International Journal of Research Instinct
(Peer-reviewed Journal)

ISSN ONLINE 2348-2095
Research Article

ENERGY EFFICIENT DISTRIBUTION CLUSTERING IN SOLUTION OF MANET

[1] Dr L. Jayasimman, [2] S.Muneeswari

1.Asst Professor - Department of Computer Science ,2.M.Phil – Research Scholar
Department of Computer Science
Srimad Andavan Arts and Science College (Autonomous)
muneeswari.selvaraj@gmail.com

ABSTRACT

Adhoc Network (ANET) is a ‘self configuring infrastructure’ that has less network of mobile devices connected by wireless links. Each device in a Adhoc is free to move independently in any direction. The lack of central coordination and shared wireless medium in Adhoc network make them more vulnerable than wired network. So, all the nodes must cooperate with each other in order to route the packets. Co-operating nodes must trust each other by exchanging trust information about nodes within the radio range. Multicast traffic within a cluster employs a one-way hash function chain in order to authenticate the message source. Cross-cluster multicast traffic includes message authentication codes (MACs) that are based on a set of keys. Each cluster uses a unique subset of keys to look for its distinct combination of valid MACs in the message in order to authenticate the source. Hence this article focuses on the importance of improving trust level in Adhoc Network. The simulation study is performed using Network Simulator NS 2.29.

Keywords-AdhocNetworks,Cluster,Messageauthentication Multicast communications.

I. INTRODUCTION

Adhoc network is an autonomous system devices connected by wireless links. The devices are free to move randomly and organize themselves arbitrarily. Ad-hoc Network is a communication network without a pre-exist network infrastructure. It is built spontaneously as devices get connected. Instead of relying on a base station to co-ordinate the flow of messages to each node in network, the individual network nodes forward packets to and from each other. As a result, nodes play the role of router, compelling them to cooperate for the correct operation of the network. Specific protocol has been proposed for Adhoc networks considering not only its peculiar characteristics, also a perfect co-operation among nodes.

In general, it is assumed that all nodes behave according to the application specifications. However, this assumption may be false, due to resource constraint or misbehavior nodes etc .If malicious nodes are present in an ADHOC, and they may attempt to reduce network connectivity by pretending to be co-operative. These actions may result in defragmented networks, isolated nodes, and drastically reduced network performance. The assumption that nodes behave correctly can lead to unexpected pitfalls, such as resource consumption, and vulnerability to attacks. Moreover, malicious nodes can work together to improve the effectiveness of the attack. For instance, nodes could lie about malicious node to cover its real nature. Therefore, mechanism that allows a node to infer the trustworthiness of other nodes become necessary. According to the paradigm of autonomic networks, nodes are capable of self-configuring, self-managing, and self-learning by means of collecting local information and exchanging information with its neighbors. Thus it is important to communicate only with trusted neighbor nodes, because the exchange of information with compromised nodes can deteriorate the autonomy of adhoc networks. In general, if the interactions among nodes have been faithful to the protocol, then trust will accumulate between these nodes. Trust has also been defined as the degree of belief level that one node can put on another node for a specific action based on previous direct or indirect observations on behaviours of the node. The nodes in the network evaluate trust for other participating nodes and then form trust relations between them. Nodes study about malicious nodes based on the information exchanged with trustworthy neighbors. Trust is dynamic, not static. Trust is not necessarily transitive; the fact that node A trusts node Band B trusts node C does not imply that A trusts C. Trust is asymmetric and not necessarily reciprocal. The trust information is based on individual experiences and on the recommendations of other nodes in the network.

In this paper proposes source and message authentication scheme for multicast traffic for MANET. It exploits network clustering and routing technique in order to cut the overhead and ensure scalability. In the intra cluster employs one-way hash chains to authenticate the message source. The authentication code is combined with message body are transmitted to the intended recipient. The recipient performs the same calculation on the received message, using the same secret key, to generate a new MAC. On the other hand, Inter cluster multicast traffic includes Message Authentication codes that are based on multiple keys. To authenticate the source, each cluster use unique combination of MACs in the message. At the time of initiating the multicast session the pool keys are generated by the sender. The keys will be securely transmitted to the head of every cluster that hosts one or multiple receivers. After that the sender transmits the messages to the head of the individual cluster. The cluster head authenticate the intended recipient using the intra-cluster authentication scheme and then deliver the message.

The rest of this paper is organized as follows. The related work is discussed in Section II and Section III describes the proposed work. Section IV describes the simulation Result of our work. Finally, section V presents the conclusion. The simulation study is performed using Network Simulator NS 2.29.

2. RELATED WORK

This section discusses about the literature survey done on various issues like mobility and topology changes, various attacks, co-operation among the nodes and malicious nodes, trust relationship among the group of nodes as well as security in the Mobile Adhoc Networks.

Pirzada A.A et al [6] proposed the “Trust establishment in pure ad-hoc networks," in which a trust-based model is used for communication in ad-hoc networks that is based on individual experience rather than on a third party advocating trust levels. The model introduces the notion of belief and provides a dynamic measure of reliability and trust worthiness in pure ad-hoc networks. But the trust mode method also affected by some kind of attacks, such as slander attack in the presence of malicious nodes.

Ishibashi et al [4] proposed “Topology and mobility considerations in mobile ad hoc networks”, in which a number of statistics were collected from the topologies and mobility patterns of mobile adhoc networks. Connectivity, node degrees, and path lengths were presented, along with link lifetimes and times to route failures. A highly dynamic topology is a distinguishing feature and challenge of a mobile ad hoc network. Links between nodes are created and broken, as the nodes move within the network. This node mobility not only affects the source and/or destination, as in a conventional wireless network, but also intermediate nodes, due to the network's multihop nature.

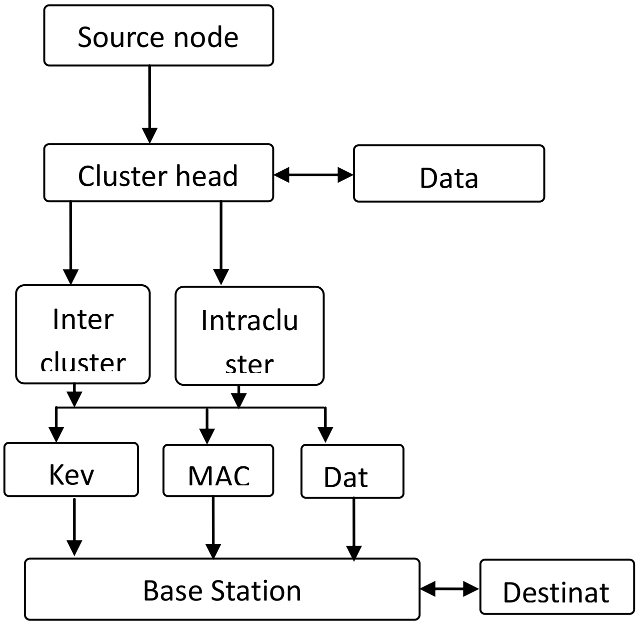
Varadharajan V [8] proposed “Security for cluster based adhoc networks. Compute Commun”, A protocol on security for cluster based adhoc networks”, all the nodes share a secret key with their respective cluster heads. Each cluster head needs to share a secret key with other cluster heads. Storage overheads are much higher in this approach since cluster heads need to store the shared keys of all the nodes within its cluster and with other cluster heads.

Edith C et al [2] proposed “Trust- and Clustering-Based Authentication Services in Mobile AdHoc Networks”, Clustering has been proven Effective in minimizing the amount of storage for Communication information, and in optimizing the use of network bandwidth. A zonal algorithm for clustering ad hoc networks is proposed to divide the network into different regions and make adjustments along the borders of the regions to produce a weakly connected dominating set of the entire graph. An adaptive method for maintaining hierarchical structure in an ad hoc network which the role of nodes and the cluster size can be changed autonomously with the status. Finally, a model of location-aware clustering in ad hoc networks. It divides the whole network into an number of geographic zones where each zone forms a logic cluster.

Jung- San Lee et al [3] proposed “Secure Communications for cluster – based ad hoc networks”, When a node wants to join the cluster it has to get the authentication token from the cluster head by executing the authentication phase with the cluster head.

3.PROPOSED WORK

The basic idea of this paper is to build a cluster model that provides nodes with a mechanism to evaluate the trust level of its neighbor nodes. In multicast wireless ad-hoc networks nodes are grouped into clusters. Any one of the nodes can be taken as cluster head. Each cluster is controlled by a cluster-head, which is reachable to all nodes in its cluster, either directly or over multi-hop paths. Nodes that have links to peers in other clusters would serve as gateways. The presence of gateways between two clusters implies that the heads of these clusters are reachable to each other over multi-hop path and that these two clusters are considered neighbors. Multicast traffic includes message authentication codes (MACs) that are based on multiple keys.



The keys will be securely transmitted to head of every cluster that hosts one or multiple receivers. The multicast message is then transmitted to the cluster-heads which authenticate the source and then deliver the message to the intended receivers using the intra-cluster authentication scheme. Multicast traffic within the same cluster employs one-way hash chains to authenticate the message source. The authentication code is appended to the message body. However, the authentication key is revealed after the message is delivered.

The main objective of proposed system is authenticating the source, ensuring the integrity of the message and clustering method to reduce overhead and ensure scalability. Also increases the performance and trust level among the group of nodes. The proposed system possesses the following advantages. They are

a) Use Multicast On Demand Routing Protocol.

b) Increase the performance and trust level among the group of nodes.

c) Authenticate the source and message to prevent any attempt infiltration by an intruder.

d) Reduces the communication among the malicious nodes in the network.

e)Time and secret-information asymmetry in order to achieve scalability and resource efficiency.

The Figure 1 shows the architecture diagram of the Cluster Network. Initially, Source node sends data to cluster head. Cluster head control by cluster member. Select the inter cluster or intra cluster operation perform. Data pending key and message authentication code to destination node.

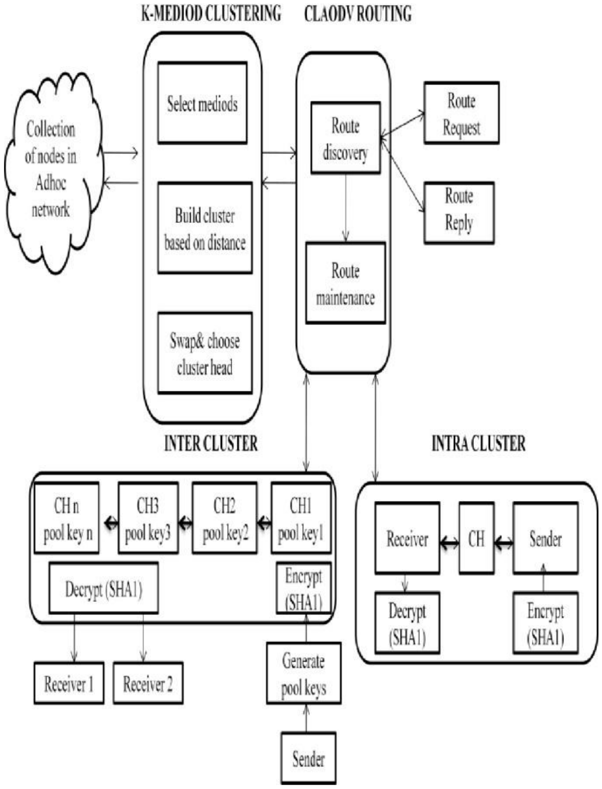


FIGURE 1: Architecture Diagram of Cluster

A. Clustering

Clustering is an important research topic for MANET because clustering makes it possible to guarantee basic levels of system performance, such as throughput and delay, in the presence mobility and a large number of mobile nodes. The process of dividing the network into interconnected substructures is called clustering and the interconnected substructures are called clusters. The cluster head (CH) of each cluster act as a coordinator within the substructure. The cluster head coordinates the cluster activities inside the cluster. The ordinary nodes in cluster have direct access only to cluster head and gateways. The nodes that can hear two or more cluster heads are called gateways.

Each CH acts as a temporary base station within its zone or cluster. It also communicates with other CHs. The Cluster based routing provides an answer to address nodes heterogeneity, and to limit the amount of routing information that propagates inside the network. The grouping of network nodes into a number of overlapping clusters is the main idea behind clustering..

1)K-Mediod Clustering

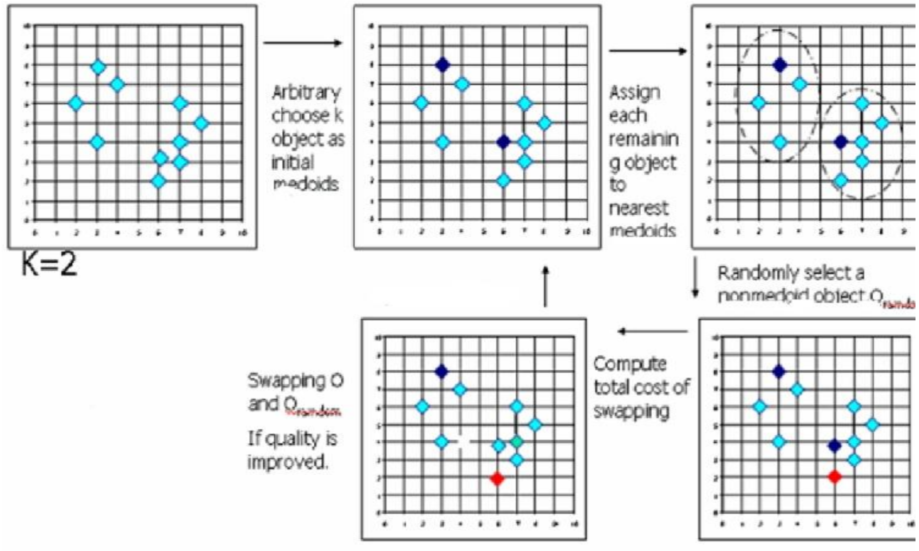

K=2
Arbitrary choose k object as initial medoids
Assign each remainin g object to nearest medoids
Randomly select a nonmedoid object O_random
Compute total cost of swapping
Swapping O and O_random
If quality is improved.

FIGURE 2:Working of K-Mediod Algorithm

The k-means method uses centroid to represent the cluster and it is sensitive to outliers. This means, a da;;ta object with an extremely large value may disrupt the distribution of data. K-medoids method overcomes this problem by using medoids to represent the cluster rather than centroid. A medoid is the most centrally located data object in a cluster.

Here, k data objects are selected as medoids to represent k cluster and remaining all data objects are placed in a cluster having medoid nearest (or most similar) to that data object. After processing all data objects, new medoid is determined which can represent cluster in a better way and the entire process is repeated. Again all data objects are bound to the clusters based on the new medoids. In each iteration, medoids change their location step by step. Or in other words, medoids move in each iteration. This process is continued until no any medoid move. As a result, *k* clusters are found representing a set of n data objects. The working principle of K-Medoids is explained in the Fig. 2 An algorithm for this method is given below.

```
1  initialize:  select $k$ of the $n$ data points as the medoids.
2  Associate each data point to the closest medoid.
3  For each medoid $m$
       i. For each non-medoid data point $o$
       ii. Swap $m$ and $o$ and compute the total cost of the configuration
4  Select the configuration with the lowest cost.
       i. Repeat steps 2 to 4 until there is no change in the medoid.
```

B. CLAODV Routing Technique

In the proposed system using the Cross-layer Ad-hoc On-Demand distance vector routing protocol. Cross-layer sharing the status information of networks is helpful to optimize the operation in one certain layer or between layers. And it will great improve network performance, such as security and energy management. To improve the performance of AODV routing algorithm in mobile Ad Hoc networks, so adopt the cross-layer method. CLAODV reduces the overhead, improves the efficiency and other performances, such as the throughput, the end-to-end delay and the success ratio.

In the CLAODV routing the sender node when ready to sends the data packets to receiver it initiate the route discovered process. Sender broadcast the Route Request Packet to all neighbour nodes. When an intermediate node receives a Route request, it either forwards it or prepares a route reply if it has a valid route to the destination. And then the neighbour node before sending the route reply it measures the signal strength. The signal strength of the received signal can be estimated at the physical layer. This information is transferred to the MAC layer along with the signal strength information. The Mac layer uses this information for making calculations, later it is passed to the routing layer along with routing control packet. In the routing layer, the information is stored in the routing table and it is used in some decision making process. When condition is satisfied sender initiates the route until found the receiver.

C. Source Authentication of Multicast Protocol

In the proposed system provide the source authentication in ad-hoc network for two ways. Initially, clusters the partitioned network, and then authenticates multicast traffic by employing time asymmetry for intra-cluster traffic and secret information asymmetry for inter-cluster traffic.

1. Intra Cluster Authentication

This section describes the implementation of intra cluster. Intra Cluster based on time symmetry. A source node generates a chain of one-time-use keys using the hash function, e.g., MD5, SHA-1, and shares only that last generated key with the receivers. A message can be authenticated only when the used key in the chain is revealed. To verify the authentication key, the receiver recursively applies the cryptographic hash function a key cannot be used outside its designated time interval and the message will be ignored if the MAC is based on an expired key. Consequently, clock source and synchronization is required to make sure that the destination has the same time reference for key expiration. The size of the time interval, which determines when a key is revealed, depends on the clock jitter among nodes in the cluster.

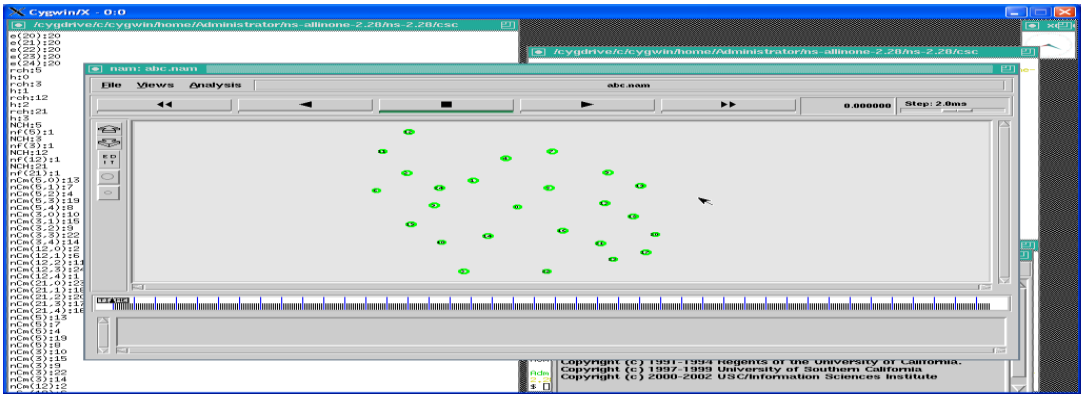
1. Inter Cluster Authentication

    This section describes the implementation of inter cluster. Inter-cluster based on secret information asymmetry. Source “s” that belongs to Cluster i will send the multicast packets to the heads of all clusters that have designated receivers. For example, if the members of the multicast group for s are residing in clusters g, h, j, and k, node sends the message to CH g, CH h, CH j, and CH k. These cluster heads will then forward the message to the receivers in their respective clusters. The rationale is that the MAC will be associated with the cluster rather than the nodes and thus the overhead is reduced significantly. In other words, the multicast from s consists of multiple multicasts; (1) from *s* to all relevant cluster heads, (2) a distinct multicast within each of the target clusters to relay the message to designated receivers. This can also be advantageous if node mobility is to be dealt with. A node that switches from one cluster to another would only introduce local changes and would not require special handling by the source with respect to the authentication process.

4. SIMULATION RESULTS

1. *NODE TOPOLOGY*

A node topology represents formation of nodes in a network and its arrangement in a network


Cygwin/X - 0:0
/cygdrive/c/cygwin/home/Administrator/ns-allinone-2.28/ns-2.28/csc
/cygdrive/c/cygwin/home/Administrator/ns-allinone-2.28/ns-2.28/csc
nam: abc.nam
File
Views
Analysis
abc.nam
0.000000
Step: 2.0ms
EDIT

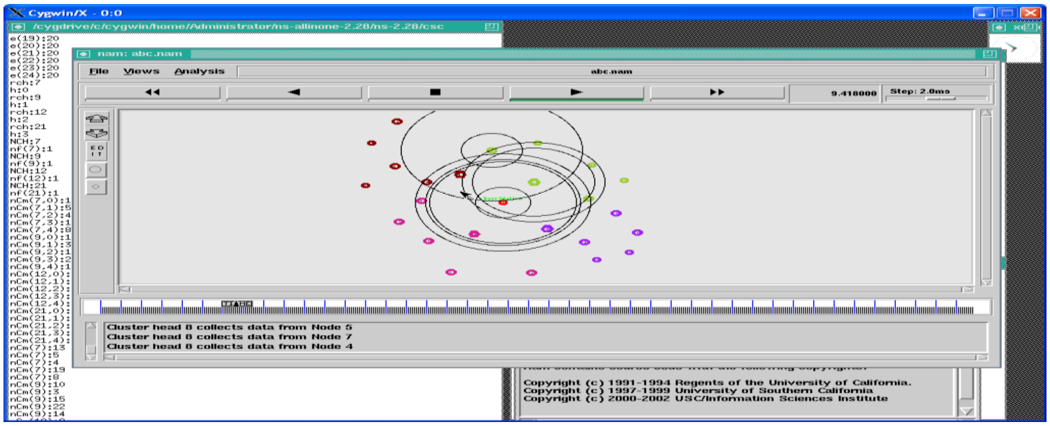
```
e(20):20
e(21):20
e(22):20
e(23):20
e(24):20
rch:5
h:0
rch:3
h:1
rch:12
h:2
rch:21
h:3
NCH:5
nf(5):1
NCH:3
nf(3):1
NCH:12
nf(12):1
NCH:21
nf(21):1
nCm(5,0):13
nCm(5,1):7
nCm(5,2):4
nCm(5,3):19
nCm(5,4):8
nCm(3,0):10
nCm(3,1):15
nCm(3,2):9
nCm(3,3):22
nCm(3,4):14
nCm(12,0):2
nCm(12,1):6
nCm(12,2):11
nCm(12,3):24
nCm(12,4):1
nCm(21,0):23
nCm(21,1):16
nCm(21,2):20
nCm(21,3):17
nCm(21,4):16
nCm(5):13
nCm(5):7
nCm(5):4
nCm(5):19
nCm(5):8
nCm(3):10
nCm(3):15
nCm(3):9
nCm(3):22
nCm(3):14
nCm(12):2
```

```
Copyright (c) 1991-1994 Regents of the University of California.
Copyright (c) 1997-1999 University of Southern California
Copyright (c) 2000-2002 USC/Information Sciences Institute
```

Figure 3:Node creation

CLUSTER HEAD FORMATION

A node with the highest energy is selected as cluster head. Cluster head will collect information from remaining nodes sent it to base station after fusing of data.



```
e(19):20
e(20):20
e(21):20
e(22):20
e(23):20
e(24):20
rch:7
h:0
rch:9
h:1
rch:12
h:2
rch:21
h:3
NCH:7
nf(7):1
NCH:9
nf(9):1
NCH:12
nf(12):1
NCH:21
nf(21):1
nCm(7,0):1
nCm(7,1):5
nCm(7,2):4
nCm(7,3):1
nCm(7,4):8
nCm(9,0):1
nCm(9,1):3
nCm(9,2):1
nCm(9,3):2
nCm(9,4):1
nCm(12,0):
nCm(12,1):
nCm(12,2):
nCm(12,3):
nCm(12,4):
nCm(21,0):
nCm(21,1):
nCm(21,2):
nCm(21,3):
nCm(21,4):
nCm(7):13
nCm(7):5
nCm(7):4
nCm(7):19
nCm(7):8
nCm(9):10
nCm(9):3
nCm(9):15
nCm(9):22
nCm(9):14
```

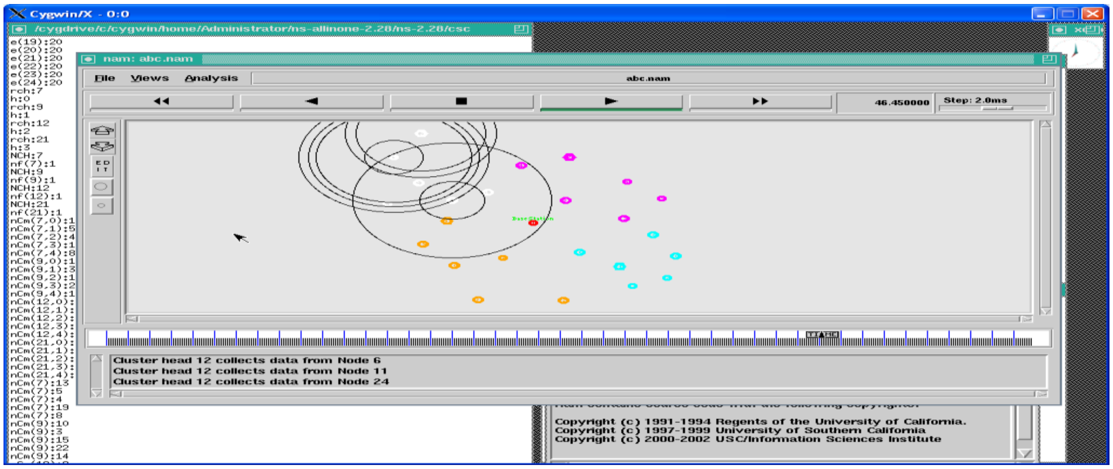
```
Cluster head 8 collects data from Node 5
Cluster head 8 collects data from Node 7
Cluster head 8 collects data from Node 4
```

```
Copyright (c) 1991-1994 Regents of the University of California.
Copyright (c) 1997-1999 University of Southern California
Copyright (c) 2000-2002 USC/Information Sciences Institute
```

Figure4: Formation of cluster head

3. *CLUSTER HEAD REELECTION*

When the energy of cluster head is lesser than the energy of other nodes cluster head reelection will be done. A node with highest energy is elected as cluster head.



```
e(19):20
e(20):20
e(21):20
e(22):20
e(23):20
e(24):20
rch:7
h:0
rch:9
h:1
rch:12
h:2
rch:21
h:3
NCH:7
nf(7):1
NCH:9
nf(9):1
NCH:12
nf(12):1
NCH:21
nf(21):1
nCm(7,0):1
nCm(7,1):5
nCm(7,2):4
nCm(7,3):1
nCm(7,4):8
nCm(9,0):1
nCm(9,1):3
nCm(9,2):1
nCm(9,3):2
nCm(9,4):1
nCm(12,0):
nCm(12,1):
nCm(12,2):
nCm(12,3):
nCm(12,4):
nCm(21,0):
nCm(21,1):
nCm(21,2):
nCm(21,3):
nCm(21,4):
nCm(7):13
nCm(7):5
nCm(7):4
nCm(7):19
nCm(7):8
nCm(9):10
nCm(9):3
nCm(9):15
nCm(9):22
nCm(9):14
```

```
Cluster head 12 collects data from Node 6
Cluster head 12 collects data from Node 11
Cluster head 12 collects data from Node 24
```

```
Copyright (c) 1991-1994 Regents of the University of California.
Copyright (c) 1997-1999 University of Southern California
Copyright (c) 2000-2002 USC/Information Sciences Institute
```

Figure5: Cluster head reelection

5. CONCLUSION

In Adhoc Networks, all the nodes must cooperate with each other in order to route the packets. Adhoc Networks in Multicast traffic authenticating the source and message to prevent any infiltration attempts by an intruder .Cluster Network provides time and secret information asymmetry in order to achieve scalability and resource efficiency. Thus the effective Cluster model is generated to reduce the communication among the malicious nodes and improve the performance of the Adhoc Network

REFERENCES

[1] Edith C. H. Ngai and Michael R. Lyu,“ Trust-andClustering-Based Authentication Services in Mobile Ad Hoc Networks”,IEEE Trans. Network Service Management, vol. 7, no. 3, Sep. 2010.

[2] B.Ishibashi “Topology and Mobility Considerations in Mobile Adhoc Networks”, Asiam journal of Adhoc Network vol, no 3,pp-362-776,225

[3] Jung – San Lee and Chin-Chen Chang Secure Communication for Cluster-based adhoc networks using node identities, journal of Network and Applications, vol 30,pp.1377-1396,2007

[4] Li and J.Kato, ”Future trust management framework for mobile Adhoc networks”, International Journal on selected Areas in Communication, vol.46,no.4,pp.108-114,2008

[5] Y. Lu, B. Zhou, F. Jia, and M. Gerla, “Group-based secure source authentication protocol for VANETs,” in *Proc. 2010 IEEE GLOBECOM Workshop Heterogeneous, Multi-hop Wireless Mobile Networks*.

[6] Perrig, R. Canetti, D. Song, and D.Tygar,“Efficient authentication and signing of multicast streams over lossy channels,” in Proc. 2000 IEEE Symposium Security Privacy.

[7] Pirzada and Donald, “Trust establishment in pure Adhoc networks”, International Journal in Wireless Personal Communication, vol.37, no.1-2, pp.19-168, 2006.

[8] Varadharajan V, Shankaran R, Hitchens M. “Security for cluster based ad hoc networks. Compute Commun”, Vol. 27, p. 488–501, 2004.