ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1945

Packet Drop Attack Prevention in DRL Based Data Rate Adaptation Scheme for MANET

Karishma M[1] (PG Scholar)
Department of CSE, Akshaya College of Engineering and Technology, Kinathukadavu, Coimbatore, Tamilnadu, India

Ashath Thauth S[2] (Professor)
Department of Science CS Academy, Kovaipudur, Coimbatore, TamilNadu, India

Abstract:- The Mobile Adhoc Networks (MANETs) are infrastructure-less and self-organised network made up of mobile nodes. Congestion control is a challenging task in MANET because of its node mobility of node, huge data transfer traffic, and actively changing nature of the network. Heavy congestion may result in huge packet loss, more delays, and expenditure of network resources due to repeated transmissions. In this work, we propose an intra-network data rate adaptation scheme to avoid packet loss which analyses the length of the queues in forwarding nodes and number of source nodes to adapt data transfer rate for transfer of data packets. The proposed scheme allows MANET nodes to select the correct transmission rates based on the traffic demands and supports dynamic transmission rate adjustments between neighbouring nodes. This paper also examines dropping attacks by malicious nodes in the network layer and to protect against such attacks, a mechanism for detection is introduced using the MANET's node supportive participation. Since the transmission overheads are only used in the exchange of transmission signals among the neighboring nodes, the proposed model may be used by MANETs even with a large number of nodes. Simulation results of this scalable model, shows noteworthy improvement in PDR and network delay and packet loss due to queue overflow and network congestion.

Keywords:- *MANETs; Congestion Control; Deep Reinforced Learning (DRL); Date Rate Adaptation; Packet Drop Attack.*

I. INTRODUCTION

Among wireless network technologies, MANET has become an hopeful research area. MANETs are self-configuring wireless network made up of collection of wireless devices. In MANETs the nodes can communicate with other nodes directly within the communication ranges without a fixed infra. In MANETs, nodes can dynamically join and leave the network anytime which does not results in a fixed network topology. Due to dynamic network topology, reliable data delivery becomes a challenging task in MANETs and during data transfer, any intermediate node may suffer from problems such as low bandwidth, high congestion and energy consumption due to limited resources. These conditions may lead to packet loss or limited usage of transmission channel rate.

In the recent decade, numerous models have been introduced to avoid loss of data packets such as finding alternate route with limited congestions[1-4], back pressure based routing, congestion-adaptive routing[5], multiple agent based routing[6] and congestion control based on data rate[7]. In all these earlier schemes congestion control is handled by finding an alternate path. Finding an alternate route increases the runtime calculation overhead in these schemes. Meanwhile, these techniques may add to the overall delay of data transfer which can significantly reduce the network performance. Therefore, it is important to have an efficient congestion control method for MANETs with dynamic topology. An efficient congestion control mechanisms should be able to make the best use of network resources and reduce delays, and thereby avoid packet loss.

Data rate adaptation schemes are more popular in recent years, used to increase bandwidth availability and network resources in a reliable way. In order to avoid wrong selection of transmission rate based on back pressure algorithm, a real time rate adapter mechanism that can adapt to network conditions is required. In this paper, we introduce a DRL based rate adaptation scheme to avoid such wrong selection of transmission rate through the most optimal and reliable path that ensures to meet its bandwidth requirements.

The proposed model avoids congestion by early detection of network conditions and adapts the data transfer rate. In this model, if packet loss is detected at forwarding node due to congestion, the data packets are buffered and congestion effect is slowly shifted towards the source nodes. An adaptation factor is calculated using the realtime network conditions, based on which the source node adapts the data transfer rate.

Due to absence of a fixed trust worthy link for data transfer, the MANETs are vulnerable and there are different attacks possible on MANET. In a black hole attack, the attacker node becomes a part of the routing path and then intercepts the data packets. Such data packets instead of being forwarded along the network are getting dropped by the attackers.

There has been lot of research on finding optimal path in MANETs for data transfer [21-23] and early recognition and avoidance of such a dropping attack in MANETs [24-26]. Most of these schemes have either low detection rate or highly complex detection algorithms. There are quite a many

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1945

security vulnerabilities and chance of high false positive rates in existing schemes as explained in Section II. A malicious packet dropping attack detection mechanism in MANETs has been also presented in our work. This model involves a protocol which is collaborative as well as distributive that utilizes the complementary relationship between number of packets sent to a neigbouring node and number of packets forwarded by it for detection of malicious packet dropping attack which is explained in Section II.

The rest of the paper is organized as follows. Section II presents related work. Section III describes our proposed technique. Performance evaluation is discussed in Section IV and finally conclusion and future work is presented in Section V.

II. RELATED WORK

Several approaches and mechanisms have been followed recently that can handle congestion in data transfer in the decentralized networks like MANETs. Congestion avoidance can be either path based or date transfer rate based. In this article, we introduce a DRL based rate adaptation scheme and discuss the existing data rate adaption schemes which led to our model in following session.

A senor based technique to control congestion in wireless networks was discussed by Yaghmaee MH et al[4]. Their model generates the average data transfer rate from the calculated rate of sending packets and compares the transfer rate between all two nodes through the path from source to destination. This method increases the network performance by reducing the transfer rate in reference to average rate if the queue of a certain node is full in order to minimise the congestion. Camp J et al[8], in their work evaluated the status of data transfer and delivery on the basis of received ACK packets and formulated the Auto-rate fallback(ARF) technique. This scheme adapted the data transfer rate by increasing the rate based on consecutive successful transmissions or decreasing the rate based successive failures. But this method does not account for the reason of failure.

Explicit congestion notification (ECN) technique proposed by Manikandan et al.[9] uses a load factor which is calculated for all links by a router. The load factor is calculated once the data packet reaches a node and congestion is predicted using the load factor and notified to the source node. Xi.Y et al[10] explained an Adaptive multi-rate auto rate feedback(AMARF) technique. In this method, success threshold is dynamically determined according to the real time network and is used to alter between different data transfer rates based available bandwidth and length of packets. In a similar technique as explained in the article [11] for every successful packet transmission data rate is increased with a parameter and is continued until buffer threshold is received from destination side and data rate can be decreased when packet transmission fails.

In article by S.M Allen et.al [12] the communication channel access probability is calculated by each node based on the number of unsuccessful transmissions. Reinforcement learning(RL) is used by each node to analyze the channel access probability. In this technique, in addition to this, each node accepts a hello message at regular time interval from its neighbours which included transmission rate, and the traffic load estimate. Thereby, the necessity to update the transmission rate is decided based on the previous actions. The major drawback of this technique is updating the transmission rate unnecessarily. It also takes in account of load on each node and then the system decides whether to alter or to maintain the transmission rate unchanged. Though it is a successful approach, initiating control transfer on a congested route is an additional overhead for the network which should be addressed.

S. Thakur et al[13] in their work explained a technique to adapt data rate at sender node based on queue length analysis of intermediate nodes. In this technique, when congestion occurs, the intermediate nodes send Congestion Indication Packet (CI Packet) to source nodes. Accordingly, the sender node ultimately modifies the data transfer rate. There by this method avoids congestion and ensures a reliable communication within MANETs and overcomes the problem of queue overflow. The limitation in this model is the data rate is adapted with fixed percentage and the system does not analyze the other network conditions. Another major drawback is that the data rate is adapted at source nodes only and extra control packets are used to communicate the congestion occurrence to the source node, which increases network overhead in the existing congested network.

O. Kachirski et. al[14] in their work have published a security architecture for MANETs which involves multiple sensors that are deployed throughout the network. These sensors monitor network traffic to implement a detection algorithm based on the audit data collected and merged by them. In this technique, the detection decisions are taken by mobile agents that travel and finally return to the source host with the collected results. In this method, the authors have introduced two different methods of decision-making techniques. They are collaborative and independent decision making techniques. The authors argue that independent decision-making by mobile agents is more vulnerable during network failure and hence recommend the use of a collaborative method for decision making. Although there is a main advantage of restriction of computational intensive operations, most of the available mobile agent frameworks are less secured and can often become the targets of attacks themselves [15].

Ahmed et al. [16] presented an extensive survey on various trust and reputation-based approaches that enables security for decision-making in Ad hoc sensor networks. According to the author, the trust approach can be categorized into two. They are node centric and system centric models. In their work unresolved issues of trust and reputation management have been explained. Due to dynamic nature of MANETs and lack of a central monitoring system, intrusion detection for MANETs is considered more complex. The various issues on intrusion detection system and techniques for MANET were explained by Sen et al. [17]

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1945

in their article. Based on the study, we also discusses the various solutions to handle such issues in intrusion detection algorithms which are proposed earlier.

In our previous work, a modified DSR protocol for MANETs that uses deep reinforced learning technique for data rate adaptation within an optimal path was presented[1]. In our previous article, we introduced a data transfer rate adaptation scheme based on the run-time network conditions which can be decided at the source node upon receiving congestion notification. In this work, we address some shortcomings and extend our previous work by (i) providing the real time data rate adaptation at intermediate nodes, (ii) consider the channel under utilization and monitor the data transmission in order to reduce the packet loss and (iii) providing a fully cooperative and secure protocol for detection of packet dropping attacks.

Since the intermediate nodes are used to forward the data packets between source node and the destination, a malicious drop of the data packets can be expected while forwarding the data packets. The success of our model was to avoid such malicious packet drops. A new technique for authenticating the regular and accurate forwarding of packets by an intermediate node was introduced by Abderrahmane et al. [18] in their article. From the survey related to security in MANET, we concluded that deep learning of network conditions may also be predominantly utilized to deduct such security threat and handle different issues related to MANET.

III. PROPOSED MODEL

To handle network data acquired from the dynamic topology of MANET, we introduce a reinforced learning (RL) technique that has the ability to train the system based on acquired data and estimate reward values. RL can be a dominant model that implement machine learning based congestion control and has the ability to find the best decision and quickly react to environment changes. Fig.1 depicts the framework for DRL for the proposed system architecture. The proposed system architecture consists of four modules: (i) Route Discovery Module, (ii) Network Construction module, (iii) Path Monitor Module and (iv) Rate Adaptation Module.

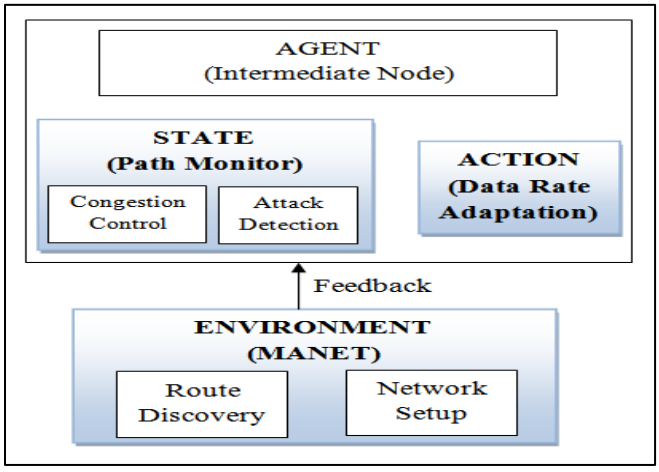

Fig 1 The DRL Framework for Proposed System

The work flow the proposed system is shown in Fig. 2. Considering an random path P_{SD} in a MANET, as shown in Fig. 3, such that the data packets are send from the source node S to the destination node D through a series of intermediate nodes $N_1, \ldots, N_K$. During data transmission an intermediate node along the selective path may forward the data packets from different source nodes. Therefore, MANETs requires an optimal path that can reduce packet drop from the communication path due to network congestion. Our system primarily establishes network of mobile nodes between source and destination identifying the optimal path with required bandwidth, energy and limited traffic in the network setup module.

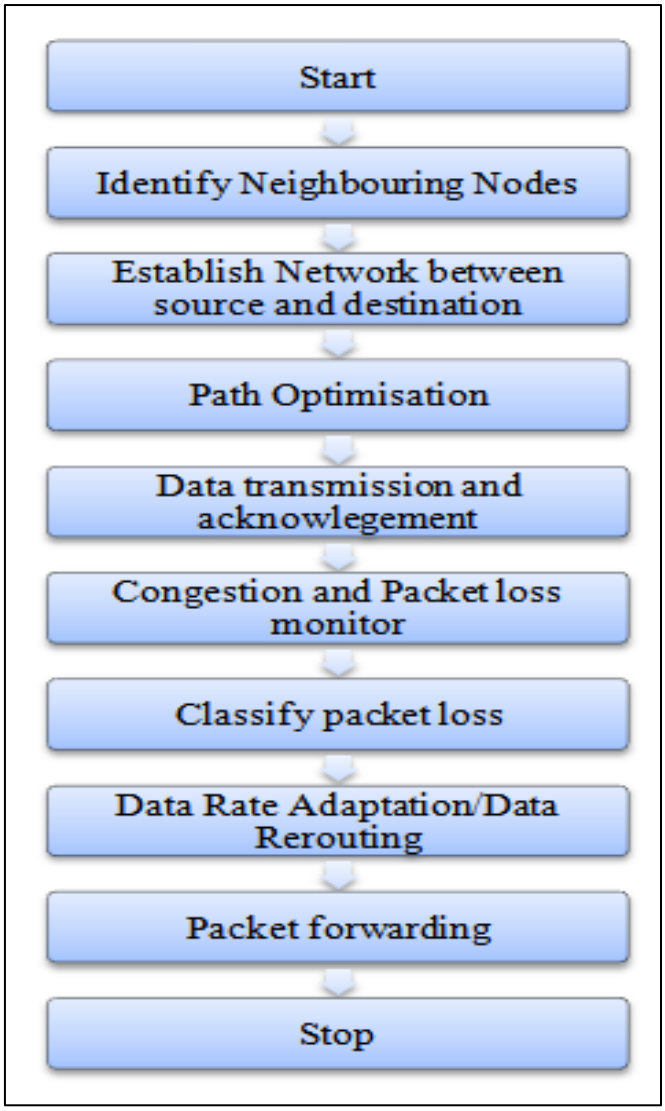

Fig 2 The Workflow of the Proposed System

The established network may compose authentic nodes, malicious nodes, and congested nodes. Authentic nodes follow the specification of routing protocol and do not drop the data packets. Malicious nodes drop the packets and do not follow routing protocol specification. Congested node may drop packets due to insufficient network resource. Based on feedback about network conditions, from the established network, the data packet transmission is initiated from source to destination.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1945

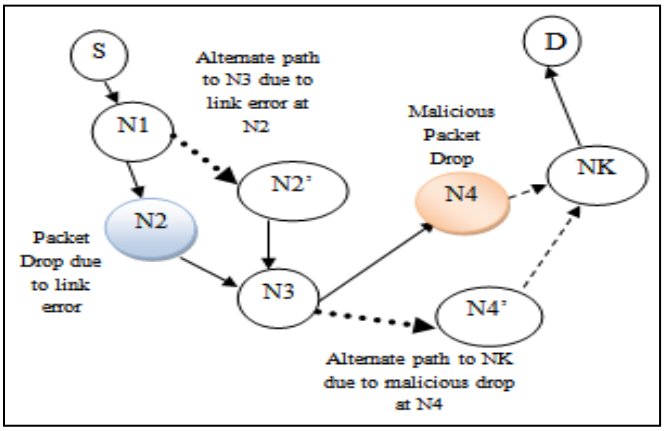

Fig 3 Model MANET Network

In the proposed scheme, an authenticated acknowledgment is used to reduce packet drops due to congested nodes and malicious nodes by the path monitor module. The path monitor module of every intermediate node verifies the authenticity of the neighbouring nodes based on its reliability index and malicious packet drops are reduced by rerouting the data packet through a more reliable node. Meanwhile if the monitor identifies an authentic neighbour it learns the status of congestion at forwarding node on the basis of queue length. The data rate is increased in case of limited utilization of queue and decreased when queue length is above maximum threshold by the rate adaptation module.

➢ *Route Discovery Module*

In this module, the main objective is to find an optimal route from source to destination meanwhile reducing the computations for route discovery. This module starts route discovery stage at source node by sending the route request packet RREQ to neighbouring nodes and reduces the computations by optimisation of cache memory. The efficiency of this cache memory optimisation is explained in our previous work[1] to find an optimal path reduce packet loss by link errors.

➢ *The Proposed Algorithm Involves the following Steps.*

Step 1: Source node S generates the RREQ packet containing Packet ID, Source ID, Destination ID, and Route Table.
Step 2: Verify the cache memory for the available path to Node D.
Step 3: If a reliable path exists in cache; send data packet to D; else, broadcast the RREQ packet to all neighbouring nodes.
Step 4: The intermediate neighbouring node N_i that receive the RREQ packet from S does the following:

- *Verify cache memory for available route to the destination. If path exists, generate RREP packet containing the route table information.*
- *If the node N_i identifies itself to be the destination node D, then generate the RREP packet.*
- *If the node N_i could not identify the required path in its cache memory, then it extends the route table and broadcast RREQ packet to its neighbour.*

Step 5: Repeat Step 4 for all N_i till it equal to the destination node D.
Step 6: Update the cache memory for all with the newly discovered route to D.

➢ *Network Setup Module*

This module starts establishing connection between source and destination nodes through neighbouring nodes and analyse the reliability of the path based on parameters traffic load, hop count, bandwidth and energy availability at each node and trains the system to find an optimal path that avoids packets loss due to link error. This module establishes connection by using Hello message and neighbour update timer. After selection of the optimal path and connection is established, the source node immediately deque the buffered packet to the next node along the path. Intermediate node receives the data packet and forward the packet until packet reaches the destination node. To handle link error due to node availability, the intermediate nodes are regularly trained to update its neighbour information and optimise all available paths to destination from them in their cache memory. Therefore during any missing node error, the rerouting of data packets are not initiated back from source nodes but identified at the intermediate node and the new path is re-established and updated in the routing table of upstream nodes.

➢ *Path Monitor Module*

The monitoring module monitors the behaviour of the neighbour nodes. Whenever a node has to sends a packet to another node, it initially stores the packet in its buffer until a timeout occurs and monitors whether the neighbour node forwards that packet or not. During this buffering time, if the neighbour node forwards the packet, then the node increments the forward counter and if the neighbour receives a packet, then the node increments the reception counters.

Based on the observed behaviour, the nodes determine the reliability index for each of its neighbours. The reliability index is the ratio of the number of the packet forwarded by the neighbour to the number of packets sent to it. Using the DRL framework of the proposed model, the decision to continue data forwarding, data rate adapting or data rerouting is done. The flow chart in Fig. 4 represents the working mechanism of the path monitor module.

Nodes in the network calculate the reliability index value for their neighbour and update them at regular intervals. The reliability status is assigned to each node based on the index value computed periodically. Based on the network conditions, the DRL framework decides a reliability threshold range for efficient data transfer. If the reliability index value falls within the threshold range then, the neighbour node is classified as AUTHENTIC and if the value is outside the threshold range then, the node is deemed to be MALICIOUS. For example if a reliable data transfer occurs within a threshold range of 30% to 80%, then nodes with reliability index is greater than 30% and less than 80% during the buffer time is considered AUTHENTIC. Nodes with less than 30% threshold are termed as MALICIOUS and no packet is sent to that node. Nodes with index value of 80%

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1945

and more are assumed to be non authentic as it would lead to false negatives, ie. the node will disturbed the data transfer efficiency even though the node is not a malicious node. By end of the buffer time monitoring of the intermediate, the neighbouring nodes along the chosen path may be label AUTHENTIC or MALICIOUS. Based on this status quo the node initiates rerouting of data packet or continue forwarding of data packets to the next neighbour.

If the next neighbour is found malicious, the packet is send to the next nearest authentic neighbour which has a predefined path to destination in its cache memory as shown in Figure 3. Since our model discovers all possible reliable paths in the route discovery stage before initiating data transfer and routing information to reach destination is stored in the cache memory of the intermediate nodes to handle link error and missing node error, the rerouting can be initiated at intermediate node level as mentioned in the above section 3A and 3B. This reduces the route rediscovery overhead by the source node and continues forwarding data packets with a little delay and without packet loss.

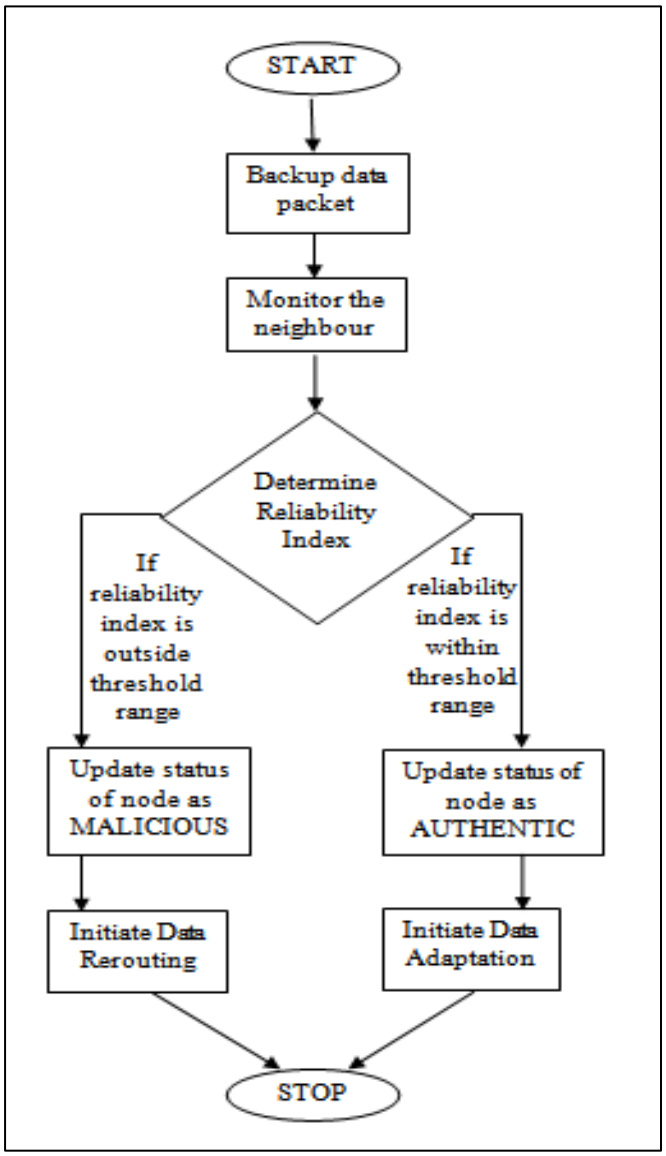

Fig 4 The Path Monitor Flow Chart

During data transmission via authenticate nodes, the path monitor module also monitors for neighbour node parameter queue length which is broadcasted across the nodes. Based on this parameter, the authentic node may initiate the data rate adaptation and continue forwarding of data packets without packet loss due to congestion.

➢ *Rate Adaptation*

In this module the source node computes an adaptation factor(f) based on the runtime network conditions. This adaptation factor will be an integral multiple by which intermediate nodes can increase or decrease the transmission rate periodically. A threshold range is also set for queue length based queue capacity of participating nodes in the network. The working algorithm of this module can be explained through following steps.

Step 1: The module takes in parameter queue length(l) from neighbouring node and parameters like maximum queue length(lmax), minimum queue length(lmin), minimum threshold queue length (qmin) maximum threshold queue length(qmax), Current transfer rate(R) and adaptation factor(f) from the MANET environment.

Step 2: If node's queue is full the transmission rate is reduced to one half of current value.

if l = lmax, then
set New rate= R / 2.

Step 3: Else if node's queue is empty the transmission rate is doubled from the current value.

if l = lmin, then
set New rate= R x 2.

Step 4: Else if the queue length is below threshold range, then transmission rate is increase by the adaptation factor.

if l > lmin and l < qmin, then
Set New Rate = R x f

Step 5: Else if the queue length is above threshold range, then transmission rate is decreased by the adaptation factor.

if l < lmax and l > qmax, then
Set New Rate = R / f

Step 6: Else if queue length lies in threshold range (between qmax and qmin) then data transmission is continued without modification.

If l < qmax and l > qmin, then
Set New rate = R

This module ensures the availability network link throughout the data transfer session and truncates any packet loss due to congestion in intermediate nodes.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1945

IV. RESULTS AND DISCUSSION

In order to analyse the performance of the system, simulations were conducted on NS-2.28 simulator. During the analysis, network performance metrics like packet delivery ratio, network overhead, delay and throughput were estimated to evaluate the performance of the proposed model.

➢ *Evaluation Metrics*

- *Packet Delivery Ratio:*

The ratio of the number of packets delivered successfully to that of the total number of packet deliveries attempted as shown in equation (1).

$$PDR = \frac{No.of\ successful\ attempts}{No.of\ delivery\ attempts} \quad (1)$$

- *End to End Delay:*

The average time taken to complete transmission of data packets from source to destination in the network as expressed in the equation (2) is termed as end to end delay.

$$Delay = \sum_{i=1}^{n} \frac{(Dest\ Time(i) - Src\ time(i))}{n} \quad (2)$$

- *Network Overhead:*

During network transmission, some redundant data are inevitably added to the signal and the data format needs to be changed, which are necessary for transmission, and the proportion of these redundant data in the data source is called overhead.

- *Throughput(TP):*

Throughput may be termed as rate of successful transmission of packets from source to destination per unit time.

$$TP = \frac{packs\ delivered \times Pack\ size \times 8}{Transmission\ Time} \quad (3)$$

➢ *Evaluation Results*

The results achieved by proposed protocol compared to the original DSR protocol, the cross layer optimization framework designed by Khan et al[27], for multicast communication in Multihop Wireless Mesh Networks(MWMN), path optimization model combines the process of both Ant Colony Optimization (ACO) and Bee Colony Optimization (BCO) given by Priya Sharma et al. [28] and the modified DSR algorithm with path optimisation[1] in terms of Packet Delivery Ratio, Throughput, End to End delay and Network overhead for different network environment with different number of nodes are shown in the figures below.

PDR evaluation results are depicted in Fig. 5. The previous protocols achieved about 86% to 95% performance with increase in the number of data packets in the network. Our model showed a noteworthy improvement in packet delivery ratio. This was because of the proposed model's ability to truncate the packet loss by link error or by malicious drop attack. During data transmission, the packet loss detection mechanism is employed which tends to repair broken links or reroute data packets in a timely manner in order to resume communication and guarantee effective data transmission.

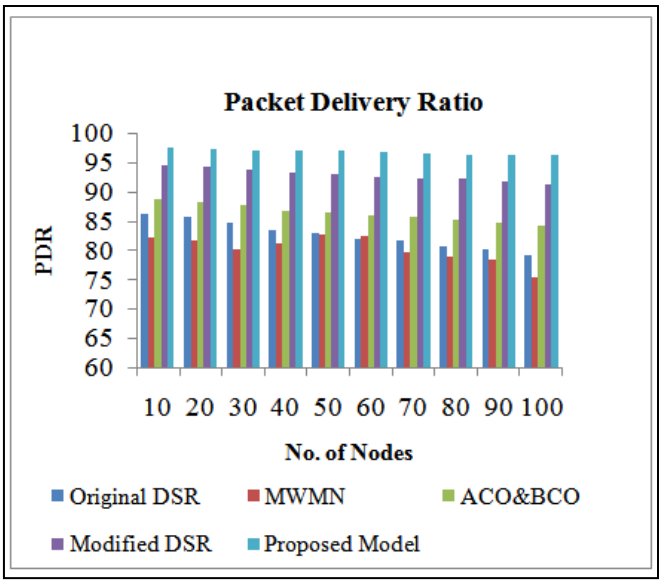

Fig 5 PDR

A major improvement in throughput estimation is pictured in Fig. 6, which depicts our model's improved efficiency over the existing systems. In Fig. 7 the comparative study of the delay performance of the traditional DSR algorithm and our modified version scheme is illustrated. It can be observed from the graph that there is periodic increase in delay with increase in number of nodes. The increase in delay may be due to runtime computation that authenticates nodes before data transfer. Though a small delay is observed the system ensures secure transmission and prevents malicious packet drop attacks.

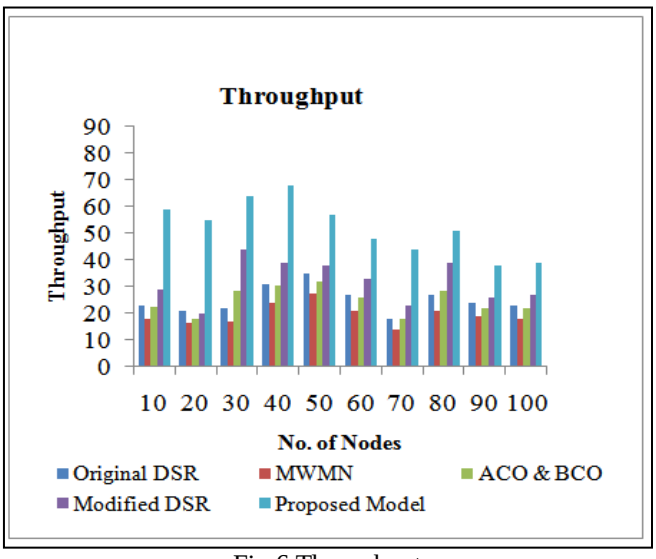

Fig 6 Throughput

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1945

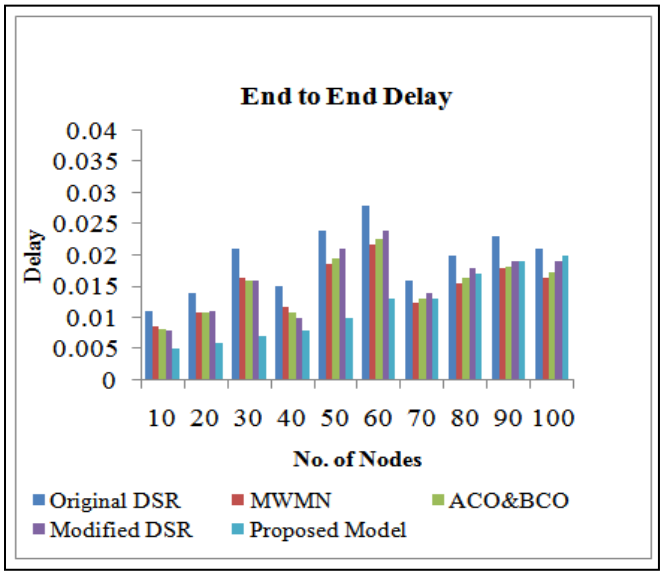

Fig 7 End to End Delay

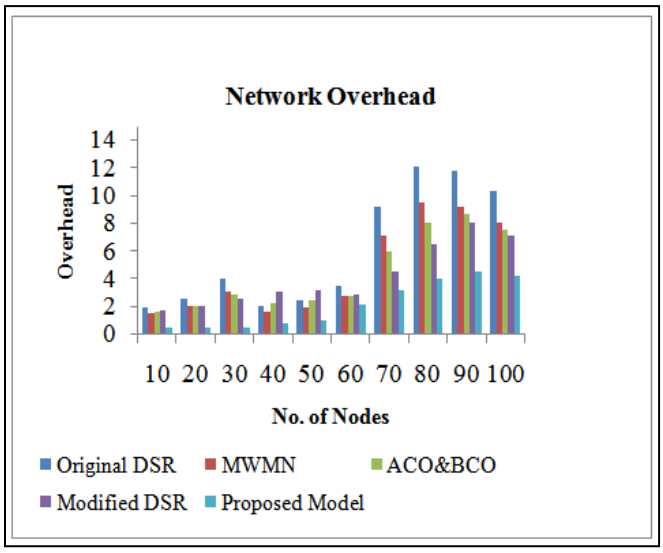

Fig 8 Network Overhead

Comparing the evaluation result and the observations made, we can conclude that the throughput in proposed scheme is greater than the existing format. Whenever there is an increase in the number of participant nodes, the overall network overhead may increase in wireless communication networks. The network overhead can be in check with efficient use of all available network resources to get the job well done. The network overhead of the proposed model with the existing techniques is compared in Fig 8 and the evaluation results shows that the proposed version has greater improvement in handling network overhead than the existing models. The network can experience a greater topology change with increase in number of participating nodes in a MANET. The proposed method can effectively reduce the overhead of protocols even with greater nodes by reducing the wastage of network resources while transmitting the same amount of data, and improve the transmission performance of the MANETs.

V. CONCLUSION AND FUTURE WORK

From our study on the existing packet drop prevention techniques, malicious packet drop can be avoided by end to end acknowledgement which is considered one of the reliable mechanisms to prevent malicious packet drops. Due to the constrained resources like buffer overflow, limited energy and node unavailability, packet drops can also occur from the intermediate nodes as well. Because of such a limitation of MANET resources there might be a probability of authentic nodes being labelled as malicious ones due to their constrained resources. Also data loss by packet drops is a serious problem in wireless networks which significantly reduces the overall network performance. The previously existing acknowledgment based packet drop detection mechanisms should include an additional mechanism to detect packet drops due to constrained resources. Thus our prime objective of the work was to improve the existing end to end acknowledgement based detection system with an additional congestion detection system. In order to achieve this, the proposed algorithm is designed as a cross layer protocol for wireless MANETs. Our system recombines the routing process and channel access management. This system includes a distributed mechanism to handle simultaneous transmission which maintains established connections and controls traffic throughout the transmission time.

The proposed model is though designed based on the traditional dynamic source routing algorithm; it adapts the advantages of other routing algorithms significantly to overcome its shortcomings. This article focuses on packet drop prevention techniques not only due to presence malicious nodes along the network path, but also reduce packet drop due to constraint resources. For future research, we like to extend our work to improve the efficiency of network for different patterns of traffic and increase accuracy of the system. In further, the proposed system can be enhanced further using the deep learning algorithms and incorporate them with real time communication systems like VANETs and FANETs.

REFERENCES

[1]. Jothi Lakshmi .S and Karishma .M, “A Modified DSR Protocol Using Deep Reinforced Learning for MANETS”, *IETE Journal of Research*, June 2023, DOI: 10.1080/03772063.2023.2223168.

[2]. Kayarkar. Bhagyashree S and Deshmukh .V.S, “A survey of congestion control in proactive source routing protocol in mobile ad hoc net-works”, *Compusoft*, Vol.3, Iss.12, Dec-2014.

[3]. Z. Long, and Z. He, “Optimization and implementation of DSR route protocol based on ad hoc network”, *International Conference on Wireless Communications, Networking and Mobile Computing*, Shanghai, China, 2007, pp.1508–1511. DOI:10.1109/wicom.2007.380

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1945

[4]. Yaghmaee .Mohammah-H, Donald .Adjeroh, “Priority-based rate control for service differentiation and congestion control in wireless multimedia sensor networks”, *Computer Networks* Vol. 53, Iss. 11, pp.1798–1811, July 2009.

[5]. Senthil Kumaran .T, Sankaranarayanan .V, ”Early congestion detection and adaptive routing in manet”, *Egyptian Informatics Journal*, Volume 12, Issue 3, pp.165–175, November 2011.

[6]. L. Ying, S. Shakkottai and A. Reddy, "On Combining Shortest-Path and Back-Pressure Routing Over Multihop Wireless Networks," *IEEE INFOCOM 2009*, Rio de Janeiro, Brazil, 2009, pp. 1674-1682, doi: 10.1109/INFCOM.2009.5062086.

[7]. S. Puri and S. R. Devene, "Congestion Avoidance and Load Balancing in AODV-Multipath Using Queue Length," *2009 Second International Conference on Emerging Trends in Engineering & Technology*, Nagpur, India, 2009, pp. 1138-1142, doi: 10.1109/ICETET.2009.62.

[8]. J. Camp and E. Knightly, "Modulation Rate Adaptation in Urban and Vehicular Environments: Cross-Layer Implementation and Experimental Evaluation," *IEEE/ACM Transactions on Networking*, vol. 18, no. 6, pp. 1949-1962, Dec. 2010, doi: 10.1109/TNET.2010.2051454.

[9]. Manikandan .K, Durai .M.A.A.S, “Active queue management based congestion control protocol for wireless networks”, *International Journal of Enterprise Network Management*, Volume 6, Issue 1, pp. 30–41, Jan. 2014, DOI:10.1504/IJENM.2014.063399.

[10]. Y. Xi, B. -s. Kim, J. -b. Wei and Q. -y. Huang, "Adaptive Multirate Auto Rate Fallback Protocol for IEEE 802.11 WLANS," *MILCOM 2006 - 2006 IEEE Military Communications conference*, Washington, DC, USA, 2006, pp. 1-7, doi: 10.1109/MILCOM.2006.302449.

[11]. T. K. Mishra and S. Tripathi, "Explicit Throughput and Buffer Notification based congestion control: A cross layer approach," *2015 Eighth International Conference on Contemporary Computing (IC3)*, Noida, India, 2015, pp. 493-497, doi: 10.1109/IC3.2015.7346732.

[12]. A. Al-Saadi, R. Setchi, Y. Hicks and S. M. Allen, "Multi-rate medium access protocol based on reinforcement learning," *2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, San Diego, CA, USA, 2014, pp. 2875-2880, doi: 10.1109/SMC.2014.6974366.

[13]. Sumendra Thakur, Mansi Gupta, “Mitigating congestion using data rate control for MANET”, *International Journal of Current Engineering and Technology*, Vol.4, pp 2887-2891, August 2014.

[14]. O. Kachirski and R. Guha, “Effective intrusion detection using multiple sensors in wireless ad hoc networks”, In *Proceedings of the 36th Hawaii International Conference on System Sciences*, pp. 57-61, 2003.

[15]. M.C. Man and V.K. Wei, “A taxonomy for attacks on mobile agents”, In *Proceedings of the International Conference on Trends in Communications*, Vol. 2, pp. 385-388, 2001.

[16]. Adnan Ahmed, Kamalrulnizam Abu Baker, Muhammad Ibrahim Channa, Khalid Haseeb, Abdul Waheed Khan, “A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks”, *Frontiers of Computer Science*, Volume 9, Issue 2, pp. 280–296 April 2014.

[17]. S. Sen, J.A. Clark, “Intrusion Detection in Mobile Ad Hoc Networks”, in *Guide to Wireless Ad Hoc Networks. Computer Communications and Networks*, S. Misra, I. Woungang, S. Chandra Misra, Eds. London: Springer, 2009, pp. 427–454.

[18]. Abderrahmane Baadache, Ali Belmehdi, “Fighting against packet dropping misbe-havior in multi-hop wireless ad hoc networks”, *Journal of Network and Computer Applications*, Volume 35, Issue 3, 2012, Pages 1130-1139, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2011.12.012.

[19]. M. Mohanapriya, I. Krishnamurthi, “Modified DSR protocol for detection and removal of selective black hole attack in MANET”, *Computers & Electrical Engineering*, Volume 40, Issue 2, 2014, Pages 530-538, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2013.06.001.

[20]. J. Zhang, C. Chen, Y. Xiang, W. Zhou and Y. Xiang, "Internet Traffic Classification by Aggregating Correlated Naive Bayes Predictions," in *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 5-15, Jan. 2013, doi: 10.1109/TIFS.2012.2223675.

[21]. Tal Anker, D. Dolev and B. Hod, "Cooperative and Reliable Packet-Forwarding on Top of AODV," *2006 4th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, Boston, MA, USA, 2006, pp. 1-10, doi: 10.1109/WIOPT.2006.1666450.

[22]. E. Sivajothi, N. Vijayalakshmi, A. Swaminathan, P. Vivekanandan, “An Overview of Route Discovery Mechanisms of Multicast Routing Protocols for MANETs”, *International Journal of Engineering and Technology (IJET)*, Volume 5 No 5, pp. 3958–3966, Oct-Nov 2013.

[23]. Mahsa Seyyedtaj, Mohammad Ali Jabraeil Jamal, “Security improvements Zone Rout-ing Protocol in Mobile Ad Hoc Network”, *International Journal of Computer Applications Technology and Research*, . Volume 3 (9), pp. 536–540, September 2014.

[24]. Yatin Chauhan, Jaikaran Singh, Mukesh Tiwari, Anubhuti Khare, “Performance Eval-uation of AODV based on black hole attack in ad hoc network”, *Global Journal of researches in engineering Electrical and electronics engineering*, Volume 12, Issue 2, Version 1.0, February 2012.

[25]. P. Michiardi, R. Molva, “Preventing Denial of Service and Selfishness in Adhoc Net-works”, *in: Proceedings of Working Session on Security in Ad Hoc Networks*, 2005, pp. 223–245.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1945

[26]. S. Bansal, M. Baker, “Observation-based Cooperation Enforcement in Ad hoc Net-works”, *in: Proceedings of ACM/IEEE International Conference on Mobile Computing and Networking*, 2004, pp. 325–355.

[27]. Khan, A.N., Tariq, M.A., Asim, M., Maamar, Z. and Baker, T., “Congestion avoidance in wireless sensor network using software defined network”, *Computing*, Volume 103(1), pp.2573-2596, November 2021, DOI:10.100/s00607-021-01010-z.

[28]. Priya sharma, Kiranbir kaur, "Hybrid Artificial Bee Colony and Tabu Search Based Power Aware Scheduling for Cloud Computing", *International Journal of Intelligent Systems and Applications(IJISA)*, Volume 10, No.7, pp.39-47, 2018. DOI: 10.5815/ijisa.2018.07.04.