International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

An Overhead Aware Multipath Routing Protocol for Improving Relay Node Selection in Manet

Uppalapati Srilakshmi, Bandla Srinivasrao

Abstract*: The primary aim of Mobile ad hoc network design is for making the availability of Internet facility at the locations and every second despite the consequences of geographical location. The MANET Application would contain the improvement of adversity, military, and scrutinizing the situation. Resource-controlled situation of MANET would build its communication procedures very tricky. Additionally, the nodes of network are prepared along with batteries that are inhibited & it is more difficult for replacing or recharging the batteries at the time of mission. The accumulation of node in MANET is finished whatever be the circumstances; for the node for communicating with another node there should be a safe & dependent technique. The judgment of a node is trust on the other node in a network; it is symbolized in arithmetic outline. Trust is computed by relying on the preceding interface amidst 2 nodes. Hence, MANET would need an aware of overhead multipath mechanism for addressing the restraints. We are attaining the efficiency energy by the layer of network, as MANET is without any infrastructure network of peer-to-peer. We would expand a protocol of the latest overhead aware multipath routing. It would choose the path of routing depending on the present residual situation of the system nodes. An outcome of Simulation would be concluding that our suggested technique is superior in comparison with the works that are existing E-AODV, MRPC with respect to the network lifetime & the stability of link. The Simulation results throughout NS2 software for verifying the efficacy of our technique.

Keywords: MANET, Multipath, E-AODV, MRPC, Overhead Aware routing, OAMRP, Trust calculation, Clustering.

I. INTRODUCTION

Planned to determine a solitary way between a source and target node too, the protocols of average routing in ad hoc wireless networks, for example AODV & DSR, remain initiated majorly. Multipath routing comprises of detection of several routes amongst a source & a target node. These multiple techniques amidst the source as well as destination node pairs may stay utilized to correspond among the dynamic as well as random ad hoc systems behavior [1]. The utilization of numerous ways targeted at accomplishment of a minor end to end delay could stay potential presumptuous the large bandwidth obtain ability. The redundant and substitute routes would stay identifies through the effective presentation of data packet transmission in multipath protocols routing. Besides the power key intake transmit nodes will remain concentrated and the network subdividing complexity that is constructed by utilizing the energy consumption of these nodes is determined. These protocols of the multipath would be remaining engaged targeted at dependability of delivering, lessening the overhead and network lifespan maximizing as well as cross routing [2]. Recognition plus conservation of several paths have stayed behind the multipath concerns of routing protocols.

The routing alongside a sole technique might not provide adequate bandwidth intended at a bond in the limited situation vision of in a wireless network. However, once several techniques would stay stagnant that is been utilized immediately to information routing, the collective bandwidth of the routes may treat the bandwidth restriction of the compliance. Additionally, the accessible bandwidth would be remaining at greater that would permit to a smaller end to end delay assuming the obtainability of a greater bandwidth. The interference of radio has to be connected into contemplation by nodes in the network communicating over the medium of wireless. Hence adaptable the possible throughput, Broadcasts would be commencing a node alongside solo route might barricade utilizing the broadcasts from a node along extra one.

The route recognition overhead of the multipath routing would remain as a great as that of sole technique routing. The acceptable functioning of the method would remain credible in a multipath routing network apart from of the occurrence of any disgrace of one or few of the multipath amid a source and its objective. Thus, the route detection frequency remains small in that particular system. Moreover, multipath routing [3] fallouts in a greater throughput, by means of the whole nodes that would remain set to practice a constrained capacity, for example processing power and bandwidth.

The reduction of energy methods were approximated by routing layer and the effort is energy competence in MANETs might remain addressed at unlike layers [4]. In recent centuries, several researchers have been providing consideration towards the expansion of energy utilization of mobile nodes, commencing special points of opinion. Several planned declarations attempt towards varying the communication control of wireless nodes. Further applications lean towards capable managing of a sleep state for the nodes and these declarations sequenceafter pure MAC-layer declarations towards resolutions that join MAC & functionality of routing.

Revised Manuscript Received on 30 May 2019.
***** Correspondence Author
Uppalapati Srilakshmi*, Department of CSE, Acharya Nagarjuna University, Guntur, India.
Dr. BandlaSrinivasrao, Department of CSE, Acharya Nagarjuna University, Guntur, India.

Finally, there subsist various submissions that effort to classify the process of effective energy routing, proficient of routing data above the system and also conserving the battery command of moveable nodes. Such applications are entirely different, when others point to improve the energy-attentive performance towards available protocols, like AODV, DSR & OLSR.

The purpose of awareness energy routing protocols would stay towards decreasing the power utilization in the packets transmission between a source and a destination, for staying away from packets routing over the nodes by tiny enduring power [5], towards optimizing routing overflowing in sequence above the structure then towards evading interference and intermediate impacts too. The definite routing protocols would begin wireless nodes into clusters, for instance leach. In Xia & Vlajic the surroundings below particular protocols will remain energy capable remains documented and also the best radius of a collection remains defined.

Towards providing opportunity in the investigation, this unit would remain devoted to determine routing overheads remain, routing overheads to expect (i.e. metrics) grounded on what extra investigation has well-defined routing overheads in accumulation to lower routing overheads might not remain considerable. In a network towards connectivity maintenance, the overheads of routing are the processing requirement targeted at a node. Various routing overheads might be understood by means of restrictions in the network and might upsurge bandwidth intake and the utilization of energy. The succeeding are generally deliberated overheads that would remain used in the MANET investigation overheads [6].

The papers like claim on that determining routing ways and the nodes' arrangement might affect the routing overheads. The abovementioned would employ GPS co-ordinate of nodes towards supporting to lessen the routing controls of the course process. It would determine an AODV protocol [7] named improved side as the ARZAODV (Adaptive Request Zone for Ad Hoc On-Demand Distance Vector) protocol that utilizes a procedure for defining the distance and positioning too of a node.

In an established routing, the advancing nodes will remain vigilantly selected grounded on static deliberations (ex: series number in AODV). Hence, comparable nodes may carefully remain endlessly selected as of their supremacy in particular deliberations. This unceasing assortment of these nodes [8] deprived of assuming their accessible possessions might result in advanced packet would delay and the losses. Correspondingly, this continuous assortment of the nodes that are carefully chosen fabricates extra overhead towards the advancing nodes.

II. RELATED WORK

In [9], writer would present and purpose is for finding the routing way for evading node for becoming bottleneck, enlarge the network's lifetime, and give the stability of connection. The selection of route metric of the protocol which has initiated routing is present residual form of node to the energy and buffer with the knap sack mechanism support. The primary involvement of the initiated mechanism is a systematic form for the node of bottleneck, computation of present residual scenario of nodes, obligation of the priority, and initiation of the routing technique. It is always a tough assignment to lessen the MANET vulnerability because of the infrastructure-less network. Different types of CR (Certificate Revocation) processes & trust computation practices have been referred to enhancesafety of the network here in this copy. Shabut et al. [10] has suggested a proposal-based form of trust. The aim of this document was to involve several properties such as value of confidence, trust, & deviation value at the same time as a cluster creation for safe node communication in the MANET. It also has given a well-organized path for calculating the trust. Also Liu et al. [11] has shown a CR method for avoiding the intruders from the activities contributions of the network. The technique has incorporated 2 types of list (Warning List) WL & (Black List) BL which are managed by CA. This kind of technique has supported in decreasing the false attainment.

Dahshan et al. [12] has recommended a trust-based threshold revocation of cryptography plan for MANETs. It explains the paths for sharing the private CA key after application of the function of hash chain. Zhao et al. [13] has suggested a path for computing a graph of trust that states whenever the nodes would be communicating with one another by taking LCM of the first communication time & exchanging trust values at the time of next interaction along with the neighboring node. It lessened the overhead communication cost when a node would move in the cyclic track.

Harn& Ren [14] have suggested the concept of GDC (Generalized Digital Certificate), the primary aim of GDC is to give user authentication/identification & agreement of key. And they would be utilizing DL (Discrete Logarithm) based & factoring of integer depending on the procedures that could attain user substantiation and the establishment of key that is secret. And then Mahmoud et al. [15] has recommended a concept of E-STAR to establish the consistent routes in separated the networks of multi-hop that are wireless. E-STAR would unite the networks of trust and compensation by depending on the trust & routing of energy-aware procedure. Li & Liu [16] have suggested an entirely circulated IMKM.It has been executed by uniting cryptography of threshold & based ID there are numerous secrets. This would eradicate the certificates inevitability of authentication & also would provide further prominence on effectual key management.

Haas et al. [17] has presented the phase's series that achieve the aim for lessening the size of CRL, an efficient approach to find out whether the certificate is available in CRL, and a technique for updates of CRL.

Jiang et al. [18] have suggested EDTM (Efficient Distributed Trust Model) that also could evaluate the reliability of sensor nodes exactly and avoid the safety abuse more successfully. Chae et al. [19] recommended a trust scheme of computation that broadly contracts with a harsh on–off attack situation. Chang and Kuo [20] had shown a path to estimate trust utilizing Markov Chain Trust form and path for keeping a secondary CA on hold in case of primary CA failure.

Abbas et al. [21] suggested lightweight IDS that defend against nodes utilizing the individuality switch for causing the attack. Venkataraman et al. [22] initiated a trust form based on regression for providing a safe routing.

III. PROPOSED SYSTEM

In the investigation effort point, an overhead conscious energy positioned multipath routing would stay presented towards enhancing the relay assortment of node and to lessen the overhead on the nodes. This would be there attained by the nodes' concept spotted narrowly nearer towards the node of sink. The nodes which are advancing would remain selected vigilantly grounded on EOR (Estimated Overhead Rate) on each node. The multipath routing would be remaining advantageous to reduce the utilization quantity of the frequencies by communication via escaping the traffic by various channels. A context of trust would remain presented grounded on node's advancing performance towards each single node in the network for giving a communal trust amongst the nodes.

3.1 Route discovery process in network:

The protocols that are reactive would never sustain the data history regarding their neighbours. Whenever a requirement for communicating along with another node, it will commence the discovery of route procedure to recognize the destination that is optimum. The source node S would be commencing the process of route discovery through building the RREQ & would forward to its neighbour nodes in the network scenario. Whenever a node would be receiving RREQ, it would compute the list of RREQ and forward to the nodes existing in the list. This procedure would reiterate until the occurrence of destination. The node of destination would build the RREP, and forward to the nodes in the list of RREP. This development will get repeated until the source achieved. The step by step procedure of route discovery is as follows

Step 1: Recognize the N/W Topology.

Step 2: Source node would begin the RREQ (Route Request) for finding the finest way from the source to destination.

Step 3: The neighbouring nodes would be receiving RREQ and inserting its neighbour details in the packet of RREQ and forward the RREQ to its neighbouring nodes without saving the RREQ details.

Step 4: The step 3 will be iterated until the occurrence of destination or till the TTL (Time To Live) would expire, if TTL would be expiring before destination recognized, then amplify the value of TTL and maintain the step 2.

Step 5: The node of destination would obtain RREQ and build the RREP (Route Replay) and forward to nodes available in the list of compliment.

Step 6: Whenever a node would be receiving RREP, it would run the step 5.

Step 7: The node of source would receive the RREP from unlike ways, and select the most favourable way.

3.2 Creating Cluster

The combination of devices is cluster in the network towards the subgroups. The cluster would stay planned by utilizing by means of the distance amid 2 nodes. This stage would lessen the number of hops while message transmission as the cluster would stay united meticulously. The space amongst 2 nodes is operated when enhancing the cluster as they stay possible for practicing the same scenarios or atmosphere, thus joining them jointly would reduce the trust variance values amongst them.

3.3 Calculating Trust

This document would offer for calculating direct trust through sum of positive and negative communication between the nodes.

$$DT = \alpha_{ij} / (\alpha_{ij} + b_{ij}) \quad (1)$$

For 2 nodes i&j, α would remain the sum of effective communication and β also would remain the sum of communication which is ineffective. The trust value would constantly be $0 \leq DT \leq 1$.

3.4 Selection of Threshold

The choice of threshold would remain a momentous attribute in the above-anticipated consummate as the secured level is manipulated by the threshold, if threshold would stand greater, the security would be great as the whole nodes below threshold would be nullified. Threshold starting 0.7 to 1.0 would be providing less probability targeted at malevolent action. Also choosing the high threshold value would be originating through definite drawback, that is whether a communication would be available being escalated owing to particular ecological or exterior component the aforementioned reduces the trust value of the resultant node and will result in node invalidation. Thus the threshold choice ought to be observed along with various aspects.

3.5 Psedocode for proposed method

```
N= nodes
D= distance
CH= cluster head
DT, IDT, AT= Direct trust, Indirect trust, Average trust
EOR = Estimated overhead rate
For all nodes N
   Calculate distance D
End for
For Each node N
   If (D [N] < D [N+1])
   CH = N
Else
   CH =N+1
End For
For all nodes N
   Initialise DT, IDT, AT
End for
For Each node N
If [path==exist]
   If ((EOR [path] < EOR [path+1]) || AT > threshold)
   RP = path
   Else
   RP = path+1
End if
End if
If (N forward [data])
   DT = DT++
   IDT = IDT++
End If
   AT = Average [DT + IDT]
End for
```

3.6 Algorithm process

Step1: Originally nodes are positioned in the network area arbitrarily

Step2: The nodes are separated into the clusters based on the distance amidst the nodes

Step3: Every node is being allocated with direct trust, indirect trust and average trust values for assessing the trustworthiness of the nodes

Step4: Nodes trustworthiness is evaluated based on behaviour of the node's forwarding

Step5: Network is partitioned into clusters for handling the trust computation in a proficient path

Step6: Every cluster is symbolized with their chosen cluster heads

Step7: The nodes of CH scrutinize intimately the nodes in the cluster for node estimation

Step8: Direct trust is evaluated by the neighbour nodes of the present node.

Step9: Indirect trust is assessed by the respective CH node of their respective cluster

Step10: From these direct & indirect trust values node's average trust is evaluated

Step11: This average trust would explain the nodes' trustworthiness in the cluster

Step12: At the time of data transmission, these values of trust are taken into account for making the forwarder decision of the node choice.

Step13: Overhead is the element which would be affecting the performance of node.

Step14: Overhead explains how much load is provided / generated on the node to execute the given assignments

Step15: At the time of forwarder selection of node, this overhead is believed as a well-known aspect for choosing the low node of overhead

Step16: Node's values of average trust are measured up with each other for recognizing the nodes of high trust as they are supposed to be most successful.

Step17: To decrease the overhead on every node, multipath routing is obtained.

Step18: All the probable ways amidst the nodes to communicate are acknowledged with the routing protocol support.

Step19: Overhead and trust are the promising aspects to choose the most appropriate forwarder nodes.

These aspects of each node are measured with their nodes of neighbour and at last the forwarder nodes are finalised.

IV. RESULT AND DISCUSSION

We would calculate the OAMRP performance by presenting comparative simulations. The suggested protocol, E-AODV, & MRPC protocols are replicated by utilizing Network simulator-2. The energy model executed is same for E-AODV, OAMRP and MRPC protocols. 21 sensor nodes in our simulation were deployed randomly in a topographical region A, of dimension 1000 m x 500 m. important constraints meant for our simulation are provided in table 1. Table 1 displays the parameters' system utilized in our simulations.

To analyze and compare the protocol's performance by active protocols, we would be considering the following metrics.

1) Network performance: The numerous packets that are transmitted are calculated in Megabits per sec.
2) Propagation Delay: Average time taken for one packet for propagating from source node to destination node.
3) Energy consumption: Total energy of nodes systematized in the network.
4) Packet delivery ratio: The data packets ratio has been delivered to the destination.
5) Overhead: Numerous routing packets needed for network communication.

Table 1: Simulation parameters

Parameter	Value
Application traffic	CBR
Transmission rate	1000 bytes / 0.5ms
Communication range	250m
Data Packet size	8000 bits
Number of sensor nodes	21
Number of simulation iterations	160
Initial energy	100j
Network area	1000x500
Number of clusters	8
Routing methods	OAMRP, E-AODV, MRPC
Routing protocol	AODV

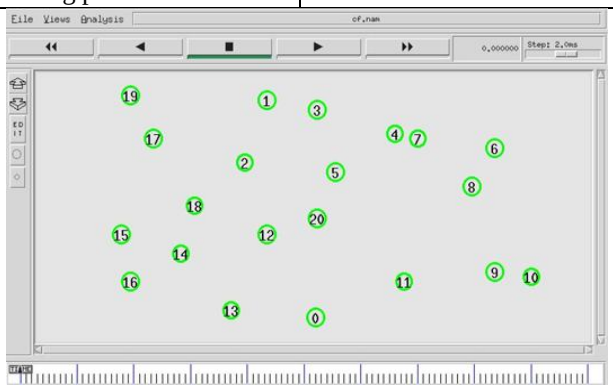

Figure. 1: Network deployment

Figure 1 would symbolize the deployment of network. All the nodes are located physically in a random approach.

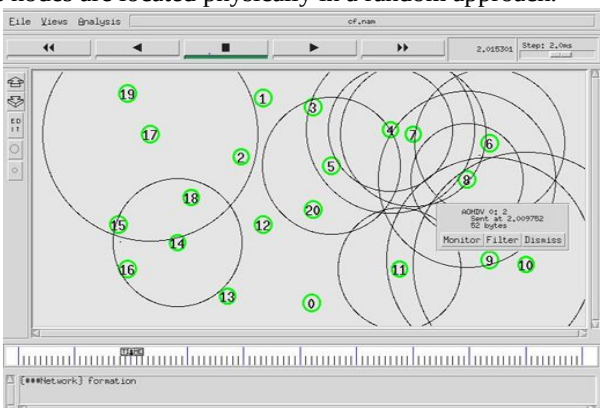

Figure. 2: Broadcasting in network

Figure 2 will be representing the process of broadcasting in the network. All the nodes here would request their neighbour nodes for reply of the route. The routing protocol in this network would decide the processes of RREP & RREQ.

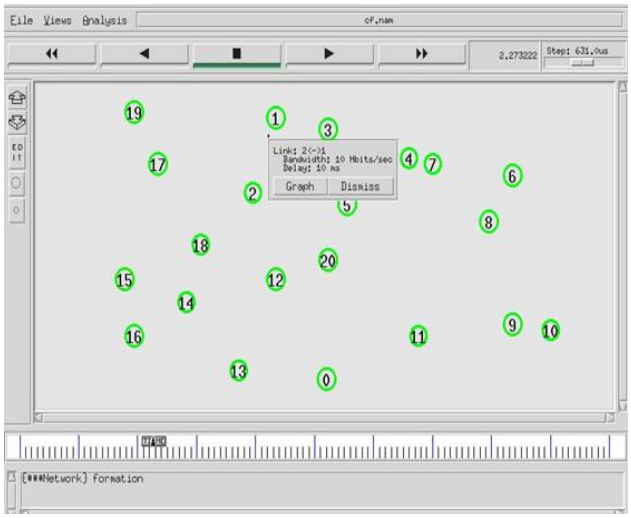

Figure.3: Cluster member to Cluster head transmission

Figure 3 displays the cluster member to cluster head for the transmission of data. The cluster heads after cluster formation are chosen based on their distance from node to node in every cluster. The link here should be signified amidst the cluster member & head.

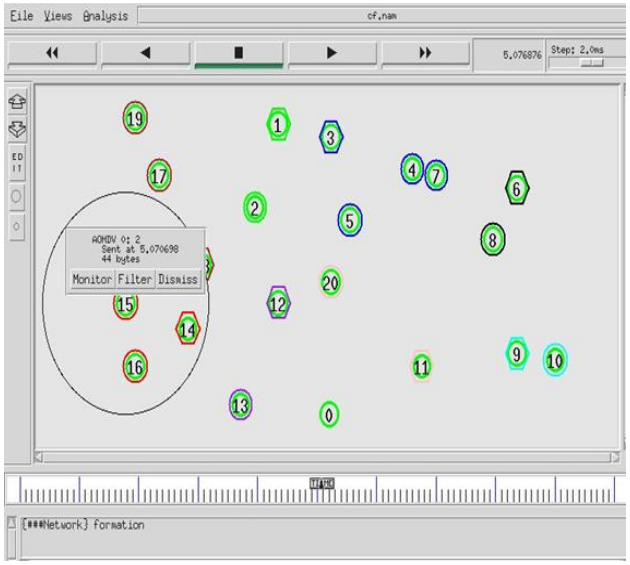

Figure. 4: Route level checking process

Figure 4 shows the route level verifying before the transmission of data. AOMDV protocol here would be deciding the path level and would substantiate whether the path is appropriate for routing or not. The routing protocol would build the multipath and will transmit the data through accessible multipath.

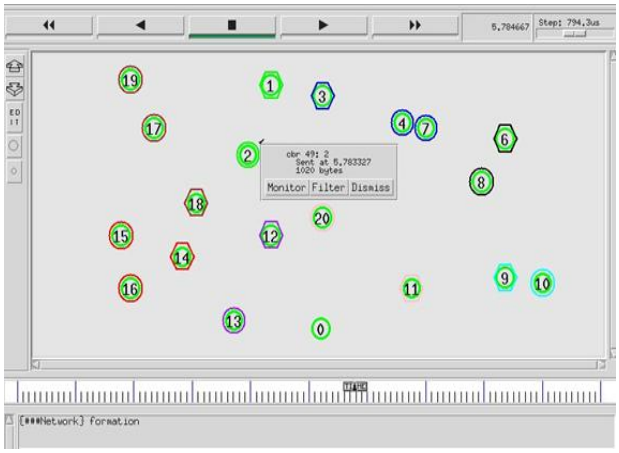

Figure. 5: Cluster member to CH Data transmission

Figure 5 stands for the cluster member to CH transmission of data. In this diagram, CBR would perform as the protocol of traffic that assists for deciding the size of packet, maximum number of packets, interval time, start and end time for the process of data.

```
Cluster - 1 : 14 15 16
Cluster - 2 : 12 13
Cluster - 3 : 11 20
Cluster - 4 : 9 10
Cluster - 5 : 17 18 19
Cluster - 6 : 1 2
Cluster - 7 : 3 4 5 7
Cluster - 8 : 6 8

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

=========================================================
Distance from Node 14 to its neighbors  14  15  16
 0.000000  136.014705  125.299641
Distance from Node 15 to its neighbors  14  15  16
 136.014705  0.000000  101.980390
Distance from Node 16 to its neighbors  14  15  16
 125.299641  101.980390  0.000000

Cluster Head(CH) is node : 16
=========================================================

=========================================================
Distance from Node 12 to its neighbors  12  13
 0.000000  178.885438
Distance from Node 13 to its neighbors  12  13
 178.885438  0.000000

Cluster Head(CH) is node : 12
```

Figure.6: Cluster file formation

Figure 6 signifies the formation of cluster files along with time update and would get through 8 clusters in the network. The process of cluster head choice would be depending on the space between neighbours in the network. After the distance assessment, the cluster head has to come to a decision which cluster member is at nearby distance to the cluster head whereas comparing with the other members in the network.

```
index :15  dest :15 source :16 nexthop :15 prevhop :16
index :14  dest :15 source :16 nexthop :15 prevhop :16
index :18  dest :15 source :16 nexthop :15 prevhop :16
index :13  dest :15 source :16 nexthop :15 prevhop :16
index :6  dest :6 source :8 nexthop :6 prevhop :8
index :7  dest :6 source :8 nexthop :6 prevhop :8
index :9  dest :6 source :8 nexthop :6 prevhop :8
index :4  dest :6 source :8 nexthop :6 prevhop :8
index :10  dest :6 source :8 nexthop :6 prevhop :8
index :10  dest :10 source :9 nexthop :10 prevhop :9
index :8  dest :10 source :9 nexthop :10 prevhop :9
index :11  dest :10 source :9 nexthop :10 prevhop :9
index :17  dest :18 source :19 nexthop :17 prevhop :19
index :1  dest :1 source :2 nexthop :1 prevhop :2
index :18  dest :1 source :2 nexthop :1 prevhop :2
```

Figure. 7: Hop file in network

Figure 7 would characterize the hop file in network. Here index, destination, source, previous hop node, and next hop node would be symbolized in this chart. In this diagram, hop nodes amidst source and destination would be deciding which way is to be chosen for routing.

```
Node 16 forwards the packet to 15 at 2.005669
Node 9 forwards the packet to 10 at 2.013001
Node 8 forwards the packet to 6 at 2.024615
Node 17 forwards the packet to 19 at 2.045913
Node 19 forwards the packet to 17 at 2.053634
Node 17 forwards the packet to 18 at 2.094233
Node 2 forwards the packet to 1 at 2.106703
Node 12 forwards the packet to 13 at 2.110601
Node 7 forwards the packet to 3 at 2.123394
Node 7 forwards the packet to 3 at 2.275067
Node 17 forwards the packet to 19 at 2.304281
Node 19 forwards the packet to 17 at 2.307337
Node 17 forwards the packet to 18 at 2.317182
Node 12 forwards the packet to 13 at 2.339364
Node 2 forwards the packet to 1 at 2.495861
```

Figure. 8: Transmission file

Figure 8 characterizes the file transmission of network. The figure displays every node that would be forwarding the facts to specific node in convinced time. The source node, time interval, destination node and are modernized in this diagram.

```
Final Trust value of node 0 is 0.742197
Final Trust value of node 1 is 0.399126
Final Trust value of node 2 is 0.724894
Final Trust value of node 3 is 0.609676
Final Trust value of node 4 is 0.384987
Final Trust value of node 5 is 0.427609
Final Trust value of node 6 is 0.314258
Final Trust value of node 7 is 0.358888
Final Trust value of node 8 is 0.252287
Final Trust value of node 9 is 0.310421
Final Trust value of node 10 is 0.212946
Final Trust value of node 11 is 0.755405
Final Trust value of node 12 is 0.829829
Final Trust value of node 13 is 0.453304
Final Trust value of node 14 is 0.427468
```

Figure.9: Trust values updating file

Figure 9 will be representing the final trust node's values. Before the estimation of final trust values, the direct trust and indirect trust values are evaluated for all the nodes. The feature of trust is the one of the constraints for the selection of route in the simulation.

```
v 0.01 eval {set sim_annotation {###Network formation }}
s 2.000000000 _16_ AGT  --- 0 cbr 1000 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000
er 0.000] ------- [16:0 15:0 32 0] [0] 0 0
r 2.000000000 _16_ RTR  --- 0 cbr 1000 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000
er 0.000] ------- [16:0 15:0 32 0] [0] 0 0
s 2.000000000 _12_ AGT  --- 1 cbr 1000 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000
er 0.000] ------- [12:0 13:0 32 0] [0] 0 0
r 2.000000000 _12_ RTR  --- 1 cbr 1000 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000
er 0.000] ------- [12:0 13:0 32 0] [0] 0 0
s 2.000000000 _9_ AGT  --- 2 cbr 1000 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [9:0 10:0 32 0] [0] 0 0
r 2.000000000 _9_ RTR  --- 2 cbr 1000 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [9:0 10:0 32 0] [0] 0 0
s 2.000000000 _19_ AGT  --- 3 cbr 1000 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000
er 0.000] ------- [19:0 18:0 32 0] [0] 0 0
r 2.000000000 _19_ RTR  --- 3 cbr 1000 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000
er 0.000] ------- [19:0 18:0 32 0] [0] 0 0
s 2.000000000 _2_ AGT  --- 4 cbr 1000 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [2:0 1:0 32 0] [0] 0 0
r 2.000000000 _2_ RTR  --- 4 cbr 1000 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [2:0 1:0 32 0] [0] 0 0
s 2.000000000 _7_ AGT  --- 5 cbr 1000 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [7:0 3:0 32 0] [0] 0 0
r 2.000000000 _7_ RTR  --- 5 cbr 1000 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [7:0 3:0 32 0] [0] 0 0
s 2.000000000 _8_ AGT  --- 6 cbr 1000 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [8:0 6:0 32 0] [0] 0 0
r 2.000000000 _8_ RTR  --- 6 cbr 1000 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er
0.000] ------- [8:0 6:0 32 0] [0] 0 0
s 2.000000000 _16_ RTR  --- 0 AOMDV 52 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000
er 0.000] ------- [16:255 -1:255 30 0] [0x2 0 1 [15 0] [16 4]] (REQUEST)
```

Figure.10: Trace file of network

Figure 10 shows the trace network file. The node would be representing the requests of route, replies, and values of energy, transmissions of data, and intervals of time that are modernized in an appropriate path.

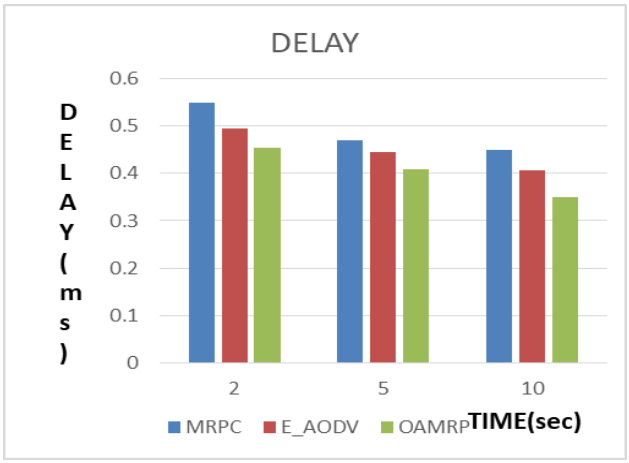

Fig.11: Performance on Delay

Figure 11 would be showing delay of the network. For huge networks, few data packets have got delayed since the heads of assured cluster are not in the others' range. The network delay is improved for protocols that are suggested (OAMRP) than MRPC, E_AODV.

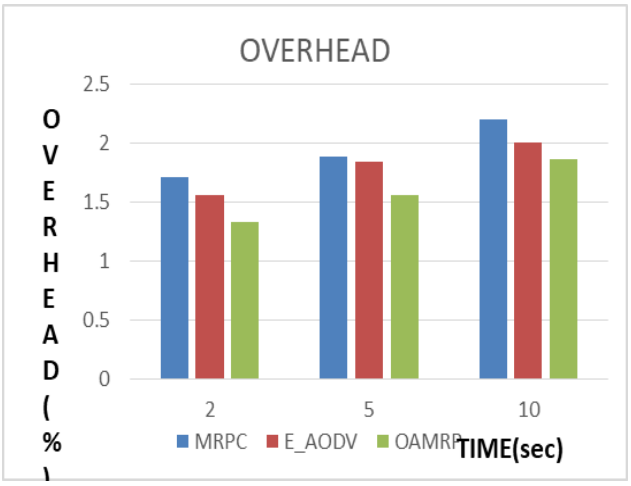

Fig.12: Routing Overhead

Figure 12 would be showing the network overhead. The planned protocol would be maintaining routing overhead while the packets of data needed for every node process of routing. The initiated protocol (OAMRP) would be lessening the network overhead while matching up with the existing protocols such as E_AODV and MRPC.

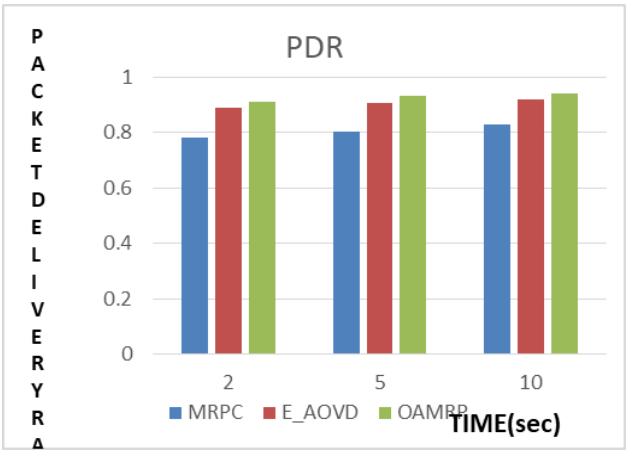

Fig. 13: Packet Delivery Ratio

Figure 13 would be showing the Ratio of Packet Delivery of the network. While data packets are transmitting at receiver for heavy networks it ought to get more packets with no dropping. The ratio of packet delivery of the network is enhanced for suggested protocols (OAMRP) than MRPC, E_AODV.

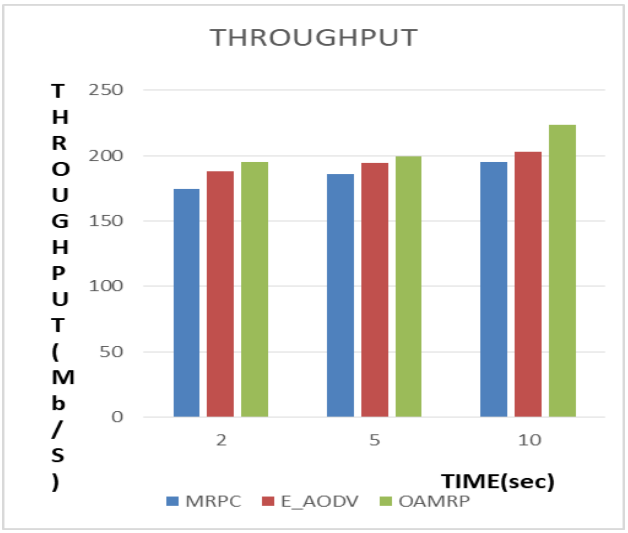

Fig. 14: Throughput

Figure 14 would be showing the network throughput. The network of suggested performance protocol (OAMRP) is enhanced than the available protocols such as MRPC, E_AODV.

V. CONCLUSION

This paper would give the overhead attentive of multipath routing protocol in MANET. We would explain regarding the routing of multipath in this chapter, routing of the energy aware, routing of overhead aware, and computations trust for each node in network. Energy of overhead conscious routing of grounded multipath would remain presented towards enhancing the assortment of relay node and towards lessening the overhead on the nodes. This would be attained by the nodes' concept situated narrowly closer towards the node of sink. The nodes that are advancing would remain selected cautiously grounded on EOR (Estimated Overhead Rate) on each sole node. The routing of multipath would be remaining advantageous to lessen the utilization sum of the communication frequencies by escaping the traffic through various channels. A trust perspective would be presented grounded on the performance of node's advancing towards each solitary node in the network to provide a trust of communal amongst the nodes. The suggested model when the replicated in terms of delay and routing overhead. The simulated form would display less overhead of routing and throughput although more overhead at the node and aligned with non-authenticated node by utilizing the computation of trust. The initiated protocol of the performance routing is resourceful than active protocol of routing such as MRPC & E_AODV.

REFERENCES

1. Kumar VV, Ramamoorthy S (2018) Secure adhoc on-demand multipath distance vector routing in MANET. in: Proceedings of the international conference on computing and communication systems. Springer, Singapore, pp 49–63
2. Priyadharshini C, Selvan D (2016) PSO based dynamic route recovery protocol for predicting route lifetime and maximizing network lifetime in MANET. In: Technological innovations in ICT for agriculture and rural development (TIAR), 2016 IEEE. IEEE, pp 97–104
3. Padwalkar US, Ambawade DD (2015) MMRE-AOMDV based energy efficient (MAEE) routing protocol for WMSNs. In: International conference on communication, information computing technology (ICCICT), Mumbai, pp 1–7
4. Jan, M. A., Jan, S. R. U., Alam, M., Akhunzada, A., & Rahman, I. U. (2018). A comprehensive analysis of congestion control protocols in wireless sensor networks. Mobile Networks and Applications, 23(3), 456–468.
5. Umapathi, N., Ramaraj, N., Balasubramaniam, D., &Adlin, R. (2015). An hybrid ant routing algorithm for reliable throughput using MANET. Intelligent Computing and Applications, 343, 127–136.
6. Jabeen, Q., Khan, F., Khan, S., & Jan, M. A. (2016). Performance improvement in multihop wireless mobile adhoc networks. The Journal Applied, Environmental, and Biological Sciences (JAEBS), 6(4S), 82–92.
7. Borkar GM, Mahajan AR (2016) "A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks. WirelNetw 23(8):2455–2472
8. Kumar A, Sachin Y (2016) QMRPRNS: design of QoS multicast routing protocol using reliable node selection scheme for MANETs. Peer-to-Peer Netw, Appl.
9. Mohammad, Arshad Ahmad &Mahmood, Ali &Vemuru, Srikanth. (2019). Energy-Aware Reliable Routing by Considering Current Residual Condition of Nodes in MANETs. 10.1007/978-981-13-0514-6_44.
10. S. Abbas, M. Merabti, D. Llewellyn-Jones, K. Kifayat, Lightweight sybil attack detection inMANETs. IEEE Syst. J. 7(2), 236–248 (2013).
11. W. Liu, H. Nishiyama, N. Ansari, J. Yang, N. Kato, Cluster-based certificate revocation withvindication capability for mobile ad hoc networks. IEEE Trans. Parallel Distrib. Syst. 24(2),239–249 (2013).
12. H. Dahshan, F. Elsayed, A. Rohiem, A. Elgmoghazy, J. Irvine, A trust based threshold revocationscheme for MANETs, in IEEE 78th Vehicular Technology Conference (VTC Fall) (2013).
13. H. Zhao, X. Yang, X. Li, CTrust: trust management in cyclic mobile ad hoc networks. IEEETrans. Veh. Technol. 62(6), 2792–2806 (2013).
14. L. Harn, J. Ren, Generalized digital certificate for user authentication and key establishmentfor secure communications. IEEE Trans. Wirel. Commun. 10(7), 2372–2379 (2011).
15. M. Yu, M. Zhou, W. Su, A secure routing protocol against byzantine attacks for MANET inadversarial environments. IEEE Trans. Veh. Technol. 58(1), 449–460 (2009).
16. L. Li, R. Liu, Securing cluster-based ad hoc networks with distributed authorities. IEEE Trans.Wirel. Commun. 9(10), 3072–3081 (2010).
17. J.J. Haas, Y. Hu, K.P. Laberteaux, Efficient certificate revocation list organization and distribution.IEEE J. Sel. Areas Commun. 29(3), 595–604 (2011).
18. J. Jiang, G. Han, F.Wang, L. Shu, M. Guizani, An efficient distributed trust model for wirelesssensor networks. IEEE Trans. Parallel Distrib. Syst. 26(5), 1228–1237 (2015).
19. Y. Chae, L.C. Dipippo, Y.L. Sun, Trust management for defending on-off attacks. IEEE Trans.ParallelDistrib. Syst. 26(4), 1178–1191 (2015).
20. B.-J. Chang, S.-L.Kuo, Markov Chain trust model for trust-value analysis and keymanagementin distributed multicast MANETs. IEEE Trans. Veh. Technol. 58(4), 1846–1863 (2009).
21. A.M. Shabut, K.P. Dahal, S.K. Bista, I.U. Awan, Recommendation based trust model with aneffectivedefence scheme forMANETs. IEEE Trans. Mob. Comput. 14(10), 2101–2115 (2015).
22. R. Venkataraman, T. Rama Rao, M. Pushpalatha, Regression-based trust model for mobile adhoc networks. IET Inf. Secur. 6(3), 131–140 (2012).