International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

A Light Weight Secure Protocol for Quick Disaster Recovery using AODV

Krishna AV
M.Tech Student
Dept of CSE
LBS Institute of Technology for Women
Trivandrum, India

Manoj Kumar G
Associate Professor
Dept of CSE
LBS Institute of Technology for Women
Trivandrum, India

Abstract—: **DANETs which have high network density and mobility are deployed over a disaster area ,the establishment of communication services over this will be challenging task. This paper proposes a novel method to recover the data and effectively operate within a limited period of time. Time period is a critical factor in a disaster area since the energy level of different nodes varying with respect to time. The message transmitted by the nodes during a time period cannot be retransmitted due to energy failures or due to different energy level of the nodes. This makes the retransmission of data nearly an impossible factor. Our method predicts the recovery of data in different communication channel over a period of time which reduces the retransmission by making use of homomorphic encryption method. To overcome the limitation due to infrastructure less, retransmission ,loss of data due to several factors .Our method uses a prediction methodology it also helps to eliminate the malicious activities in a group due to link failure, we conduct simulation experiment by using ns-3.21 to varying that our method achieve significant improve in preventing critical data loss in presence of malicious node.**

Keywords— AODV, El-gamal Encryption, Hidden Markov model, Homomorphic Encryption

I INTRODUCTION

Vanets, which is similar to that of Manets, which has high mobility network density. The exchanging of data may depend on driving status of traffic, weather condition, road condition etc. It exchange various messages which includes information about hazards, events, traffic details or location of nearby hotels, restaurants etc. Focusing on the disaster area , the information exchanging within the limited period of time is crucial one. The paper basis on data exchanging of vanets in the disaster area which introduce pre -defined header such as RREQ and RREP. The header can be modified by attaching an encrypted information regarding the source by using El-gamal encryption method. Here the disaster area can be partitioned into different region and this region be considered as different clusters, from those cluster a cluster head can be chooses based on nodes with high speed, distance and velocity.In a disaster environment we cannot predict the path or traffic on a limited period of time due to its nature. Ensuring security and quality of service is the advantage of the proposed method which can used to scale on regular applications also. The proposed system can be deployed with minimal changes on an existing environment. The network path prediction is done by making use of hidden markov model which helps the users to access the validation functions. Due to the homomorphic nature of this encryption method all the path requests route will be encoded and finally the destination would have the entire path in an encrypted form . A comparison can be done within the header itself for a mismatch that would help to identify the intruders within a path .If packet loss or delays occur then the same can be identified from the header itself thus we can achieve integrity in routing.

The rest of the paper organized as follows Section II describes the related work. Section III introduces the proposed system, the concept, routing scheme, probabilistic prediction and data recovery methods. Section IV describes the evaluation results of the proposed method, finally the conclusion is provided in section V.

II RELATED WORKS

A. WORKING OF AODV

AODV is a distance vector routing protocol for extemporary mobile networks, it grant route between nodes only when the routes are requested by the source node and the network is workable to allow and leaves based on its demand. During the path establishment time, to generate route by engulf Route Request RREQ packets in the network. This RREQ message redirects continues till the destination or neighboring nodes find the route to destination. The destination nodes send the Route Reply RREP, it travels the reverse route when the source node receives the RREP packets it checks the destination sequence number which should be greater than destination sequence number of packets. If RREQ is received more than one times, that are discarded. If a data is flowing and a link breaks is noticed a route error message (RERR) is send to the source of the data in a hop by hop fashion. As the RERR generate near the source each intermediary node invalidates routes to any unavailable destinations. When the source of the data receives RERR it negates the route and re initiative route discovery if needed.

B.. VARIANT OF AODV AND PATH PREDICTION

Modification of aodv protocol on rreq header and rrep header can be explained in ISDSR+[1], it is a centralized approach can generate secret key with the help of key generation centre. In this the node which need to communicate send a KREQ message to Key Generation Centre(KGC) to generate a secret key code and rebound the key to node by KREP. In

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

the route analysis mechanism ,the node receives SRREQ add its own identity in the received route information and generates a signature using a signature algorithm an node broadcast SRREQ including the signature this steps iterated until it reaches the destination, when this reached the destination the node verify the received signature via signature algorithm. And in route maintenance of ISDSR+ if any node find disconnection the intermediate node ID and source generate as signature and forward SRERR, then the source node. V2V is a division of manets ,it is used for link among nodes in a changing environment. The route detection, path supply fulfilled by AODV protocol. Here routing can be modified by applying artificial intelligence (aiAODV)[2] using fuzzy neural network algorithm. The data is overflow through various path by sending RREQ and seeing attributes such as distance, overhead, power consumption and expected time for better throughput, packet drop and avoid collision effectively. Advance adhoc on demand distance protocol[3]a alteration of standard AODV aid to bear secure communication between the nodes beyond any blitz from invaders. Conquer method to catch on collapse node and intruder node in the network and likelihood to forecast whether the node is intruder or black hole attacker during the transmission. Trust aware adhoc routing protocol[4] insures trust experiences between nodes in the dynamic differing topology, proposed routing assemble the neighbor log information to conclude the loss or gain rate of packet transfer between the node. The confidence value of node in determined depend on energy model calculation, packet sequence ID matching rate and mobility estimation. To organize certainty, the conventional AODV apply public key encryption of RSA [5]. Here security can be furnish on all route discovery and route maintenance and uses i)Digital Signature that assign nobility in the routing message(ie non mutable field) ii)Hash Chain ensures the mutable field from miss interruption. Vehicle clustering is an essential effort in network management to address the broadcast problem with changing environment[6]. The paper come up with a combination of algorithms such as sociological pattern clustering and route stability clustering . In sociological pattern clustering it design cluster employing nodes and elect the cluster head based on nodes with maximum energy level and in RSC it focus on vehicles or nodes communication that means exchange of beacon message between neighbors about the nodes identifier ,location, speed, stability of routes and time stamp etc. The paper also point out how to manage cluster and aerial due to clustering. In Vehicular adhoc network path prediction[7]can based on by Trajectory Predictability for Vehicles, feasibility and availability . Besides focused on a routing frame work which consist of vehicles present area through GPS such that communication between neighbors over beacon. In dynamic varying situation, the location of vehicles changes immediately so that the terminal of vehicles can be call based on source, present location and moving direction etc. Along with the paper target a vehicular mobility arrangement by handle the variable order markov model.

III PROPOSED SYSTEM

a. Modified AODV Protocol

This thesis proposed an optimized AODV protocol which can achieve for rapid communication and high throughput. Here the protocol functions similar to that of conventional AODV protocol with the subsequent changes. An adjunct aspect is joined to the RREQ and RREP request .The adjunct is self-assured with of source node id, destination id, location, direction, velocity which is in encrypted form.. Although a RREQ message is acknowledged by an intermediary node, the route is created by the source itself. If the receiving node is not the destination and does not. have a route to destination, it rebroadcast the RREQ message and the accepting node is the target one or has a present route to the destination it setup a RREP message.

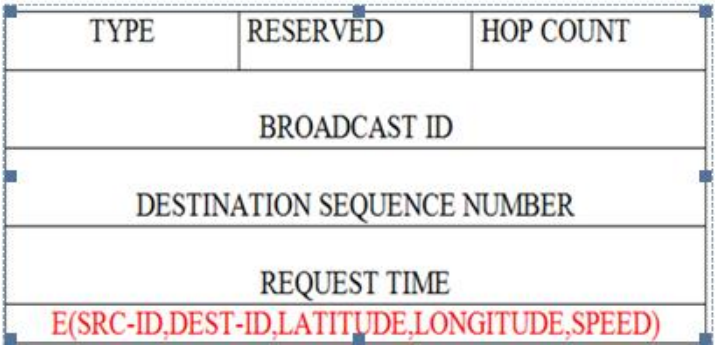

Fig 1: MODIFIED AODV RREQ HEADER

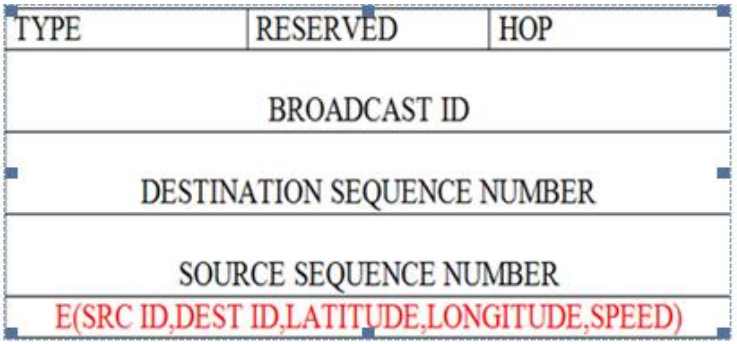

Fig 2: MODIFIED AODV RREP HEADER

During the propagation of RREP, each one of the intermediate nodes starts forming routes to the destination. Upon receiving the RREP the source begins to record the route towards the destination and starts to send the data. If the source receives multiple routes, one route with the shortest hop count is selected. Here we provide an extra field for RREP header which contains the encrypted id of the sender. If the source receives multiple RREP the route with the shortest hop count and trust value which is generated based on some movement parameters is selected as the route. Each node which is present on the route updates the timers which are linked with the route to the source and destination, thus maintaining the different routes in the routing table. In case of a link break during data flow, route error message RRER is

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

forwarded to the data source in a hop by hop fashion. During the propagation of RERR towards the source, routes to unreachable destination are invalidated by each intermediate node. If the data source receives a RERR then it invalidates that route and would restart route discovery if required.

a. Formation Of Clusters

When a disaster occurs, it is very difficult to establish communication services. Communication equipment should work effectively without any interruption in order to perform tasks such as route prediction, optimized route calculation etc. In disaster affected area the existence of such equipment cannot be ensured this leads to implement new mechanisms for establishment of communication in such areas .This thesis proposed an enhanced AODV protocol which can achieve for rapid communication and high throughput by making using of a cluster head for a particular region.

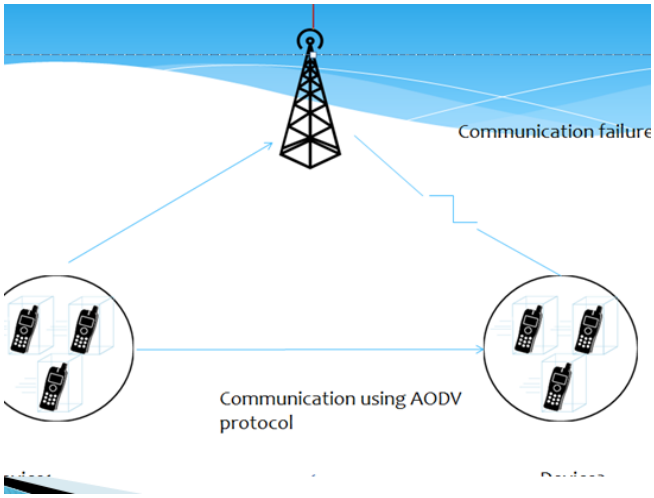

Fig 3: Communication of nodes in disaster area

In disaster area node tries to create a cluster have the same pattern ,among them the node with high speed, distance and velocity be selected as cluster head. And when a cluster member moves out from the transmission region ,it is removed from the cluster and become free .suppose the cluster head itself moves out from the region ,the remaining nodes with high speed ,distance and velocity be selected as cluster head. If two cluster head come within each other's transmission range, the cluster merging process takes place.

b. El-gamal Encryption Scheme

In this thesis the encryption of rreq and rrep header can be modified and secured with the help of a cryptosystem. In order to encrypt and decrypt the header a key transaction mode is used, in which keys are interchanged between the source and destination. This paper follows el- gamal system, which is a public key cryptosystem and modified Diffiie - Hellman protocol, comparing to this el-gamal deals with the communication scheme where both sender and receiver are not apt to collaborate in feasible time .Because of deferrals in transmission or in convenience of receiving party. It includes three processes, the key generation ,the encryption and the decryption. [8].

Key Generation

To bring about an efficient definition of a cycle groupG ,of order q, with generator g and chooses a random x ϵ {1...q-1}

$$y=g^x$$

To put out y along with the description of G ,q, g, as public key and possess x as private key which requisite be kept secret.

Encryption

To encipher a message m, to public key(G, q, g,y),and elect a random r ϵ 1...q-1 then computes

$$C_{1=}\, g^r$$

compute the shared secret as

$$s= y^r$$

To switch secret message m, into a component m'ϵ G and compute as

$$c_{2=}\, m`s$$

This sends the cipher text $(c_1,c_2)= (g^r;m',y^r)$ to key generator. Since one can simply find y^r if one knows m'. Therefore a new r, is bring out for every message to enhance security. For this reason r is also called an ephemeral key.

Decryption

To decrypt a cipher text(c1,c2) with private key x, and calculate the common secret key as

$$t=c_1^x$$

and then computes

$$m`=c_{2t}^{-1}$$

which the converts back into the plaintext message m, where t^{-1} is the inverse of t in the group G.

c. Hidden Markov Model

The important characteristics of vanet network are mobility of vehicles, where each vehicles has a particular range to communicate with its neighbor. If the destination node is within the same range the source node directly communicate, otherwise a multi hop communication is needed to establish the communication with the destination node. Because of the dynamic characteristic of vanet, the location of vehicles rapidly changes that would affect the stability of the path during the communication and path break occurs. In order to fix the problem of risk prediction for vehicles and to get back the communication ,the paper focuses on Hidden markov model that consider the mobility ,behavior, environmental, characteristic, traffic etc of the nodes.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

The conditional probability $P(q_i|x_i)$ can be rewritten[9]according to Baye's rule:

$$p(qi|xi) = \frac{p(xi|qi)p(qi)}{p(xi)}$$

or for the n items and Q sequence and sequence X as

$$p(q1 \dots qn|x1 \dots xn) = \frac{p(x1 \dots xn)|p(q1 \dots qn)}{p(x1 \dots xn)}$$

The probability P(q1…qn|x1..xn) can be estimated as $\prod_{i=1}^{n}$ as $P(q_i|x_i)$ if we assume that, for all i, the qi, xi are independent of all xj and qj ,for all j ≠ i. To get the probability, which is comparable to the probability, and which we will illustrate as the likelihood. L. P(q1…qn|x1..xn)∞L(q1…qn|x1..xn)=P(q1…qn|x1..xn).P(q1..qn)With first order Markov acceptance it turns to: P(q1…qn|x1..xn)∞ L(q1…qn|x1..xn).

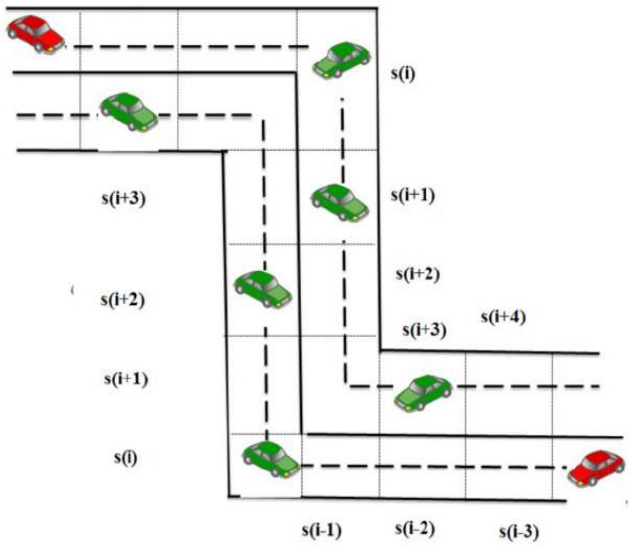

Fig 4: Vehicle Transition state

Consider ${}^{i}v_j$ be shows position and velocity of a node in a given geological area. where v^i serve as the position of a node in the area and j stand for travel time of a node in the area. By changing the state ${}^{i}v_j$ to ${}^{i+1}v_{j+1}$ the nodes either remains in the same state with same velocity and time period or vice versa. In order to realize the real-time driving risk prediction, driving state parameters of the nodes need to be collected in real time through direction and velocity. The time interval of data recovery by direction and velocity divides the continuous time variable into a discrete time series [10].

$$t = \{\dots, i-3, i-2, i-1, i, i+1, i+2, i+3, ..\}$$

The continuous emerging process of nodes driving state can be reveal as a discrete progression comparable to each discretized time moment:

$$(t) = \{\dots, (i-3), (i-2), (i-1), (i), (i+1), (i+2), (i+3), \dots\}.$$

The discrete progression (t) has steady changeability and the probability of the node being at the next state depends only on the current state and not the previous states

$$P\{S(i+1)=S'|S(i),S(i-1),\dots S(1) = P\{S(i+1)=S'|S(i)$$

d. Homomorphic Encryption

The proposed method is used to recover the data and effectively operate within a limited period of time. Time period is a critical aspect in a disaster area since the energy level of different nodes varying with respect to time .The message transmitted by the nodes during a time period cannot be re transmitted due to the energy failure or due to different energy level of the nodes this makes the re transmission of data nearly an impossible factor. Our method predicts the of data in different communication channel over a period of a time which reduce the re transmission by making use of homomorphic encryption method[11]. It is the reorganization of input into cipher text that can be classified and worked with as if it were still in its original form. It grant complicated mathematical operation to be executed on encrypted data without negotiate the encryption.

IV RESULT

In this section we depict the simulation outcome of prospective system. The modified secure aodv protocol can be successfully carry out using NS3 simulator. NS3 is a distinct-event network simulator, focus primarily for analysis and academic purpose. NS3 also backing a real-time scheduler that helps a number of "simulation-in-the-loop" use cases for cooperate with real systems. For example, users can give off and receive ns-3-generated packets on real network devices, and ns-3 can give as an interrelationship framework to add link effects between virtual machines. The paper compared modified AODV routing protocol with existing AODV routing protocol.

SIMULATION PARAMETERS

No of Nodes	50
Packet Size	512
Protocol Used	AODV
Max speed of nodes	30 m/s
Bandwidth	2mbps
Mobility mode	Random way point
Data rate	12mbps
Simulation Time	500s
Topology	1000*800m

Table I

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

OUTPUT

Average PDR	91.15%
Packet Loss Ratio	10.17%
Throughput	23.62 Kbps
Delay	0.115ms

Table II

i. Packet Delivery Ratio

The estimation of Packet Delivery Ratio is formulate on the accepted and precipitated packets as noted in the trace file. In common, it is explained as the ratio between the acquired packets by the destination and the created packets by the source.

$$PDR=\frac{\text{Number of accquired data packets}}{\text{Number of created data packets}} * 100$$

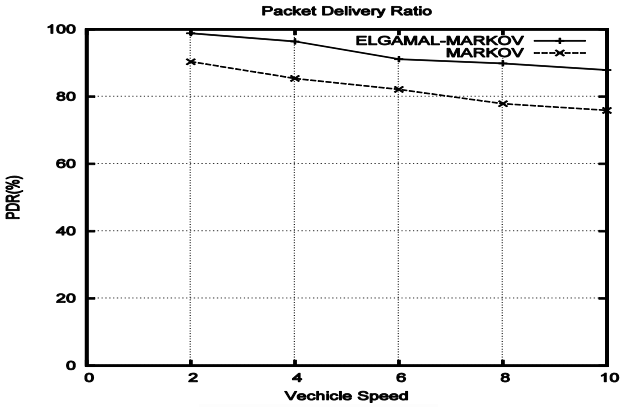

Fig 5:Packet Delivery Ratio

ii. Packet Loss Ratio

. PLR can be calculated by using the formula:

$$PLR = \frac{\text{Number of packets drop}}{\text{Number of accepted packets}}$$

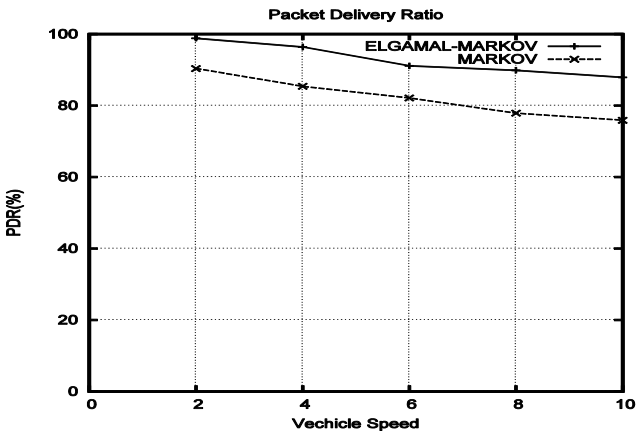

Fig 6: Packet Loss Ratio

iii. Throughput

Throughput is described as the total size of data packets accurately received by a destination node in every second. It gives the information whether the data packets are properly delivered to the destinations are not.

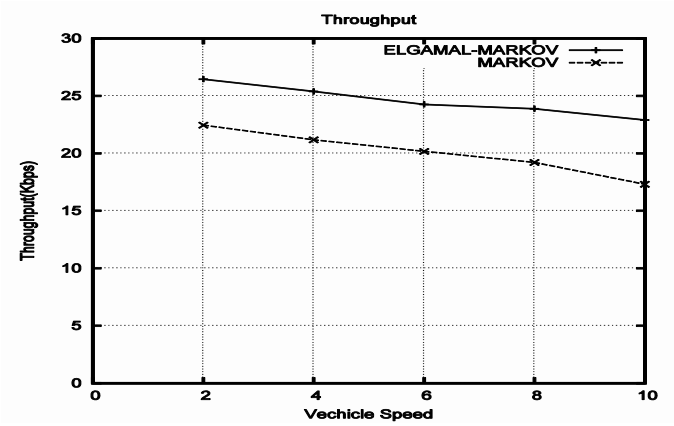

Fig 7: Throughput

iv. Delay

The moderate end to end delay consist of the queue delay and propagation delay from the origin to the destination.

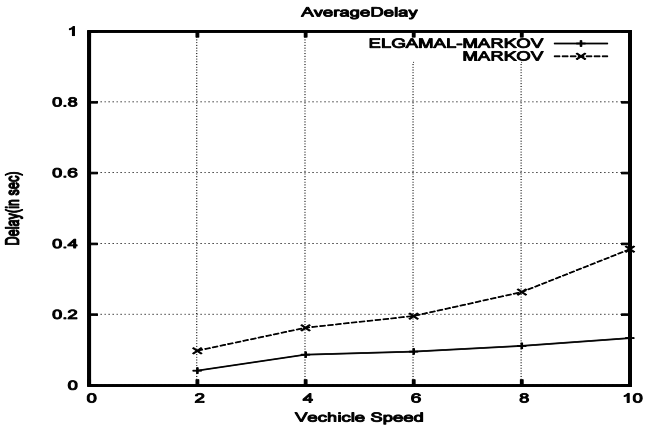

Fig8: Delay

V. CONCLUSION

The challenging task of telecommunication network and network operators is to immediately restore the communication in the disaster area. Route prediction, calculation etc during the route recovery process is a tedious task. Here we explained the variant of AODV protocol that mainly concentrates on an adhoc network. The modified AODV protocol keeps the network connectivity without a centralized infrastructure and also helps to maintain security energy efficient and quality of service etc.. The advanced method mainly concentrates on an ad-hoc network where all nodes simultaneously keeps network connectivity without a centralized framework. The modified AODV routing protocol

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

using el-gamal encryption is used for encrypt and decrypt the headers. Nodes movement in the disaster area and path prediction are effectively done by using hidden markov model and communication recovery by homomorphic encryption. The modified system with accuracy which are entitled using these procedure shows a sensational enhancement in ,packet delivery ratio, throughput, delay and packet loss etc

REFERENCES

[1] ISDSR+:Improving the Security and Availability of Secure Routing Protocol",preparation of papers for IEEE Transcations and journal volume 4,2016

[2] Neural Network Based Modified AODV Routing Protocol in VANET", Soumen Saha, Utpal Roy and Devadutta Sinha,European Journal of Advances in Engineering and Technology, 2015, 2(10): 17-25

[3] Energy Optimization in Directional Advanced Intruder Handling AODV Protocol in MANET " S.Hemalatha1, P.C. Senthil Mahesh 2018 SWANSEA PRINTING TECHNOLOGY LTD TAGA JOURNALVOL. 14 ISSN: 1748-0345 (Online).

[4] T2AR: trustaware adhoc routing protocol for MANET",Gayathri Dhananjayan andJanakiraman Subbiah,SpringerPlus (2016) 5:995

[5] POWER AWARE QOS MULTIPATH ROUTING PROTOCOLFOR DISASTER RECOVERY NETWORKS",S.Santhi, D Sadasivamr.G.Sudha, International Journal of Wireless Mobile Networks(IJWMN) Vol. 3, No. 6, December 2011

[6] Social Clustering of Vehicles based on Semi markov process",IEEE Transactions onVehicular Technology(Volume: 65 , Issue: 1 , Jan.2016).

[7] Driving Path Predication Based Routing Protocol in Vehicular Adhoc Networks",Yong Feng, Feng Wang, Jingjing Liao, and Qian Qian,Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013, Article ID 837381, 10 pages.

[8] ElGamal:Public-Key Cryptosystem, Jaspreet Kaur Grewal, Math and Computer Science Department Indiana State UniversityTerre Haute, IN,USA 9/30/2015 Hidden Markov Models ,http://www.igi.tugraz.at/lehre/CI.

[9] Vehicle Driving Risk Prediction Based on Markov Chain Model", Xiaoxia Xiong[1], Long Chen[2], Jun Liang, Hindawi Discrete Dynamics in Nature and Society Volume 2018,

[10] Homomorphic Encryption",Monique Ogburna, Claude Turnerb,Pushkar Dahalc,Published by Elsevier B.V.Selection and peer-review under responsibility of Missouri University of Science and Technology Open access under CC BY-NC-ND license.