International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 2, Issue 6, June 2015)

Secure Communication in the Wireless Sensor Networks Using Cluster Mechanism

Seema Firdose
IV Sem M.Tech
CSE Dept,PACE
seema.firdose25@gmail.com

Mohammed Hafiz
Asst.Professor
CSE Dept,PACE
HAFIZ123STER@gmail.com

Jamrud khan
Asst.Professor
E&C Dept
jamrudkhan@gmail.com

Abstract -Cluster is a divided into group of 4-5 nodes and after that the communication takes place between the mobile nodes. Inside the cluster there is cluster head. Cluster node/cluster head will be controlling and managing the working of whole cluster. Cluster head is elected according to the priority. Inside the cluster the nodes are authenticated using one way Hashing. Inter-cluster communication is done using digital signature. The main aim is to ensure the secure communication which will be energy efficient as we have segmented the whole network into small set of clusters. The cluster head ensures secure key management and communication between the mobile nodes. The cluster head is not permanent as other nodes stay in queue and based on priority cluster head is selected.

Keywords-MANET, Cluster, Routing, Key distribution.

I. INTRODUCTION

MANETs is a network which does not have a particular infrastructure where all the nodes are scattered freely or lightly. Since it does not have the proper structure there are many issues in order to gain secure communication in this network. There are some issues like small memory capacity, power supply; managing key distribution is also not unique. Security in MANETs is a big issue because these are rapidly used in military applications. The military systems will be having very critical tasks and information. If something goes wrong while transmitting the information then there will be improper results. So we should provide good security while sending the data or information. A security scheme in MANETs must provide efficient key distribution technique. The main aim of this paper is to gain secure communication between the nodes in the network, and the energy saving method while sending the data in network should consume less energy.

II. RESEARCH STUDY

This Chapter Presents Route map and described the literature survey and comparison of the pervious papers and extract the results:-

1) Since the WSN are widely used everywhere .WSNs have many applications in the network field. Many security solutions have been proposed in the domain of WSN so far. Here we have made a hard work to survey well known security problems in WSNs and study the performance of WSN nodes. We calculate required time and power used by the network [1].

2) In this paper, we are going to introduce how MANET and WSN security design may be improved with vast information of cryptography. Securing MANETs and WSNs requires consideration of the following factors: dynamic geometrical arrangement of networks (topology), resource conditions, no proper infrastructure, and limited security. Because WSNs typically have many nodes and less power than MANETs, their security design requires individual attention to computational capabilities and memory resources [2]. 3) Cluster Based Routing Protocol achieves a better performance in lifetime by balancing the energy load to all the nodes. Here the data is seen which is used to send to the base station which can better handle the different energy of the nodes. The network lifetime is increased [3].

4) Secret Sharing method is used to share a system key among preselected set of nodes called, DPKG's that offers a joined distributed key generation to satisfy the asks for keys during network working time and identified small attacks against D-PKGs and propose anonym zing D-PKGs as the countermeasure [4].

5) Cluster-based trust evaluation method is proposed, cluster head is selected and it was proposed to detect the unknown nodes in the network [5].

6) A framework is proposed for key management technique that provides powerful method for Security. Their proposed Key Systems uses a changed model in which nodes can constantly change their management roles. The system gives high resources sharing for the network members. This KMS gives more service availability, more flexibility in establishing of new nodes, takes pre-arrangement time is less, and can dynamically re arrange itself based on the network requirement [6].

7) A hierarchical routing protocol of two steps was proposed called Cluster Based Hierarchical Routing Protocol (CBHRP). The head-set members are responsible for controlling and managing of the network. According to the result CBHRP protocol is less energy consuming and extends the life of sensor network [7].

8) They designed a multiple access method to know control messages, ABCP in which cluster formation is done by the result of the multiple accesses. ABCP is manageable, used easily by the layers which are in upper position. It takes clustering decision directly based on the outcome of channel access [8].

9) In this routing protocol is proposed having the features of self-arrangement of the parts and hierarchal routing, so that the nodes are equally load balanced [11].
10) A Cluster Node:- A node that is decided to be a cluster head. A cluster head is also called as cluster node [12].
Cluster Member: This member is used for sharing data with other[12].

III. PROPOSED METHOD

There are four methods implemented

1. Network Model

In this model we are going to establish the network which will be containing many sensor nodes. Sensor nodes will detect the changes in the network.
After the network is created we have to divide the network into small group of clusters. Each cluster will be having 4-5 nodes. Each node will be sending the data to each other using one way hash function.

2. Cluster Head Selection

After the clusters are created in the network next step is to select the cluster head or cluster node .Its selected according to the priority basis. Even the cluster head is elected on 3 criteria's:-
(a)Energy details of nodes and density of the nodes

The cluster head is selected on the energy basis which node will be having more energy it is selected as a cluster head. We see the remaining energy of the node and more energy node is elected.
(b)Area selection
The node is selected in such a way that it is capable of working in all the area of the network.
(c) Electing Head Node
Energy of the node should be maximum.
Frequent mobility should be less.
Density should be less.
(3) Authentication and Data communication
(a)Direct Authentication
(b)On Demand Authentication
(4)Inter Cluster Communication
There are two clusters which will be communicating here. They communicate using digital signature.

IV. CBSRP MODEL DESCRIPTION

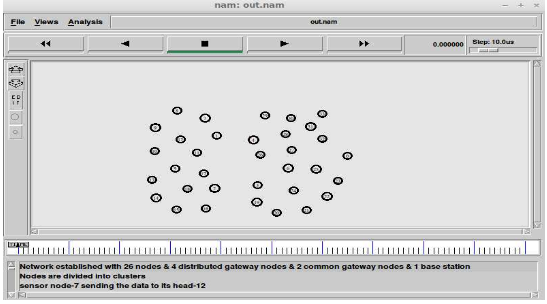
All the members of clusters are communicating within that cluster head and other cluster members only. It won't communicate with other cluster members and cluster head. Communication in an Intra –cluster mechanism is done by two hops from member node to base station .During first hop member node communicate with cluster head and then during second hop from cluster head to base station. In this model for secure routing, a network is established into clusters which consists of 4-5 member nodes along with a cluster node. A network composed of both cluster head and cluster members.

In a single cluster the one way Hashing is used to communicate between the nodes. A node is configured to be a cluster head. It is head of the cluster which monitors the working of that cluster. A present active member of the current cluster. This member shares the data. Limited power source in MANETs and WSNs are expected. Network is small so that keys are easily shared.

Each mobile node will have their own the Hash key. Here, we generated the Hash value by referring Node ID, Private Key of that node, message or data, and Network conditions which is ensuring the security of node's personnel key as other nodes do not know the sequential arrangement of private key, they know only the hash key sequence. The mobiles nodes will start sharing each other's Hash Key through Cluster node. Once the mobiles nodes are authenticated then data is transmitted securely. As a result, while unknown nodes come in the network then the mobile nodes will detect easily, malicious nodes will be discarded. The reason is malicious nodes do not know how to generate Hash value, so it cannot form such Hash value. One Way Hashing between cluster member1 and cluster member2. The usage of One Way Hashing is to ensure secure authentication between members. In starting, Node1 send requests to Node2, to establish a communication path and sends Node1's Hash value and required network information i which also known as parameters of the network like probability of channel access, Radius , Load of network, Nodes density, Latency, Data Rate, Error Bit Rate and consumption of energy. Next, Node2 sends N2 (Node2's Hash Key) and N1 requests information to cluster node. In next step, Cluster node sends N1 (Node1's Hash Key) and N2 (Node2's Hash Key) to Node1. Finally both the nodes verify the hash key value, if they are matched the information is sent. In an Inter-cluster routing members of cluster are communicate with cluster head by using either single hop or multiple hop communication then cluster head is communicate with base station via another cluster head. During Inter-cluster routing two or more cluster heads involve. Single hop Inter-cluster communication is easy to communicate sink or base station. Although simple, this approach is not only inefficient in terms of energy consumption, it is based on unrealistic assumption. The sink is usually located far away from the sensing area and is often not directly reachable to all nodes due to signal propagation problems.

V. RESULTS

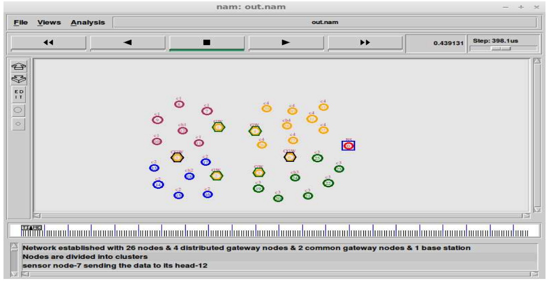
In the fig 1 below, This is the Initial executing window. This window is seen after giving ns main dot tcl command in Linux mint open terminal. In this window the sorting of the lists are done and files are been initialized.



```
Network established with 26 nodes & 4 distributed gateway nodes & 2 common gateway nodes & 1 base station
Nodes are divided into clusters
sensor node-7 sending the data to its head-12
```

Fig 1

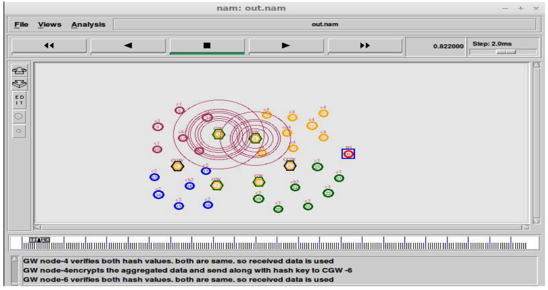
In the below fig 2, after the initial window is executed, the network is established which consists of nodes. By using network animator output window we are going to see the simulation results.



```
Network established with 26 nodes & 4 distributed gateway nodes & 2 common gateway nodes & 1 base station
Nodes are divided into clusters
sensor node-7 sending the data to its head-12
```

Fig 2

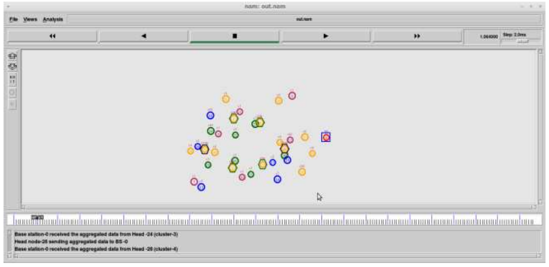
In the below fig 3, the network is divided into group of 4 clusters. The network consists of 26 nodes,2 common gateways and one base station.



```
GW node-4 verifies both hash values. both are same. so received data is used
GW node-4encrypts the aggregated data and send along with hash key to CGW -6
GW node-6 verifies both hash values. both are same. so received data is used
```

Fig 3

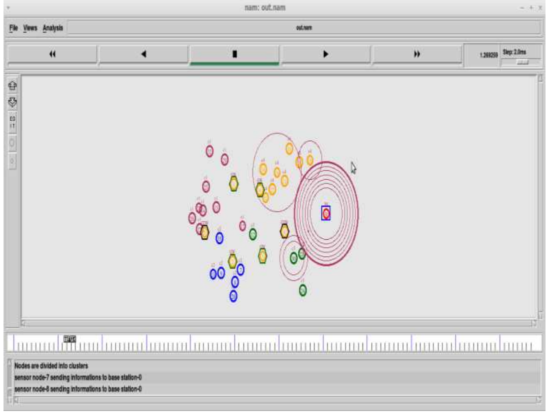
In fig 4, The cluster head is selected in all the clusters. The cluster head starts receiving the information from all the sensor nodes and transmits to the base station through the common gateways.



```
Base station-0 received the aggregated data from Head -24 (cluster-3)
Head node-26 sending aggregated data to BS -0
Base station-0 received the aggregated data from Head -26 (cluster-4)
```

Fig 4

In fig 5, When the data gets transmitted to the base station through the cluster heads of all the clusters the mobility occurs between the sensor nodes and nodes get dispersed.



```
Nodes are divided into clusters
sensor node-7 sending informations to base station-0
sensor node-8 sending informations to base station-0
```

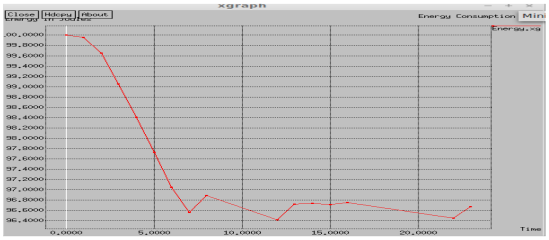
Fig 5

GRAPHS

Xgraphs

**Graph 1 : ** Energy Consumption

In the below figure we can see the energy is not consumed more.

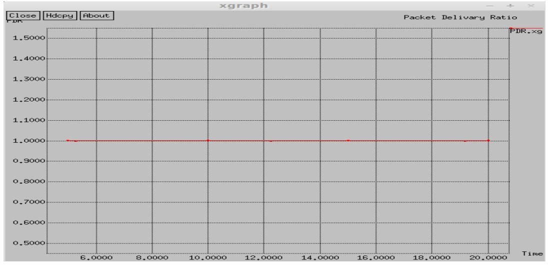


Graph 1

Xgraph 2 : Packet Delivery Ratio

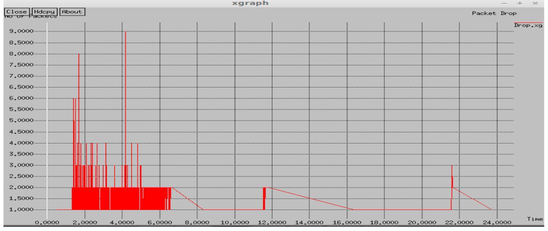
The ratio of number of packets sent will be delivered to the destination.

∑ Number of packet receive / ∑ Number of packet send



Graph 2

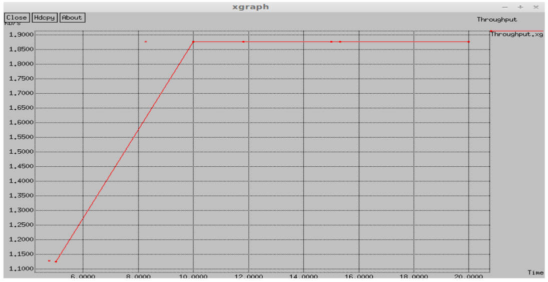
Xgraph 3 : Packet Drop Packet loss is the failure of transmitted packets to reach the destination.



Graph 3

Xgraph 4 : Throughput is the number of successful packets received multiply by the packet length and divided by the total simulation time.

.



Graph 4

VI. CONCLUSION

In this paper we have proposed 4 models network model, cluster head selection, data authentication and communication and inter cluster communication. The cluster head is main part in the network which is used to collect and send the data to the base station. Here we established the network than divided into 4 clusters. Each cluster will be having its cluster head which collects the data and sends to the base station. The information is transmitted in per hop manner so it can reach destination securely. The load is balanced in the network .All nodes have same load. Network is safe.

This frame work is also used for ad hoc network applications where overall population is stable. This is also applicable in secure cloud computing.

In future each and every node will be sending the data to the base station .Only the personnel data is shared between the nodes. Information sharing will be very less, only the data required is send.

The encryption and decryption is done between the sender and receiver while sending the data. The encryption and decryption is done twice in order to gain more security while transmitting the data between the clusters.

REFERENCES

[1]. J. Chen and J. Wu, "A Survey on Cryptography Applied to Secure Mobile Ad Hoc Networks and Wireless Sensor Networks" to appear in Handbook of Research on Developments and Trends in Wireless Sensor Networks: From Principle to Practice, H. Jin and W. Jiang (eds), IGI Global, 2010.

[2]. Bager Zarei, Mohammad Zeynali and Vahid Majid Nezhad, "Novel cluster based routing protocol in wireless sensor networks". IJCSI Intl. J. Comput. Sci. 7(4), 32-36, 2010.

[3]. G. Hadjichristofi, W. Adams, and N. Davis, "A Framework for Key Management in Mobile Ad Hoc Networks", International Conference on Information Technology: Coding and Computing (ITCC'05) - Volume II, 2005.

[4]. Md. Golam Rashed, M. Hasnat Kabir, Muhammad Sajjadur Rahim, Syaikh Enayet Ullah, "Cluster Based Hierarchical Routing Protocol For Wireless Sensor Network", International Journal of Computer and Network Security (IJCNS) Edition Volume 2 No, May 2010.

[5]. Ting-Chao Hou and Tzu-Jane Tsai, “An Access-Based Clustering Protocol for Multihop Wireless Ad Hoc Networks,” IEEE JSAC, vol. 19, no. 7, July., 2001, pp. 1201–10.

[6]. Jalil Jabari Lotf, Mehdi Nozad Bonab and Siavash Khorsandi. A Novel Cluster-based Routing Protocol with Extending Lifetime forWireless Sensor Networks, In Proceedings of International Conference on Wireless and Optical Communications Networks(WOCN ’08), 2008.

[7]. Y. Hu, A. Perrig, D. Johnson, Ariadne: a secure ondemand routing protocol for ad hoc networks, in: ACM Annual International Conference on Mobile Computing and Networking (MOBICOM), September 2002, pp. 12–23.

[8]. Vagner Schoaba, Felipe Eduardo Gomes Sikansi, Luiz Castelo Branco, "Digital Signature for Mobile Devices: A New Implementation and Evaluation"; International Journal of Future Generation Communication and Networking, Vol. 4, No. 2, June, 2011.