Congestion Free Routing in MANET based on Node Reliability Supported AODV

Bhawana Pillai
PhD Scholar
Electronic & Communication
UIT, RGPV
Bhopal, M.P.

Rakesh Singhai, PhD
Professor
Electronic & Communication
UIT, RGPV
Bhopal, M.P.

ABSTRACT

In MANET nodes communicate using Adhoc On-Demand Distance Vector routing protocol(AODV). This protocol works on demand, when node wants to communicate, it starts finding the route by flooding the control packets and increases the network congestion. It's a big challenge as the available channel bandwidth is limited. Earlier many congestion detection and avoidance technique were proposed but they were not feasible for all network situations in MANET due to its adhoc nature.

The paper suggests the solution for the problem of congestion based on node reliability mechanism, to handle any type of network based on its size (small or medium) for the controlled communication in case of congestion. The paper proposes the local route repair and node reliability methodology for route establishment process and at the same time Clear To Send / Request To Send (CTS/RTS) mechanism is used to resolve the collision while multiple nodes are competing for the channels availability. Further congestion is minimized with the help of intermediate queue aware based data rate control technique in order to improve overall network performance. The results are taken in different scenario and analyzed the performance for the network parameters routing load, normalized routing load, packet delivery ratio and network throughput.

Results demonstrated Packet Data Ratio(PDR) is near about 91 % as compared to normal AODV which is near about 84%. Also the throughput increased from 180 packets/sec to 300 packets/sec.

General Terms

Mobile Ad hoc Network, Ad Hoc On-Demand Distance Vector,Congestion control

Keywords

MANET, AODV, Local Route Establishment, Route Reliability

1. INTRODUCTION

Adhoc network is a self organizing adaptive collection of wireless terminals connected with wireless links. This is normally a decentralized network. This network is said to be an adhoc because nodes dynamically participate to forward the data. These wireless nodes are mobile and so this network is termed as Mobile Adhoc NETwork(MANET). Wireless medium has limited bandwidth, it is error prone and factors like multiple-access, signal fading, noise and interference causes significant throughput loss in MANET.Routing is an important procedure for any type of network as it initiates node communication. However in the wireless network routing protocols have to handle mobility of the nodes within the system sometimes executed using intermediate devices such as routers. But in infrastructure less network such as MANET, there is complete change of nature of routing protocol as there is no special infrastructure support of routers and nodes are randomly moving to set new network.

Node mobility, frequent change of topology and resource constraints govern special need to design the routing protocol for MANET and indeed this has been area of focus of researchers for the last few years and even optimizing today.

Reactive routing protocols appear to be more suitable for ad hoc network as they create routes as per demand and availability of nodes. These protocols must address the issues of mobility such as destination node might be out of range, wireless link does not exists between source and destination node, random movement of source, target and intermediate nodes, common shortest path for data sending of multiple nodes in adhoc network.Reactive protocols find the route on demand by flooding the network with Route Request packets. For the maintenance of route ACK messages and HELLO messages are the two methods that are used. Advantages of this type of protocol are low setup time, on demand route establishments and latest short route due to timely traversal of response packets. At the same time, disadvantages are multiple response packets in response to single request packets, heavy control packets overhead for route establishment from original source, unnecessary bandwidth consumptions and flooding leading to node and link congestion. As it is based on underlying connection oriented TCP and using reliability mechanism of TCP, it miserably fails in congestion control in case of MANET. This will further degrade the performance of MANET. In short, due to dynamic nature of MANET, designing communication protocol such as on demand routing protocol is a challenging process for these networks to control the congestion and provide guarantee of performance on the MANET.A considerable research work has been done in this area and modified reactive protocols have been developed. To further enhance the congestion control of reactive routing protocol and enhance performance of MANET, this paper proposes local route discovery and reliable route establishment at any intermediate node on the route instead of flooding control packets to original source. Further to handle the issues of congestion avoidance and resolving the congestion, some measures are taken and implements with NS2 medium size ADHOC network scenario. The performance of MANET is studied with packet drop ratio, packet delivery ratio, throughput and end-to-end delay and demonstrated betterment in existing reactive routing protocol.The root of congestion is common channel accessed by number of packets. Control this common access in same time slot, will it be done to delay the contending packets until packets in transmission complete their end-to-end session. It can be said that if node reliability is processed , up to some extent congestion may be controlled as reliable node can increase successful end-to-end transmission. Similarly improved route discovery can control number of control messages. Still congestion detection and avoidance remains unresolved

1.1 Objective

The aim of this work is to improve the congestion control for improving the performance in MANET by reducing the limitation, through the enhancement of AODV routing protocol.

To apply local route discovery procedure, identifying the intermediate node to find an alternative path instead of routing RERR to source. To identify the reliable node, direct trust computation using network performance parameter based on number of packets transmitted and received by node. One of such measure can be PDR. To regularize the process, threshold can be determined. The objective is to determine formula for threshold calculation and PDR calculation. Whenever the reliability (packet delivery ratio) becomes lower than the fixed threshold value, a local route discovery procedure has to be on track to search other available path by the predecessor of that node instead of the sender which generally search a new path only when the detected route have been destroyed due to node movement or route failure. To transmit the data packets by delaying them after certain time. To analyze and identify RTS/CTS mechanism and role of RTT to work on congestion avoidance.

The main objective is to improve congestion control to minimize end-to-end delay, buffer overflow, reduce control packets to improve PDR and to improve throughput for the better performance of the network

2. EXISTING WORK

In the paper[1], the author presents performance parameters and common congestion control metrics packet delivery ratio, throughput, end-to-end delay, hop-by-hop delay and network lifetime. After the careful study of the parameters, PDR is the most significant in congestion control that directly leads to the number of packets delivered to the node and also references cited that PDR value can be estimated as high as possible closer to 100% for better functionality of the protocols. However taking into account the inefficiencies of existing congestion control, a paper has not clearly stated the implementation of these parameters.

The authors[2] discussed a method for dynamic congestion detection and control routing (DCDR) in ad hoc networks based on the estimations of the average queue length at the node level.1. In this paper, the level of congestion is detected at any time moment and notified to its neighbor nodes as an alert message. When the neighbor's nodes got a warning message from previous nodes, it starts the new congestion free route discovery path for alternate communication. When the number of nodes increased to 30-40 or beyond 40, the performance degrades and congestion control and end-to-end delay seems to be insignificant. By using the above (DCDR) technique, E2E (End to end)delay is reduced approx by 20-28%, increased PDR approx by 28% and reduced routing overhead approx by 23% for 20-30 number of nodes. Results are compared from EDOCR, EDCSCAODV, EDAODV, and AODV.

In paper[3], author wrote a survey paper elaborating the contribution of previous literature on trust computation in MANET. The paper has pointed out a very important issue of trust computation of nodes in the case of heterogeneous, large scale networks for ensuring proper functionality. Suggested the way to quantify and compute trust value using some metrics. The classification of trust computing is provided. The proposed work is based on direct trust computation. Important issues are listed which are not yet addressed such as the impact of network dynamics and heterogeneous nodes on trust and computation of trust in a cooperative environment. The proposed work in provided solution for heterogeneous nodes and dynamic topology.

The paper[4] is the survey paper in which authors elaborating the contribution of previous literature on congestion control strategies in MANET and discussed hop-by-hop and end-to-end potential mechanisms for transfer reliability and congestion avoidance for single-copy and multi-copy forwarding. Following issues remained unresolved: interaction of routing and congestion control, which are taken care by the proposed work, and improved local measures of node importance.

The paper [5] authors presented a parameterized approach to the Ad Hoc On-Demand Distance Vector (AODV).proposed approaches in the paper: 1. Implementation of HELLO message to detect link break and failure and performance matrix is link break detection time (lb).2. The second is a link break position parameter (bp) for AODV's local route repair. The results show that the default AODV setting does not yield the best results for most defined network scenarios. Routing overhead and end-to-end delay are not considered. The route-repair mechanism is not suggested. Performance analysis is done by measuring PDR and found that in most cases PDR gain is 20% to a maximum of 38%. The authors have concluded that performance can be improved by combining link failure detection as well as route repairing mechanism.

In the paper[6], web-based time-delay In AODV routing protocol is proposed by the authors, based on the random selection algorithm. In accordance with the principles of dynamic time allocated to different paths, the network congestion, and network latency is reduced, further improved the network QoS. This method improved the existing throughput of 3-4 Mbps of AODV up to 15 Mbps and also controlled the network delay. The main disadvantage is in the beginning network setup delay is higher as time reaches peak point degrading the performance. however, after the route discovery process, it has been in control and minimized, after increasing control overhead.

In paper [7] authors stated about IEEE 802.11 MAC with the distributed coordination function (DCF): It has the packet sequence as request-to-send (RTS), clear-to-send (CTS), data and acknowledgment (ACK) and concluded with a reduction in end-to-end delay however congestion avoidance in dynamic topology was not implemented in the work.

After studying and analyzing [2], the implementation of PDR and setting its value high closer to 100% is the first step which is identified so as to find a trustworthy node in routing protocol. Secondly, the hop-by-hop delay can be considered as a second important parameter so as to reduce control overhead and so it can be modified in the existing protocol, to traverse the packet to the previous intermediate neighbor node instead of the source node.

Similarly, a number of nodes are taken in a wide range for the medium sized network in simulation software. Conventional Distributed Coordination Function mechanism can be enhanced to resolve the congestion in dynamic topology. The limitations of the existing literature are identified and incorporated in the proposed work .

3. PROPOSED WORK

The problems identified in the literature review are:
Control message overhead due to the route discovery process always initiated by source whenever congestion occurs at the intermediate node or route.

The possibility of congestion on the newly identified route on demand whenever RREQ in broadcasted to all neighboring nodes and any random node gives RREP and routing table entry is updated accordingly

A number of intermediate nodes are using the same common channel for data transmission within the same time interval using the RTS/CTS mechanism.

In order to accommodate these factors and verify the performance, the existing AODV scenario is simulated using network simulator NS2. Following modification are suggested and planned in AODV in the simulated scenario, by focusing on three issues:

if node faces the packet loss due to the congestion at node or forwarding path, then it reports to RERR to its just previous node, not the original source node, This can control RERR control message transmission to the source node. The previous neighbor node will start the route discovery by multicasting RREQ to only its neighbors. This node will send the RREQ packet to a group of node except the congested node and source node. This first step will try to reduce congestion due to flooding of RERR and RREQ. This converts the route discovery process to local route establishment [1].

To identify an alternate route to control further congestion, it is proposed to apply local route discovery by finding a reliable node for data transfer. To ensure the reliability of the node, trust computation can be done. There are direct and indirect trust computation methods [2] as summarized in the section 2. This work is based on direct trust computation based on network performance factor Packet delivery ratio(PDR)[5]. PDR is a significant contributory factor while determining the congestion status of the network. Its calculation is stated in the next section. After receiving the RREQ packet, every node will reply with the RREP packet with its Packet Data Ratio (PDR) value. Sender node receives RREP by a different neighbor and compares the received PDR values with the threshold value(this work has fixed it as 70% by averaging simulation runs). Thus a reliable node and reliable route is discovered.

To take care of collision detection and avoidance control on this reliable route, the RTS/CTS mechanism is implemented on the route. To avoid collision of packets on a common channel, upon finding the probability of congestion, the sender node will delay transmission of the next packet by three times RTT (Round trip time). This will delay the next packet until the previous packet will complete its transmission on the one-way path and acknowledgment will be received by the sender. This mechanism will control the congestion and avoid collision up to some extent.

3.1 Modules in detail

A Local Route Establishment and Trust Computation

During the communication of source and a destination node, if the links along the paths are likely to congest, if node queue length is overflowing, because of link unavailability and node congestion, data packets may be lost. In this case, after detecting the congestion, the node upstream closer to the source node invalidates the congested route to each of those destinations in its route table. It creates a route error message RERR. In this message, it lists all of the destinations that are now unreachable from the node due to congestion. This RERR message is propagated to the upstream neighbor only. This node reinitiates the RREQ, requesting alternate route discovery if the route is still needed. RREQ packet is broadcasted by the adjacent node which require to communicate to the alternate node and if it is not having routing information in the table. Every node maintains two separate variables, a node sequence number, and a broadcast id. A node may receive multiple copies of the same route broadcast packet from various congested nodes. When the adjacent node receives RREQ, it checks whether it has an unexpired route to the destination. Also if it had already received RREQ with the same broadcast id and next neighbor node, it drops the redundant RREQ and avoids redundant control messages. The destination sequence number is used to find the most recent route.

To find out non contestant route, the intermediate adjacent node broadcasts RREQ to all neighbors except the sender node which is likely to be congested. Route reply is generated by the receiver node if it is already having a valid route to the destination. The proposed protocol RREP is modified by including the PDR value of a node in addition to the information contained in RREP. After reading RREP, node unicasts it to sender intermediate node. On receiving RREP from the neighbor nodes, the sender node compares the PDR value with the set threshold of the protocol is 70%. That trust value is calculated from the total number of data forwarded out of a total number of packet receives multiply by hundred that is the packet delivery ratio of the node (PDR). The RREP containing PDR less than 70%, forward route entry for the destination node is created. It uses the node from which reliable RREP is received as the next hop toward the destination. The hop count is incremented by one. This forward route entry for the destination will be utilized if the source selects this congestion free path for transmission to the destination.

Trust value is calculated for each node during routing and is checked against the threshold value. In our case, the threshold value is 70% PDR which is calculated as the average of trust values of the nodes that take part in the routing after calculating and observing PDR at every node in simulation for 100 times. If trust value is above the threshold then the node is treated as trustworthy and reliable whereas lesser than threshold value indicates the possibility for the node to drop packets for the current transmission and will not be considered suitable for routing and an alternate path is selected for routing[10]. However, this node may be the best node for some other transmission between some other source and destination in the same network at a different time interval. To select the next reliable hop, the trust value of all neighboring nodes from the current intermediate node is calculated and finally, a node with the highest trust value than the threshold is selected as the next hop node for the current routing.

This will reduce the control messages, involvement of intermediate nodes and destination node will increase accurate transmission and efficiency.

B Collision Resolving

Mobile ad-hoc network are habitually changing their topology due to mobility of nodes, so that multiple senders can detect common shortest path and arises the problem of congestion or collision. Then the problem of collision is resolve through the request to send (RTS) and clear to send (CTS) message technique and congestion tenacity through the utilization of queue and delay measuring method. The first problem collision resolves, while multiple senders sends the route request packets through same link but that request packets receives by the intermediate nodes in some discrete delay differences than the intermediate node broadcast the CTS wining message by sender number, whose receives first come first serve bases and intimate all the remaining senders for wait next round trip time or completion of communication of first wining sender so collision are not occur on the network. Another issue of congestion is initially aware based on queue utilization of each intermediate node and while the queue demand is exceeded as compare to queue limit than the queue size increase based on demand but that enhances the network delay and delay is minimized through concede delay difference based and sender control the data rate based of delay variation.

Packets experience a variation in the RTT and retransmission timeout no longer appropriate. To avoid possible retransmission proposed protocol must detect route congestion as soon as it occurs and modify the RTT estimation to achieve quickly reliable estimate for new RTT. In practice, congestion is detected when multiple senders use the same route. New RTT estimates are heavily influenced by new RTT samples. This allows to achieve a reliable estimate of new RTT immediately after the route congestion is detected, after this parameter values are restored.

Proposed AODV protocol reduces control overhead due to transmission of RERR to adjacent nodes, multicasting of RREQ as local route establishment. Trust computation helps to choose reliable path which further reduces the possibility of packet drop due to congestion.

In order to increase fruitful utilization of common channel contended by multiple users, the packets are controlled by delaying the preceding packet till previous packet is successfully acknowledgement. On continuous non-congestion scenario rate is revised and delay is reduced. By dynamically changing the flow control, congestion due to collision of packets on common route is reduced.

4. EXPERIMENTAL RESULTS

The simulation is done by using widely used powerful network simulator NS-2 version 2.31 for Mobile Ad-hoc Networks[1]. AODV protocol is in built part of NS-2 installation**.** By using following simulation parameters, shown in Table 1, it has been modified to implement proposed modules**.**

Table 1 Simulation Parameters

Parameters	Type
Physical Medium	Wireless Physical
Propagation Modes	Two Ray Ground
Antenna Type	Omni Directional Antenna
Simulation Area	800*800 m2
Simulation Time	100 seconds
Frequency	914e+6 Mhz
MAC Layer	802.11
Routing Protocol	AODV, Enhanced AODV
Queue Type	Drop tail/ Priority Queue
Channel Sensing Mechanism	CTS/RTS
Traffic Type	CBR
Agent Type	TCP
Node Mobility	Random waypoint
MAX_SPEED NODE	30 m/s
Pause time	0 sec

4.1 Data Packet send analysis

In the simulation scenario, deploy the network with the help of network simulator -2 and use the AODV routing for route establishment. The graph shows that comparative analysis of existing methodology and proposed congestion and collision prevention methodology in different network size i.e. 10,25,50,75 and 100 nodes. From the result, we hereby conclude that, proposed time data sending is always greater than the existing methodology due to local route establishment.

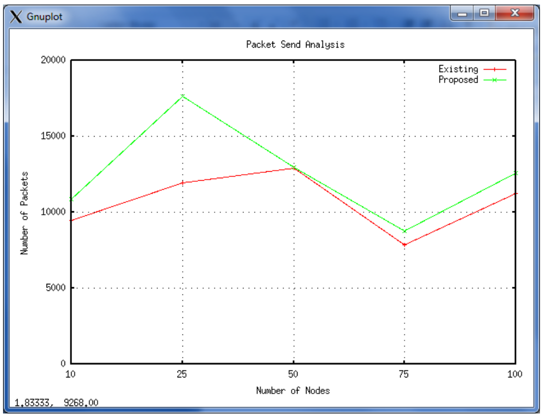

Fig. 1: Number of nodes v/s Number of packets sent

4.2 Data Packet received analysis

Mobile ad-hoc network is a communal form of mobile nodes that established the routing in on demand bases so the network performance diverge time to time and data receiving is also effected that is not dependent number of intermediate mobile nodes. The graph shows the comparative analysis of data receives by the genuine receiver at the time of existing AODV routing and proposed AODV with queuing methodology. Where the x-axis's shows number of mobile nodes and y-axis's shows the number of packets receives by the receivers, through the result conclude that proposed methodology every time receives higher data packets as compared to existing AODV routing due to local-route-repair and reliable route discovery.

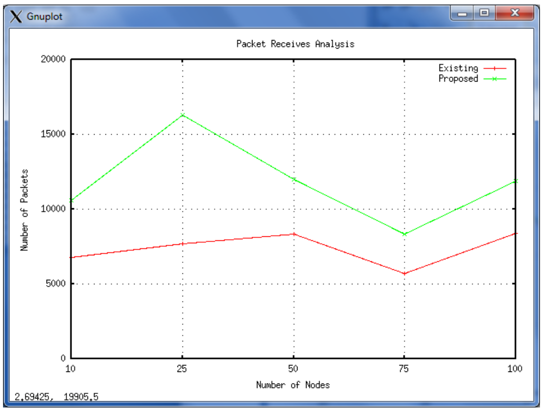

Fig. 2: Number of nodes v/s Number of packets received.

4.3 Analysis of Data Drop

Ad-hoc network are a fleeting network where routes are frequently switch, based on node mobility and channel accessibility which arises the quandary of data plummeting. During the communication data are plummet from various reasons i.e. channel not available, mac error, route error, congestion problem, collision etc. while the data plummeting is greater that means network performance is poor. In our proposed work, we aim to minimize the data plummet from the network with the help of CTS/RTS mechanism as well as rate control mechanism and simulation result are authenticated in the proposed work. This graph shows the data plummet in different scenario and evaluate with existing to proposed approach, that upshot concludes that proposed approach case data plummet is less than the existing AODV.

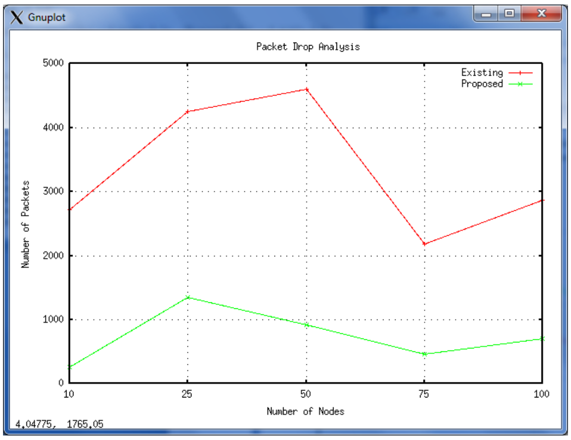

Fig. 3: Number of Nodes v/s Packets Dropped

4.4 Packet Delivery Ratio Analysis

Packet delivery ratio (PDR) is analyzed in the appearance of percentage of data receiving by the genuine receiver. While the network is reliable than PDR is higher, in this graph we compare the PDR performance in both cases at the time of 10, 25, 50, 75 and 100 nodes. The graph inference that proposed mechanism gives performance greater than the 90% and another side existing AODV gives performance lower than the 80% in every simulation case. PDR is depends on the network behavior and it's an important parameter for measuring network performance, that matrix oscillated or debased while network congestion of jam arises.

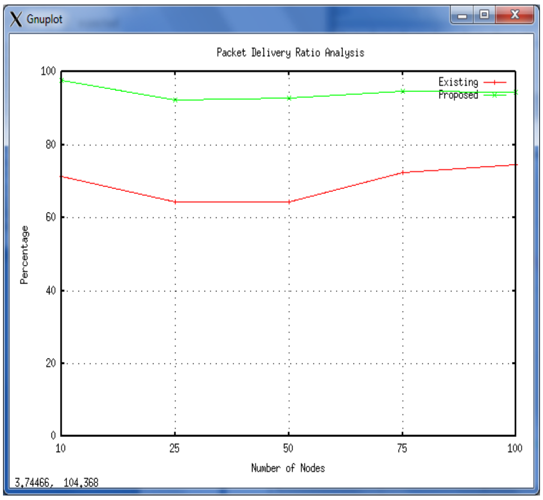

Fig. 4: Number of Nodes v/s Packet Delivery Ratio.

5. CONCLUSIONS

Mobile ad-hoc network, faces the problem of congestion for the reason that is unknown and number of senders simultaneously send the data on common channel hampering the channel utilization as well as bandwidth capability. That problem is resolved with the help of rate control and reliable local route establishment methodology. Proposed protocols addressed the limitation of existing AODV and to study the performance of modified work, finally the simulation scenario is implemented to acquire the result and from the results it is concluded that proposed approach is more reliable and more improved in terms of throughput as compared to existing AODV protocol

6. REFERENCES

[1] T.SenthilKumaran et al.," Dynamic congestion detection and control routing in ad hoc networks",Journal of King Saud, C& IS(2013,Vol.25,pp.25-34.

[2] Kannan Govindan, Member IEEE and Prasant Mohapatra, Fellow IEEE," Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey", IEEE Communications surveys &Toutorials, vol. 14, no. 2, second quarter 2012,pp.279-298

[3] Bambang Soelistijanto and Michael P. "Transfer Reliability and Congestion Control Strategies in Opportunistic Networks: A Survey", Howarth, IEEE Communications surveys & Tutorials, vol. 16, no. 1, first quarter 2014,pp.538-555.

[4] Saaidal Razalli Azzuhri , Muhammad Badri Mhd Noor , Jafferi Jamaludin , Ismail Ahmedy and Rafidah Md Noor,"Towards a Better Approach for Link Breaks Detection and Route Repairs Strategy in AODV Protocol," Hindawi,Wireless ommunications and Mobile Computing ,Volume 2018, Article ID 9029785, 9 pages, https://doi.org/10.1155/2018/9029785,pp.1-9.

[5] Zhu Qiankun, Xu Tingxue, Zhou Hongqing, angChunying, Li Tingjun, "A Mobile Ad Hoc Networks Algorithm Improved AODV Protocol", Elsevier Procedia Engineering , Vol.23(2011), pp.229-234..

[6] C.Sergiou, P. Antoniou, V. Vassiliou, "Congestion control protocols in wireless sensor networks: A survey", IEEE Commun. Surv., Tutor. Vol.16, pp. 1839-1859 (2014).

[7] Rajesh Mohan and JM Gnanaseksr, "Congestion control using AODV protocol scheme for wireless ad-hoc network",Adv. In CS & Engg., Vol.16(No.1-2),2016, pp.19 – 37(2016)