Scientific Journal of Impact Factor (SJIF): 4.72
e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 8, August -2017

An efficient and Secure AMDMM routing protocol in MANET

Neha Sharma[#1], Dr. Harpal Singh[*2]

[# CGC]College of engineering, Mohali,Landra, India.

Abstract— *MANET is an important field in wireless network. Lot of work has been done in this field but only few techniques presented good efficiency and secured communication. This paper presents a complete scenario on how the data can be secured while it is being routed over an Ad-hoc network. For implementing the same a protocol named as AMDMM is employed along with a security technique to encrypt the data while it is travelling across the network.*

Keywords— *MANET, routing protocols, ZRP, security in MANETs, AMDMM.*

I. INTRODUCTION

A mobile unplanned network is described as the class of network in which the nodes which are not formed gets into the network by forming associate ad-hoc rasping without employing any central coordinator. As a result these networks introduce a change which developed into expertise of harsh cluster and will be suited to associate setting where infrastructure is not present or where infrastructure associated with deploy mechanism is not really priced effectively. An abundant IEEE 802.11 "WI-FI" motions are proficient in case of ad-hoc network evolution where underpinning management takes hold ,when there is no access purpose but during this whole scenario all of the nodes in the network are just allowed to send or receive the information but they cannot take part in routing mechanism going on in a network. Fluid ad-hoc network basic structure move independently or one can say that there is a probability of it being connected to an extended network as the internet.

When we shift the firmness of these networks it result into change of their orientation to get connected at anyplace ,anywhere and anytime with the real world application .As an envelope we have the stamina that permits the use of household computers in an official meeting that is carried out at the locality where there is no network connection available. This sort of networks spunk merely by networking their attachable resulting into associate unplanned network. All of the above specification of these networks can be used by the examples which can use these networks efficiently and effectively.

MANET is associate IEEE 802.11 framework. Unfixed ad hoc networks can be easily created at anywhere and time. Flexible ad hoc networks strength step in a very standalone fashion or would possibly in all probability be connected to a much bigger network just like the net. They suit data and services irrespective of their geographic positions .It's connected set of junction transistor nodes neighbourhood relating to is inconsequential network undignified advantageous the name whole of repulsive stations, devices do not need to be at intervals every other's communication vary to held conversation, the end users devices in addition acts as routers, nodes can enter and leave over time, data packets units are forwarded by intermediate nodes to their final destination.

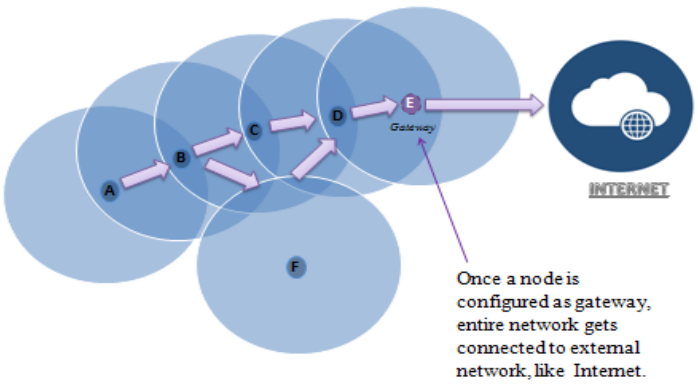


Figure 1: Mobile Ad-hoc Networks (MANETs)

The equipments needed to construct a mobile advertisement hoc network includes transmitter, receiver and antennas ,connection between transmitter and receiver is end to end, and broadcasting of packets is done in one direction only. The different performance measures of transmitter and receiver like the area covered by them, Intensity with which they communicate with each other and co-channel interference are considered while making out the position of nodes in the network to form a random temporary network i.e. termed as ad-hoc network. The network thus formed by the nodes is not permanent as the nodes are mobile in nature and also the performance measures of transmitter and receiver keeps on changing at all times. The eradicate properties of these networks can be summarized as follows:

(a) No communication medium.

(b) Depending upon the scenario in which the network prevails each node can act as Router as well as host.

(c) Limited range of frequency, space occupied is variable.

(d) Operation uses minimum possible energy.

(e) Security mechanism is not that much effective.

(f) Powerful configuration

(g) Regular routing updates prevail at each node.

II. ROUTING IN MANET

Nodes in MANET are mobile in nature, which results into a dynamically created environment, thereby resulting in the formation of self constructing and self arranging multi hop radio network. Nodes in these types of networks have a cooperative nature, wherein they access identical medium to forward the data to the destination node. Nodes not only serve the purpose of hosts but also that of a router that does the work of routing information from various nodes to other nodes in the network. There is a need of routing procedure to create a communication channel between sink and supply node as the sink node may not be in the area of a supply node, so in this case source node accesses the information of destination node with the help of intermediate nodes that provide it with routing information to the destination. We need to use this routing technology in these types of networks as there is absence of infrastructure. This procedure of sending and receiving between source and destination is simple in case of wired networks as infrastructure is maintained before carrying out further procedure of transferring packets. Nodes continuously transmit updated routing information to all other nodes, thus resulting in unpredictable property change.

The process of finding best possible alternatives to reach destination is known as routing. This method deals with exchange of packet of information between two adjacent hosts in a network, with this method best paths are chosen to send data by employing certain algorithms like dijisktra's algorithm for finding shortest path, this upgrades the efficacy of the system by selecting optimized and best path to traverse a packet to destination. Routing is performed in several forms of networks that take into account the phone network (circuit switching), electronic information networks (such as internet) and transportation networks. In packet switching routing is done with the help of intermediate nodes, these nodes are the hardware devices like bridges, gateways, routers, firewalls etc.The routing basically focuses on maintaining routing tables at each node, which are forwarded from node to node at particular intervals; with the help of routing table each node has numerous possible ways to send a packet to the destination. So, it is mandatory that each node should construct and update its table periodically to stay in the network for more time span otherwise it would be treated as malicious node and finally network will discard it. Certain parameters can be stated as under:

- Preceding length: It is preferred where subnet masks are lengthy.
- Metrics/cost: It is preferred where it is economically viable.
- Governing distance: It is preferred where path is shorter.

III. SECURITY IN MANET

One of the main important issues in MANET is to effectively utilize and allocate the number of resources present in the network. Shared resources accumulate bandwidth and queues on each node. Packets that are to be transmitted are queued up in the queues waiting for their turn to arrive. When most of the packets wants same access link, packets are to be dropped as the queue gets over full. When dropping of packets keeps on happening again and again in the network, then problem of congestion arises. And for maintaining and controlling the congestion each and every node should have turn to access the same link. In unplanned networks, topology keeps on changing frequently so, each node can act accordingly sometimes it can be a router and sometimes host. So as a result every node can route the packet not only single node is employed in any routing mechanism. In present methods of controlling the congestion source node is updated with congestion information at regular intervals of time so that it does not route any packet at high pace or can take any other path to traverse the packet to the destination. Path chosen must be the shortest path and there should be minimum

possible congestion at that path. Nearly all of the methods or mechanisms of controlling the congestion employ a special protocol named as TCP (transmission control protocol).

One of the most important mechanisms for security is encryption. If a document or slot of information is written in special coded language then that piece of work is said to be encrypted; only authorized users are allowed to access it. Employing encryption does not mean preventing interception, but the context is made invisible to the person or individual who tries to intercept. In the process of encryption, the text known as cipher text is generated for a simple text stated as plain text by using variety of algorithms. Cipher text is the one which can be read or retrieved only after it is being decrypted by the authorized authority only. This decryption can be done either with the help of some algorithms or by using special keys. Special keys are the one which are held only by the authorized individuals. It is even possible to decrypt a message without employing any of the above mentioned option but for the same individual must be a strong technocrat. An individual who is being authorized as a legitimate user by the originator can only access the information by using the keys provided to him by originator itself; this prevents unauthorized users to hack any information while it is travelling across the network medium. By using decryption key, only authorized user can access the information and same fulfil the encryption process. Encryption can prevent all confidential messages from being hacked but then to make it stronger other mechanisms are also used to protect the message from unauthorized access, for instance this whole process can be jointly used with digital signature or MAC. Encryption plays important role in securing communication between various military and government agencies. Not only is it employed with above two but also in several kinds of systems that are related to civilians. In recent research done by computer security institute, it was analyzed that most of the companies use this encryption to secure their data in transit and in storage as well. According to this research 70% of the companies used encryption to see to their transmitted data to various organizations whereas 7% of them used it for checking their stored data. Encryption is utilized to prevent the data that is stored on our computers for very long span of time. Recently many cases of theft of information are being addressed which can be solved by using encryption techniques. One would not suffer from loosing data because of physical aspects of security like failure of power or whole system. Encryption can be used to protect data that travels across the networks like ATM machines, Cellular phones, M-commerce transactions, Banking done from internet and many other cases in our day to day scenarios. To prevent data from dropping and hacked it should be encrypted while transmitting it over any other network. One should be careful while doing any purchasing or transactions online as it may lead to theft of one's personal information like their login credentials, their account balance etc. so one should only use the secure version of any website while making any transaction online. Security of any website can be easily interpreted by seeing https in address bar before the actual address of any site.

IV. RELATED STUDY

S. Gopinath and N. Nagarajan (2015) [1] introduced a protocol that supports multicast approach for routing which is based on residual energy concept. The protocol was named as AMDMM; and it is considered to achieve augmented network span and increased delivery of packet and its forwarding degree. A backbone is created to traverse a packet by using a group of familiar and trustworthy nodes of a network. A bench work is chosen to forward the packet, that benchmark is best reliable route which is chosen amongst various alternatives of paths. Vijaya Kumar. A et al. (2015) [2] designed a framework which deals with identifying the nodes which are misbehaving and discard them for participating further in mobile networks. For the same, a routing protocol (AMDMM) is used which looks after the nodes that are continuously dropping the packets which are to be forwarded to reputed nodes. In this research AMDMM not only monitors the nodes that are misbehaving but also equally participate in conducting audits at regular intervals to manage reputation and trustworthy paths from which packets can be travelled. AMDMM carries out this whole audit mechanism on the basis of how each node sends one packet at particular interval of time i.e. per-packet scenario. Gajiyani Rizwana, Ghada Wasim (2015) [3] researched on IDS mechanism, which is a technique by which self-centered nodes can be detected. They also contemplated a technique which is based on credits. According to this credit mechanism possible attacks incurred by self-centric nodes can be found out and these nodes are motivated to give their full corporation in the network. The nodes which are self-centric are the ones who misbehave and do not pass correct information to other nodes of the network.

Bob Briscoe et al. (2014) [4] laid stress on classifying various techniques used by networks to maximize throughput of the network, which prove to be useful in the following problems: (1) Hoe the network devices like servers and routers are placed in network.(2) Calculating round trip time(RIT) between two communicating parties .(3) Delay incurred because of transmission routes are also considered along with propagation delay ,nowadays delays are kept in queues.(4) Resources should be shared equally so that latency is not inflicted.(5) In full duplex system delay occurs because of buffering of operating system, hardware interaction etc. All of the above problems are to be kept in mind while classifying a network to reduce latency and increase throughput.

Arif Sari (2014) [5] figured out various security aspects in mobile unplanned networks of IEEE 802.11,as security is of main concern in any research area.DOS are classified as most hazardous threats.DOS attacks being the superior of attacks is pyramid of attacks, so various security mechanism are proposed to solve these types of attacks in ad-hoc

networks. The two popular methods to avoid the DOS attacks are named as RAS and USM. They both use the simulator named as OPNET; to check out the performance of network each time whenever new security method is employed.

Elhadi M. Shakshuki et al. (2013) [6] designed and executed an advance version of IDS which was named as EAACK (Enhanced Adaptive Acknowledgement) which is used in case MANETs only. When it is compared with the present methods of detecting misbehaving nodes it proved to be far more effective and efficient in dealing with malicious nature without making any drastic amendments in network performance. When wired media was in use, not many applications were employed, but when era of wireless media evolved it gave rise to mobility as well as scalability because of which large number of applications participated in day today life. In spite of many number of wireless networks, the MANETs are considered to be most important and solitary applications on the other hand, if classical networks are considered, they have fixed architecture, whereas in MANETs it is not the case, each and every node can both transmit and receive simultaneously. In MANETs, zones are considered for communications, nodes within same zone communicate faster. In case of farther zone, nodes depend on intermediate nodes for transmitting their messages. Nodes can enter or leave the network whenever they want in case of MANETs so; these types of networks are used in eristic mission use like in military or recovering from the emergencies. Network is open and large which leads to more number of attackers entering the networks. Because of this property of networks it is a cumbersome task to prevent attacks in MANETs.

Ranjana Pathak et al. (2013) [7] designed an amalgamated approach to deal with both sides of communication even if sender and receiver links gets exchanged. Here protocol is designed in such a manner that it transmits the packets only when rote is available, otherwise it waits for best route to get formed and once the route gets formed it transfers the packets. With the help of this protocol overall performance of the network gets increased as packet is transferred from source to destination directly without taking any help from immediate nodes.

Eman S. Alwadiyeh et al. (2013) [8] designed two routing protocols namely,EDMRC(Efficient Disjoint Multipath Routing Protocol) and ESMDR (Efficient, Stable, Disjoint multipath routing protocol).Both these protocols takes into account the interference property between different nodes and routes. With the help of these protocols, the effect of interference between the routes is reducing up to some extent. In addition, these protocols also look after overhead of controlling the packets i.e. in how much time packets is transferred from source to destination. These protocols have much greater throughput and transmission rate as compared to SMR (Split Multipath Routing protocol).Throughput is increased by selecting more numbers of channels that are available between preferred dislocated routes. Transmission rate gets increased by lowering down hidden terminal issue.

Ranjana Pathak et al. (2013) [9] proposed a hybrid technique to enable dynamic switching between modes of communication according to the link conditions. This technique is used when end to end routing fails and gives another path to send the data. It also use the AODV and OLSR for the better performance and results.

Kumar Prateek et al. (2013) [10] explained that MANET is a new network formed to serve some purposes, these networks are not permanent, they are created for a while wherein nodes do not stick to one position, they helps on changing their position with time and can leave or enter the networks anytime or at anyplace they want. Each node is free to move and can serve the purpose of both routers as well as host. Some of the properties of MANETs include distributed operation, loop-free dynamic topology, and easy deployment. Many Routing protocols are compared for their performance by using NS-2 simulation environment like DSDV.DSR,AODV .Some of these protocols are tale oriented and some are demand oriented but their interval working results into some differences is performance which make them different from each other.

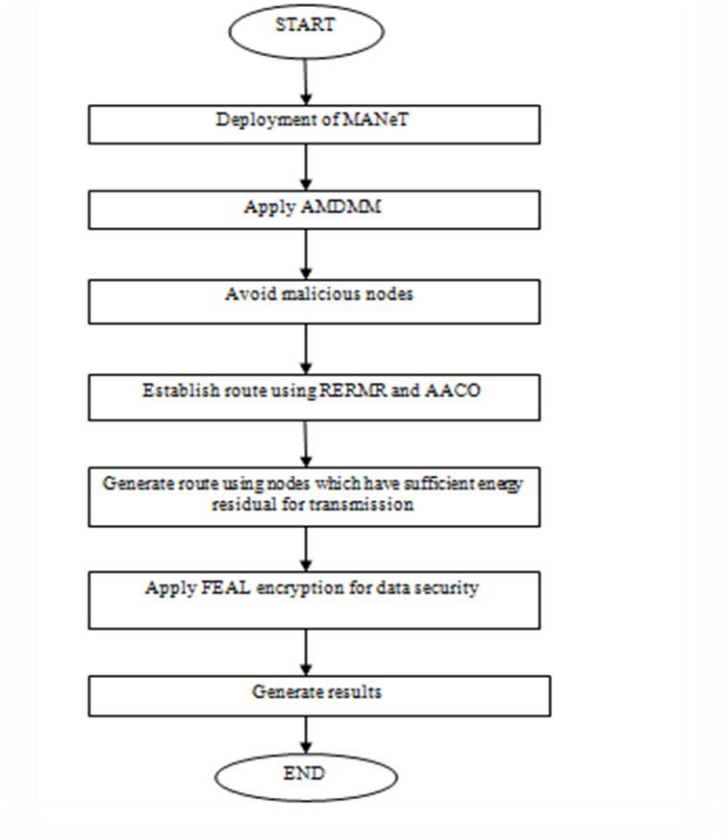
V. PROBLEM FORMULATION

A mobile unplanned networks (MANET) consists of huge number of nodes which are mobile by nature (also referred to as ichors nodes), each and every one of which communicates directly or indirectly in the air the neighbour nodes within its radio range. The area of MANET is continuously developing because of it various benefits and applied areas range. Proceeding tendency is an issue of concern in foremost all routing formalities. All these requirements of a network cannot be accomplished by employing only a single protocol for routing mechanism . It is required for the certain scenarios.

i. Absence of successive paths for downloading any content or information carried by packets
ii. Packets comprising of information are dropped because of downlinks.
iii. Degraded throughput of the system
iv. Whenever there is any failure in communication link network has to be scanned again and again which consumes more battery hence, the battery life reduces and also system becomes less efficient and reliable.
v. No amendments in case of huge increase in delay.
vi. Exaggerate the maximized network lifespan.
vii. Absence of security mechanism while transmitting any information over the network.

As a result we'll compose a protocol that has greater security aspects and efficiency techniques and that protocol is named as AMDMM, this protocol will look after the security of the packets that are transmitted over the network as security is a challenging task to accomplish while designing any system. As absence in security constraints can adversely affect the other parameters as well like data that has been dropped, lifespan of battery (as mobile nodes are battery oriented) etc.

VI. FLOWCHART



VII. AACO

To optimize the path and enhancing the system performance AACO algorithm is used widely. It is a technique that is being adapted to provide solutions for complex problems which were either difficult to solve or whose results cannot be easily obtained. Whenever any scheduling of task is to be done this algorithm is a best option to get opted. As it is a most widely used algorithm so, many researches are going on till now to make it more enhanced every time. This algorithm give rise to many of the popular strategies like construction of solution in a dynamic network, merging results obtained from various local searches, partitioning ant into two individual groups-lead ants and common ants, updating new pheromone trails etc.

In the proposed approach, AACO is used so that network performance can be enhanced. It reduces the space complexity of the system up to certain extent. Moreover path can easily be obtained in case of emergencies.

VIII. AMDMM

This protocol is named as Audit Misbehavior Detection and Monitoring Method. This is one of the efficient and effective protocols to make MANET environment safe and secure. The primary function of this protocol is to identify the nodes that are acting maliciously in the network and secondly it also looks after the nodes that are continuously dropping the packets that are being sent by the other nodes or sending the selective information to its neighbors. It basically aims at monitoring the behavior of each node of the network and accordingly decides the reputation of each node amongst the other and with the help of reputed nodes only route mechanism is carried out.

It not only monitors but also eliminates the malicious nodes from the network environment so as to enhance the overall network performance. The factors that are being evaluated by this protocol are- misbehaving nodes, establishing trustworthy routes, identifying the reputation of each node of the network. As far as reputation is considered for evaluating this metrics each node utilizes two information-one is its own view regarding the neighboring node whether it is malicious or trusted node and the other being the view of its neighboring nodes regarding the other nodes. Each node

utilizes these two information to detect malicious nodes. The three basic processes of AMDMM protocol includes: Reputation process, Auditing process, Route discovery process.

IX. RERMR

To enhance the lifespan of MANETs it is mandatory to find out the energy level associated with each and every node of the network, this leads to conserved energy that fulfils the gap between the available power and consumed power. For achieving the above stated objective a protocol named as RERMR (Residual Energy based Reliable Multicast Routing) is used which is very efficient and secured routing protocol. This protocol is used to increase the packet delivery and forwarding rate, mobile nodes are selected in a manner so as to conserve the principle of energy stated in proposed methodology. Mobile nodes that have more remaining energy are considered to traverse the packet. In this protocol all the nodes reach other neighboring nodes by multicast process of routing. The routes that are more stable and have more amount of energy to traverse a packet are chosen. Packets are then forwarded to all these paths whose reliability meets the desired criteria. To design the desired protocol certain assumption are to be made for packet forwarding rate and higher delivery rates.

X. RESULTS AND DISCUSSION

In the below figures a comparison is shown between hybrid routing scheme.

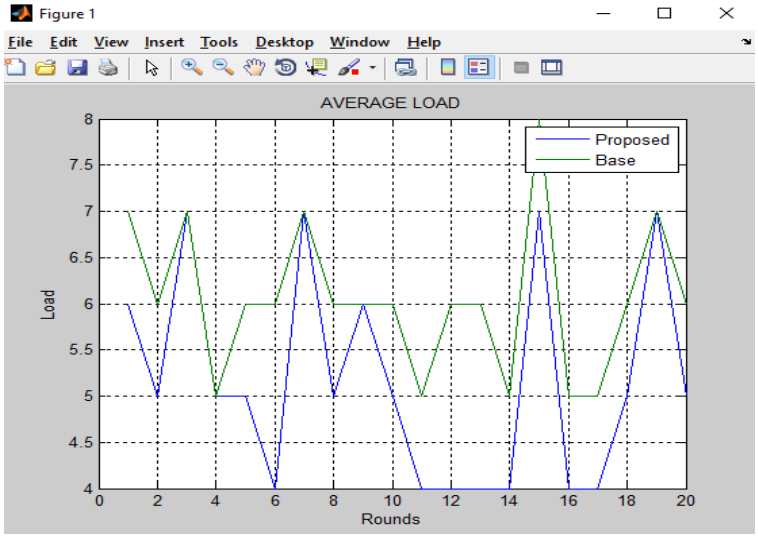


Fig 3: Average load

Load: It represents the average system load over a period of time.In the above figure it is easily shown that the average load is less in proposed approach than existing approach.

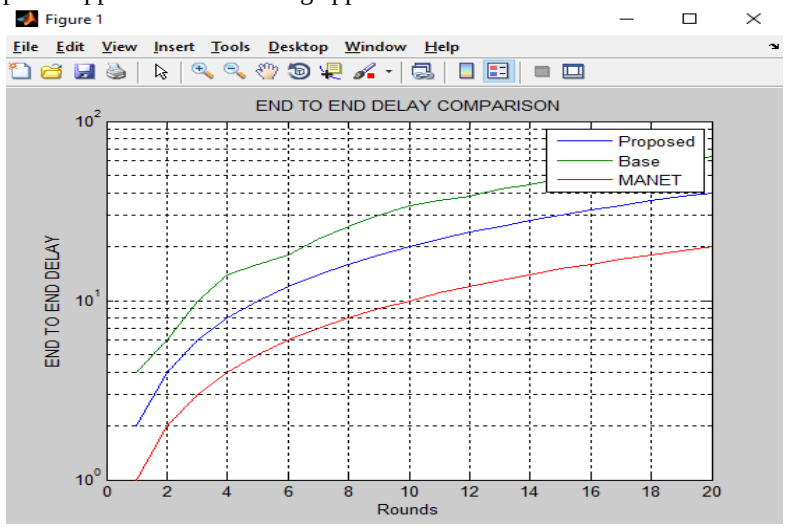


Fig 4: Delay

Delay: The time taken by the data packets to deliver at the destination is called delay. The delay in enhanced AMDMM is very less than the existing AMDMM.

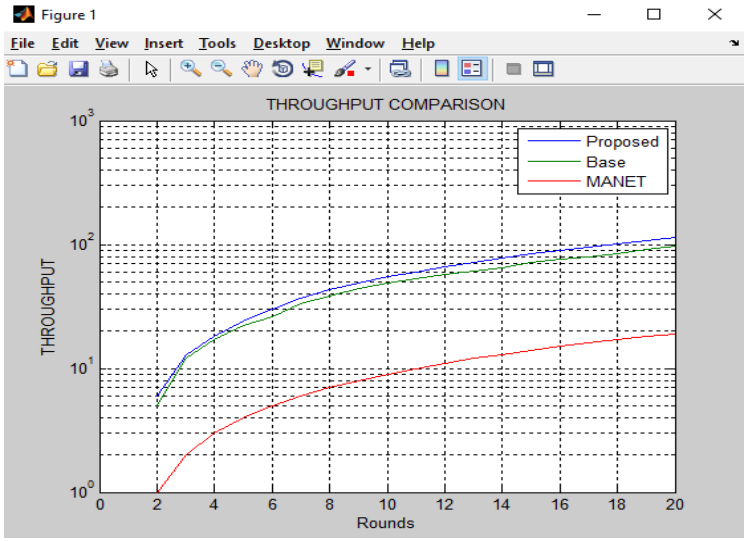


Fig 5: Throughput

Throughput: It is defined as the total number of the packetsdelivered over the simulation time.The throughput comparison shows that the proposed system delivers the more packets than the existing system.

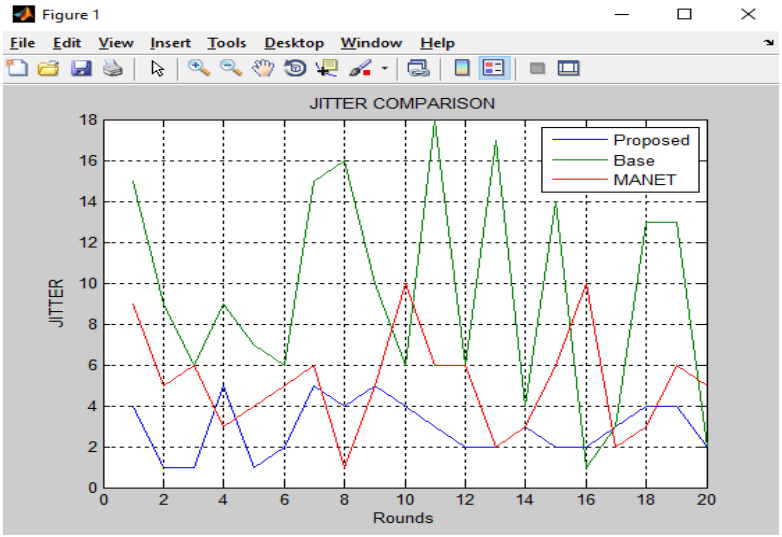


Fig 6: Jitter

Jitter: It defined as a variation in the delay of a received packet. It occurs due to the many reasons like congestion,improper queuing and delay in packets For good and secured communication the jitter should be less.From the graph it is easily shown that the jitter in enhanced AMDMM is approx 4 sec and in existing case it is above 8 sec.

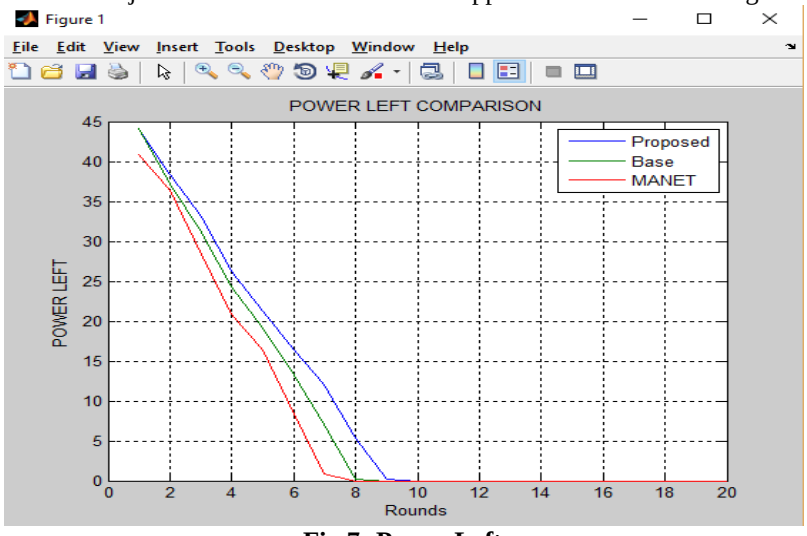


Fig 7: Power Left

Power Left: Power Left means how much power is left after sending and receiving the data. From the graph it is seen that the power in enhanced AMDMM is more than that of existing AMDMM protocol.It is approx 10 rounds and in existing case it is approx 8 rounds.

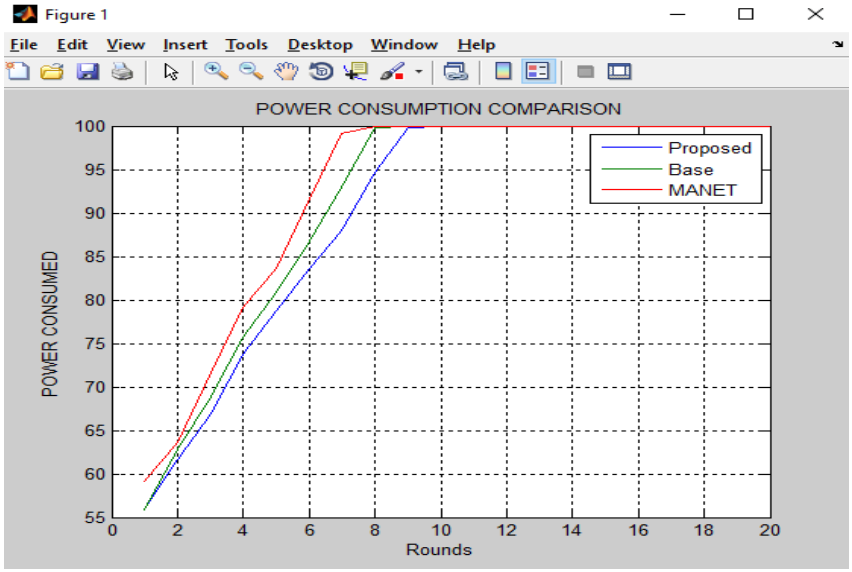


Fig 8: Power Consumption

Power Consumption: It is defined as the power used during the sending and receiving the data . In the above graph it shown that the power in enhanced AMDMM is more than that of existing AMDMM protocol. It is approx 10 rounds in proposed and in existing case it is approx 8 rounds.

XI. CONCLUSION

MANET is combination of mobile nodes which has no fixed topology. In the current research the enhancement of the secured MANET routing protocol is done. The protocol is used to maintain the QoS in existing AMDMM . Encryption is very important in MANET . To make AMDMM more secure cryptography technique is used. By applying the encryption in AMDMM , overheads are introduced. To overcome this problem we adopt the optimization technique i.e. AACO (Adaptive Ant Colony Optimization).By using this technique losses and the dropping of packets will reduce to some extent. The above parameters , results and discussions show that this is done using a MATLAB simulator .The optimization technique makes the alternative path to send the data fast and more secured.The parameters like delay, load and throughput are improved by using AACO technique.By using the proposed approach the result are improved upto20%.

XII. REFERENCES

[1] S. Gopinath, N. Nagarajan, "Energy based reliable multicast routing protocol for packet forwarding in MANET", Journal of Applied Research and Technology, ISSN: 1665-6423, Vol.13, 2015, pp: 374-381

[2] Vijayakumar.A, Selvamani K, Pradeep kumar Arya, "Reputed Packet Delivery using Efficient Audit Misbehaviour Detection and Monitoring Method in Mobile Ad Hoc Networks", International Conference on Intelligent Computing, Communication & Convergence, Volume: 48, 2015, pp:489-496

[3] Gajiyani Rizwana, Ghada Wasim, "Enhanced Intrusion Detection & Prevention Mechanism for Selfishness in MANET", International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801, ISSN (Print) : 2320-9798, Volume: 3, Issue: 9, September 2015, pp: 8544-8549

[4] Bob Briscoe, Anna Brunstrom, Andreas Petlund, David Hayes, David Ros, Ing-Jyh Tsang, Stein Gjessing, Gorry Fairhurst, CarstenGriwodz, Michael Welzl, "Reducing Internet Latency: A Survey of Techniques and their Merits", ISSN: 1553-877X, IEEE Communications Surveys & Tutorials, Volume: PP, Issue: 99, 2014, pp: 1-56

[5] Arif Sari,"Security Approaches in MANET", International Journal Of Communications, Networks and System Sciences, ISSN:1913-3715, 2014

[6] Elhadi M. Shakshuki, Nan Kang, Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, Vol: 60, No: 3, March 2013, pp:1089-1098

[7] Ranjana Pathak, PeizhaoHuy, Jadwiga Indulska, Marius Portmann, "Protocol for Efficient Opportunistic Communication", 38th Annual IEEE Conference on Local Computer Networks, Sydney, ISSN: 0742-1303 Print ISBN: 978-1-4799-0536-2, DOI: 10.1109/LCN.2013.6761240, 2013, pp: 244-247

[8] Eman S. Alwadiyeh, Ala'F A Aburumman, "Interference-Aware Multipath routing protocols for Mobile Ad hoc Networks", 13th Annual IEEE Workshop on Wireless Local Networks, Sydney, DOI: 10.1109/LCNW.2013.6758492, ISBN: 978-1-4799-0539-3, 2013, pp: 980-986

[9] Ranjana Pathak, PeizhaoHuy, Jadwiga Indulska, Marius Portmann, SaaidalAzzuhri, "A Performance Study of Hybrid Protocols for Opportunistic Communications", 9th IEEE International Workshop on Performance and Management of Wireless and Mobile Networks, Sydney, Print ISBN: 978-1-4799-0539-3, DOI: 10.1109/LCNW.2013.6758492, 2013, pp: 9-16

[10] Kumar Prateek, NimishArvind, Satish Kumar Alaria, "MANET-Evaluation of DSDV, AODV and DSR Routing Protocol", International Journal of Innovations in Engineering and Technology (IJIET), ISSN: 2319 – 1058, Vol. 2, Issue 1, February 2013, pp:99-104

[11] Anit Kumar, Pardeep Mittal, "A Comparative Study of AODV & DSR Routing Protocols in Mobile Ad-Hoc Networks", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Vol. 3, Issue 5, May 2013, pp: 658-663

[12] Bhalinder Kaur and Sonia, "Performance Evaluation of MANET Routing Protocols with Scalability and Node Density issue for FTP Traffic", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Vol. 3, Issue 5, May 2013, pp: 544-548

[13] Rajesh Sharma, Seema Sabharwal, "Dynamic Source Routing Protocol (DSR)", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Vol. 3, Issue 7, July 2013, pp:239-241

