the intruder hits the sensing range of a sensor belonging to the large sensor cluster. The key result in this work demonstrates a significant gap in the delay between the first contact time with a sensor and the first contact time with the large connected sensor cluster in a random WSN with uniform node density. Cao et al. derive analytical formulas for detection probability and the mean delay in a uniformly distributed WSN with tunable system parameters such as node density and sleep duty cycle. They consider both stationary intruder and mobile intruder that moves on a straight line at a constant speed. Lazos et al. [13] formulate the intrusion detection problem as a line-set intersection problem and derive analytic formulas of the intrusion detection probability until a target is detected in a random WSN with uniform node density. Most recently, Medagliani et al. [14] propose an engineering toolbox which contains a set of models for describing the probability of missed detection, the alert transmission latency, and the energy consumption to optimally configure a given WSN for a variety of quality of service requirements. This work adopts and extends the analytical framework used in [13] and assumes a linear intrusion path. Different from adopting a linear path, Wang et al.

[15], [16] propose a Sine-curve mobility model that can simulate different intrusion paths by adjusting its features and examine the interplays between network settings and the intruder mobility patterns. It is found that an intruder following a Sine-curve intrusion path can be more beneficial than following a straight-line path as the probability of being detected can be decreased, however with a side effect of reducing intrusion progress toward the destination to some extent. In other words, the straight-line path provides the maximum possible intrusion progress toward the destination when the moving distance is fixed.

III.PROPOSED SYSTEM

In this paper we are propose mainly three concepts for the authentication of nodes, performing clustering of nodes and security of transferring data. by implementing those concepts we can improve efficiency of wireless sensor network and also provide more security of transferring data. In this paper we are performing authentication of nodes we are using identity based polynomial signature algorithm. After performing the authentication using the mid-point clustering algorithm we perform the clustering of nodes in the wireless sensor network. After completion of clustering of nodes we are performing data transferring from source node to destination node. Before transferring data the source node will convert the data into unknown format. The conversion data to unknown format we are using the bit sequence message integrity protocol. After that converting the source node will send the cipher data to destination. The destination node will retrieve cipher data and send the decryption process of bit sequence message integrity protocol. After performing the decryption process we can get original plain format message. The implementation procedure of each concept is as follows.
Nodes initiation process:

In this module we are generating communication process of each node to server. Before performing all three concepts we are generate communication of each node. The communication process can be done by sending ip address and port number of server. After sending request the server will accept the request and generate communication between nodes. Before performing the communication the server will generate points (X_i,Y_i) for each node and send to the each node in a wireless sensor network.

A) *Polynomial Key Xor based signature algorithm:*

After completing communication process the server will choose one shared value (S). the server will divide shared value into six parts, where any three sub parts is sufficient for the re construing of shared value. The server will randomly choose a and b using those value the server will generate following polynomial equation.

$$f(x) = S+bx+ax^2$$

after generating polynomial equation the server will generate six points to satisfy the polynomial equation. The server will generate D1,D2,D3,D4,D5 and D6 points and send the any three points to individual client. The client will retrieve those three points again will generate polynomial equation and get the shared value. Using that shared values each client will generate signature and send to server. The generation of signature can be done by using message digest five hash function. Before generating signature each client will perform the following steps.

$$\text{Xor value} = S_i \wedge U_i$$

$$\text{Sig} = H(\text{xor value})$$

Here H is one way hash function and generates the hash code. After generating hash code each client will send to server. The server will retrieve those signature from the clients we can perform verification process. After performing verification process that status will send to individual users.

B) *Nodes Distance clustering algorithm:*

After completion of authentication status the server will perform the clustering of nodes. The clustering of nodes can be done by implementing mid-point clustering algorithm. The implementation of mid-point clustering algorithm is as follows.

1. The server will retrieve all points of individual clients.
2. After getting those points the server will find out difference between source nodes to other nodes by using the following formula.
   diff= X1- X2/Y1-Y2
3. After finding the difference of each node we can cluster all nodes.
4. Before performing clusterization the server will randomly choose the centroids by giving the number clusters.
5. After that the server will find out distance of centroid nodes to other nodes.
6. Based on the distance we can get all nodes into clusters.

C) *Binary sequence message integrity protocol:*

By using this protocol we can perform the encryption and decryption of transferring message. After completion of clustering of nodes the source will send the data to destination node. Before

transferring data from source node to destination node the source will encrypt the transferring message and send to destination node. Before transferring message to destination node the server will find out which cluster contain the destination node. After that the server will send the message to destination node. The implementation process of encryption and decryption of bit sequence message integrity protocol is as follows.

Encryption process:

Declaration of variables:

```
char en[32]= { 0xe2, 0x12, 0xa6, 0x8e, 0x9a, 0xf1, 0x2e, 0x3f,0xe7, 0xca, 0xb1, 0x4e, 0x58, 0x83, 0x3a, 0xe4, 0x13, 0x23, 0x65, 0xae, 0x8e, 0xd4, 0x9d, 0x35, 0x90, 0x3a, 0x63, 0x8e,0x2a, 0x14, 0x54, 0xa2};
char mm[8];
char mic_ch;
char seq_1,seq_2;
cahr mic;

void Encrypt(unsigned char * info, int *len)
{
// info: MSG data;
// len : the length of MSG data
seq_1 = 0; seq_2 = 0;
while( seq_1+seq_2 == 0)
{
seq_1 = rand() % 16; //randomly generating number.
seq_2 = rand() % 16; //randomly generating number.
}
seq_2 +=16;
for (int i = 0; i< 8; i++)
{ // to produce the encryption table
mm[i] = en[(seq_1+ i) %32] ^ en[(seq_2 + i) %32];
}
mic_ch = 0x5a;
char info_m[ MAXLENGTH];
for (i=0; i < *len; i++)
{
mic_ch = mic_ch ^ info[i];
info_m[i] = info[i] ^ mm[i%8];
mm[i%8] = mm[i%8] ^ en[(seq_1 +8+ i) %32]^ mic_ch;
mic +=info_m[i] ^ en[(seq_1+i)%32] ;
}
info[0] = (seq_1<<4) + seq_2 - 16; // the key bit sequence
info[1] = mic; // the MIC
for (i=0; i < *len; i++)
{
info[i+2] = info_m[i];
}
*len += 2;
}
```

After performing the encryption process the source node will send the cipher format data to destination node. The decryption process bit sequence message integrity protocol is as follows.

Decryption Process:

The destination node will retrieve the cipher format data and perform the decryption process will get the original message.

```
bool Decrypt(char * info, int *len)
{
 char step_mic;
seq_1 = (info[0]>>4) & 0x0f;
seq_2 = (info[0] & 0x0f) + 16;
step_mic = info[1];
mic = 0;
for (int i = 0; i< 8; i++)
{
mm[i] = en[(seq_1 + i) %32]^ en[(seq_2 + i) %32];
}
mic_ch =0x5a;
for (i=0; i< *len -2 ; i++)
{
mic +=info[i+2] ^ en[(seq_1+i)%32];
info[i] = info[i+2] ^ mm[i%8];
mic_ch = mic_ch ^ info[i];
mm[i%8] = mm[i%8] ^ en[(seq_1 +8+ i) %32]^ mic_ch;
}
if (mic != step_mic) return false;
*len -= 2;
info[*len] = 0;
return true;
}
```

So that by implementing those concepts we can improve efficiency of wireless sensor network and also provide more security of transferring message.

IV. CONCLUSIONS

In this paper we first review the security of transferring message in the wireless sensor network. By provide security of transferring message we are one of the protocol for message encryption and decryption. Before transferring message each node will perform the authentication process and send the message to destination node. The process of authentication can be done by using polynomial key xor signature algorithm. After completion of authentication the server will perform the clustering process on nodes. By implementing the clustering process we can group minimum distance nodes into single group. In this paper we are using Nodes Distance clustering algorithm for the generation of clusters. After that the source node will encrypt the transferring message and send to destination node. The destination node will retrieve the cipher format message and decrypt the message. By performing decryption process the destination node will get original message. The encryption and decryption of message can be done Binary sequence message

integrity protocol. By implementing those three concepts we can enhance efficient of wireless sensor network and also improve security of transferring message.

REFERENCES

[1] "21 ideas for the 21st century", Business Week, Aug. 30 1999, pp. 78-167.

[2] S.K. Singh, M.P. Singh, and D.K. Singh, "A survey of Energy-Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks", International Journal of Advanced Networking and Application (IJANA), Sept.–Oct. 2010, vol. 02, issue 02, pp. 570–580.

[3] S.K. Singh, M.P. Singh, and D.K. Singh, "Energy-efficient Homogeneous Clustering Algorithm for Wireless Sensor Network", International Journal of Wireless & Mobile Networks (IJWMN), Aug. 2010, vol. 2, no. 3, pp. 49-61.

[4] Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE, 2009.

[5] Ying Liao, Huan Qi, and Weiqun Li "Load-Balanced Clustering Algorithm With Distributed Self-Organization for Wireless Sensor Networks" IEEE SENSORS JOURNAL, VOL. 13, NO. 5, MAY 2013.

[6] I.Bekmezci and F. Alagöz, "Energy efficient, delay sensitive, fault tolerant wireless sensor network for military monitoring," Int. J. Distrib. Sensors Netw., vol. 5, no. 6, pp. 729–747, 2009.

[7] M.Younis, K. Akkaya, "Strategies and techniques for node placement in wireless sensor networks: A survey", Ad Hoc Networks 6 (4), pp.621-655, 2008.

[8] R.Mulligan, H.M. Ammari, "Coverage in Wireless Sensor Networks: A Survey", Network Protocols and Algorithms, ISSN 1943-3581, 2010.

[9] J.Hill, M. Horton, R. Kling, L. Krishnamurthy, ―The platforms enabling wireless sensor networks‖, Communications of the ACM, pp. 41 – 46, 2004.

[10] Xuxun Liu, ―A Survey on Clustering Routing Protocols in Wireless Sensor Networks‖, Sensors, 2012.

[11] Y.Wang, X. Wang, B. Xie, D. Wang, and D.P. Agrawal, "Intrusion Detection in Homogeneous and eterogeneous Wireless Sensor Networks," IEEE Trans. Mobile Computing, vol. 7, no. 6, pp. 698-711, June 2008.

[12] Y.Wang, F. Li, and F. Fang, "Poisson versus Gaussian Distribution for Object Tracking in Wireless Sensor Networks," Proc. Second Int'l Workshop Intelligent Systems and Applications (ISA), pp. 1-4, 2010.

[13] L.Lazos, R. Poovendran and J. Ritcey, "Analytic Evaluation of Target Detection in Heterogeneous Wireless Sensor Networks," ACM Trans. Sensor Networks, vol. 5, no. 2, article 18, 2009.

[14] P.Medagliani, J. Leguay, V. Gay, M. Lopez-Ramos, and G. Ferrari, "Engineering Energy-Efficient Target Detection Applications in Wireless Sensor Networks," Proc. IEEE Int'l Conf. Pervasive Computing and Comm. (PerCom), pp. 31-39, 2010.

[15] Y.Wang, Y. Leow, and J. Yin, "A Novel Sine-Curve Mobility Model for Intrusion Detection in Wireless Sensor Networks," Wireless Comm. and Mobile Computing, 2011.

[16] Y.Wang, Y.K. Leow, and J. Yin, "Is Straight-Line Path Always the Best for Intrusion Detection in Wireless Sensor Networks," Proc. Int'l Conf. Parallel and Distributed Systems, pp. 564-571, 2009.