A QoS BASED PROGRESSIVE LINK PREDICTION MATHEMATICAL APPROACH FOR DATA TRANSFER IN MANET

A.MAHENDRAN[1], Dr.C.KAVITHA[2] , K.SAKTHIVEL[3]

[1]Ph.D Research Scholar, Dept of Computer Science, Periyar University, Salem-636011.

[2]Assistant Professor, Dept of Computer Science, Thiruvalluvar Govt Arts College, Rasipuram-637401.

[3]Professor, Dept of CSE, KSR College of Technology, Tiruchengode-637215.

E-mail: [1]ayem22@gmail.com

ABSTRACT

The MANET (mobile ad hoc network) is a self-designed, self-coordinated, foundationless network comprising mobile nodes. Every node can move the data packets with one another over one or the other radio or infrared. All networks should give an acceptable and helpful degree of Quality of Service (QoS) to guarantee that applications are very much upheld. This becomes a challenge regarding Mobile ad-hoc networks (MANETs). To help the developing requirement for multimedia and constant applications, quality of service (QoS) support by the networking protocol is required. A few significant QoS boundaries that are required by such applications can be distinguished. They incorporate transfer speed, start to finish delay, delay jitter, and spot blunder rate. So in this paper, we proposed a QoS based Progressive Link Prediction Mathematical Approach for Data Transfer in MANET. Model to estimate the future status of link availability using a QoS based Progressive Link Prediction Mathematical Approach for Data Transfer in MANET. A mathematical model for preventing Attacks in MANET by Using Elliptic Curve Cryptography Algorithm. The experimental result based on the proposed model with AODV routing is better than the existing methods.The proposed model combines a mathematical approach and ECC, along with AODV routing, for predicting links and preventing attacks. The main objective of this research is to provide an efficient data transfer using an optimized prediction and attack prevention model.

Keywords: *MANET, QoS, Link prediction, data transfer, mathematical approach, AODV routing.*

1. INTRODUCTION

MANET (mobile Adhoc network) is a self-coordinated, self-configured, infrastructure-less network associated remotely. This network is Adhoc because it does not rely upon a prior infrastructure like access focuses in remote networks or switches in a wired network. An ad hoc network is a self-coordinating multi-jump remote network that doesn't depend on fixed networks or predefined networking. In this network engineering, every node is utilized to advance the data packets to different nodes. Traditional optical network performance concentrates on center around working out network layer boundaries, for example, the network throughput and blocking probability, which are just founded on the accessible limit and traffic load of the network. Be that as it may, in real network situations, mainly on account of straightforward optical networks, the deterrent to the light way is not generally just controlled by the network layer factors; the actual layer factors, like the quality of transmission (QoT).

Giving QoS support in MANETs includes every one of the layers of the OSI model, beginning with the application layer at the highest point of the stack down to the actual layer at the base.

This paper centers on QoS provisioning in the network and medium access control (MAC) layers. Moreover, it presents a hypothetical diagram establishment that is straightforwardly connected with giving obstruction free activity in a remote environment. An option is to adopt service reaction prediction for QoS on the board. Given a transmission capacity assignment, a service reaction prediction plot estimates the related service quality [1]. The QoS of the executives is then completed from the prediction results subject to the ideal transmission quality. Albeit a few existing service prediction techniques [2], [3] and [4] are successful, offline preparation is typically required.

It might then be hard to adapt the preparation results for a home network environment with time-changing nature.

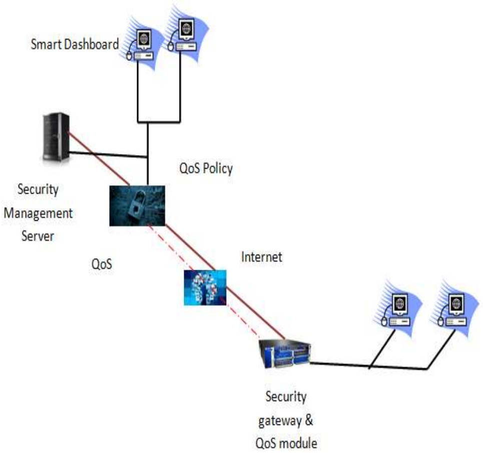

Figure 1:The architecture of QOS Transmission

QoS uses the business' most advanced traffic investigation and bandwidth control advances. Check Point-protected Stateful Inspection technologies catches and powerfully refresh itemized state data on all network traffic. This state data is utilized to characterize traffic by service or application. After a bundle has been arranged, QoS applies to the parcel through an imaginative, various leveled, Weighted Fair Queuing (WFQ) calculation to control bandwidth allocation.

2. LITERATURE SURVEY

1. **M. Naresh, Assistant Professor, and Aayushi Raje, Karanam Varsha (2019)** et al. "Link Prediction Algorithm for Efficient Routing in VANETs" Extraordinary attributes of Vehicular Ad Hoc Networks (VANETs) for example enormous network sizes and fast geography changes make it challenging to keep up correspondence links bringing about successive link separations. Since VANETs are an essential component of Intelligent Transport Systems (ITS), steering ought to be given in a way that satisfies any Quality of Service (QoS) limits. This proposes a link prediction-based way to deal with anticipating the span of accessibility of the current path. The AQRV protocol chooses the best direction in urban vehicle environments while satisfying specific quality-of-service necessities. Since the geography of VANETs is continually evolving, it is hard to save up a link between source and destination for data exchange. to appraise the lifetime of a functioning link to ts adjoining modules, we utilize the Newton Divided Difference Interpolation technique. In light of this data, when a connection is going to fizzle, a substitute way is developed by AQRV, which decreases the drops of data packets and recovery time.

2. **Diyawu Mumin1 Lei-Lei Shi1 Lu Liu2(2019)** et al. proposed "An efficient algorithm for link prediction based on local information: Considering the effect of node degree" There has been much interest in link prediction research with significant studies on the most proficient method to anticipate missing links or future links in a network dependent on noticed information. Notwithstanding, the critical answer for tackling the link prediction issue is the way to gauge the closeness between the nodes in a network with higher accuracy. A few techniques have been recommended that use the similitude between nodes to appraise their proximity in the network. This paper proposes a practical link prediction calculation that predicts connections between links utilizing the network structure. This calculation involves ordinary neighbors and the degree appropriation of the nodes to gauge the chance of a link between two nodes in a network dependent on nearby information. Boundary based similitude measure is proposed that consolidates the qualities of ordinary neighbors and the level of nodes to foresee the probability of the presence of a link between two nodes in a network. In the trials directed, we exhibited the prevalence of our calculation in prediction accuracy contrasted and other nearby based measurements and efficiency contrasted and CN+PA, Katz, and LP

3. **Jian Shu, Qifan Chen, Linlan Liu, and Lei Xu(2017)** et al. proposed "A link prediction approach based on deep learning for opportunistic sensor network" Link prediction for opportunistic sensor networks has been drawing increasingly more consideration. Nonetheless, the intrinsically powerful nature of an opportunistic sensor network makes it a provoking issue to guarantee the quality of service in an opportunistic sensor network. This article proposes a clever, deep learning structure to foresee links for opportunistic sensor networks. The system stacks the contingent confined Boltzmann machine, which models time series by annexing past time steps. A likeness record dependent on time boundaries is proposed to portray similitudes between nodes. Through tuning the learning rate layer adaptively, the recreation mistake of the confined Boltzmann machine goes stable quickly with the goal that the intermingling time is abbreviated. A CDBN model dependent on deep learning is proposed to accomplish the link

prediction of OSNs. By combining the CDBN with the proposed similitude record, the change law of OSN can be caught accurately while working on the QoS in OSN.

4. **Wen-Jyi Hwang, Tsung-Ming Tai, Bo-Ting Pan, Tun-Yao Lou, and Yun-Jie Jhang (2019)** et al. proposed "An Intelligent QoS Algorithm for Home Networks" An original quality of service (QoS) the executive's algorithm for home networks is introduced in this letter. The algorithm depends on service prediction for intelligent QoS on the board. The service prediction is made by an overall relapse neural network with a profile containing the previous records of the service. An original profile refreshing strategy is proposed to allow the profile size to stay small for quick bandwidth allocation. The logical review and examinations of genuine LAN uncover that the proposed algorithm gives dependable QoS to the executives of home networks with low computational overhead. Assessments of bandwidth allocation consequences of different executions at the QoS level. Scientific studies uncover that the proposed algorithm is QoS-mindful. Additionally, tests over genuine LAN networks show that the proposed algorithm offers quick adaptation with low computational intricacies to the varieties of the source data rates.

5. **J.N GladissMerlin(2015)** proposed an associate imperceptible secure routing theme [5] SECURE to supply complete unlinkability and content unobservability for every kind of packet. MANET may be a network that is freelance network. As a result of figureless property, the network could also be laid low with attackers. Numerous researchers have fictionalized security strategies like encoding strategies to avoid security drawbacks. To enhance security, they tend to mistreat standard two strategies, one RSA formula and the Sha-1 formula. During this project, they tend to prompt unobservability by providing protection for the asking and replying. Their proposed system's main aim is to provide ultimate security in military applications. SECURE is economical because it uses a unique combination of cluster signature and ID-based encoding for route discovery. The simulation results show that SECURE not solely has satisfactory performance compared to AODV but achieves more robust privacy protection than existing schemes like MASK. This research is implementing high-security data transfer; therefore, we will avoid hacking; in contrast to information security, it provides fundamental packet security additionally. By integrating the AES algorithm, authors can provide security to avoid RSA algorithm hacking. Routing protocol SECURE supported cluster signature and ID-based cryptosystem for impromptu networks. The conceptions of SECURE offer solid privacy protection, complete unlinkability, and content unobservability for impromptu networks. The protection analysis demonstrates that SECURE does not solely provide robust privacy protection; it is also a lot of resistant to attacks due to node compromise.

6. Gaurav Soni and Kamlesh Chandra wanshi (2013) proposed an IDS Algorithm that identifies the behavior of selfish nodes and blocks their misbehavior activities[6]. In the case of a selfish node attack, network performance is almost negligible, but after applying IDS on the attack, performance is enhanced up to 92% and provides a 0% Infection rate from the attack. A mobile ad hoc network (MANET) is a collection of mobile devices that can communicate with each other without the use of a predefined infrastructure or centralized administration. In addition to freedom of mobility, a MANET can be created quickly at a low cost, as it does not rely on existing network infrastructure. Due to this suppleness, a MANET is helpful for applications such as disaster relief, emergency operations, military service, maritime communications, vehicle networks, business meetings, site networks, robot networks, and so on. In these networks, besides acting as a host, each node acts as a router and forwards packets to the correct node in the network. Once a route is established, nodes can transfer their data to other nodes. To support this connectivity, nodes use routing protocols such as Proactive routing protocols and Reactive routing protocols. In proactive routing protocols such as Destination Sequence Distance Vector (DSDV) protocol, nodes obtain routes by periodic topology information exchange to maintain the routing table. Reactive routing protocols such as AODV (Ad hoc On-Demand Distance Vector) are ad hoc on demand routing protocols here, and nodes find out routes if required. . Effect on packet loss is visualized in PDF and throughput. A malicious node is the greatest security threat that affects the performance of the AODV routing protocol. Its detection is the primary matter of concern. The acknowledgment (ACK) of TCP represents that due to fake information in the network, most of the senders do not obtain the ACK from the receiver, which means all the ACK are lost, and after applying the IDS scheme, every node that takes part in the routing will show the information of ACK packets. Therefore the proposed IDS scheme work will be excellent for detecting and defending the network from Selfish node attacks. It cannot detect the effect of the selfish attack in performance matrices, and also, the Selfish node for AODV can be implemented in real life scenarios, and its analysis can be compared with the analysis results.

Similarly, topology control, capacity performance, and efficiency [7]-[21] were discussed by several authors in MANET.

3. PROPOSED METHODOLOGY

This paper introduced a model to estimate the future status of link availability using a QoS based Progressive Link Prediction Mathematical Approach for Data Transfer in MANET. Figure 2 shows the proposed approach to workflow

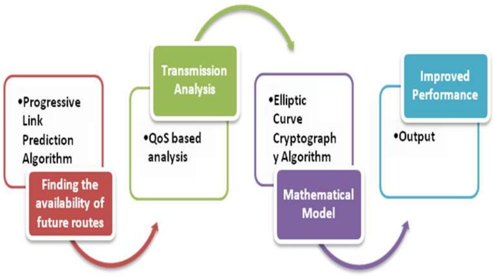
Transmission Analysis
•Progressive Link Prediction Algorithm
•QoS based analysis
•Elliptic Curve Cryptograph y Algorithm
Improved Performance
•Output
Finding the availability of future routes
Mathematical Model

Figure 2: Proposed approach Workflow

3.1Progressive Link Prediction Algorithm

In customary versatile and wired-network routing calculations, a difference in way happens when a link along the way falls flat or another shorter way is found. A link disappointment is exorbitant because multiple retransmission breaks are required to distinguish the frustration, and after that, another method must be discovered, prompting a delay in reclamation. Since ways bomb so rarely in wired networks, this isn't a vital issue. Notwithstanding, as directing conventions in versatile networks pursue this model despite the fundamentally higher recurrence of disconnections, QoS gets influenced. This section uses a progressive link prediction calculation to anticipate the time after a functioning link will break. This is finished by assessing the time at which got signal strength of the information parcels will fall beneath a limit control. They got a power level beneath the limit, demonstrating that the two nodes are moving far from one another's radio transmission. The prediction of link break cautions the source before the way leaves, and the source can rediscover another way ahead of time. In this methodology, three sequential estimations of signal strength of parcels from the forerunner node are utilized to anticipate the link disappointment using the Newton partitioned contrast strategy. The Newton interjection polynomial has the accompanying summed up articulation.

The got flag qualities of the three most recent information parcels and every recipient keeps up their time of the event for every transmitter from which it is accepted. Utilizing three got information bundles' flag control qualities as P1,P2,P3 and the time when parcels touched base as t1,t2,t3 moments individually and Pr as the limit flag solidarity to be operative at the time tp, one can foresee tp. We accept that at the predicted time tp, the connection will break when the control level lessens to limit control. The edge flag quality Pr is the base power receivable by the gadget. This is the power at the maximum transmission go. For instance, WaveLAN cards have maximum transmission scope of 250 meters in open situations in the 900 MHz band. The estimation of the edge flag quality is 3.65x10-10 Watts (for example, typical for the WaveLAN card). The standard flag quality of the parcels can be processed as underneath, where the first and second partitioned contrast separately.

$$P_r = P_1 + (t_p - t_1)\Delta + (t_p - t_1)(t_p - t_2)\Delta^2. \quad (1)$$

$$P_r = P_1 + \frac{(t_p-t_1)(P_2-P_1)}{(t_2-t_1)} + (t_p - t_1)(t_p - t_2)(\frac{(P_3-P_2)}{(t_3-t_2)} - \frac{(P_2-P_1)}{(t_2-t_1)})/(t_3 - t_1) \quad (2)$$

$$Let\ A = ((P_2 - P_1)/(t_2 - t_1)), \quad (3)$$

$$B = \left(\frac{(P_3-P_2)}{(t_3-t_2)} - \frac{(P_2-P_1)}{(t_2-t_1)}\right)/(t_3 - t_1) \quad (4)$$

Equation (2) becomes

$$P_{r=}P_1 + (t_p - t_1)A + (t_p - t_1)(t_p - t_2)B \quad (5)$$

Rearranging equation (5),

$$Bt_p^2 + (A - Bt_1 - Bt_2)t_p + (P_1 - P_r - At_1 + t_1 t_2 B) = 0 (6)$$

This is of the form

$$\mathbf{a}t_p^2 + b\,t_p + c = 0 \tag{7}$$

Where *a=b*,

b=(A-Bt₁- Bt₂) **and**

c=(P₁ – Pᵣ - At₁ +t₁ t₂ B).

Therefore, the predicted time t_p at which the link will fail is

$$t_p = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \tag{8}$$

Routing protocol needs time to set up another or exchange way. Hence a period parameter, primary time, is presented. The basic time ts ought to be sufficient to send blunder messages to the upstream node to the wellspring of the parcel and for the source to locate another course. Thought to be only littler than connection break time ts. After time ts, the node goes into a primary state, and the node should locate a backup course of action. At the point when a connection is relied upon to bomb between nodes, the upstream node first endeavors to discover a path to the destination. If such a course isn't found within a fixed time called the disclosure period, a connection disappointment caution is sent to the sources whose streams utilize this connection. Source nodes can conjure the course revelation instrument to set up reclamation ways. At times ts, they got power that is sufficient for sending cautioning messages to the upstream node and finding a substitute way either by a nearby course fix around the connection, which is going to split or by setting up new ways from sources. As two nodes move outwards, the flagging intensity of the nodes drops. Along these lines, we characterize connect break when nodes are the first intersection the radio transmission goes, and broken connections are repaired locally in k bounces. The estimation of k is two, I. e., broken links can be restored in two bounces. The proposed neighborhood course fix system endeavors to fix erratic courses locally with minimum control overheads for quicker healing.

Proposed Algorithm:

Each time a data packet is received, the receiving node monitors the link with the following algorithm:

```
Step 1:Start the process
Step 2:  Send packet to each neighbor
Step 3:  Update the record of (received power, time) for the last three packets,
Step 4:If ((p1>p2) and (p2>p3)) than prediction ()
Step 5:  Estimate and update the $t_p$ and update the $t_s$,
             when a node enters into a critical state before the link break
Step 6:If current_time is greater than or equal to $t_s$than
Step 7:  Send a warning message to the source node &Sleep for a fixed duration
Step 8:  On receipt of the repair message, Set the route and link status as soon-to-be-broken
Step 9:  Local route repair ()
Step 10:        Find path to next node nj;
Step 11: If (found a path in k hops within time)
Step 12:        Use this path for rerouting.
Step 13: Else
Step 14:        Find path to destination
Step 15: If the path is found
Step 16:        Route the packet through new path,
Step 17:        Send message to sources to find shortest path.
Step 18: Stop the process
```

First, find all possible paths to the destination at the source place, then fix the three best paths. Then it finds sequential estimations of these paths' signal strength, selects the path with the best strength, and then redirects traffic through a new path.

3.2 Transmission Analysis

This QoS based way of creation includes two stages; a solicitation stage and an answer stage. Solicitation stage summons route discovery procedure to discover courses to anycast servers through stable and noncongestion transitional nodes. The answer stage includes updating RIC and conforming to the methods found in the solicitation stage. Regular nodes are the person who fulfills dependability criteria and no congestion necessity of an application because of our solidness and clog models. These stable and no congestion nodes go about as middle nodes and help to make any cast courses from customer to server. In the accompanying segment, we present the procedure of the solicitation stage, answer stage, and course support stage.

A client node finds the course to it any cast server by utilizing RR packets. The arrangements of activities that happen are as per the following.

(1) Client node prepares a RR packet.

(2) Selective forwarding of RR packet to neighbors who satisfy stability and congestion criteria set by the network administrator. We have seen better results from recreation tests, with the Blockage factor (CF) threshold shifting somewhere between 0.1 and 0.3 and the node development stability factor (Nsf) threshold fluctuating somewhere between 0.6 and 0.8. Neighbors with Nsf greater than Nsf threshold and CF not as much as CF threshold are chosen for forwarding of RR packet.

(3) A node receiving RR packet will dispose of it, on the off chance it is already received (by utilizing succession number and client address), and stop forwarding RR packet.

(4) If RR packet is certifiably not a copy, checks RIC for accessibility; if accessible, RP packet will be produced and begins reply engendering to the client.

(5) If a course isn't accessible in RIC, advances the RR packet by refreshing its fields (course record, stability esteem, clog factor, LET and nexthop address) to its neighbors as in stage 2.

(6) Perform stages 3 to 5 until anycast server is reached, and

(7) If server isn't reached inside specific bounces, send RE packet to the client node.

3.3Mathematical Model

A mathematical model is a conceptual model that utilizes mathematical language to depict the framework's behavior. Set hypothesis and mathematical model for preventing Attacks in WSN by Using the Elliptic Curve Cryptography Algorithm.

Step 1: *Let S be the system defined asS = {I, O, F}*
Step 2: *I is main set of inputs of the system. I = {S, BS, A}*
Step 3: *S is main set of Normal Nodes like s1, s2, s3.... S = {s1, s2, s3, ……..., sn}*
Step 4: *A is main set of Cluster Head nodes like a1, a2, a3.... A = {a1, a2, a3…….., an}*
Step 5: *O is main set of Accused Nodes or Attack Nodes like c1, c2, c3.... O = {c1, c2, c3, ……….….., cn}*
Step 6: *Let F be the set of processing function. F = {Ffit, Fecc}*
Step 7: *Ffit is Fitness function defined as: Ffit = {C, DD, Entry, SD, TV}*
Step 8: *Let C be the set of cluster.*

$$\boldsymbol{C = \sum_{i=1}^{N} dist_{i,BS} + dist_{CH,BS}}$$

Step 9: *Let DD be the set of distance.*

$$\boldsymbol{DD = \sum_{i=1}^{N} dist_{i,BS}}$$

Step 10: *Let Entry be the set of Energy.*

$$\boldsymbol{Entry = \sum_{j=1}^{k} Entry_{Tx_{j,CH}} + K \times Entry_{Rx} + Entry_{Tx_{CH}}}$$

Step 11: *Let SD be the set of cluster distance with deviation.*

$$\boldsymbol{SD = \sqrt{\sum_{i=1}^{CH} (\mu - dist_{cluster-i})^2}}$$

Step 12: *Let TV be the set of trust values of nodes.*

$$\boldsymbol{TV = \sum_{i=1}^{N} TV(Node_i) \geq TV_{th}}$$

Step 13: *Fecc is an elliptic curve cryptography function defined as:*

Fecc encrypt =

$$\boldsymbol{Cm = \{xG, Pm + xPB\}}$$

Where Cm is cipher text message.
Pm is plain text or an original message.
x is random integer selected by the sender of the message, A sender.
G is a point of a,b.
PB is B's public key.

Fecc decrypt =

$$\boldsymbol{Pm + xPB - nB(xG)}$$
$$\boldsymbol{Pm + xBG - nB(xG)}$$
$$\boldsymbol{nB \text{ is } B's \text{ private key}}$$

Step 14: *Fs is the successful case defined as- Fs= Malicious nodes detected and placed out of the network. In short, network contains no malicious node. Normal nodes are differentiated from malicious nodes using fitness function and elliptic curve cryptography.*

***Step 15:** Fi is the failure case defined as- Fi = Network consists of the malicious node.*

3.3 Data Transfer

The server initiates the answer. When RR packet achieves the server, the following activities are performed in the response.

- The server processes RET for all the got RR packets.
- Among the numerous ways, the server chooses a path with higher RET.
- RP packet is produced for RR packet, which has higher RET. Server advances RP packet to neighbor address as present in course record by refreshing RIC at the server. Updates RIC with server id/anycast address, way data, RET, bounces, and recorded time stamp.
- Node accepting RP packet refreshes RIC by utilizing substance of RP packet and advances to next neighbor. Updates will happen if the current time is more prominent than the time recorded in RIC. On the off chance that the next neighbor or connection is fizzled, sends RE packet to the server and visited intermediate nodes, and stopped RP packet engendering.
- Perform stage 3 until the customer is come to without connection/node disappointments.
- If the customer isn't found because of connection breaks, send the RE packet to the server.
- Once all RP packets achieve the customer, the customer node picks a server dependent on the way with higher RET.
- For the picked server, select a way with lesser jumps, and hold different ways to the server as reinforcement. The customer will use the chosen way to the server as a source for data transmission.

Course support is required if there should arise an occurrence of connection disappointments. There are three connection disappointments; interface blow between stable intermediate nodes, connection disappointment among source and regular intermediate node, and connection disappointment among goal and stable intermediate node. We can handle the issue in the following ways.

- Suppose connection disappointment between two stable intermediate nodes should arise. In that case, the node recognizing the disappointment condition will utilize RR and RP packets to discover a steady and less clogged way between itself and the goal. The new path from the intermediate node to the destination will be educated to customer. If another method isn't discovered, the node sends an RE packet to the customer to rediscover the ways.
- Incase of connection disappointment among customers and stable intermediate node, the customer node will test reinforcement. On the off chance it is working, it will utilize support. Courses will be rediscovered if reinforcement way does not exist.
- Suppose there should arise an occurrence of connection disappointment among goal and stable intermediate node. In that case, the intermediate node will utilize RR and RP packets to find ways to reach the destination from itself and advises the customer about the method. Ifa course isn't found, the node sends RE packet to the customer to start course rediscovery. The customer develops another way in every one of the cases for further routing of packets.Through this model, we try to minimize the end-to-end delay, Low energy consumption, high and efficient Packet delivery ratio, and high data transmission speed.

4 EXPERIMENTAL RESULTS

End-to-End Delay Ratio

Table 1: Comparison table of Energy Consumption Ratio

Delay	AQRV	CDBN	Proposed model+AODV
2	443	428	221
4	478	436	260
6	521	502	252
8	576	597	265
10	621	660	278

The comparison table of Packet Delivery Ratio described the different values of existing (AQRV[2,3], CDBN[6,7,8]) and proposed AODV. While comparing the existing and proposed methods, values are higher than the existing method. The existing values start from 443 to 621 and 428 to 660. The proposed AODV values start from 221 to 278. The proposed AODV gives the best result.

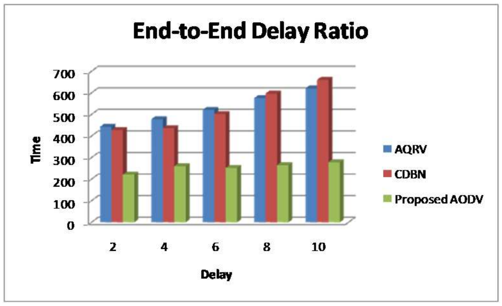

Figure 3: End-to End Delay Ratio

The figure end-to-end delay ratio describes the different values of the existing and proposed methods. While comparing the existing and proposed method values the proposed method values are lower than the existing method. Delay in x axis and time in Y axis. The existing values start from 443 to 621 and 428 to 660. The proposed AODV values start from 221 to 278. The proposed AODV gives the best result.

Energy Consumption Ratio

Table 2: comparison table of Energy Consumption Ratio

Energy	AQRV	CDBN	Proposed model+AODV
1	25.23	18.67	12.05
2	32.63	24.55	16.02
3	39.72	31.65	21.71
4	46.65	38. 79	29.33
5	61.56	47.63	35.47

The Packet Delivery Ratio's comparison table described the existing values (AQRV, CDBN) and proposed AODV. While comparing the existing and proposed methods, values are higher than the existing method. The existing values start from 25.23 to 61.56 and 18.67 to 47.63. The proposed AODV values start from 12.05 to 35.47. The proposed AODV gives the best result.

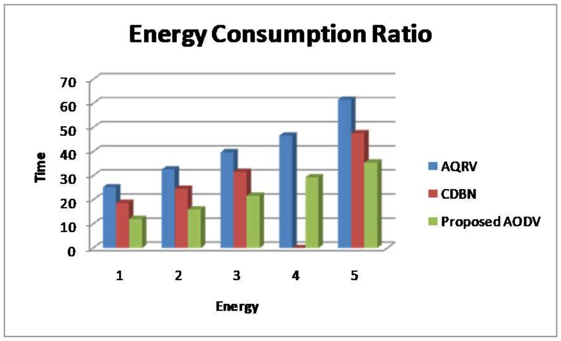

Figure 4: Energy Consumption Ratio

The figure energy consumption ratio describes the different values of the existing and proposed methods. While comparing the existing and proposed method values, the proposed method values are lower than the existing method. The energy on the x axis and time on the Y axis. The existing values start from 25.23 to 61.56 and 18.67 to 47.63. The proposed AODV values start from 12.05 to 35.47. The proposed AODV gives the best result.

Packet Delivery Ratio

Table 3:comparison table of Packet Delivery Ratio

Packet Exchange	AQR	CDBN	Proposed model+AODV
1.000	08.65	10.89	11.02
1.500	05.21	12.32	18.43
2.000	10.26	15.68	26.72
2.500	13.54	13.92	35.81
3.000	15.92	16.34	45.51
4.000	18.23	17.86	51.62

The Packet Delivery Ratio's comparison table described the existing values (AQRV, CDBN) and proposed AODV. While comparing the existing and proposed methods, values are higher than the existing method. The existing values start from 1.45 to 3.26 and from 1.98 to 3.43. The proposed AODV values start from 2.62 to 5.21. The proposed AODV gives the best result.

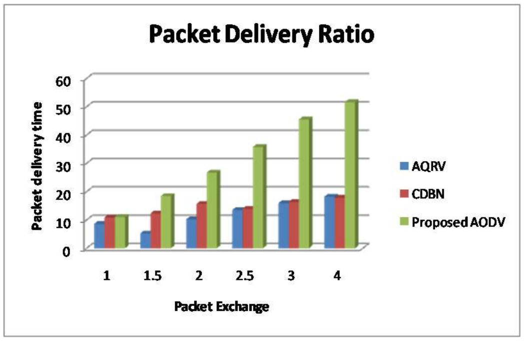

Figure 5: Packet Delivery Ratio

The figure packet delivery ratio describes the different values of existing and proposed methods. While comparing the existing and proposed method values, the proposed method values are higher than the existing method. Packet exchange on the x axis and time on the Y axis. The existing values start from 1.45 to 3.26 and from 1.98 to 3.43. The proposed AODV values start from 2.62 to 5.21. The proposed AODV gives the best result.

Average Throughput Ratio

Table 4: comparison table of Average Throughput Ratio

Throughput	AQRV	CDBN	Proposed model+AODV
2	1.45	1.98	2.62
4	1.98	1.32	3.62
6	2.26	2.65	4.31
8	2.96	3.08	4.96
10	3.26	3.43	5.21

The Average Throughput Ratio comparison table described the different values of existing (AQRV, CDBN) and proposed AODV. While comparing the existing and proposed methods, values are higher than the existing method. The existing values start from 1.45 to 3.26 and from 1.98 to 3.43. The proposed AODV values start from 2.62 to 5.21. The proposed AODV gives the best result.

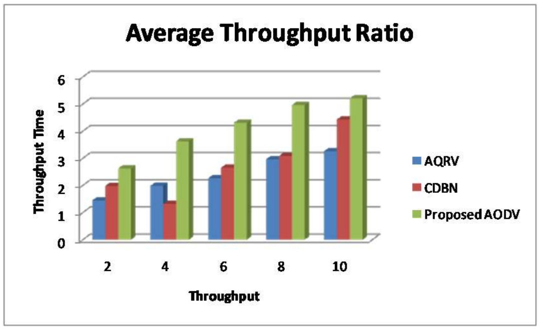

Figure 6: Comparison chart of Average Throughput Ratio

The comparison average throughput ratio describes the different values of the existing and proposed methods. While comparing the existing and proposed method values, the proposed method values are higher than the existing method. Throughput in x axis and time in Y axis. The existing values start from 1.45 to 3.26 and from 1.98 to 3.43. The proposed AODV values start from 2.62 to 5.21. The proposed AODV gives the best result.

Data Transmission Speed

Table 5 comparison table of Data Transmission Speed

Transmission Speed	AQRV	CDBN	Proposed Model+AODV
2	0.452	0.985	1.623
4	0.987	1.321	2.628
6	1.265	1.654	3.312
8	1.967	2.087	3.965
10	2.263	2.432	4.211

The data transmission ratio comparison table described the different values of existing (AQRV, CDBN) and proposed AODV. While comparing the existing and proposed methods, values are higher than the existing method. The existing values start from 0.452 to 2.263 and 0.985 to 2.432. The proposed AODV values start from 1.623 to 4.211. the proposed AODV gives the best result.

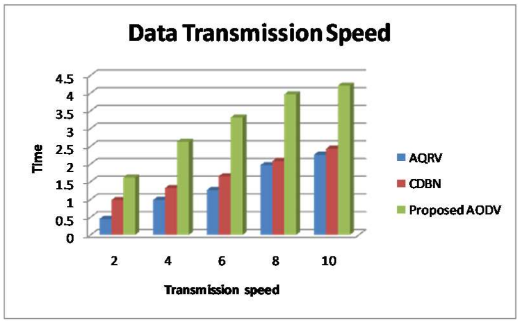

Figure 7:Comparison chart Data Transmission Speed

The figure data transmission ratio describes the different values of the existing and proposed methods. While comparing the existing and proposed method values, the proposed method values are higher than the existing method. Transmission speed on the x axis and time on Y axis. The existing values start from 0.452 to 2.263 and 0.985 to 2.432. The proposed AODV values start from 1.623 to 4.211. The proposed AODV gives the best result.

5. CONCLUSION

In this part, we have proposed AODV routing protocol with connection prediction for Adhoc systems. A prediction work that predicts connect breaks dependent on the flag quality of the three back to back got bundles and a limit flag quality has been introduced. The AODV can, along these lines, proactively start the fix process even before the occurrence of disappointment. The execution of the proposed AODV with connection prediction has been assessed and contrasted, and AODV utilizes reproductions. The recreation results demonstrate that the proposed calculation performs well and results in lower end-to-end delay and higher parcel conveyance proportion because of nearby and proactive fix forms, prompting improvement of the Quality-of-Service. AODVLP can be additionally improved by constraining the overhead of redundant control messages. The reasonableness of AODVLP for continuous traffic should be examined by testing it with smaller, measured CBR bundles at higher parcel age rates. The execution of other routing calculations can likewise be assessed by incorporating join prediction. One can again investigate better connection prediction techniques.The limitation of this model is proposed only for reactive protocol data transfer. In the future, this can be adopted for proactive and hybrid protocols.

REFERENCES

[1] M. Naresh, A. Raje, and K. Varsha, “Link prediction algorithm for efficient routing in VANETs,” in 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), 2019.

[2] D. Mumin, L.-L. Shi, and L. Liu, “An efficient algorithm for link prediction based on local information: Considering the effect of node degree,” in 2019 15th International Conference on Semantics, Knowledge and Grids (SKG), 2019.

[3] J. Shu, Q. Chen, L. Liu, and L. Xu, “A link prediction approach based on deep learning for opportunistic sensor network,” Int. J. Distrib. Sens. Netw., vol. 13, no. 4, p. 155014771770064, 2017.

[4] W.-J. Hwang, T.-M. Tai, B.-T. Pan, T.-Y. Lou, and Y.-J. Jhang, “An Intelligent QoS Algorithm for Home Networks,” IEEE Commun. Lett., vol. 23, no. 4, pp. 588–591, 2019.

[5] G. Soni and K. Chandravanshi, “A Nobel defence scheme against selfish node attack in MANET,” arXiv [cs.NI], 2013

[6] E. M. Shakshuki, N. Kang, and T. R. Sheltami, “EAACK—A secure intrusion-detection system for MANETs,” IEEE Trans. Ind. Electron., vol. 60, no. 3, pp. 1089–1098, 2013.

[7] J. Laneman, D. Tse, and G. Wornell, “Cooperative diversity in wireless networks: Efficient protocols and outage behavior,” IEEE Trans. Inf. Theory, vol. 50, no. 12, pp. 3062–3080, 2004.

[8] M. Grossglauser and D. N. C. Tse, “Mobility increases the capacity of ad hoc wireless networks,” IEEE ACM Trans. Netw., vol. 10, no. 4, pp. 477–486, 2002.

[9] E. L. Lloyd, R. Liu, M. V. Marathe, R. Ramanathan, and S. S. Ravi, “Algorithmic aspects of topology control problems for ad hoc networks,” in Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, 2002.

[10] J. E. Wieselthier, G. D. Nguyen, and A. Ephremides, “On the construction of energy-efficient broadcast and multicast trees in wireless networks,” in Proceedings IEEE INFOCOM 2000. Conference on Computer Communications. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Cat. No.00CH37064), 2002.

[11] R. Ramanathan and R. Rosales-Hain, “Topology control of multihop wireless networks using transmit power adjustment,” in Proceedings IEEE INFOCOM 2000. Conference on Computer Communications. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Cat. No.00CH37064), 2002.

[12] A. Mchergui, T. Moulahi, and S. E. Khediri, “On the comparison of broadcasting techniques in vehicular ad hoc networks,” in 2021 International Wireless Communications and Mobile Computing (IWCMC), 2021.

[13] F. Dai and J. Wu, “Performance analysis of broadcast protocols in ad hoc networks based on self-pruning,” IEEE Trans. Parallel Distrib. Syst., vol. 15, no. 11, pp. 1027–1040, 2004.

[14] J. Wu and F. Dai, “Mobility-sensitive topology control in mobile ad hoc networks,” IEEE

Trans. Parallel Distrib. Syst., vol. 17, no. 6, pp. 522–535, 2006.

[15] S. M. Mousavi, H. R. Rabiee, M. Moshref, and A. Dabirmoghaddam, “Mobility aware distributed topology control in mobile ad-hoc networks with model based adaptive mobility prediction,” in Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2007), 2007, pp. 86–86.

[16] “Games of friends: A game-theoretical approach Giovanni zappella Alexandros karatzoglou,” studylib.net, 23-May-2016. [Online]. Available: https://studylib.net/doc/13896851/games-of-friends--a-game-theoretical-approach-giovanni-za... [Accessed: 16-Jan-2023].

[17] G. T. Chavan and V. Srikanth, “Zone based effective location aided routing protocol for MANET,” in Mobile Communication and Power Engineering, Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 404–407.

[18] K. Balaji and P. Sai Kiran, “Efficient resource allocation algorithm with optimal throughput in cloud computing,” Journal of Advanced Research in Dynamical and Control Systems, vol. 9, pp. 1902–1910, 2017.

[19] Z. Huang, X. Li, and H. Chen, “Link prediction approach to collaborative filtering,” in Proceedings of the 5th ACM/IEEE-CS joint conference on Digital libraries, 2005.

[20] P. Venkateswara rao and D. Mohammed Ali Hussain, “A Novel Filtered Based Grid partitioning multiple reducers skyline computation using Hadoop framework,” Int. J. Eng. Technol., vol. 7, no. 2.7, p. 686, 2018.

[21] P. Bogdanov and A. Singh, “Accurate and scalable nearest neighbors in large networks based on effective importance,” in Proceedings of the 22nd ACM international conference on Conference on information & knowledge management - CIKM ’13, 2013.