International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 9 (2015) pp. 23909-23923

http://www.ripublication.com

Optimizing Energy Consumption and Providing Security Using Hybrid Approach in MANET

Pooja Chahal

M.Tech Student

Lovely Professional University

Phagwara, Punjab

Pjchahal.chahal86@gmail.com

Gaurav kumar Tak

Assistant Professor

Lovely Professional University

Phagwara,Punjab

gauravtakswm@gmail.com

Anurag Singh Tomar

Assistant Professor

Lovely Professional University

Phagwara, Punjab

anuragtomar3105@gmail.com

Abstract

In recent years wireless communication become common. Wireless networks can be in infrastructure or infrastructure less. Mobile Ad hoc Network (MANET) is special type of infrastructure less network. Since MANET is infrastructure less so nodes does not form any topology. The communication is done with the help of routing protocols. Due to high mobility and multipath propagation network is vulnerable to attacks. There are various attacks that can be possible on MANET like Denial of Service attack, Black hole attack, Wormhole attack, Sybil attack etc which can disturb the communication between the nodes. There are many techniques to prevent or control this attack. But each technique may slow down the process of data transfer. So there is need for some improvement in routing protocol to transfer the data at high speed. The aim of the thesis is to combine two protocols (DSR and AOMDV) and make a hybrid protocol and then apply SBPGP on it. In this work an attempt is made to enhance security using SBPGP security model, minimizing RREQ, minimizing the energy consumption, time complexity and

increasing the network lifetime. Simulation is done on MATLAB and compared with the original protocols.

Keywords: AOMDV, DSR, RREQ, SBPGP

Introduction

A wireless network is a network that does not require any wires for communication. All the nodes or hosts in a network are wirelessly connected with each other. It does not require any set of cables so it is a cheap process as compared to wired connection. Generally homes, enterprises, telecommunication networks prefer wireless communication over wired. An ad hoc network is a network that is formed by collection of two or more nodes (devices) that moves in an unpredictable manner. It follows infrastructure architecture yet has a potential of service discovery, routing and packet forwarding [1]. These networks are autonomous and decentralized in nature. The nodes present in network can anytime join or leave the network. All nodes should be able to find the presence of other nodes so that further communication and sharing of data can take place [2]. As there is diversity in the wireless devices so the battery capacity also varies tremendously from one device to another device. For the communication purpose routing protocols are used. They basically transfer packets or information from source to destination. There are three types of routing protocols

- Table drive routing protocols
- On demand routing protocols
- Hybrid

In table driven routing protocols every node has to maintain its routing table which contains all the information of source and destination and nodes position [3].

In on demand routing protocol whenever communication needs to take place then first it will check for its cache it the route exists it will retrieve that route and if route does not exist then only it will start route discovery. There are two processes of on demand routing protocol, one is route discovery in which route is discover only when it is demanded and second one is route maintenance in which if there is any route failure or link breakage then RERR message will be sent back and then new route is selected [3].

Hybrid routing protocol is a combination of both table driven routing protocols and on demand routing protocols [3].

Literature Review

Madhup Shrivastava, M.A Rizvi [4] discussed about the problem of packets dropped and provided a solution for the same and it also increases Packet Delivery Ratio using Dijkstra's algorithm. Dijkstra algorithm is used find out the shortest distance between source and destination. This algorithm has great significance in routing. Basically Dijsktra's algorithm was first used to find out the shortest distance

between one city to another city. In this paper author used Euclidean distance to find out the distance between nodes and it can be calculated by using a formula:

$\sqrt{(X_n^2-X_m^2)} - (Y_n^2-X_m^2)$

Where M (X_m, Y_m) are the coordinates of node M

N (X_n, Y_n) are the coordinates of node N

If distance ≤ Transmission Range then nodes are said to be neighbors

If distance ≥ Transmission Range then nodes are not considered to be neighbors

Then the shortest distance will be selected and message will be transmitted through this route only. By using this technique author solved the problem of packet dropped, link breakage, mobility and scalability. This method also increases the packet Delivery ratio.

R.Senthil Kumar and Dr. C.Suresh kumar [5] discussed about a method that will minimize the Route Rediscovery Process. Author used two schemes to do so. First one will minimize the Route Discovery process by applying flooding process optimization algorithm which uses TTL (Time to Live) value to find out the stable route between sender and receiver. Second scheme will minimize the link failure by using Received Signal Strength (RSS) value. With these methods author improved the performance of AODV protocol by minimizing route request message during route discovery process. Also this method has very effective result as compared to original AODV.

J. Nandhini and D.Sharmila [6] proposed a new energy efficient mechanism known as Modified Progressive Energy Efficient Routing (MPEER) with scheduling mechanism. In this method threshold value is set for all the nodes and shortest path will be selected between source and destination. If there are many shortest paths between source and destination then the efficient one and the foremost one will be selected.

- If energy of source node > Link cost +energy of neighbor nodes, then nodes will be discarded
- If energy of source node < Link cost +energy of neighbor nodes, then nodes will be considered as intermediate nodes.

This procedure will go on and choose all the intermediate nodes between source and destination. Once the destination will be found the RREP message will be sent back using these intermediate nodes. Once the path is selected then for each node transmission power will be checked and store in RREQ message with its ID. At last priority based packet scheduling is applied on it. Result shows that less energy is consumed for path setup and delay is also minimized.

Ranjeet Singh and Harwant Singh Arri [7] discussed about the multicast routing protocol IODMRP and AAMRP. A security model known as SBPGP applied on these protocols to provide some set of security. Performance is analyzed by observing various parameters like Packet Delivery Ratio, throughput and end to end delay. Result shows that AAMRP proved to show better Quality of Services parameters and IODMRP shows better result in end to end delay as compared to AAMPRP.

Indrani Das, D.K Lobiyal and C.P Katti [8] discussed about the effect of node mobility on A OMDV. Three models have been discussed in this paper. First one is Random Waypoint model, in this model movement of node depends on mobility speed and pause time. Second one is Probabilistic Random Walk mobility model, in this movement of nodes depend on probability defined in probability matrix. 3 states were defined in this model 0 represents current state, 1 represents previous state and 2 represents next state. P (a,b) means probability that a node P moves from position a to position b. Third model is Random direction model, in this node can only move up to the boundary of simulation area and after reaching to boundary it will pause for some time. Then it will choose random direction from 0 to 180 degree. Result shows that random direction proves better than other model.

Abhishek Gupta and Samidha D Sharma [9] reviewed various methods of location based routing like Location Aided routing (LAR), Location Area Based Ad hoc Routing (LABAR) protocol, ALARM, Distance Routing Effect Algorithm for Mobility (DREAM), Greedy Perimeter Stateless Routing (GPSR), Local Area based Routing protocol called Location Aided (LARDAR), Energy efficient Location Aided Routing, A Location based Routing scheme for opportunistic networks. Each method has common aim to reduce overhead, minimizing the energy and end to end delay.

Maqsood Razi and Jawaid Quamar [10] had proposed a security model for small networks using Seniority based trust model and PGP type authentication service. Author also explained some of the related algorithm such as mechanism of certification authentication and certificate revocation mechanism. Then the performance is estimated and author concluded that the particular model is easy, reliable, efficient and easy to deploy.

Proposed Work

In this work two protocols one is Dynamic Source Routing (DSR) and Ad hoc on demand distance vector routing (AOMDV) is combined to make a hybrid protocol and then a security model Seniority Based Pretty Good Privacy (SBPGP) is applied on it.

Dynamic Source Routing (DSR)

Dynamic source routing is an on demand routing protocol. Route discovery process will be started only when it is required. In this protocol Route Request (RREQ) is send to all the neighbors of the node. And then these nodes will further send RREQ message to their neighbors and this process will go on until destination source is found out. Each node contains a sequence number and the path it has traversed.

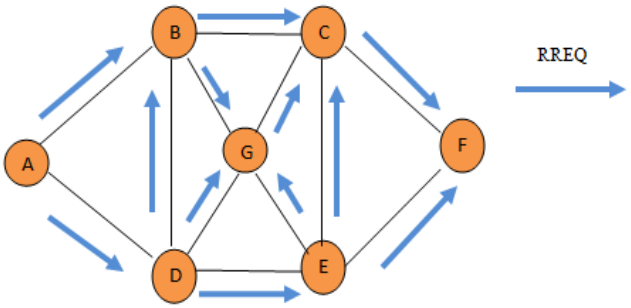

Figure 1: Dynamic Source Routing

In figure 1 source is node A and destination is F. Node A send RREQ message to its neighbor i.e. to node B and node D then node B and node D will further send RREQ message to their neighbors and this process will go on until RREQ is reached to destination F.

ADHOC on Demand Multipath Routing Protocol (AOMDV)

It is the advance version of Ad hoc on demand distance vector (AODV) routing protocol. In this for every route discovery process multiple paths is discovered. It keeps the information of hop counts and next hops and assigns the same sequence number to next hops. When RREQ message is reached to destination then RREP is traversed back through multiple paths. If any route failure is there then alternate route is selected. New route discovery is needed when all routes fails. AOMDV is used to compute multiple loop free and link disjoint paths [11].

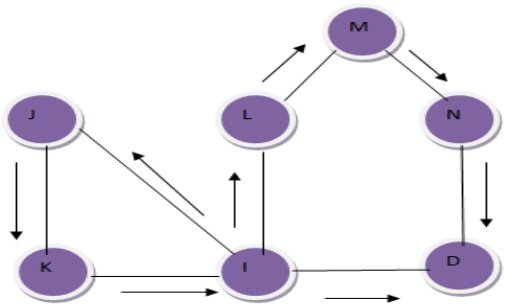

Figure 2: Routing loop with multipath computation

Security Model: Sb Trust Model

In this work for issuing PGP type certificate SB model is applied. Suppose a MANET is established in an area where many people are communicating with each other and the wireless channel over which they are communicating is not secure. Let us consider there are N nodes and they are randomly moving from one place to another and any mobile node if free to join or leave the network at any time. In this scenario the

mobile nodes that joined the network at the beginning are said to be senior nodes and the nodes that joined the network later on that are said to junior nodes.

In this model two or more senior nodes collectively form a Certifying Authority (CA). Whenever a new node comes in the network these senior nodes will check all the information about that new node and if they are satisfied with the information then only they collectively sign on the certificate of new node [12].

SN = ceiling (N × M %) + 1
SCA = ceiling (SN × K%) + 1
JN = N – SN
Where
SN is senior nodes
JN is junior nodes
N is total number of node in the network
SCA is set of nodes required for CA functionality
M is variable %
K is variable % (depends on M)

Proposed Methodology

Step 1) Combine two protocols to make a hybrid protocol using this algorithm
Algorithm 1 send data
If route exist && energy> threshold
Then send (packet DATA)

Else
For each NODE
If co-ordinates of node are in between sender and destination
Then send (packet RREQ)
End if
End for
i=0
repeat
if NTT is elapsed **then** NTT=NTT*2 **endif**
i=i+1
until i>=3 **and** no RREP is received
if RREP is received **then**
update the routing table
send DATA to destination
else cannot reach the destination
endif
endif
endif

Algorithm 2 receive_RREQ
If source.RREQ_ID< node.RREQ_ID **then** drop the packet RREQ

Else
update the reverse route to the source if necessary
if node know a path to destination **then** send the packet RREP
else
save the Previous_IP into RREQ_LIST
if source.RREQ_ID>node.RREQ_ID **then** update RREQ
update node.RREQ_ID
If node's co-ordinate is in between sender and destination
Then send packet RREQ
Endif
endfor
endif
endif
endif

Algorithm 3 receive_RREP

Delete from the RREQ_LIST the node whose address is equal to RREP_PREVIOUS_IP Send the packet RREP only to the nodes whose addresses are stored in RREQ_LIST.

Step 2) Create a wireless ad hoc network with multiple nodes that are connected wirelessly with each other.

Step 3) Select the source and destination (node from which the data has to be send)

Step 4) Both the protocols that are used in this work are on demand routing protocols so the resulting hybrid protocol is also on demand routing protocol. On demand routing protocol initiate the route discovery process only when it is demanded.

Step 5) Start the route discovery process

Step 6) Initially all the nodes were idle. As soon as route discovery process starts Route Request (RREQ) message is send to only those nodes whose coordinates fall in between the source and destination and the nodes which is in the range of source and destination. And all other nodes will remain idle. But when comparison is done with the original method then in that case RREQ message is send to all the neighboring nodes then these neighboring nodes will further send RREQ message to their nodes and so on until destination is found. In this method no node will remain idle. Every node has to take part in the route discovery process no matter if in future they are used or not in the communication. As all the nodes are used so energy consumption is more in this case but in our method the nodes which are idle does not consume any energy and hence energy consumption is less.

Also previous method (DSR and AOMDV) is time consuming as compared to new method because RREQ message is send to all nodes present in the network.

Step 7) Once the RREQ message is received by the destination through intermediate nodes then RREP will be sent back to source by selecting the shortest and most stable path. It is done by using Dijkstra's algorithm. It is used to find the shortest distance between source and destination.

Step 8) When the path is selected then Route Reply (RREP) message is send from destination to source through the shortest path which is accompanied by certification number which is unique for every route and it will provide security to the network.

Results

Implementation of the proposed technique shows that there is minimization in Route Discovery process and energy and enhancement in the security.

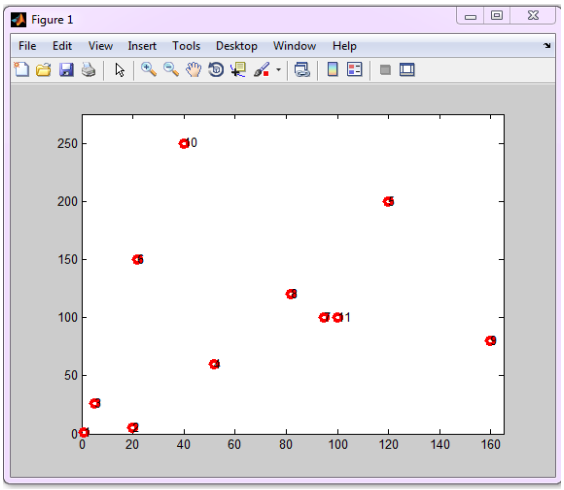

Figure 3: MANET

This figure represents Mobile Ad hoc Network

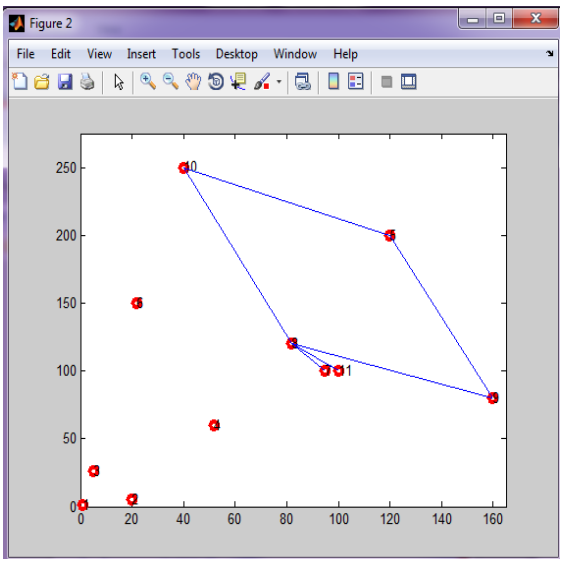

Figure 4: Source is 10 and Destination is 9

In figure 4 RREQ is sent to only those nodes whose coordinates fall in between source and destination, no other nodes will get RREQ message from source

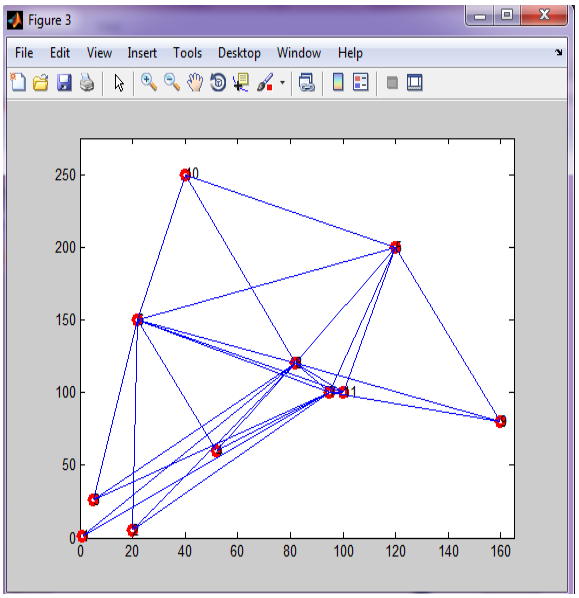

Figure 5: Path selected in original DSR and AOMDV

In figure 5 RREQ is sent to all nodes that are present in the network

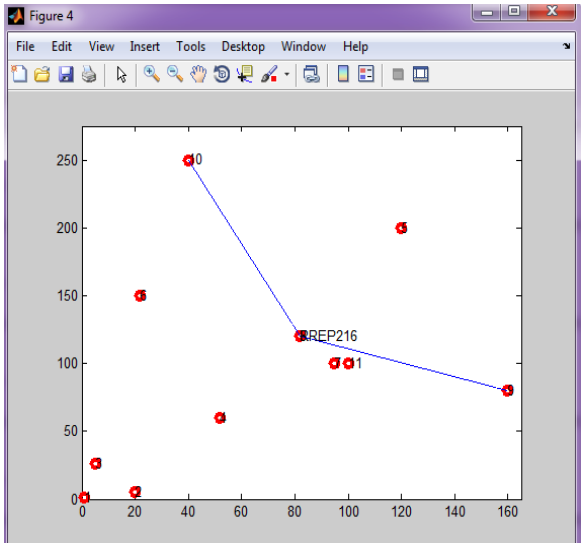

Figure 6: RREP from node 9 to 10

In figure 6 RREP is sent back from destination to source by choosing shortest path (using Dijsktra's algorithm)

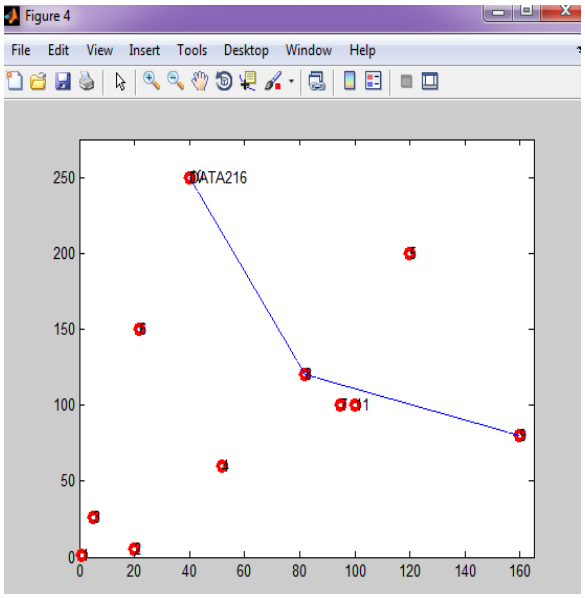

Figure 7: Data sent from source to destination with certification ID

In figure 7 data is sent from node 10 to node 9 and it has certification ID which is different for different path and in this case it is 216.

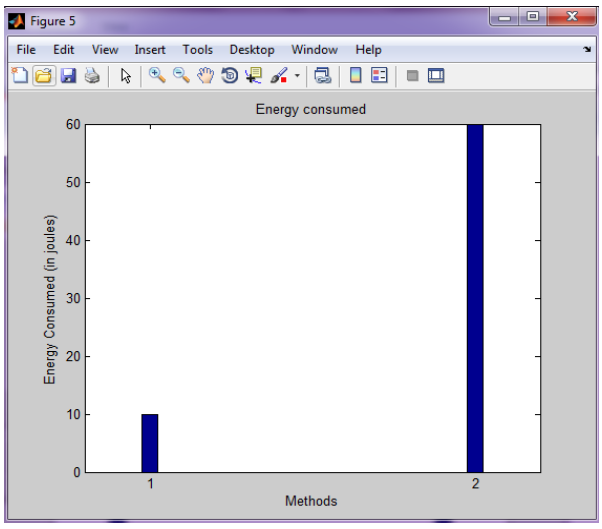

Figure 8: Energy consumed in method 1Vs method 2

Figure 8 represents total energy consumed in new method and previous method. And it is shown that new method consumes less energy as compared to previous method

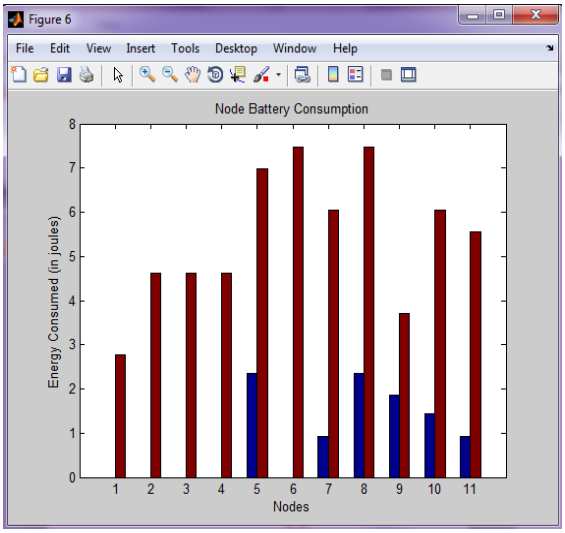

Figure 9: Energy consumed by each node

New method

Previous

From figure 9, it is clear that all nodes are consuming energy because in DSR and AOMDV RREQ are sent to all the nodes. Hence energy consumption in this case is more as compared to new method as only node 5, 7, 8, 9, 10 and 11are involved.

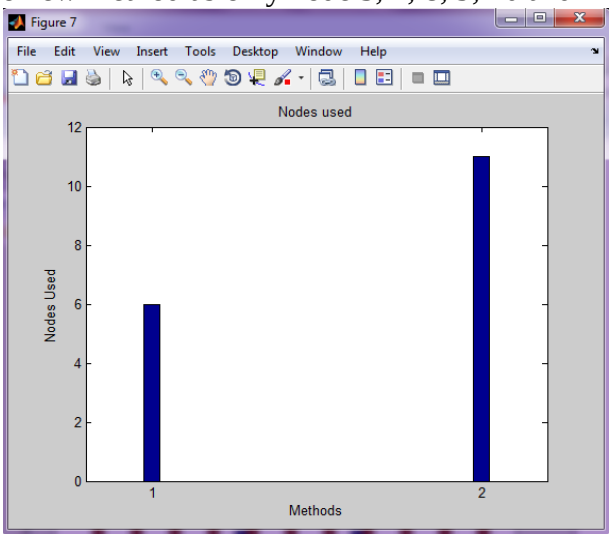

Figure 10: Nodes used in method 1 Vs method 2

Figure 10 shows that number of nodes used in both the method and less number of modes are used in method 1 i.e. new method.

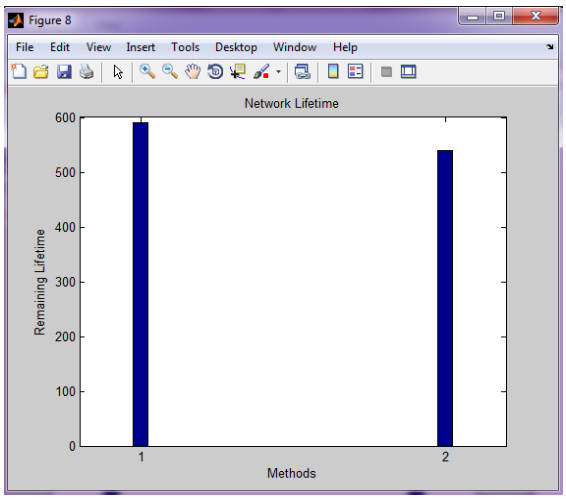

Figure 11: Remaining lifetime of new method Vs old method

Figure 11 represents how much lifetime is remaining and it shows method 1 have more remaining lifetime than method 2.

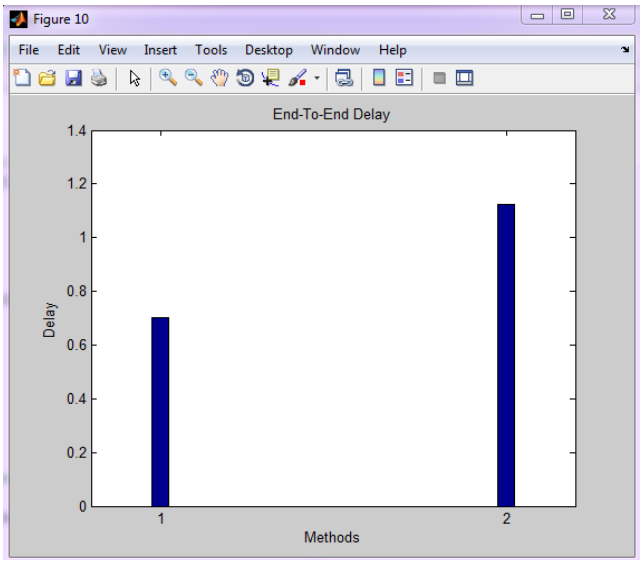

Figure 12: End -to-End delay of method 1 Vs method 2

Figure 12 clearly shows that end-to-end delay in method 1(new) is less than old method.

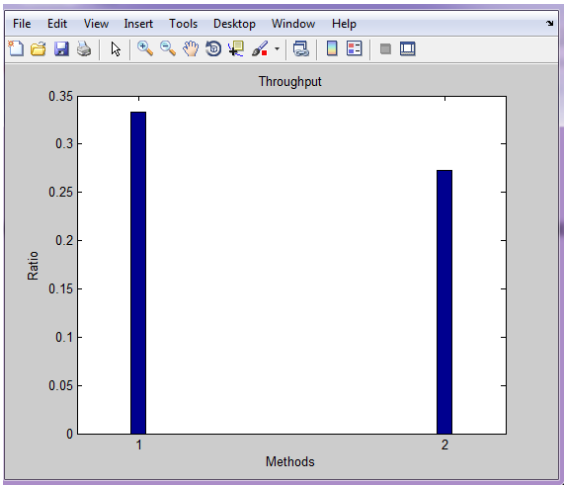

Figure 13: Throughput

Figure 13 shows that through of new method is higher than old method

```
failure occur at:
No failure

New
path:
    10     8     9

duration:
  3.6667e-004


All
path:
    10     8     9

duration:
  4.0000e-004

efficiency in %=
    8.3533
```

Figure 14: Duration and Efficiency

Figure 14 shows the duration or time taken to send data from source and destination. Here new path represents new method and all path represents old method. And efficiency is also shown in this figure which is approx 8% greater than old method.

Conclusion and Future Scope

Successfully implementation of a hybrid approach in MANET has been done in this paper and it is giving good result in terms of energy, time, security and efficiency. Minimization of energy is there which is done by using a technique in which RREQ is only send to those nodes whose coordinates come in between source and destination. And if nodes coordinates are not in between source and destination then that node will be discarded. Then RREP is sent back from destination to source using the shortest path .This technique proves to be advantageous as rest of the nodes present in the network will not lose their energy and they will remain idle. Time complexity is also reduced. And security is provided by using SBPGP security model. When RREP message is sent back it is attached with certification ID (which is unique for every path). And when any other node try to send packet then it is not possible because of this certification ID. Hence by applying all these techniques efficiency of the network is also improved. In future this technique can be applied to various multicast routing protocols like Distance Vector Multicast routing protocols (DVMRP) and Multicast Open Shortest Path First (MOSPF).

References

[1] Toh, C.K. 2001, "Ad hoc mobile wireless networks: protocols and systems", Pearson Education.

[2] Aarti., Tyagi, S.S., 2013, " Study Of Manet: Characteristics, Challenges, Application And Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013 ISSN: 2277 128X, pp. 252-257.

[3] Ali, M., Sarwar. Y., 2011," Security Issues regarding MANET (Mobile Ad Hoc Networks): Challenges and Solutions", Thesis no: MCS-2011-11.

[4] Shrivastava, M., Rizvi., M. A., 2013,"A proficient approach to amplify packet delivery ratio adapting shortest path algorithm", International Journal of Computer Application, Issue 3, Volume 14, ISSN: 2250-1797

[5] Kumar, R.S., Kumar, C.S., 2014,"Miniminzing the route rediscovery process in MANET", Journal of Theoretical and Applied Information Technology, Volume 6, No.3, ISSN 1992-8645, E-ISSN 1817-3195.

[6] Nandhini, J., Sharmila, D., 2013,"Power aware progressive energy routing protocol for MANET", International Journal of Computer Application (0975-8887), Volume 80, No.6

[7] Singh, R., Arri, H.S., 2013,"Analysis of QOS parameters of AAMRP and IODMRP using SBPGP security model", International Journal of Computer Application (0975-8887), Volume 69, No.15.

[8] Das, I., Lobiyal, D.K., Katti, C.P., 2014, ”Effect of node mobility on AOMDV protocol in MANET”, International Journal of Wireless and Mobile Networks (IJWMN), Volume 6, No.3.

[9] Gupta, A., Sharma, S.D., 2014,”A survey on location based routing protocols in MANET”, International Journal of Computer Science and Information Technology, Volume 5(2), ISSN 0975-9646

[10] Maqsood, R., Quamar.2008. A Hybrid Cryptography Model for Managing Security in Dynamic Topology of MANET, Biometrics and security Technologies, ISBAST 2008, International Symposium on IEEE, 2008 , pp. 1-7.

[11] Marina, MK., Das, SR. 2006. Ad hoc on-demand multipath routing protocol, Wireless communication and mobile computing.

[12] Mittal, N., Janish. 2013. Performance Evaluation of AODV and DSDV under Seniority Based Pretty Good Privacy Model (SBPGP). International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 943 ISSN 2229-5518.

23924 *Pooja Chahal,Gaurav Kumar Tak, Anurag Singh Tomar*