Survey on Secure and Energy Efficient Cluster Optimization by using Hierarchical Clustering Technique

P.Poonkodi[1] D.Akshara[2] S.Gaayathri[3] S.P.Jeevakanth[4]
[1,2,3,4]Department of Computer Science & Engineering
[1,2,3,4]SNS College of Technology Coimbatore-35

Abstract— *Wireless sensor based communication system plays a vital role in communication. Wireless infrastructure is a network that guarantees communication between various devices associated through an infrastructure protocol. A new innovative approach is proposed to increase the lifetime of network. Routing the Data in sensor nodes plays a vital role in transferring the data to the base station (BS). Multihopping, grid based, hierarchical based and clustering based such as LEACH (Low-Energy Adaptive Clustering Hierarchy), HEED etc., are some of the different types of routing algorithm. The existing LEACH protocol designed so for does not consider security as a serious issue. But in this paper we have concentrated mainly on incorporating clustering technique based on hierarchy technique namely EEHC-ECC clusters optimization to provide security and also improve the lifetime of the sensor nodes. We compare our proposed clustering model with LEACH protocol and analyze its efficiency.*

Keywords— WSN, Clustering, Hierarchy Clustering Technique

I. INTRODUCTION

Many clustering technique have been developed to achieve the energy efficiency in sensor network especially to overcome the energy efficiency issue in LEACH [6] protocol such as LEACH-F, LEACH-Centralized [5], PEGASIS [2], APTEEN [6], TEEN [6], LEACH-P [1], multi-level LEACH [3], [4] all the above mentioned protocol addresses the energy efficient issues of leach and improved the lifetime of sensor network but none of them have used any security measure that sensor network required. In [6] they surveyed some of leach based security protocol such as SLEACH, SC-LEACH, Armor LEACH, SecLEACH and MS-LEACH. SLEACH is one of the first protocols to introduce security scheme. All these methodology suffer from overhead due to improper session management and key generation overhead which affect the lifetime of sensor.

II. EXISTING SYSTEM

The existing clustering protocol known as LEACH is not efficient and suffers in term of life time of network. The existing security model for sensor network proposed so far adopts RSA or Diffe Hellman cryptography mechanism which induces key generation overhead that result in degradation of lifetime of sensor node. In Survey on LEACH-based security protocols it is surveyed that some of leach based security protocol such as SLEACH, SC-LEACH, Armor LEACH, Sec LEACH and MS-LEACH in which SLEACH is one of the first protocol to consider the security issue. All these methodology suffer from overhead due to improper session management and key generation overhead which affect the life time of sensor.

A. Disadvantage of Existing System

1) Most of the Existing methods send data directly from cluster heads (CHs) to the base station (BS) without intermediate node which utilizes more energy for transmission.
2) Frequent failure of sensor node life time
3) More unsecured Methods

III. PROPOSED SYSTEM

The proposed hierarchical clustering model considering security and lifetime of sensor node. The asymmetric ECC security model is incorporated into EEHC protocols reduce the overhead in providing security for wireless sensor network. Clustering has been well received as an effective way to reduce the energy consumption of a wireless sensor network. Clustering is defined as the process of selecting a set of wireless sensor nodes to be cluster heads for a given wireless sensor network. Therefore, data traffic generated at each sensor node can be sent via cluster heads to the sink/base station. Clustering is also used for data aggregation, where the cluster heads aggregate the data collected at the cluster members. Hierarchical routing protocols proved to have sufficient reduction in energy consumption of the wireless sensor network (WSN). In hierarchical routing protocols, tree is created with numbers of clusters and a head node is assigned to each cluster. Head nodes are the leaders of their groups. They have some responsibilities like collection and aggregation the data from cluster node of their corresponding clusters heads and transmitting the aggregated data to the base station (BS). This aggregated data in the head nodes which reduces energy consumption in the network by reducing the information to be sent to the BS which result in less energy consumption and increases the network life time.

A. Advantage of Proposed System

- Proposed hierarchical based clustering protocol (EEHC-ECC) improves energy efficiency with public key based security in sensor network.
- TDMA avoids unnecessary collision of cluster heads (CHs) in wireless sensor network (WSN).
- In wireless sensor network communications have enabled low cost, power, dynamic sensor devices for the development that are tiny and short communication range

IV. MODULES

A. Wireless Network Formation Module

This module helps in transferring information to Receiver node by sending current IP address of the system. File need to be send will have to give IP and files are send from sender to receiver system

B. Cluster Module

In the first stage of cluster module, the BS first broadcast a hello message to all the sensor devices about its position in the network then the sensor devices start computing the value of its qualifier specifier. The sensor devices in the network broadcast their qualifier specifier to fellow sensor device using radio propagation. The cluster head is based on the qualifier specifier that has been obtained by the fellow sensor devices then the sensor devices compare their qualifier specifier with the fellow sensor devices. If the qualifier specifier is higher than that of its fellow devices the device itself elect as cluster head.

In the next step, first stage cluster head behave like a normal device and the cluster selection process takes place among cluster head. In this process the associate devices of first stage will be in sleep node. The radio communication frequency range of devices will be doubled in this phase. Till we get the singe cluster head in the network the cluster selection process will go on.

C. Reclustering Module

Here the reclustering message is broadcasted to its associate of cluster once the first sensor device reaches 10% of residual energy to its initial energy and the clustering process is initiated. In this stage the device that is having a residual energy greater than 10% of its initial energy calculate their qualifier specifier and transmit cluster head message to its associate or else behave as associate device for FSC stage.

D. Data Gathering Module

The associate device in stage one transmit the information gathered to their respective cluster head. The cluster head then aggregate the information obtained from its associate and then transmit the information to its respective cluster head till the information is obtained by the base station.

E. ECC based Routing Model

Encryption and Decryption is done using ECC Scheme, this algorithm is a deviation of public-key encryption. ECC encryption for certain data integrity and authentication, use session keys for data encryption, Session keys are exchanged using ECC encryption. To authenticate the sensor devices and generate session keys between the sensor devices and the sink (cluster head or the base station), in between the devices need to communicate. Public key Encryption is support for semantic security. The ECC Scheme to encrypt the message to select the random numbers, for cluster divide into two stage clusters by using EEHC-ECC and form a two stage cluster to select the cluster head that select the key by using ECC Algorithm. To decrypt a cipher text to perform a key validation on check, verify, compute the Keys. We use proactive strategy to communicate with in cluster and reactive strategy for among cluster and also use the ECC authentication scheme.

V. ALGORITHMS

```
// encryption and decryption
def encrypt_mv_eg (Kpub ,m1 ,m2 ):
x,y = 0,0
while ( (x ==0) or (y ==0) ):
r = floor ( p* random () )
x = (r* Kpub )[0]
y = (r* Kpub )[1]
return r*G, m1*x, m2*y
def decrypt_mv_eg (kpri ,enc ):
x = ( kpri *enc [0])[0]
y = ( kpri *enc [0])[1]
return enc [1]* x^-1, enc [2]* y^-1
//text to number
def encoding ( text ):
result = 0
for c in text :
result = 256* result +ord(c)
return result
//number to text
def decoding ( number ):
number = Integer ( number )
result = ''
for i in number . digits (256):
result = chr(i) + result
return result
```

Actually in our case we need to divide into an even number of blocks. If we think in a character as a number < 256 (its ASCII code) and we employ Fp as a field then we can encode at most log256 *p* characters in each block.

VI. CONCLUSION

In this paper, we analysed the factors which is used to improve the security and the existing clustering protocol known as LEACH is not efficient and it also suffers in term of life time of network so there was a need for new clustering protocol to increase the lifetime of network. In this hierarchical based clustering protocol namely EEHC-ECC is proposed to improve energy efficiency with public key based security in sensor network. In future work we would conduct simulation study to check the performance of other network parameter such as node decay rate, packet delay and by varying node and check how the proposed protocol perform by varying the simulation area size and changing the position of base station to the middle of sensor network area and also propose a cluster optimization technique based on evolutionary technique.

REFERENCES

[1] Gupta, N.; Gupta, H.; Yadav, R., "Life Time Enhancement of Sensor Network by Using Concept of SEP & LEACH (LEACH-P)," in Advances in Computing and Communication Engineering (ICACCE), vol., no., pp.198-201, 1-2, 2015.

[2] Joppe W. Bos, J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, and Eric Wustrow, “Elliptic Curve Cryptography in Practice” 2014

[3] Kodali, R.K., "Energy efficient routing in multi-level LEACH for WSNs," in Advances in Computing, Communications and Informatics (ICACCI), vol., no., pp.959-965, 2015.

[4] Kodali, R.K.; Venkata Sai Kiran, A.; Bhandari, S.; Boppana, L., "Energy efficient m- level LEACH protocol," in Advances in Computing, Communications and Informatics (ICACCI), vol., no., pp.973-979,2015.

[5] S. Lindsey and C. Raghavendra, "PEGASIS: Power-Efficient Gathering in Sensor Information Systems," IEEE Aerospace Conf. Proc., vol. 3, 9–16, pp. 1125–30, 2012.
[6] Rahayu, T .M.; Sang-Gon Lee; Hoon-Jae Lee, "Survey on LEACH-based security protocols," in Advanced Communication Technology (ICACT), vol., no., pp.304-309, 16-19, 2014.