Advancement of Network Performance using Improved AOMDV Protocol in MANET

Sweety P. Jain
Department of Computer Engineering
Hasmukh Goswami College of Engineering, Gujarat, India

Prof. Hitesh Patel
Department of Computer Engineering
Hasmukh Goswami College of Engineering, Gujarat, India

Prof. Ashwin Prajapati
Department of Computer Engineering
Hasmukh Goswami College of Engineering, Gujarat, India

Abstract

Multipath On demand protocol (AOMDV) is the hop by hop routing protocol wherein the intermediate node continues more than one course entries of their respective routing desk. The protocol ensures loop freedom and disjointness of alternate paths. In this scheme nodes are do routing with AOMDV protocol by means of using shortest path. The goal of this paper is to reduce the routing overhead with the assist of overall delay and the routes having excessive delay may be prevented from the system of packet forwarding. So in this paper we choose Cryptography to secure the packets in opposition to assaults and enhance network protection.

Keywords: AOMDV, Cryptography, ECC, Transmission power, Throughput

---

I. INTRODUCTION

Mobile ad-hoc networks (MANET) are characterised by multi-hop wireless mobile nodes that communicate with one another while not centralized management or established infrastructure. There are varied challenges in Manet like routing, dynamic topology, quantifiability, information measure optimisation. however the main challenge in Manet is link failure because of high quality. Topology-Based routing protocols become unsuitable for Manet once the nodes are extremely mobile and topology changes dynamically. Geographic routing protocols are thought to be economical and ascendible once quality is high. Therefore, geographic routing protocols have attracted plenty of attention within the field of routing protocols for Manet. Position-based approaches are planned to handle some drawbacks of topologic-based techniques by exploitation data concerning physical or geographical position of nodes which will be obtained by positioning services like GPS (Global Positioning System).

Mobile Ad-hoc networks have potential applications in civilian and military environments. The dynamic changes within the topology of Manet create routing a difficult task, because the existing path is rendered inefficient and unworkable.

Mobile impromptu Networks (MANETs) are composed of wireless nodes or devices that may join forces and communicate with every others with none mounted infrastructure. they will be used as communication infrastructure of diverse applications like vehicle-to-vehicle communication. thanks to the absence of the infrastructure and therefore the frequent quality of nodes, finding and maintaining info concerning routes could be a nontrivial task and represents the massive issue that ought to be self-addressed within the routing protocol style of mobile nodes, several problems have to be thought of so as to supply many vital properties like quantifiability, QoS support, security, low power consumption so on. Here we tend to target the safety purpose by providing the energy potency.

Finally, we'll use the elliptic curve cryptography in our planned formula that is predicated on the higher output, pdr and network improvement in Manet.

A. Objective

The objective of this research is to improve the throughput by analysis of the following parameters:

- Packet Delivery Ratio
- Throughput
- End to End Delay
- Routing Load
- Link brakeage resistant

B. AOMDV Protocol

The AODV Routing protocol uses associate on-demand approach for locating routes, that is, a route is established only it's needed by a supply node for transmission information packets. Operation of the protocol here is additionally divided in 2 functions, route discovery and route maintenance. Initially all the nodes send salutation message on its interface and receive salutation messages

from its neighbors. This method repeats sporadically to work out neighbor property. Once a route is required to some destination, the protocol starts route discovery.

The supply sends Route Request Message to its neighbors. If a neighbor has no info on the destination, it'll send message to any or all of its neighbors and then on. Once request reaches a node that has info concerning the destination (either the destination itself or some node that incorporates a valid route to the destination), that node sends Route Reply Message to the Route Request Message leader. Within the intermediate nodes (the nodes that forward Route Request Message), info concerning supply and destination from Route Request Message is saved. Address of the neighbor that the Route Request Message came from is additionally saved.

In this means, by the time Route Request Message reaches a node that has info to answer Route Request Message; a path has been recorded within the intermediate nodes. This path identifies the route that Route Request Message took and is termed reverse path. Since every node forwards Route Request Message to all or any of its neighbors, over one copy of the first Route Request Message will make a node. Once a Route Request Message is made at the leader, it's appointed a novel id. Once a node receives Route Request Message, it'll check this id and therefore the address of the leader and discard the message if it had already processed that request.

C. *Modified AOMDV*

The conception behind the changed protocol is to seek out the nodal residual energy of every route within the method of choosing path, choose the trail with minimum nodal residual energy and type all the routes supported the drizzling order of nodal residual energy. Once a brand new route with larger nodal residual energy is rising, it's once more hand-picked to forward remainder of the info packets. It will improve the individual node's battery power utilization and thus prolong the complete network's period of time. The steps concerned are:

1) Find the nodal residual energy of each route in the route discovery Process.
2) Find the path with minimum nodal residual energy.
3) Sort out all the routes based on the descending value of nodal residual energy
4) Select the route with maximal nodal residual energy to forward the data packets.

II. LITERATURE SURVEY

Sunita Gupta, Ghanshyam Prasad Dubey in "Enhanced Load Balancing and Delay Constraint AOMDV Routing in MANET" developed multiple routes to a destination, selects one route with low hop for knowledge delivery and uses it as various choices with equal or bigger hop count routes. These routes would be used for info delivery as alternate routes just in case of established link failure. The load transfer to various paths is to boost effective utilization of the network. During this analysis rate base congestion management mechanism management the incoming and outgoing packets balance in dynamic network.[15].

G. Pathak, K. Kumar in "Traffic aware load balancing in AOMDV for mobile Ad-hoc networks" developed QoS is needed for applications for an efficient communication and load balancing is a feature in the routing protocol that can help in a better use of the resources and can help to increase the performance of the network. We propose a new approach for load balancing in AOMDV routing protocol for MANETs that can enhance the network performance by selecting paths using the temporal load on the intermediate nodes and by distributing the load amongst the free nodes while transmission of data, which is proved by simulations in NS-2.

Mueen Uddin, Aqeel Taha , Raed Alsaqour , Tanzila Saba in "Energy Efficient Multipath Routing Protocol for Mobile ad-hoc Network Using the Fitness Function " developed energy consumption in MANET by applying the Fitness Function technique to optimize the energy consumption in Ad Hoc On Demand Multipath Distance Vector (AOMDV) routing protocol. The proposed protocol is called Ad Hoc On Demand Multipath Distance Vector with the Fitness Function (FF-AOMDV). The fitness function is used to find the optimal path from the source to the destination to reduce the energy consumption in multipath routing. The performance of the proposed FFAOMDV protocol was evaluated by using Network Simulator Version 2 (NS-2), where the performance was compared with AOMDV and Ad Hoc On Demand Multipath Routing with Life Maximization (AOMRLM) protocols, the two most popular protocols proposed in this area.

Rajaram Jatothu, Dr. RP Singh in "Efficient routing and High security transmission using AODV and Distributed protocol key generation with Dual RSA" developed higher security in Mobile Ad-Hoc Networks (MANET), Ad hoc On-Demand Distance Vector-Dual RSA-Quantum Cryptography (AODV-DRSA-QC) technique is introduced. In this AODV-DRSA-QC method, Cryptography method is employed for security purpose in between the source (Alice) and destination (Bob) with the help of Key values. In our AODV-DRSA-QC system, QC method is used for same encryption purpose and the cryptographic key is additionally encrypted through the dual RSA method as well as Advanced Encryption Standard (AES) is employed to encrypt and decrypt the message based on the Dual RSA key. AODV algorithm is employed for Routing purpose. The AODVDRSA-QC method gives better results in terms of throughput, number of alive nodes, number of dead nodes, and energy compared to the existing systems.[19].

K.S.Abitha, Anjalipandey , DR.K.P.Kaliyamurthie in "Secured Data Transmission Using Elliptic Curve Cryptography" developed survey about Secured data transmission using elliptic curve cryptography. The main problem in existing system is security issues in transmitting data between source and the destination. After the survey on various literature papers, we are concluding a new way, that increases security considerations of the network using AODV algorithm for transfer of data and to increment the efficiency of AODV algorithm using ECC(Elliptic Curve Cryptography). Efficiency, and reliability will be increased

for each transmission of data, while enclosing the proposed method by using the ECC algorithm which allow itself to encrypt and decrypt the data that is to be transferred and performs the active classification.

III. PROBLEM STATEMENT

Mobile Ad Hoc network are maintained dynamic topology with random mobility that we can't identify the location of nodes. Multipath protocols have definitely sort the problem of single path by providing alternative route in between sender and receiver. It means, if the existing route is break than in that case the alternative route is available but it is not providing the location of mobile nodes. AOMDV has more message overheads during route discovery due to increased flooding.

IV. PROPOSED METHOD

In MANET, provision of secure communication protocol should satisfy the following security requirement.

1) Mutual Authentication: Ensures the authenticity of communicating nodes mutually.
2) Confidentiality: Ensures the secrecy of the message content is known only between the authenticated communicating nodes (or users).
3) Data Integrity: Ensures the receiver, that the received message is intact.
4) Non - Repudiation: Ensures the origin of the message cannot deny having sent the message.
5) Non - Impersonation: Ensures unauthorized users cannot pretend to be an authorized one to do malfunction.

A. *Why ECC?*

Elliptic Curve Cryptography (ECC) is used to describe group of cryptographic tools and protocols where the security is based on the discrete logarithm problem. ECC is based on sets of numbers and equations that are associated with elliptic curves.
ECC works in the following phases:

1) Key Generation

a) Global Public Elements

1) Ep(a,b) elliptic curve with parameters a, b & p in the equation: Y2 mod p=(X3 +aX+b) mod p
2) G is the base point on elliptic curve

b) User A Key Generation

1) Select private key nA ; nA< n
2) Calculate public, P = nA × G

c) User B Key Generation

1) Select private key nB ; nB < n
2) Calculate public , M = nB × G

Generation of Secret Key by user A

$$P1 = k = nA \times M$$

Generation of Secret Key by user B

$$P2 = k = nB \times P$$

The two calculations produce the same result because nA × M = nA × (nB × G) = nB × (nA × G) = nB×P.

2) ECC Encryption

- Consider a message 'Pm' sent from A to B.
- 'A' chooses a random positive integer 'k', a private key 'nA' and generates the public key PA = nA × G .
- Chooses G, the base point selected on the Elliptic Curve Ep (a, b).
- Produces the ciphertext 'Cm' consisting of pair of points Cm = { kG , Pm + kPB } = (C1,C2) where, PB= nB × G ,
- The public key of B with private key 'nB'.

3) ECC Decryption

- To decrypt the ciphertext, Cm, B multiplies the first point in the pair, C1 by B's secret key.
- Subtracts the result from the second point, C2,

Pm + kPB - nB (kG) = Pm + k (nB G) – nB (kG) = Pm
Subtracts the result from the second point, C2,
PM + KPB - NB (KG) = PM + K (NB G) – NB (KG) = PM.

B. *Flow Chart of the Proposed Algorithm*

The AOMDV protocol first discovers the multipath route to the destination and sends the encrypted packet to it. The flowchart of the discovery is shown in Fig. 5.1. After discovering the route to the destination, the data packet is encrypted by ECC. This is done by creating a secure agent that generates the encrypted packet. The packet is then reached the destination through one of the selected multipaths.

Fig. 1: Flow chart for route discovery with AOMDV protocol

C. *Proposed Algorithm*

1) Step 1: Declaration of source and destination node.
2) Step 2: Broadcast every RREQ.
3) Step 3: Now it find next hop.
4) Step 4: Then process every RREQ
5) Step 5: It encrypt every packet with ECC.
6) Step 6: Select node with higher residual energy.
7) Step 7: If node found with same energy & distance, Packets will be transmitted according timestamp value otherwise, Continue until the destination is found.
8) Step 8: If both node with same energy then, packets transmitted according to their timestamp valu otherwise, packet from higher energy will be transmitted first.
9) Step 9: Packets successfully received by the destination.

V. SYSTEM IMPLEMENTATION

The entire simulations were administrated mistreatment NS-2.31 network machine that may be a separate event driven simulator developed at UC Berkeley as a component of the VINT project. The prime goal of NS-2 is to support analysis and Education in networking. it's appropriate for coming up with new protocols, scrutiny completely different protocols and traffic evaluations. NS-2 machine developed as cooperative atmosphere of networks is distributed as open supply code. sizable amount of Institutes and Researchers use it as network machine tool for epitome of network simulation in analysis studies.

The simulations were performed using network simulator 2(NS-2.34) which is popular in the adhoc networking community. The traffic sources are CBR (continuous bit rate), data packet size is 512 bytes. The source – destination pairs are spread randomly over the network in a rectangular filed of 1000 *500. The simulation time is 300 seconds. The primary energy of all nodes is 50 joules.

Table - 1
Simulation Parameters

Parameters	*Value*
Simulator	*NS-2 (Version 2.34)*
Channel Type	*Wireless*
MAC Type	*Mac/802.11*
Mobility Model	*Random way point Mobility Model*
Numbers of Mobile nodes	*60 nodes*
Traffic Type	*CBR*
Routing Protocols	*AOMDV*
Simulation Time	*3000 ms*
Simulaton Area	*1000/500m*
Packet Size	*512 bytes*

After performing simulation as per simulation environment, a NAM file is generated as in Fig. 2 NAM file shows the graphical representation of packet transfer between nodes of a MANET.

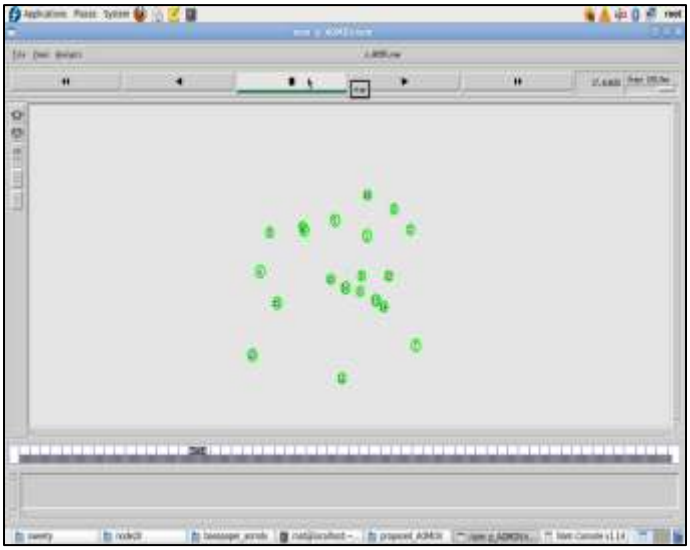

Fig. 2: NAM file

Fig 2 is NAM file generated for improved AOMDV protocol. Node has green color indicated it has high energy.

A. Simulation Results and Charts

Table – 2
Simulation Result- 1 (for 60 nodes)

No. Of Packets	*Basic AOMDV*	*Proposed AOMDV*
Sent	*1039*	*1045*
Received	*879*	*1036*

Table - 3
Simulation Result- 2 (for 20 nodes)

No. Of Packets	*Basic AOMDV*	*Proposed AOMDV*
Sent	*2452*	*2454*
Received	*2337*	*2396*

Table - 4
Simulation Result- 2 (for 60 nodes)

Types	*PDR*	*Average Throughput*
Basic AOMDV	*84.69 %*	*49.68*
Proposed AOMDV	*99.16 %*	*65.54*

Table – 5
Simulation Result- 2 (for 20 nodes)

Types	*PDR*	*Average Throughput*
Basic AOMDV	*95.31 %*	*77.83*
Proposed AOMDV	*97.64 %*	*79.71*

B. Experimental Results

1) Energy Efficiency for basic AOMDV and Proposed AOMDV

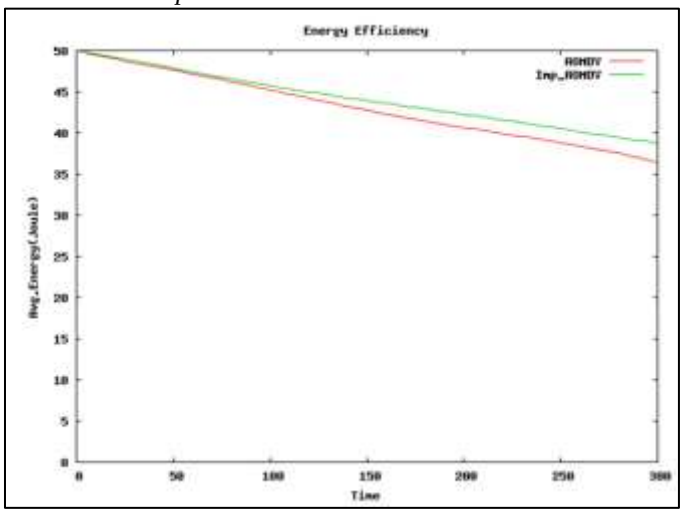

Fig. 3: Energy Efficiency for basic and Proposed AOMDV

Fig 3. Shows the Energy Efficiency for basic and Proposed AOMDV.

2) Packet delivery ratio for 20 nodes and 60 nodes for Basic AOMDV and Improved AOMDV

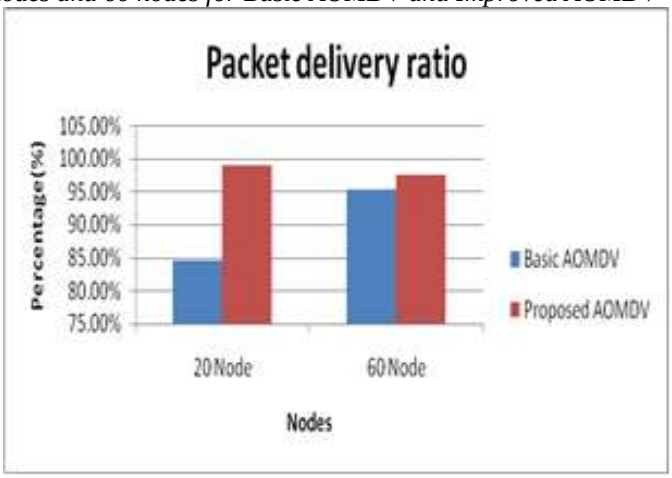

Fig. 4: Comparison of Packet delivery ratio for 20 nodes and 60 nodes for Basic AOMDV and proposed AOMDV

Fig 4. Indicates the comparison of Packet delivery rati of Basic AOMDV and Improved AOMDV is increase for 20 nodes and 60 nodes.

3) Average Throughput for 20 nodes and 60 nodes for Basic AOMDV and Improved AOMDV

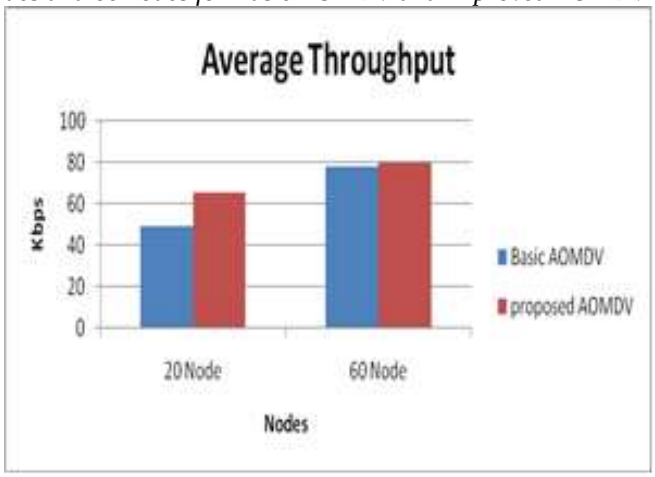

Fig. 5: Comparison of Average Throughput for 20 nodes and 60 nodes for Basic AOMDV and proposed AOMDV

Fig 5. indicates the comparison of Average Throughput of Basic AOMDV and Improved AOMDV is increase for 20 nodes and 60 nodes.

VI. CONCLUSION

Here we implement elliptic curve cryptography which provide an energy efficiency higher than AODV when compared with AOMDV. ECC algorithm which allow itself to encrypt and decrypt the data that is to be transferred and performs the active classification.

Therefore the long lifetime of the nodes in the network is achieved and with an increased throughput and packet delivery ratio. Simulation results show that using the proposed algorithm creates a significant improvement in energy efficiency, PDR and throughput using 25 nodes and 60 nodes.

VII. FUTURE WORK

We will try to achieve more improvement in proposed method. Also try another type of technique to improve network performance by using increasing throughput, packet delivery ratio and performance of the network

REFERENCES

[1] "Mueen Uddin,Aqeel Taha1,Raed Alsaqour,Tanzila Saba, "Energy Efficient Multipath Routing Protocol for Mobile ad-hoc Network Using the Fitness Function", IEEE-2017.
[2] "Mohammed Moizuddin , Dr.Joy Winston, Mohammed Qayyum, "Quantum Cryptography"978-1-5090-5814-3/17/$31.00 ©2017 IEEE.
[3] "Sunita Gupta, Ghanshyam Prasad Dubey , "Enhanced Load Balancing and Delay Constraint AOMDV Routing in MANET", 978-1-5090-0669-4/16/$31.00 © 2016 IEEE .
[4] "Ms. V. Padmavathi , Dr. B. Vishnu Vardhan , Dr. A. V. N. Krishna ,"Quantum Cryptography and Quantum Key Distribution Protocols: A Survey ", 2016 IEEE 6th International Conference on Advanced Computing.
[5] "Dr. RP Singh Professor, Rajaram Jatothu, Efficient routing and High security transmission using AODV and Distributed protocol key generation with Dual RSA, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 23 (2017)".
[6] "Mrs. Poonam Meghare, Prof. Preeti Deskhmukh, Packet Forwarding using AOMDV Algorithm in WSN , International Journal of Application or Innovation in Engineering & Management (IJAIEM)."
[7] "Prof. Hitesh Patel, Advancement in Performance of Wireless AdHoc Network using AOMDV in MANET. IJIRST –International Journal for Innovative Research in Science & Technology - March 2018 ".
[8] "Neha Ingley, Prachi Gawande, Latency Reduction with Cryptography based security in MANETs, International Research Journal of Engineering and Technology (IRJET)- April 2016".
[9] "Gaurav Pathak, Krishan Kumar, Traffic aware load balancing in AOMDV for mobile Ad-hoc networks, Journal of Communications and Information Networks, Vol.2, No.3, Sept. 2017".
[10] "Brahm Prakash Dahiya, Performance Analysis and Evaluation of AODV & AOMDV in MANET, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering – January 2014 ".
[11] "Jeenat Sultana , Tasnuva Ahmed Department of Computer Science and Engi, Securing AOMDV Protocol in Mobile Adhoc Network with Elliptic Curve Cryptography , International Conference on Electrical, Computer and Communication Engineering (ECCE), February 16-18, 2017".
[12] "Khushboo Gandhi , Pinakini Patel , Nisarg Patel, ANALYSIS OF NETWORK PERFORMANCE USING IMPROVED DREAM PROTOCOL IN MANET , International Journal For Technological Research In Engineering Volume 3, Issue 7, March-2016".
[13] "Jaya Jacob , V. Seethalakshmi , EFFICIENCY ENHANCEMENT OF ROUTING PROTOCOL IN MANET , International Journal of Advances in Engineering & Technology, May 2012. ".
[14] "P.Periyasamy,Dr.E.Karthikeyan , PERFORMANCE EVALUATION OF AOMDV PROTOCOL BASED ON VARIOUS SCENARIO AND TRAFFIC PATTERNS , International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.1, No.6, December 2011".
[15] "Neetha Paulose, Neethu Paulose" , Comparison of On Demand Routing Protocols AODV with AOMDV, International Journal of Science, Engineering and Technology Research (IJSETR), Volume 5, Issue 1, January 2016".
[16] "Fubao Yang, Shengzhi Ling, Hui Xu, and Baolin Sun", Network Coding-based AOMDV Routing in MANET, 2012 IEEE International Conference on Information Science and Technology Wuhan, Hubei, China; March 23-25, 2012".
[17] "Surendra Ladiya , Enhance multipath routing in topology transparent network for better QoS in MANET, IJECS Volume 05 Issue 12 Dec., 2016".
[18] "Ajay Kumar, Rohit Vaid, Sandhya Katiyar, Shumaila Rizwan, Adaptive Data Size Compressed Algorithm to Reduce Energy and Provide Route Security using AOMDV Protocol in WSN, International Journal of Computer Applications , August 2016.
[19] "Achu Anna Antony, Bino Thomas, Enhanced Mobile Ad-hoc Routing Technique based on Reduction in Packet Loss, IJESC-2018".
[20] "V.Chandrasekaran, K.Lalitha, Secure Energy Aware Multi-hop Routing Protocol for Wireless Sensor Networks, IJARCS-2010".