Privacy Preserving of Data transmission for Cluster Based Wireless Sensor Network

K. Mallikarjuna Reddy[1], Mula.Sudhakar [2]

[1]*Final M.Tech Student, Asst.professo*[2]
[1,2]*Dept of CSE, Sarada Institute of Science, Technology and Management (SISTAM), Srikakulam, Andhra Pradesh, India*

Abstract: *Efficient data transmission in wireless sensor network is an important issue in the networks. So that to provide the efficient data sharing in the wireless sensor network we can perform the any one of cryptography technique. Before provide security of data we can perform the clustering of nodes in the wireless sensor network. Clustering of nodes is an effective way of to enhance the performance of wireless sensor network. By performing the clustering of nodes in the network we improve the network efficiency and also reduce the time complexity for the transmitting data. The clustering node can be performed by the dynamically and periodically. In this paper we proposed the mid-point clustering algorithm for the generation of number of cluster group. Before generation of clusters we can perform the authentication process of each node in the wireless sensor network. The authentication process can be done by implementing identity based polynomial signature algorithm. After that we can perform the clustering process and also provide security of transferring data. To provide security of data we are using bit sequence message integrity protocol. By using this protocol we can perform the encryption and decryption of transferring message. By implementing those concepts we can improve efficiency of wireless sensor network.*

Keywords: *Cluster-based WSNs, secure data transmission, digital signature, privacy, cryptography.*

I. Introduction

One of the fundamental goals of wireless sensor network is to collect information and sent to specified clients in the network. In a wireless sensor network efficient data transmission is a one most important issue. Because so many nodes are available in network. Usually many WSNs are installed in unobserved, harsh and often adversarial physical environments for specific applications, such as armed forces domains and sensing tasks with unreliable surroundings. So that to provide more efficient transmission of data is thus very essential and is required may realistic wireless sensor network. So many techniques are available for transferring data through wireless sensor network. In this paper we are implementing one of the concepts for cluster based wireless sensor network. By implementing this concept we can improve the efficiency wireless network and also provide more security of transferring data. In a cluster based wireless sensor network we can perform the clustering of nodes. By performing clusterization we can group all near nodes into single group. After that the central service provider will identify destination contains which group. After finding that the central service provider will send data through the destination node.

In the cluster based wireless sensor network we can also perform the authentication of each node in network. Because by performing authentication of nodes in network we can identify each node is trusted node or untrusted node. If the node trusted node central service provider will send data to destination node. Otherwise it will not send data to destination node. Before performing authentication process each node will generate signature, sending values by the central service provider. By using those shared values each node will generate shared key. Using that shared key each node will generate signature and sent that signature to central service provider. The central service provider will retrieve those signatures and again generate signature. If the both signatures are equal they are authenticated users else not authenticated.

Another concepts can be implemented in the cluster based wireless sensor network is clustering of nodes in a network. The clustering process can be done by the central service provider. By implementing clustering process we can group all near nodes into one group. Because we are not necessary to traverse all nodes available in a network for transferring of message to destination node. So that it will reduce time complexity for searching of destination node in a wireless sensor network. After performing clusterization process each will transfer information to destination node. Before transferring information each node will perform one the cryptography technique for transferring data form plain format to unknown format. In this paper we are using one of simple and best cryptography technique for provide more security of transferring data.

II. RELATED WORK

Cluster-based data transmission in WSNs has been investigated by researchers to achieve the network scalability and management, which maximizes node lifetime and reduce bandwidth consumption by using local collaboration among sensor nodes [1]. Another approach is proposed for performing cluster based wireless sensor network [2] is a low energy adaptive clustering hierarchy is presented by Heinzelman et al. by using this protocol we can effectively transfer data through the wireless sensor network. By implementing this idea we can improve so many protocols for performing the cluster base wireless sensor network functionalities. Researchers have been widely studying CWSNs in the last decade in the literature. However, the implementation of the cluster-based architecture in the real world is rather complicated [3]. Adding security of protocols will face challenging issue because the clusterization process can performed dynamically, periodically and randomly rearrange the clusters and data links[8].

Maan Younis Abdullah *et al* in inspected the problem of security addition to cluster based communication protocols for homogeneous wireless sensor networks containing sensor nodes with very limited resources, and proposed a security resolution where clusters are created periodically and dynamically. Their explanation depicts re-keying function protocol for wireless sensor networks security. They have projected the local administrative functions (LAFs) as master function, derivation function and rekeying function is imprinted with sensor node. A security and performance study proved that it is very proficient in communication, storage, computation and this technique is very successful in defending against a lot of complicated attacks as in [4]. Tingyao Jiang *et.al* presented a new dynamic intrusion detection method for cluster-based wireless sensor networks (CWSN). The nodes in a wireless sensor network are assembled into clusters depending on the particular relationships with a cluster head (CH) in every cluster. The projected scheme initially makes use of a clustering algorithm to construct a model of standard traffic behavior, and then uses this model of standard traffic to detect anomalous traffic patterns. Along with the diverse network conditions of clusters, this method might also dynamically set different detection factors for different clusters to accomplish a more proper detection algorithm. The performance study showed that the projected intrusion detection method can progress the detection accuracy and decrease the false positive rate, and is extremely efficient of the energy preservation as in [5].

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.

Identity based polynomial 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.

Xor value= $S_i \wedge U_i$

Sig= H(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.

Mid-point 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.

Bit 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 identity based polynomial 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 mid-point 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 bit sequence message integrity protocol. By implementing those three concepts we can enhance efficient of wireless sensor network and also improve security of transferring message.

V. References

[1]. A.A. Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks," Computer Comm., vol. 30, nos. 14/
15, pp. 2826-2841, 2007.

[2]. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-
670, Oct. 2002.

[3]. K. Pradeepa, W.R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks," Int'l J. Computer Applications, vol. 47, no. 11, pp. 23-28, 2012.

[4]. Abdullah, M.Y., Gui Wei Hua," Cluster-Based Security for Wireless Sensor Networks", Communications and Mobile Computing, CMC '09.
WRI International Conference on Volume: 3, Page(s): 555- 559, Publication Year: 2009

[5] Tingyao Jiang, Gangliang Wang, Heng Yu, "A dynamic intrusion detection scheme for cluster-based wireless sensor networks", World Automation Congress (WAC), Page(s): 259-261, Publication Year: 2012

[6]. A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," Proc. Advances in Cryptology (CRYPTO), pp. 47-53,1985.

[7]. R. Yasmin, E. Ritter, and G. Wang, "An Authentication Framework for Wireless Sensor Networks Using Identity-Based Signatures," Proc. IEEE Int'l Conf. Computer and Information Technology (CIT), pp. 882-889, 2010.

[8]. H. Lu, J. Li, and H. Kameda, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using ID-Based Digital Signature," Proc. IEEE GLOBECOM, pp. 1-5, 2010.

[9]. J. Sun et al., "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," IEEE Trans. Parallel & Distributed Systems, vol. 21, no. 9, pp. 1227-1239, Sept. 2010.

[10]. F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings," Proc. Ninth Ann. Int'l Workshop Selected Areas in Cryptography (SAC), pp. 310-324, 2003.

[11]. Y. Jia, L. Zhao, and B. Ma, "A Hierarchical Clustering-Based Routing Protocol for Wireless Sensor Networks Supporting Multiple Data Aggregation Qualities," IEEE Trans. Parallel & Distributed Systems, vol. 4, nos. 1/2, pp. 79-91, 2008.

[12]. D. Liu and P. Ning, "Multilevel _TESLA: Broadcast Authentication for Distributed Sensor Networks," ACM Trans. Embedded Computing Systems, vol. 3, pp. 800-836, 2004.

BIOGRAPHIES:

K. Mallikarjuna Reddy is student in M.Tech (CSE) in Sarada Institute of Science Technology and Management, Srikakulam. He has received His B.TECH (CSE) from Aringar Anna Institute of Science and Technology, Pennalur, Chennai . His interesting areas are Data Mining and network security.

Mula.Sudhakar is working as a Asst.professor in Sarada Institute of Science, Technology And Management, Srikakulam, Andhra Pradesh. He received his M.Tech (SE) from Sarada Institute of Science, Technology And Management, Srikakulam. JNTU Kakinada Andhra Pradesh. His research areas include Cloud Computing, Dataminig,Network Security.