European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 05, 2020

An Enhanced Multipath Relay Node Selection Strategy Using Modified Multipath Routing Protocol In MANET

Yamini Swathi L[1] P S V Subba Rao[2] K Samatha[3]

[1]*PhD Scholar, Dept. of Physics, Andhra University, Visakhapatnam, Andhra Pradesh, India*

[2]*Associate Professor, Dept. of Physics, Andhra University, Visakhapatnam, Andhra Pradesh, India*

[3]*Professor, Dept. of Physics, Andhra University, Visakhapatnam, Andhra Pradesh, India*

Abstract- In despite of the geographical location, internet connection is provided always and everywhere with the implications of designing of Mobile ad hoc network (MANET). Different types of applications of MANETs are included environment monitoring, military and disaster recovery. The resource-constrained environment of MANET is not allowed to perform the communication processes easily. For the network nodes, the limited batteries are utilized as an equipment. Throughout this process, the major challenging issue is replacing and recharging of these batteries. Within the MANET, the nodes are added without considering the circumstances. To process the communication among nodes, the trustworthy and reliable techniques should be inculcated. The definition of trustworthiness is about the opinion of a node on the other node with the numerical representation. The trust is computed based on the previous communication among current nodes. To address the limitations, a technique of modified multipath routing is needed. By using the network layer, efficiency is achieved in terms of energy utilization as the MANET is an infrastructure-less network and a peer-to-peer network. The routing path is chosen according to the network nodes' current residual condition with the improved modified multipath routing protocol. The proposed technique is performed efficiently in terms of network stability and network's lifetime than the existing methods like MRPC and E-AODV. To determine the proposed method's effectiveness, NS2 software is utilized to assess the simulation results.

Keywords: MANET, Multipath, E-AODV, MRPC, Overhead Aware routing, MMPRP, Clustering.

1. INTRODUCTION

Intended for determining a single route amongst a source as well as target node, average routing protocols in ad hoc wireless networks, for instance AODV as well as DSR, remain proposed primarily. Multipath routing comprises of detection of several routes amongst a source as well as a target node. These multiple paths amongst source as well as destination node pairs may remain utilized for corresponding among the dynamic as well as random behaviour of ad hoc systems [1]. Usage of multiple paths aimed at attainment of a minor end to end delay can remain possible assuming the obtainability of huge bandwidth.

Redundant as well as alternative routes remain recognized by presentation of effective information packet transmission in multipath routing protocols. Moreover The power intake of key relay nodes remains condensed and the network subdividing difficulty produced using

the energy consumption of these nodes is resolved. These multipath protocols remain engaged aimed at delivering dependability, decreasing overhead as well as maximizing network lifespan as well as cross routing [2]. Detection plus conservation of multiple paths have remained the concerns of multipath routing protocols.

Routing alongside a single path might not offer sufficient bandwidth aimed at a bond in view of the restricted environment of in a wireless network. Nevertheless, once numerous paths remain utilized instantaneously towards routing information, the collective bandwidth of the routes might indulge the bandwidth limitation of the submission. Moreover, the existing bandwidth remains greater that might allow a smaller end to end delay assuming the obtainability of a greater bandwidth. Radio interference must be engaged into consideration by nodes in the network communicating over the wireless medium. Thus regulating the attainable throughput, Broadcasts commencing a node alongside single route might obstruct using broadcasts from a node along additional one.

The Route detection overhead of the multipath routing remains as great as that of single path routing. Acceptable working of the technique remains probable in a multipath routing network regardless of the happening of any downfall of one or some of the multipath amid a source as well as its destination. Hence, the frequency of route detection remains small in such system. Moreover, multipath routing [3] fallouts in a greater throughput, by means of the entire nodes remain set to practice a restricted capability, for instance bandwidth as well as processing power.

Energy reduction techniques estimated by routing layer, as well as the effort is energy capability in MANETs may remain addressed at unlike layers [4]. In latest centuries, several investigators have been giving consideration towards the expansion of energy usage of mobile nodes, commencing special points of opinion. Certain scheduled resolutions effort towards changing the communication control of wireless nodes. Additional applications lean towards proficient managing of a sleep state for the nodes and these resolutions sequences after pure MAC-layer resolutions towards resolutions joining MAC and routing functionality.

Lastly, there exist several suggestions that effort to categorize an energy effective routing process, proficient of routing information above the system as well as conserving the battery power of portable nodes. Such applications are frequently completely different, when others purpose to enhance energy-attentive performance towards available protocols, such as AODV, DSR and OLSR.

The objective of energy awareness routing protocols stays towards reducing energy usage in the transmission of packets amid a source as well as a destination, to stay away from routing of packets over nodes by small enduring energy [5], towards optimizing overflowing of routing in sequence above the system then towards avoiding interference as well as intermediate impacts. Certain routing protocols establish wireless nodes into clusters, for example leach. In Xia & Vlajic the situations below such protocols remain energy capable remains documented as well as the best radius of a collection remains defined.

Towards providing opportunity in the investigation, this unit shall remain devoted to define what routing overheads remain, what routing overheads to expect (i.e. metrics) grounded on what additional investigation has well-defined routing overheads in addition to why lower routing overheads might not remain significant. In a network towards maintaining connectivity, Routing overheads are the processing necessity aimed at a node. Several of these routing overheads may be understood by means of limitations in the network and may

upsurge bandwidth intake, as well as energy utilization. The succeeding are the usually deliberated overheads that will remain utilized in the investigation of MANET overheads [6].

Papers such as claim upon that determining routing paths as well as position of nodes may affect the overheads of routing. The aforementioned employs GPS co-ordinate of nodes towards helping to decrease routing path procedure controls. It determines an improved version of the AODV protocol [7] named as the Adaptive Request Zone for Ad Hoc On-Demand Distance Vector (ARZAODV) protocol that uses a process to define distance as well as positioning of a node.

In traditional routing, the advancing nodes remain carefully chosen grounded on static considerations (ex: series number in AODV). Thus every now and then similar nodes might remain carefully chosen endlessly as of their preeminence in specific considerations. This unceasing assortment of these nodes [8] deprived of assuming their obtainable possessions may outcome in advanced packet delays as well as losses. Similarly this unceasing assortment of the carefully chosen nodes produces additional overhead towards the advancing nodes.

2. RELATED WORK

In [9], author presents and finding the routing path for avoiding the node for becoming the bottleneck, extending the lifetime of the network and for providing the stability of the link is the aim of this method. In terms of energy as well as buffer using the knapsack approach, the existing residual condition is the Route selection metric of the proposed routing protocol. An inquisitive pattern towards bottleneck node, calculation of current residual condition of nodes, priority assignment, as well as routing path initiation are the essential contributions for the proposed method.

As a result of infrastructure-less network, Reducing MANET's susceptibility is a challenging task. The network's safety within this literature is improved by various certificate revocation (CR) methods as well as trust calculation approaches. A recommendation -built trustworthy model is presented by Shabut et al. [10]. Including the different characteristics such as trust, confidence value, as well as deviation value during the creation of a cluster in order to obtain the secure node communication in MANET is the main aim of this method. The trustworthy is calculated by providing an effective method. The intruders towards the contribution of the network operations are prevented by presenting a certificate revocation technique proposed by Liu et al. [11]. WL (Warning List) as well as BL (Black List) are the 2 kinds involved in this approach and CA handles these listings and the false acquisition is reduced using this approach.

A trust-based threshold cryptography revocation approach on behalf of MANETs is presented by Dahshan et al. [12]. Once, the hash chain operation is applied, the modes for distributing the CA key is described here. An approach for calculating a trustworthy graph which defines the duration of the communication of the nodes with others with the considerations of LCM of the initial communicating period as well as exchange of the trusted values throughout the succeeding communication using the adjacent node is presented by Zhao et al. [13]. The movement of the nodes within a cyclic order is obtained by reducing the communication overhead.

The generalized digital certificate (GDC) model is presented by Harn and Ren [14] and providing the user identification or authentication as well as key agreement is the major

objective of GDC. The Discrete logarithm (DL) built as well as integer factoring built protocols are used by them in which the user authentication as well as the establishment of the secret key is achieved. In order to establish the effective paths within the mixed multi-hop wireless networks is discussed by Mahmoud et al. [15]. The trust systems as well as the payment using a trust-built in addition to energy-aware routing protocol is combined by E-STAR. A completely circulated IMKM is presented by Li and Liu [16] with the combination of ID built multiple secret as well as threshold cryptography. The importance of the certificated in order to authenticate and to provide additional significance upon the efficient key management is eradicated by it.

A sequence of steps which attains the objectives for reducing the size of CRL is proposed by Haas et al. [17] and the existence of the certificate within CRL is found using this efficient technique in addition to the technique for the updates of CRL. An Effective Distributed Trust Model (EDTM) which could evaluate the trust of the sensor nodes in an accurate way is presented by Jiang et al. [18] and the safety violation can be prevented in an efficient way. A trustworthy evaluation technique which is dealt widely using a harsh on–off attack situation is presented by Chae et al. [19]. A technique for calculating the trustworthy with the help of Chain Trust model is proposed by Chang and Kuo [20] and moreover, it presents a method for keeping a secondary CA suspended during the initial CA failure is proposed by Chang and Kuo [20]. A light weighted IDS in which the nodes are defended with the help of the identity switch that causes the attack is presented by Abbas et al. [21]. A trustworthy model depending upon the regression for providing secure routing is presented by Venkataraman et al. [22].

3. PROPOSED SYSTEM

In this phase of the research work, an overhead aware modified multipath routing protocol (MMPRP) is introduced to improve the node selection and to reduce the overhead on the nodes. This is done with the concern of the nodes closely located nearer to the sink node. The forwarder nodes are selected based on estimated overhead rate (EOR) on each node. The multipath routing is useful to reduce the occupancy rate of the communication channels by bypassing the traffic through multiple channels. A trust framework is introduced based on node's forwarding behavior to each and every node in the network to provide a mutual trust between the nodes.

In this point of the investigation effort, an overhead aware energy grounded multipath routing remains presented towards improving the relay node assortment as well as towards reducing the overhead on the nodes. This remains achieved by the concept of the nodes narrowly positioned closer towards the sink node. The advancing nodes remain carefully chosen grounded on estimated overhead rate (EOR) on every single node. The multipath routing remains beneficial for reducing the usage amount of the communication frequencies through evading the traffic via several channels. A trust context remains presented grounded on node's advancing performance towards every single node in the network for providing a communal trust among the nodes.

a. Route discovery process in network:

The reactive protocol doesn't maintain account of data regarding their neighbors. When a necessity to communicate with further node, it initiates the route detection procedure towards identifying the optimal towards the destination. In network scenario (figure 2), the source node S initiates Route discovery procedure in building the RREQ and onwards towards its

neighbor nodes. When a node obtains RREQ, it computes the RREQ list and forwards towards the nodes existing in the record. This procedure endures till the destination befalls. The destination node builds the RREP, and forwards towards the nodes in the RREP list. This procedure continues until the source is obtained. The gradual procedure of route discovery is as follows:

Step 1: Recognize the N/W Topology.

Step 2: Source node initiates the Route Request (RREQ) towards finding the optimal route from source towards destination.

Step 3: The neighboring nodes obtain RREQ and introduce its neighbor data in the RREQ packet and forward the RREQ towards its neighboring nodes deprived of preserving the RREQ information.

Step 4: The step 3 repeated until the destination arise otherwise until the Time To Live (TTL) pass away, If TTL terminates afore the destination is recognized, at that time increase the TTL value and continue the step 2.

Step 5: The destination node obtains RREQ and build the Route Replay (RREP) and forwards towards the nodes present in the approval list.

Step 6: Whenever a node obtains RREP, it will run the step 5.

Step 7: The source node obtains the RREP from unalike routes, and select the optimal route.

3.2 Creating Cluster

Cluster remains the combination of expedients in the network towards subgroups. Cluster remains designed using by means of the expanse amid 2 nodes. This phase would reduce the hops when transferring information since a cluster would remain thoroughly combined. The distance among two nodes remains utilized when developing cluster since they remain feasible to practice the similar situations or atmosphere, hence combining them collected would decrease the variance of trust standards among them.

3.3 Calculating Trust

This method offers the calculation of direct trust by sum of positive as well as adverse communication amongst the nodes and shows in equation 1.

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

Aimed at twofold nodes i and j, α remains the sum of effective communication as well as β remains the sum of ineffective communication. The trust value would constantly remain $0 \leq DT \leq 1$.

3.4 Selection of Threshold

The selection of threshold remains a significant characteristic in the above-anticipated exemplary as the safety level is influenced by the threshold, if threshold stands greater, the safety will remain great because the entire nodes below threshold will remain invalidated. Threshold beginning 0.7 to 1.0 would offer less possibility aimed at malicious action.

Selecting high threshold value originates by certain drawback, i.e., if a communication remains inflated owing to specific ecological or exterior module the aforementioned lessens the trust value of a resultant node too outcome within invalidation of a node. Hence selection of threshold ought to remain examined along with several aspects.

3.5 Algorithm process

Step1: Initially nodes are deployed in the network area randomly

Step2: The nodes are divided into clusters based on the distance between the nodes

Step3: Each node is assigned with direct trust, indirect trust and average trust values to evaluate the trustworthiness of the nodes

Step4: Nodes trustworthiness is assessed based on node's forwarding behaviour

Step5: Network is divided into clusters to manage the trust calculation in an efficient way

Step6: Each cluster is represented with their elected Cluster heads

Step7: The CH nodes closely monitor the nodes in the cluster to evaluate the node

Step8: Direct trust is calculated using the neighbour nodes of a current node.

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

Step10: From these direct and indirect trust values node's average trust is calculated

Step11: This average trust describes the trustworthiness of the nodes in the cluster

Step12: During data transmission, these trust values are taken into account to make the forwarder node selection decision.

Step13: Overhead is the factor which affects the node performance.

Step14: Overhead describes how much load is given / generated on the node to perform the given tasks

Step15: During forwarder node selection, this overhead is considered as a prominent factor to select the low overhead node

Step16: Node's average trust values are compared with each other to identify the high trust nodes as they are believed to be most successful.

Step17: To reduce the overhead on every node, multipath routing is taken.

Step18: All the possible paths between the communicating nodes are identified with the help of a routing protocol.

Step19: Overhead and trust are the deciding factors to select the most suitable forwarder nodes.

These factors of every node are compared with their neighbour nodes and finally the forwarder nodes are finalised.

4. RESULTS AND DISCUSSION

Through the implementation of the relative simulations, the MMPRP efficiency can be measured. With the help of Network simulator-2, the simulation of the proposed protocol, E-AODV, and MRPC protocols are performed. The proposed energy model is comparable with the E-AODV, MRPC protocols and MMPRP. The deployment of the 21sensor nodes is done within a topographical area A of 1000 m x 500 m in this simulation. Table 1 presents the essential metrics of this simulation.

Table 1 demonstrates the system parameters employed in our simulations.

The following metrics are considered in order to analyze as well as to compare the performance of this proposed method and the existing protocols.

1) **Network performance:** The amount of transmitted packets is evaluated in Megabits per sec.

2) **Propagation Delay:** Average time taken for one packet to propagate from source node towards the destination node.

3) **Packet delivery ratio:** the Ratio of Data packets transmitted towards the destination.

4) **Overhead:** Number of 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	1000 bytes
Number of sensor nodes	21
Number of simulation iterations	160
Initial energy	100j
Network area	1000x500

Number of clusters	8
Routing methods	MMPRP, E-AODV, MRPC
Routing protocol	AODV
Simulation time	10sec

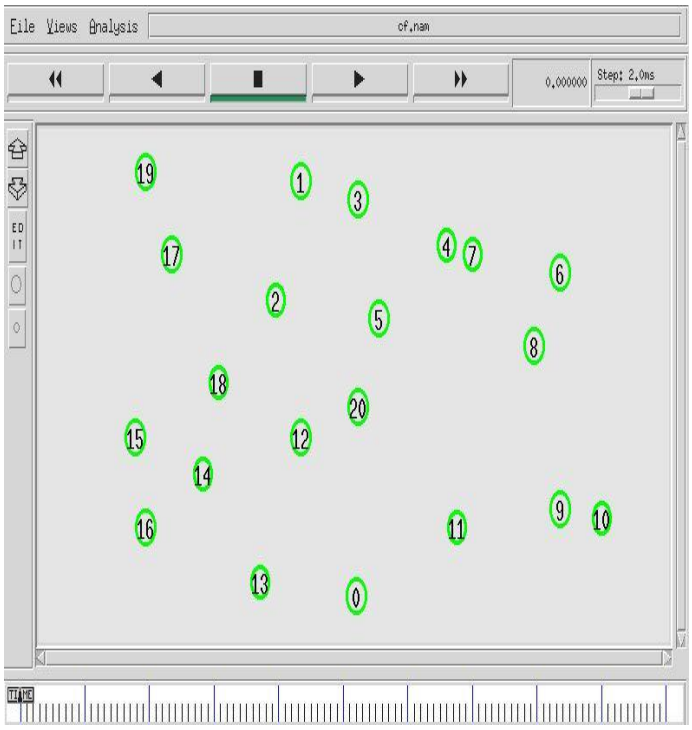

Figure. 1: Network deployment

Figure 1 represents the network deployment. All the nodes are physically located in a random approach.

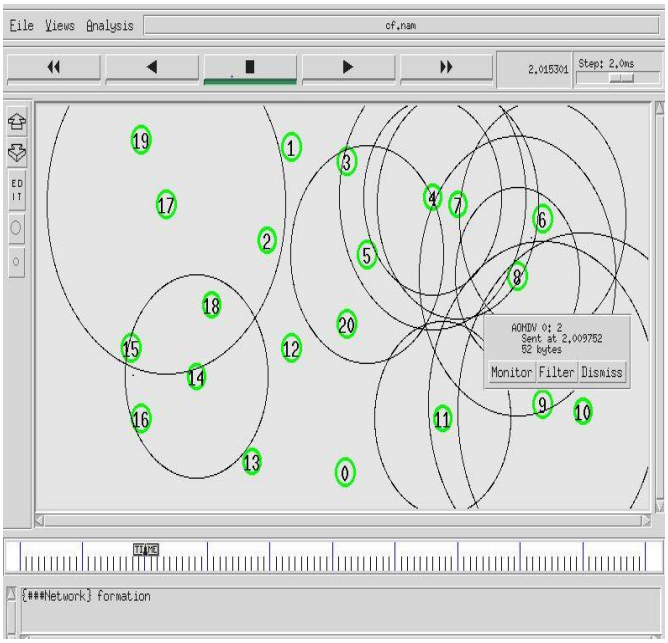

Figure. 2: Broadcasting in network

Figure 2 represents the broadcasting process in the network. Here all the nodes request their neighbor nodes for route reply. In this network, routing protocol decides the RREQ and RREP processes.

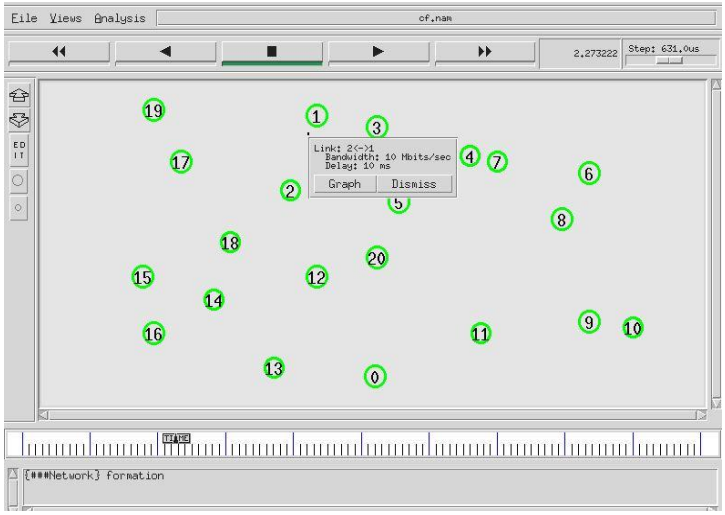

Figure.3: Cluster member to Cluster head transmission

Figure 3 represents the cluster member to cluster head for data transmission. After cluster formation, cluster heads are selected based on their distance from node to node in each cluster. Here, link should be signified between the cluster member and cluster head.

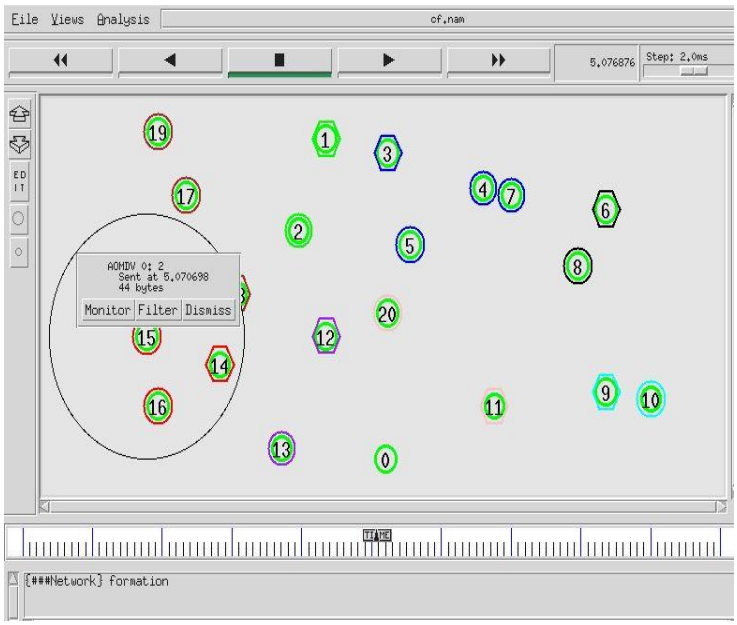

Figure. 4: Route level checking process

Figure 4 represents the route level checking before data transmission. Here AOMDV protocol decides the path level and confirms whether the path is appropriate for routing or not. The routing protocol constructs the multipath and sends data through available multipath.

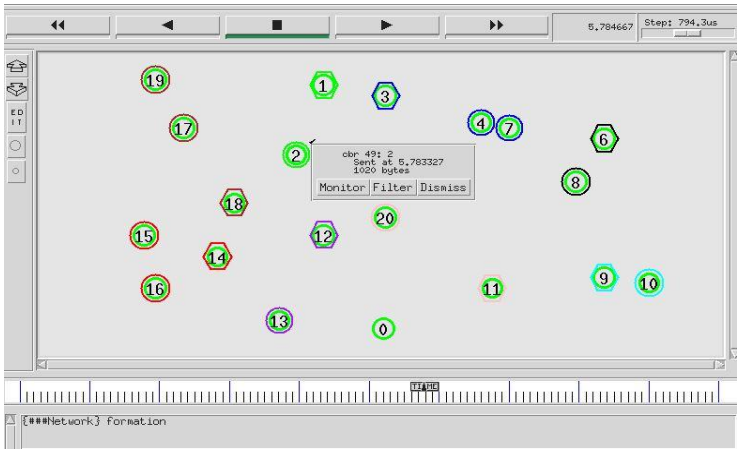

Figure. 5: Cluster member to CH Data transmission

Figure 5 represents the cluster member to CH data transmission. In this figure, CBR acts as traffic protocol that helps to decide the packet size, time interval, maximum number of packets, start and end time for data process.

```
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 represents the cluster files formation with time update and consumes eight clusters in the network. The cluster head selection process is based on the distance between neighbors in the network. After the distance calculation, the cluster head has to decide which cluster member is at nearest distance to the cluster head while 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 represents the hop file in network. Here index, source, destination, previous hop node, and next hop node is represented in this table. In this figure, hop nodes between source and destination decides which path is to be selected 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 represents the transmission file of network. Here, the figure represents each node that forwards the data to particular node in certain time. In this figure, source node, destination node, and time interval are updated.

```
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 represents the final trust values of all the nodes. Before the calculation of final trust values, the direct trust and indirect trust values are calculated for all the nodes. In our simulation, trust factor is the one of the parameters for route selection.

```
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 represents trace file of network. Here node represents the route requests, replies, energy values, data transmissions, and time intervals that are updated in a proper way.

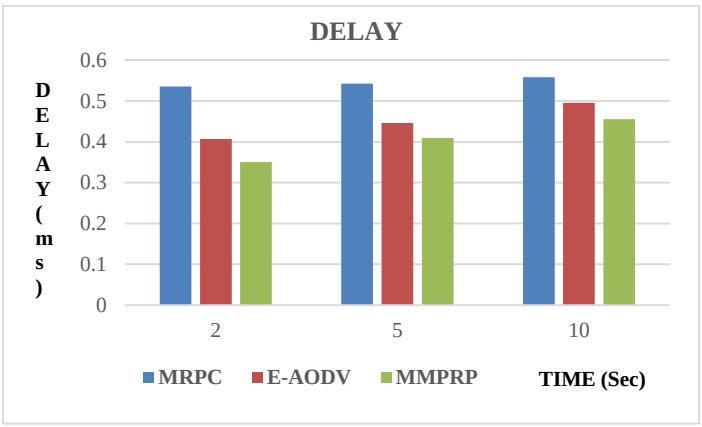

Fig.11: Performance on Delay

Figure 11 shows delay of the network. As some of the CHs are not in the vicinity of their transmission, certain packets are forwarded with some delay. Delay of the network is better for proposed protocols (MMPRP) than MRPC, E_AODV.

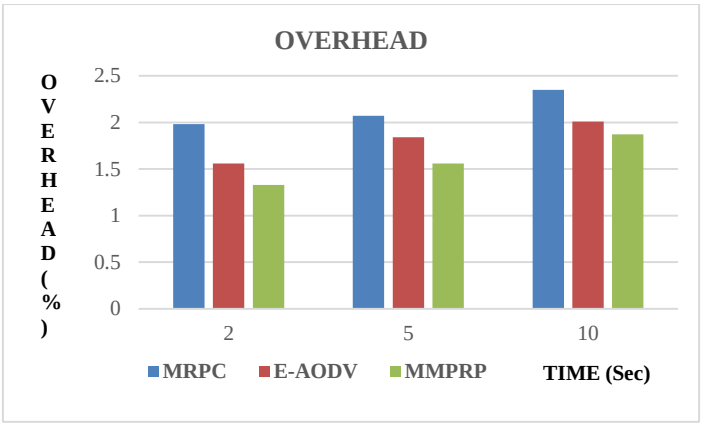

Fig.12: Routing Overhead

Figure 12 shows overhead of the network. The proposed protocol maintains routing overhead while data packets required for each node routing process. The proposed protocol (MMPRP) reduces the network overhead while comparing with the existing protocols like MRPC, E_AODV.

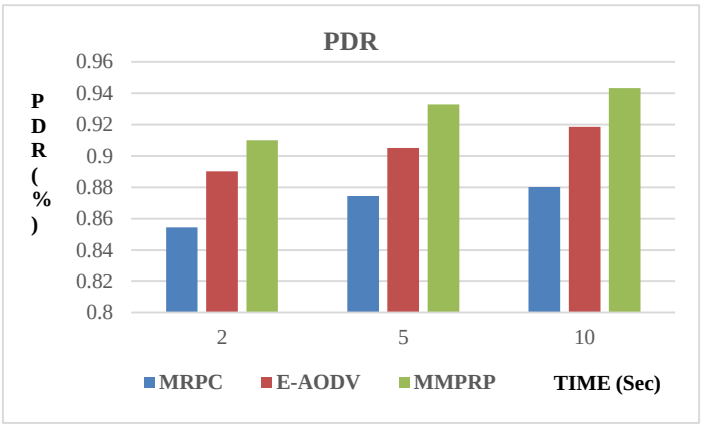

Fig. 13: Packet Delivery Ratio

Figure 13 shows Packet Delivery Ratio of the network. For large networks, while data packets are transmitting at receiver it should get more packets without any dropping. Packet Delivery Ratio of the network is better for proposed protocols (MMPRP) than MRPC, E_AODV.

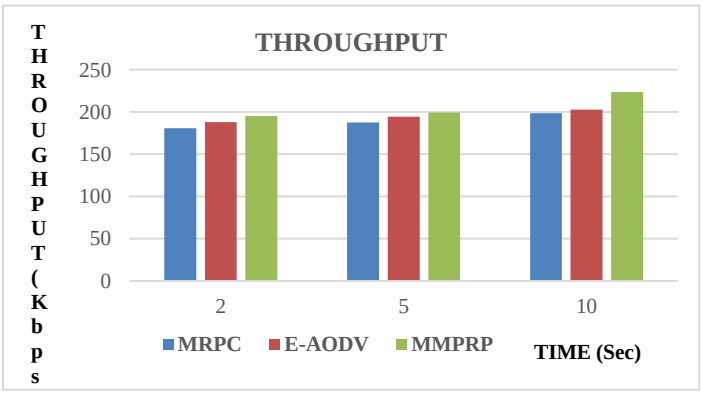

Fig. 14: Throughput

Figure 14 shows Throughput of the network. The network performance of proposed protocol (MMPRP) is better than the existing protocols like MRPC, E_AODV.

5. CONCLUSION

This chapter present the modified multipath routing protocol in MANET. In this chapter, we describe about multipath routing, energy aware routing, overhead aware routing, and trust calculations for every node in network. In this point of our research work, an overhead aware energy grounded multipath routing remains presented towards improving the relay node assortment as well as towards reducing the overhead on the nodes. This remains achieved by the concept of the nodes narrowly positioned closer towards the sink node. The advancing nodes remain carefully chosen grounded on estimated overhead rate (EOR) on every single node. The multipath routing remains beneficial for reducing the usage amount of the communication frequencies through evading the traffic via several channels. A trust context remains presented grounded on node's advancing performance towards every single node in the network for providing a communal trust among the nodes. The proposed method when simulated with respect to delay and routing overhead. The simulated model would demonstrate a smaller amount of routing overhead and throughput while more overhead at the node and against non-authenticated node by using trust calculation. The efficiency of proposed routing protocol is efficient than existing routing protocol like E_AODV, MRPC.

6. 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. Wirel Netw 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 in MANETs. IEEE Syst. J. **7**(2), 236–248 (2013).
[11] W. Liu, H. Nishiyama, N. Ansari, J. Yang, N. Kato, Cluster-based certificate revocation with vindication 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 revocation scheme 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. IEEE Trans. Veh. Technol. **62**(6), 2792–2806 (2013).
[14] L. Harn, J. Ren, Generalized digital certificate for user authentication and key establishment for 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 in adversarial 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 wireless sensor 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. Parallel Distrib. Syst. **26**(4), 1178–1191 (2015).
[20] B.-J. Chang, S.-L.Kuo, Markov Chain trust model for trust-value analysis and keymanagement in 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 an effective defence 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 ad hoc networks. IET Inf. Secur. **6**(3), 131–140 (2012).