Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 11, November 2014, pg.735 – 745

RESEARCH ARTICLE

AN EFFICIENT CLUSTER MAINTENANCE AND SECURED IN MOBILE AD-HOC NETWORK

Miss. S.Jothilakshmi[1], Mrs. R.Kavitha[2]

[1]M.Phil Research Scholar, Department Of Computer Science, Vivekanandha College for Women
[2]Assistant Professor, Department Of Computer Science, Vivekanandha College for Women
Tiruchengode, Namakkal (India)
[1] clickjothi76@gmail.com, [2] kavithamscmphil@gmail.com

ABSTRACT: The main task of the Mobile Ad-hoc Network is to reduce traffic and achieve high accuracy of the network. By using the KNN Query processing, the query-issuing node first forwards a KNN query using geo-routing to the nearest node from the point specified by the query. Then, the nearest node from the query point forwards the query to other nodes close to the query point, and each node receiving the query replies with the information on itself. In this process, the adopt two different approaches: the Explosion method and the Spiral method. But the security of the network is moderate, the Quality of service parameter is low and the network is will reach high if this method is used to the larger network.

The Elliptical Curve Cryptography (ECC) algorithm is used to increase the security in the Mobile Ad-hoc Network. The security of the data is monitored and maintained by the Elliptical Curve Cryptography. It also provides clustering to increase the authentication in the network. Authentication provides access control to the network. The network control is increased by the clustering concept. The clustering includes cluster formation and cluster head selection in the network during the process of communication in the network. In order to increase the network performance the Quality of Service parameters are increased.

Keywords: MANET, KNN Query processing, Explosion and Spiral method, Elliptical Curve Cryptography (ECC) algorithm.

1. INTRODUCTION

Mobile Ad-hoc Networks (MANET) are self configuring and self-organizing multi hop wireless networks where, the network structure changes dynamically. In a MANET nodes (hosts) communicate with each other via wireless links either directly or relying on other nodes as routers. The nodes in the network not only acts as hosts but also as routers that route data to/from other nodes in network The operation of MANETs does not depend on preexisting infrastructure or base stations. Network nodes in MANETs can move freely and randomly.

1.1 Aodv Routing Protocol

As mobile ad hoc networks are characterized by a multi-hop network topology that can change frequently due to mobility, efficient routing protocols are needed to establish communication paths between nodes, without causing excessive control traffic overhead or computational burden on the power constrained devices.

There are two types of routing protocols which are reactive and proactive. In reactive routing protocols the routes are created only when source wants to send data to destination whereas proactive routing protocols are table driven. Being a reactive routing protocol AODV uses traditional routing tables, one entry per destination and sequence numbers are used to determine whether routing information is up-to-date and to prevent routing loops.

The maintenance of time-based states is an important feature of AODV which means that a routing entry which is not recently used is expired. The neighbors are notified in case of route breakage. The discovery of the route from source to destination is based on query and reply cycles and intermediate nodes store the route information in the form of route table entries along the route. Control messages used for the discovery and breakage of route are as follows :

- Route Request Message (RREQ),
- Route Reply Message (RREP),
- Route Error Message (RERR),
- HELLO Messages.

2. METHODOLOGY

2.1 Elliptical Curve Cryptography

The Elliptical Curve Cryptography (ECC) algorithm is used to increase the security in the Mobile Ad-hoc Network. Cryptography is generally used to provide data security in the Mobile Ad-hoc Network. The multi hop network is constructed to increase the parameters of the network Quality of Service (QOS) parameters are increased.

Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible — this is the "Elliptic Curve Discrete Logarithm Problem" or ECDLP.

The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements, i.e. that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key – e.g., a 256-bit ECC public key should provide comparable security to a 3072-bit RSA public key.

For current cryptographic purposes, an elliptic curve is a plane curve over a finite field (rather than the real numbers) which consists of the points satisfying the equation

$$y^2 = x^3 + ax + b,$$

along with a distinguished point at infinity, denoted ∞.

Key Generation

Key generation is an important part where it has to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key. Now, it have to select a number'd'within the range of 'n'.

Using the following equation it can generate the public key

$$Q = d * P$$

d = the random number selected within the range of (1 to n-1).

P is the point on the curve.

'Q' is the public key and'd' is the private key.

Encryption

Let ‘m’ be the message are sending. It has to represent this message on the curve. This has in-depth implementation details. All the advance research on ECC is done by a company called certicom.

Consider *‘m’* has the point *‘M’* on the curve *‘E’*. Randomly select ‘k’ from [1 - (n-1)].

Two cipher texts will be generated let it be **C1**and**C2.**

$$C1 = k*P$$

$$C2 = M + k*Q$$

C1 and C2 will be send.

Decryption

It has to get back the message ‘m’ that was send to us,

$$M = C2 - d * C1$$

M is the original message that it have send.

Proof

How does it get back the message,

M=C2 – d*C1

‘M’ can be represented as ‘C2 – d*C1’

C2 – d*C1=(M+k*Q) –d*(k*P) [C2=M+k*Q and C1=k*P]

=M+k*d*P – d*k* P [cancelling out k*d*p]

=M [original Message]

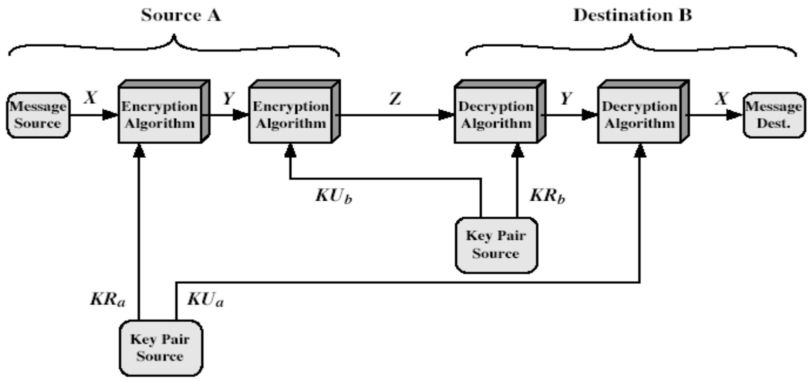


Figure 2.1(a):Public-Key Cryptosystem: Secrecy and Authentication

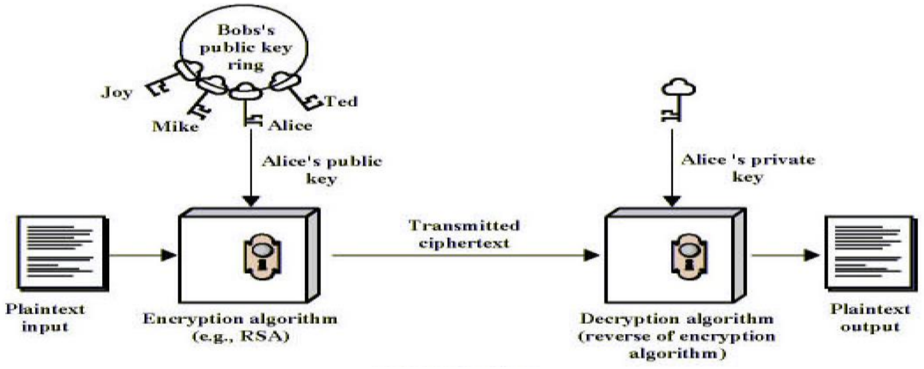


Figure 2.1(b):Encryption

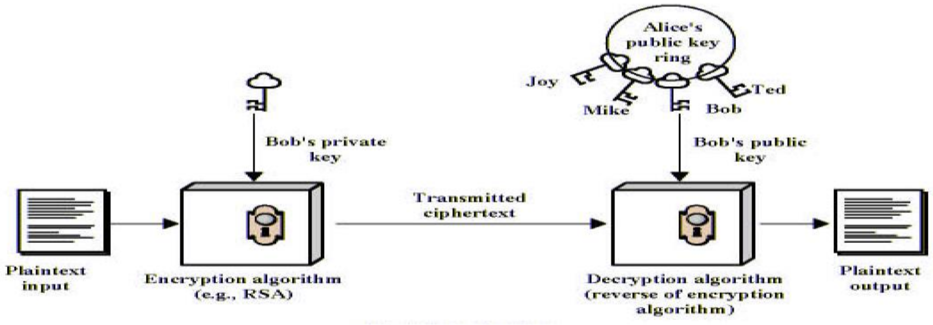


Figure 2.1(c):Authentication

2.2 Topology Discovery

The introduce a new path cost metric which is based on the distance between two neighbor nodes, hop count to sink node and the residual energy of node. This metric is very useful in path selection. Topology discovery is used to provide the structure to the network. In general the random topologies are employed. The location of the node is identified by the concurrent values.

2.3 Dynamic Cluster Maintenance

In general the group of node is called cluster. One of the node is act as a cluster head inside the cluster. The scheme uses stateless clusters in which all the ordinary node in the cluster maintain only the previous hop and corresponding sink. This means the cluster head does not need to maintain information on its children in its cluster, which simplifies cluster maintenance considerably.

Cluster Formation and Cluster Head Selection

In general, the Cluster is referred as the formation of the group of nodes in the network and the cluster head is called as; it is head among the cluster children. At the end of the Top-Disc topology discovery process, the node network is divided into n clusters and each cluster is represented by one node, which is called the cluster head. The cluster head is able to reach all the nodes in the cluster directly because they are all within its communication range. On behalf of using the cluster and the cluster head concept in the network can increase the tolerance of the network. The network monitoring are also increased by using this concept.

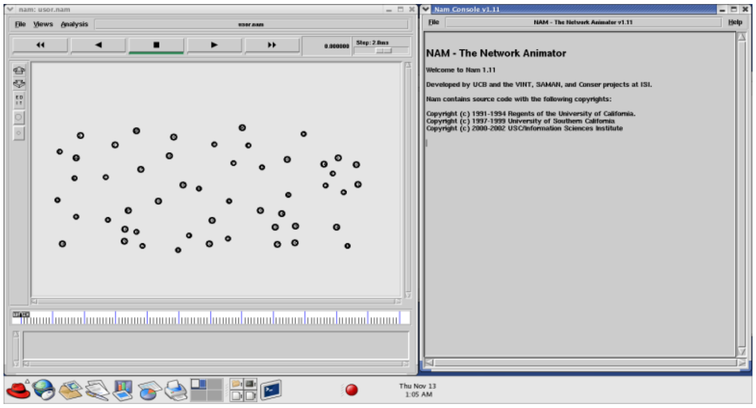
2.4 Cluster Path Switching

Introduce mechanisms for path switching when the energy of the nodes in original primary path has dropped below a certain level. This allows us to distribute energy consumption more evenly among the nodes in the network. To increase the energy efficiency of the network the path switching concept is introduced.

3. EXPERIMENTS AND RESULTS

Manet Topology Design

The Network topology is represented in this design. The formation of the network is carried out in the random manner. This is the beginning stage of the data transmission in the network. The speed of the network animator window 2.0ms. There are totally 50 nodes present in the network for processing.



NAM - The Network Animator

Welcome to Nam 1.11

Developed by UCB and the VINT, SAMAN, and Conser projects at ISI.

Nam contains source code with the following copyrights:

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 3.1 : MANET Topology Design

Manet Topology With Cluster Formation

The cluster formation is identified in this animator window. There are five clusters are created. Here cluster 1 consist of 5 nodes, cluster 2 consist of 7 nodes, cluster 3 consist of 4 nodes, cluster 4 consist of 5 nodes, cluster 5 consist of 5 nodes in the network. The speed of the network animator window is 2.0ms.

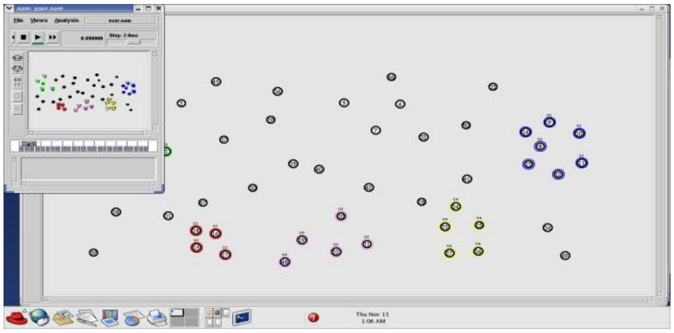


Figure 3.2 : MANET Topology With Cluster Formation

Manet Topology With Data Transmission In Clusters

In this design, 50 nodes have been created and a transmission range is established. Since the nodes are mobile they keep moving independently. The data packets are sent to various nodes from source to destination. The acknowledgement is obtained when the data packet is received by the destination node. The data loss takes place when destination receives different data packets from various source nodes. So, to avoid the data loss time interval is used that is, within the time interval only the data packet can be sent from source to destination.

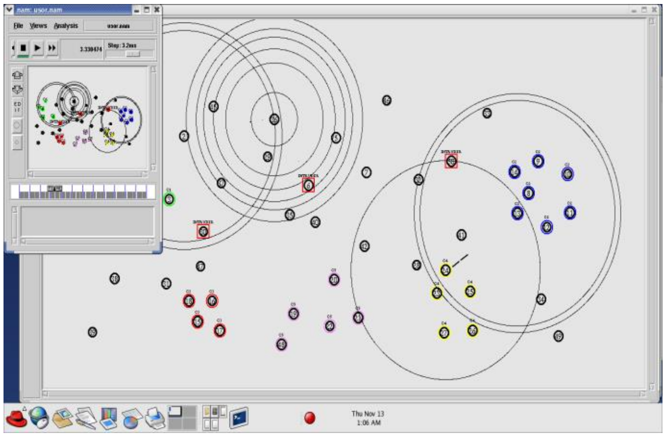


Figure 3.3 : MANET Topology With Data Transmission In Clusters

Manet Topology Design With Data Transmission

The mobility of the nodes are identified in the window. The data transmission is also carried out with reduced loss in the network. The data transmission of the cluster 2 is high compared to the other clusters in the network. The speed of the network animator window is 2.0ms. The time period of the data transmission is 9.4564s.

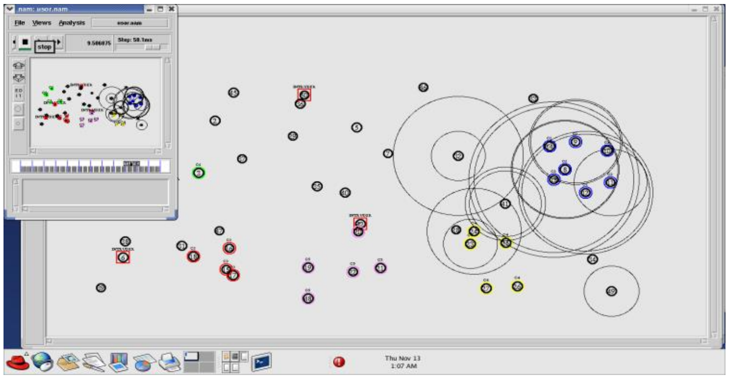


Figure 3.4 : MANET Topology Design With Data Transmission

X-Graph For Bandwidth Vs Number Of Packet Transmitted

The X-graph is designed between the Bandwidth and the number of data packet transferred in the network during the process of communication in the network. While compared with the existing method and the proposed method performed well in terms of bandwidth in the network. The Bandwidth achieved by the proposed method is 9.100mpbs. The Bandwidth achieved by the existing method is 7.500mpbs.

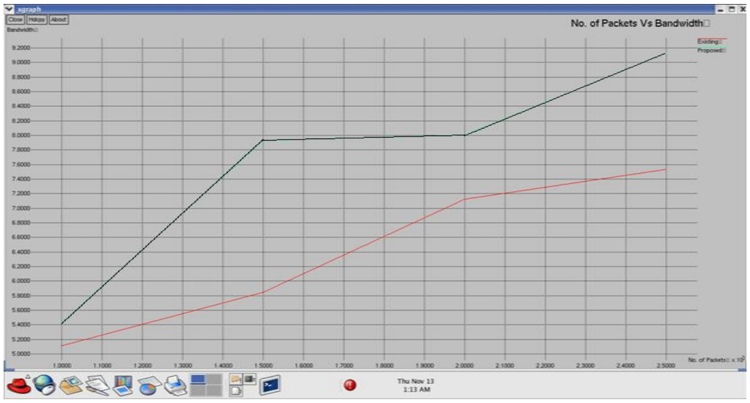


Figure 3.5 : X- Graph For Bandwidth Vs Number Of Packet Transmitted

X-Graph For Mobility Vs Delay

The X-graph is designed between the Mobility and the Delay in the network during the process of communication in the network. While compared with the existing method and the proposed method performed well in terms of delay in the network. The delay produced by the existing method is 19.500s and the delay produced by the proposed method is 16.100s.

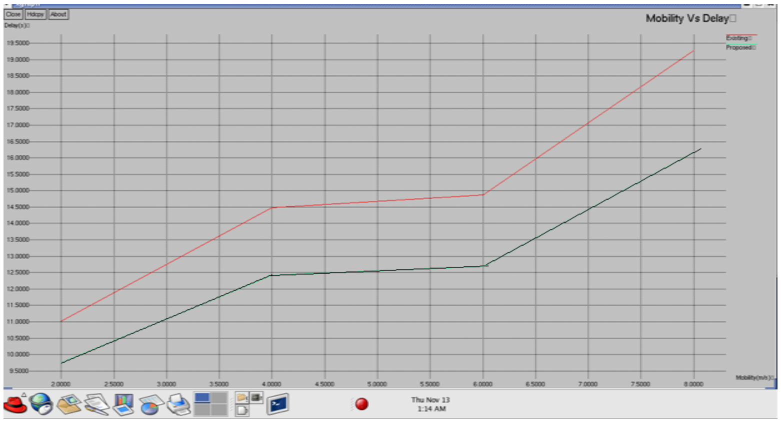


Figure 3.6 : X-Graph For Mobility Vs Delay

X-Graph For Throughput Vs Delivery Ratio

The X-graph is designed between the Throughput and the Delivery Ratio of the network during the process of communication in the network. While compared with the existing method and the proposed method performed well in terms of delay in the network. The delivery ratio of the existing method is 65.3 and the delivery ratio of the proposed method is 89.5.

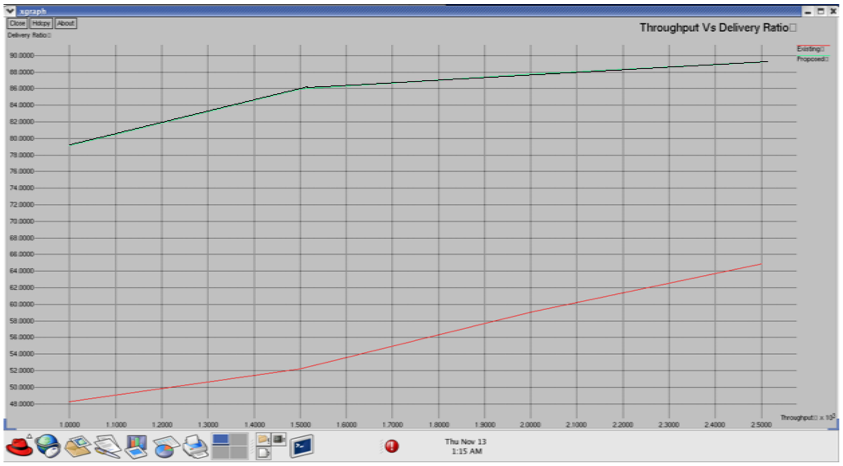


Figure 3.7: X-Graph For Throughput Vs Delivery Ratio

CONCLUSION

The Elliptical Curve Cryptography (ECC) algorithm is used to increase the security in the Mobile Ad-hoc Network. With the security model, the proposed method is also suitable for the larger network. The security is the main goal of this project. The encryption and the decryption process is carried out by the elliptical curve cryptography method. The segmented secrete key method is also followed for strong authentication in the network.It also provides clustering to increase the authentication in the network. Authentication provides access control to the network. The network control is increased by the clustering concept. The clustering includes cluster formation and cluster head selection in the network during the process of communication in the network. The result shows that the delay of the proposed method is low. The bandwidth and the throughput is increased in the proposed method when compared with the existing method.

REFERENCES

[1] T. Camp, J. Boleng, and V. Davies, “A survey of mobility models for ad hoc network research,”Wireless Commun. Mobile Comput., vol. 2, no. 5, pp. 483–502, 2002.

[2]C.-Y.Chow,M.F.Mokbel,andH.V.Leong,“Onefficient and scalable support of continuous queries in mobile peer-to-peer environments,”IEEE Trans. Mobile Comput., vol. 10, no. 10, pp. 1473–1487, Oct. 2011.

[3] T. Hara and S. K. Madria, “Consistency management strategies for data replication in mobile ad hoc networks,”IEEE Trans. Mobile Comput., vol. 8, no. 7, pp. 950–967, Jul. 2009.

[4] M. Heissenbüttel, T. Braun, T. Bernoulli, and M. Walchli, “BLR: Beacon-less routing algorithm for mobile ad-hoc networks,”Comput. Commun., vol. 27, no. 11, pp. 1076–1086, 2004.

[5] Y.-B. Ko and N. H. Vaidya, “Flooding-based geocasting protocols for mobile ad hoc networks,”Mobile Netw. Applicat.,vol.7,no.6, pp. 471–480, 2002.

[6] T. P. Nghiem, A. B. Waluyo, and D. Taniar,“A pure peer-to-peer approach for kNN query processing in mobile ad hoc networks,” Pers. Ubiquit. Comput., vol. 17, no. 5, pp. 973–985, Jun. 2013.

[7] C. E. Perkins and E. M. Royer, "Ad hoc on demand distance vector routing,"inProc. WMCSA, New Orleans, LA, USA, 1999, pp. 90–100.

[8] B. Xu, F. Vafaee, and O. Wolfson, "In-network query processing in mobile P2P databases," in Proc. GIS, Seattle, WA, USA, 2009, pp. 207–216.

[9] X. Yu, K. Q. Pu, and N. Koudas, "Monitoring k-nearest neighbor queries over moving object," in Proc. ICDE, 2005, pp. 631–642.