International Journal of Engineering & Technology, 7 (4) (2018) 2218-2224

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.10086
Research paper

Solution for packet reordering in manet's using cross layer based routing protocol

K. Praveen Kumar Rao [1] *, Dr. T. Senthil Murugan [2]

[1] Research Scholar, Department of Computer Science & Engineering, Vel Tech Rangarajan DrSagunthala R & D Institute of Science and Technology, Avadi, Chennai
[2] Associate Professor, Department of Computer Science & Engineering, Vel Tech Rangarajan DrSagunthala R & D Institute of Science and Technology, Avadi, Chennai
**Corresponding author E-mail:praveenkumarrao.k@gmail.com*

Abstract

TCP allows sharing the information about network status using Cross Layer mechanism for the different layers. The Cross Layer approach in wireless MANETs is provided for improving TCP performance. The Optimal Path or Route Selection is an important aspect for increasing energy efficiency and lifetime of the network. A proposal for Trust Aware Routing protocol is described for selecting an optimal route in MANETs. Direct and Indirect trust values are used for estimating the trust value of every node in the network. The route cost amount is estimated and the best path with minimum cost value is chosen for the network. The data packet is transmitted on the optimal path, and the optimal path is selected on the minimum cost value of the network. There is a possibility of the packets being dropped due to congestion and / or mobility and there are chances of the packets being reordered during the transmission process. Reorder Identification mechanism is the procedure used for dropped and / or reordered packets. The simulation results of the proposed work are compared with the existing work and it shows more effective in terms of energy efficiency and network lifetime.

Keywords:*Cross Layer approach; MANET; Reorder Identification; TCP; Trust Aware Routing Protocol.*

1. Introduction

A large number of mobile hosts falling within the communication range of the remaining set of hosts establish a wireless network in the absence of a centrally controlled infrastructure and initiate communicating with every other node, is a MANET. All the nodes in a MANET implement the routing and construct a self – organizing network. Some of the characteristics such as increase in mobility, limited processing resources, inadequate memory, and limited power storage facility are in MANETs [1–3]. A MANET has been capable of increasing the access of internet reach of the mobile hosts. The applications of MANETs include military battlefield situation, disaster aids, during emergency situations, teleconferencing, data distribution, control the logistics and automation, security, transportation management, battle fields, nature monitoring, hazardous situations, home networking, civilian uses, and so forth [4].

Ubiquitous computing or pervasive computing is the growing trend, and it is anticipated that MANET can be appear anywhere and everywhere. MANETs have many technical difficulties. The architecture of MANET is the most important difficulty being faced. The hierarchical layer of TCP / IP model is used for networking. The inflexibility of the hierarchical approach of network protocols is not possible to manage with dynamics of MANETs.
The Cross Layer approach is the better than the traditional approach. All the layers of the protocol stack run separately and the data is shared only among the adjacent layers of the protocol stack. This protocol stack approach is not suitable for MANETs, as there is an explicit dependency between the physical layer and the upper layers [5–7]. The Cross Layer approach allows the dynamic interchange of data between different protocol layers [7]. This approach design helps in interchanging the data across the various layers of the protocol stack without any intermediary. All the resources are contended at the same time by physical, MAC and routing layers, in a wireless network. The route decision and MAC affects are decided by the amount of transmission energy and data rate. Wireless channel scheduling, allocation is the responsibility of the MAC layer. The MAC layer would determine available bandwidth and the packet delay. The selection of the link is also dependent on the available bandwidth and delay, and this is the responsibility of the routing layer. Thus, routing layer selects the best route to send the transmission packets towards the destination [8], [9].

Most of the applications viz., Telnet, FTP use TCP as transport layer protocol. It delivers reliable data transmission between the nodes. Round trip time is the term used to calculate the time spent in traversing the data from host to destination and back from destination to host called ACK. Many timers are used for the functioning of the TCP. The transmission timer is one among them. This timer starts as soon as the packet is sent. The timer stops, if the acknowledgement for the packet is received before it expires. If the acknowledgement is not received before the timer expires, TCP assumes the loss of packet and retransmits it. The congestion of the network and mobility of the nodes are the reasons for packet drop and reordering. Here, a proposal for packet reordering is presented.

The idea presented in [11], fuzzy based cross layer routing mechanism used has no energy efficiency for the selection of optimal

path, and nothing is dealt with respect to packet dropping or reordering, if it occurred in the selected path.

A trust aware routing protocol based on cross layer approach is presented here. The optimal path is selected based on the direct and indirect trust values of each node with this protocol. This optimal path is used for traversing the data packets through the network. The congestion of the network and mobility of the nodes are the reasons for dropping packets and its reordering. In this event, Reorder Identifying TCP is proposed for reordering of the packets.

2. Related works

The nodes in a MANET change their positions time to time and reconfigure themselves to form a new structure. As such, there is always a chance for the typical network behavior. The reasons for this include errors in the link, overflow of the buffers, layers etc.

M. Anuradha and G. S. Anandha Mala [11] proposed cross layer based congestion detection and routing protocol using Fuzzy logic. This protocol helps in detecting the type of event occurred and act accordingly. The notion of fuzzy logic is applied for determining the alternate paths for data traversal. Applying the fuzzy inference rules, the optimal route is selected for data transmission. The energy used for this optimal path is more. Thus, the idea of applying trust aware routing protocol is proposed.

Hsung – Pin Chang et al [12] have indicated about the constraints of the layered network architecture by taking cross layer protocol design for TCP and routing algorithms in ad hoc networks. The packets lost during transmission are all due to network related events like errors, overflow, contention and any disconnections are allowed to be detected by the low layered ad hoc networks. The method proposed is energy efficient for link quality but lacks in the improvement of lifetime of the network.

TassioCarvalho et al [13] proposed a mechanism for improving the routing protocol. The best path is chosen with efficient use of energy by allowing decision metrics to all the layers in a fuzzy approach with parameters Quality of Service, Quality of Experience guarantees, mobility and energy. This mechanism has shown improvement in lifetime of the network. They have not provided any results with respect to packets being dropped or reordered.

Chao Gu and Qi Zhu [14] presented a model based on Minimum Interference Cross Layer Routing protocol called Random Way Point. The interference in the network was categorized into two types.

i) Affect only channel contention.
ii) Other affects channel contention and collision of packets.

The proposal for a mechanism was shown which included both the interferences in building a routing metric that assures a stable route and that it does not have breaks very frequently and also maintains least interference. The selected optimal route breaks in the presence of least interference. To overwhelm this issue, a trust aware routing protocol is presented in this paper.

Alireza Shams Shafigh et al [15] proposed a solution for multicast service that uses tree and mesh based multicast routing protocol. This approach used the cross layer mechanism for managing the congestion efficiently. This proposed approach lacks lifetime of the network poorly.

Mohammed Hawa et al [16] proposed a new mechanism Dynamic Packet Guidance for MANETs for the implementation of cross layer routing. It worked for highly populated networks with medium speeds and low load. It resulted in good performance when contrasted to other ad hoc protocols. This approach produced less energy consumption, small overhead and lower delay. The approach focused more on achieving energy efficiency, but less focus was given on reordering the packets.

3. Cross layer based routing protocol and a solution for packet reordering

3.1. Overview

Trust aware routing protocol is proposed for best path selection in this paper. The best path is to be selected from a number of paths available in the MANET. The optimal path is selected based on the direct and indirect trust values of each node with this protocol. This optimal path is used for traversing the data packets through the network. The best path is selected based on the minimum cost metric value. The normal functionality of TCP is enhanced by allowing the senders to identify if the sent packet has been dropped or reordered. Here, we present a new protocol Reorder Identification TCP. The reordered packets are recognized by this protocol, which the receiver received. The approach is shown in Fig. 1.

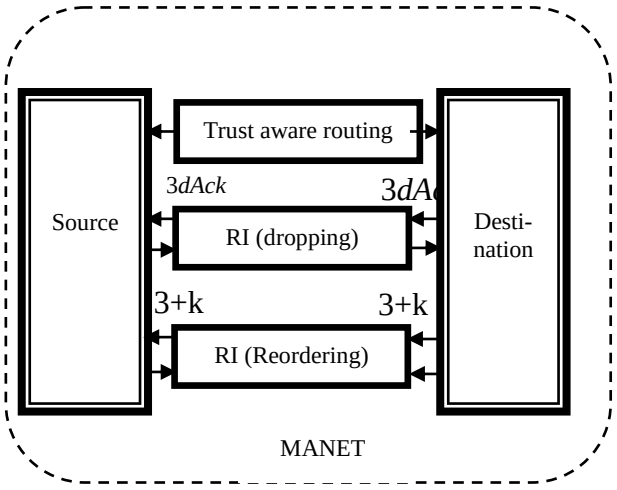

Fig. 1: Block Diagram of the Proposed Approach.

3.2 Trust aware routing protocol in Manet

The new approach for reducing the errors in transmission is presented. The trust aware routing protocol is used for cross layer. The information regarding the quality of the link present in MAC or physical layer is used. A direct trust is a relationship when there is direct connection between the nodes. An indirect trust is a relationship when a trust arises from the opinions of a trusted or a chain of trusted nodes. Every node in the network maintains the trust value for each and every other node in the network. This shows the trust level of each node with its neighbor. The local information of each node is used to calculate the trust value.

Assume, $T_{m,n}(t)$ represents the trust degree of m node with its neighbor time t. the range of the trust value is from 0 to 1. The value 0 expresses absolute distrust, and the value 1 expresses absolute trust.

Tm,n (t) is represented as the weighted average of two fractions Tm,n (t) = ω1

$$T_{m,n}(t) = \omega_1 T^{d}_{m,n}(t) + \omega_2 T^{i}_{m,n}(t) \quad (1)$$

$T^{d}_{m,n}(t)$ emphasizes the degree of direct trust between node m and node n, relying on node m 's knowledge of node n 's packet forwarding performance at time t. At time t, $T^{d}_{m,n}(t)$ is the value calculated by way of forwarding ratio of node n as

$$T^{d}_{m,n}(t) = \frac{f_{m,n}(t)}{r_{m,n}(t)} \tag{2}$$

$f_{m,n}(t)$ is the number of packets being sent in an accepted manner by node n at time t.

$r_{m,n}(t)$ is the number of packets correctly received by node n from node m at time t.

$T^{i}_{m,n}(t)$ is the degree of indirect trust that the neighbors of node m maintain in node n by considering at time t. ω_1 and ω_2 values indicate the weight factors of $T^{d}_{m,n}(t)$ and $T^{i}_{m,n}(t)$ respectively. If node n has N number of neighbors, $T^{i}_{m,n}(t)$ can be evaluated as

$$T^{i}_{m,n}(t) = \frac{1}{N}\sum_{k=1}^{N} T^{d}_{k,n}(t) \tag{3}$$

$T^{i}_{m,n}(t)$ is the way for obtaining trust degrees of the neighbor nodes at time t. The indirect trust degree value calculation is dependent on the information from its neighbors.

A node can stop sending packets through malicious nodes whenever detected. The nodes selected are the ones having high trust values for relaying the packets.

Whenever a path is selected from source to destination through intermediate nodes, the trust degree of the entire route is to be computed. Assume path p, consisting v nodes be represented with the sequence $\{1, 2, \ldots, p\}$. For the path p, trust degree of the route p is expressed by P_p

$$P_p = \prod_{m=1}^{v-2} T_{m,m+1}(t) \tag{4}$$

The path that satisfies the trust degree of a node and the required QoS, must be used in data transmission of packets. Hence, $cost_p(t)$ can be given as shown, with the new routing cost metric

$$cost_p(t) = \sum_{m \in p} l_m(t) \bullet \left(1 - T_{m,n}(t)\right) \tag{5}$$

Where, $l_m(t)$ indicates as the link delay for the path, and is described as

$$l_m(t) = DTX_m(t) \bullet \left(t_d + p_{d_m}\right) \tag{6}$$

$DTX_m(t)$ is desired transmission count which is used to link quality. This is also used to estimate regarding the retransmissions required to propagate packets. It is conducted by estimating the number of packets lost between pair of nodes adjacent to each other. This is given by

$$DTX_m(t) = \frac{1}{F_m(t) \times R_m(t)} \tag{7}$$

Where, $F_m(t)$ is the forward delivery ratio and $R_m(t)$ is the reverse delivery ratio.

Optimization is managed by the equation

$$Min\ cost_p(t) \quad m, n \in p \tag{8}$$

If the next hop chosen by node m joins the route with minimum cost value, then $cost_p(t)$ is increased for the path with the value of next hop and is chosen as the optimal path.

A route request packet having cost metric value of each node is used, when the source node transmits data to the destination node along the set of intermediate defined by $N_1, N_2, \ldots, N_n$.

$$S \xrightarrow{RREQ(cost\ metric\ of\ intermediate\ nodes)} D$$

The destination nodes send a route reply packet with cost metric for each node to the source node.

$$D \xrightarrow{RREP(cost\ metric\ of\ intermediate\ nodes)} S$$

On the receipt of the route reply from destination, the source node selects the best route having the least cost metric value. If there is a link failure or disconnection in the links, the source selects the next optimal path from the cost metrics and establishes a new route.

3.3. Solution for packet reordering to improve the performance of TCP

The transmission of packets start after the best path is selected. The transmission of packets is done from S to D, using the intermediate nodes. The data packets may be received by the destination in out-of-order due to congestion, heavy traffic, and heavy loads. The other reasons for out-of-order delivery packets are high mobility, link layer retransmissions. These are the mains causes for packet reordering.

For example, consider that the source node transmits data packets D1, D2 and D3 to the destination node. Suppose consider the data packet D1 arrives later and D3 arrives first. This process is called forward path reordering. Correspondingly ACK1 arrives after ACK2 and ACK3 at the source node. This process is termed backward path reordering as shown in Fig. 2.

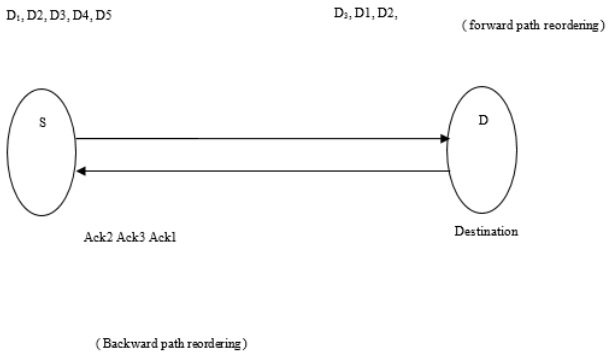

Fig. 2: Forward and Backward Path Reordering.

Reordering of data packets may cause receiver to transmit more the three successive $dubACKs$. This result in fast retransmit mechanism to trigger on the sender side, which might not be correct, as the packets might not be lost. The bandwidth is wasted because of the needless retransmission of data packets. The receiving node should receive packets in order is the task of TCP. If unnecessary data packets are transmitted, TCP at the receiver end faces the problem of buffer overflow. The receiver must be able to buffer the out-of-order packets until it receives the correct data for filling the gaps.

Mobility of the nodes and congestion of the network are the reasons for data packets being dropped or reordered, when data is sent from source to destination. It is the function of receiver to identify whether the packets received are reordered or not. Reorder Identification mechanism is proposed. Maximum and minimum sequence numbers are assigned for each data packet being transmitted to separate data packets on the basis ofit being dropped or reordered.

Each time a packet is dropped at any node during transmission, the maximum and minimum sequence number of the dropped packet is appended to the next incoming packet at the same node. These entries are checked at the receiver end.

On the receipt of three *dubACKs*, sender starts retransmitting the lost packets, assuming the packets have been dropped in the network. Otherwise, sender waits for (3 +n) *dubACKs* to be received, before retransmitting the packets, assuming the packets have been reordered in the network.

For example, let D1, D2, D3, D4 and D5 be the data packets being transmitted from S to D, via N1 and N2. Due to congestion in the network, node N1 drops the packets D2 and D3. The minimum and maximum sequence number would be D2 and D3. The maximum and minimum sequence numbers of the dropped packets are included into D4 data packet when it enters node N1. Since no gaps are found, the receiver understands that packets D2 and D3 have been dropped by the network. Subsequently, the receiver sends *dubACKs*. Sender, on the receipt of *dubACKs* from receiver retransmits the dropped packets only after 3 successive *dubACKs* This is shown in Fig. 3(a) and Fig. 3(b).

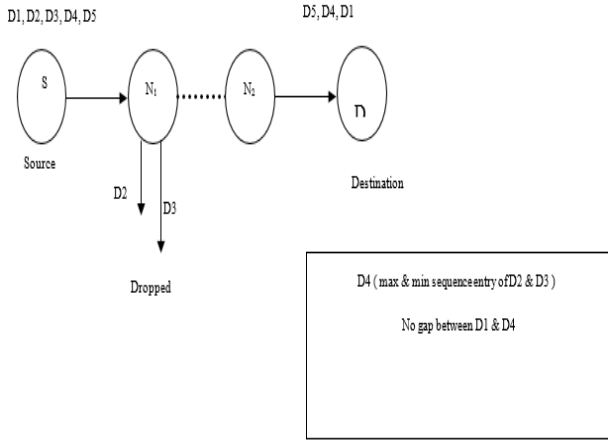

Fig. 3: A): Identifying the Dropped Packet.

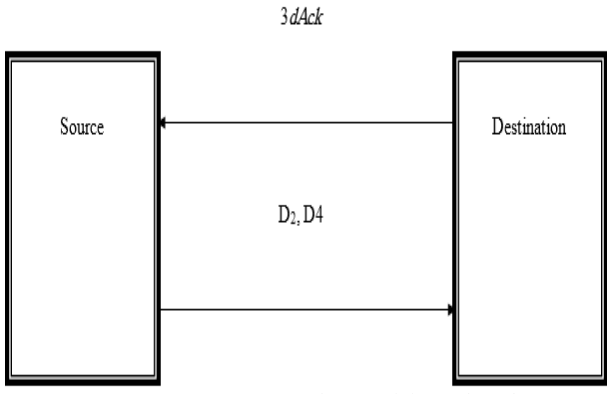

Fig. 3: B): Retransmission after Receiving '3dupack'.

Suppose packet D3 is again dropped by the intermediate node N1 and D2 has been reordered. Then, node N1 on receiving D4 will insert the maximum and minimum entries of D3 into D4. The receiver on receiving the packet D4 checks for any gaps. With this check, the receiver identifies the gap between the last received packet D1 and the maximum and minimum dropped entry in D4, concludes packet D3 has been dropped. The receiver identifies that packet D2 has been reordered. The receiver acknowledges with *dubACKs* for the reordered packet. On the receipt of acknowledgement, sender knows the status of the reordered packet. The sender on receiving (3 + K) *dubACKs*, assumes the packet to be dropped and retransmits the packet. This is shown in Fig. 4(a) and 4(b).

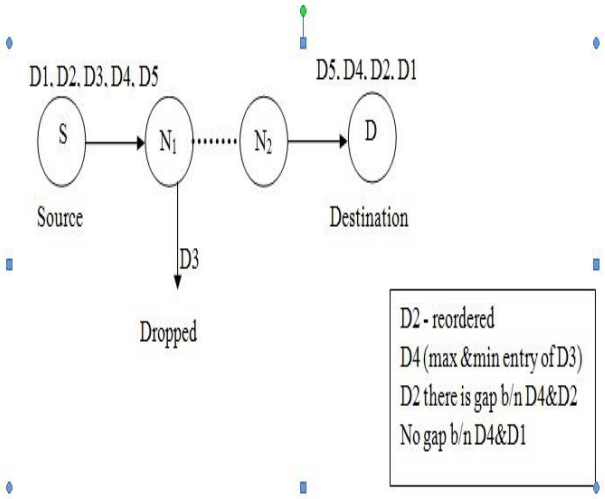

Fig. 4: A): Identifying the Reordered Packet.

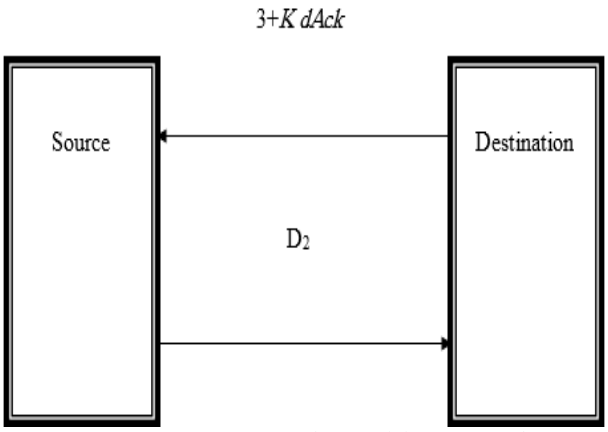

Fig. 4: B): Retransmission After Receiving '3+K Dack'.

4. Results and discussions

Network simulator is used to implement the proposed method. 100 nodes in the region 1500 × 1500 m is considered for experimentation. The transmission range considered is 250 meters. The simulation parameters are stated in Table 1. Trust aware routing protocol is chosen to evaluate the the optimal path. The transmission of packets begins, only after the selection of the best path. The packets may be dropped or reordered for many reasons during transmission. The solution for dropped packets is to retransmit the packet on the receipt of '3dAck' from the receiver. For reordering, the source retransmits the packet on the receipt of '3+dAck'. This procedure is Reordering Identification. Fig. 5(a) and Fig. 5(b) shows source node circled with colors on the receipt of acknowledgement from the receiver. Cross – Layer Based Congestion Detection and Routing Technique (CCDRT) [11]is identified to compare the simulation results with the proposed work.

Table 1: Simulation Parameters

Parameters	Value
No. of Nodes	100
Area Size	1500 X 1500
Mac	8021.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	FTP
Packet Size	512 bytes
No. of Flows	1 to 5
Initial energy	100J
Transmit power	0.66W
Receiving power	0.395W

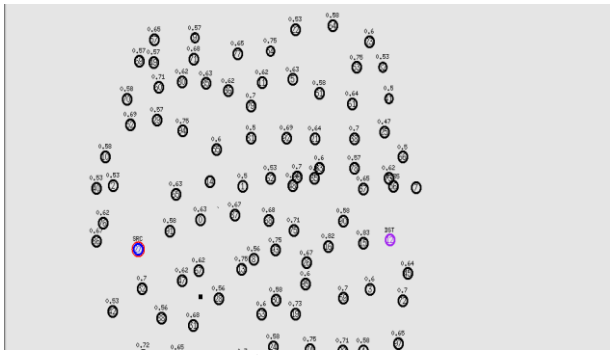

Fig. 5: A): Simulation Out of Acknowledgement Received by Source.

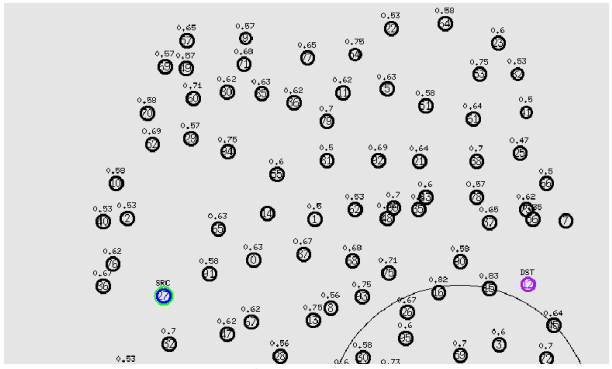

Fig. 5: B): Simulation Out of Acknowledgement Received by Source.

4.1. Performance based on flows

The performance metrics of the proposed work is calculated by varying the number flow 1–5. For each performance metric, our proposed work CRPPR is compared with the existing work CCDRT. Fig. 6 and Fig. 7 show the packet delay and energy consumption of our proposed work respectively. When the number of flows increases, packet delay of our proposed work also increases, but compared to the existing work, delay of our proposed work is reducedto 29 % as shown in Fig. 6. Although energy consumption of our proposed work is reduced to 9 % than existing work, it increases when the number of flow increases as shown in Fig. 7. Because of the Trust Aware Routing protocol, optimal path with high residual energy nodes is selected. So, there is less delay and energy consumption for data packet transmission. Fig. 8 shows the packet drop of our proposed algorithm. Compared to the packet drop of existing work, our proposed work has 32 % less drop because of the Reorder Identification which identify the packet drop and reorder packet and acknowledges the source to retransmit the data. Delivery ratio and throughput of our proposed work are shown in Fig. 9 and Fig. 10 respectively and those are increased 42 % and 98 % than that of existing work respectively. They have increased by selecting the trusted nodes for routing in the network. Life time of our network is also increased to 96 % than existing work as shown in Fig. 11.

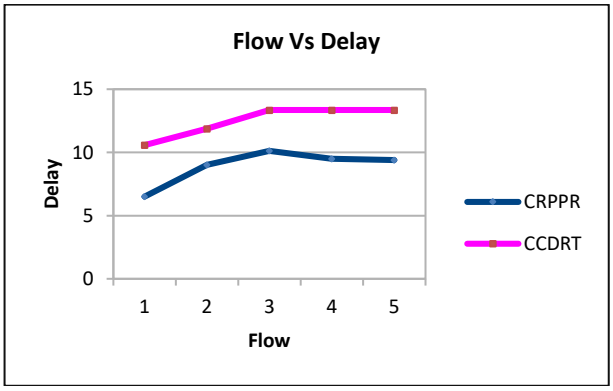

Fig. 6: Flow vs Delay.

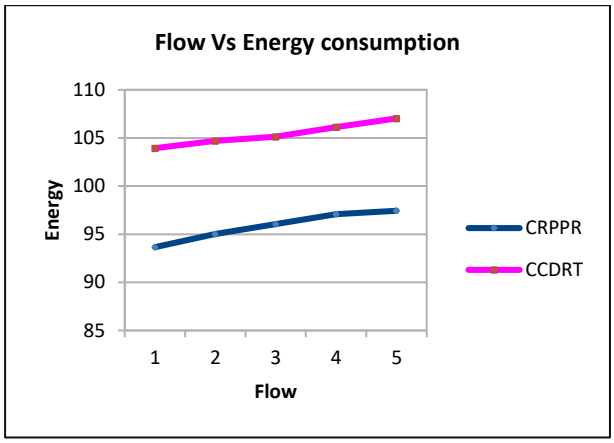

Fig. 7: Flow vs Energy Consumption.

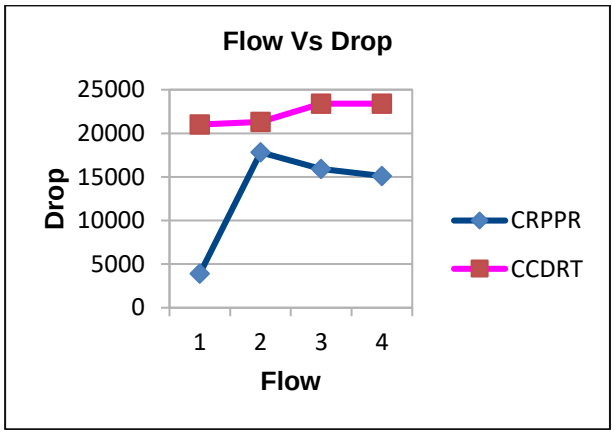

Fig. 8: Flow vs Packet Drop.

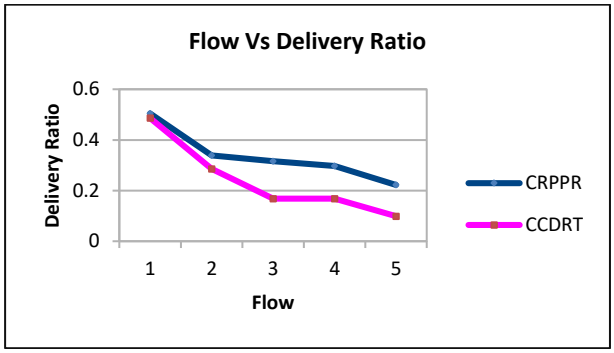

Fig. 9: Flow vs Delivery Ratio.

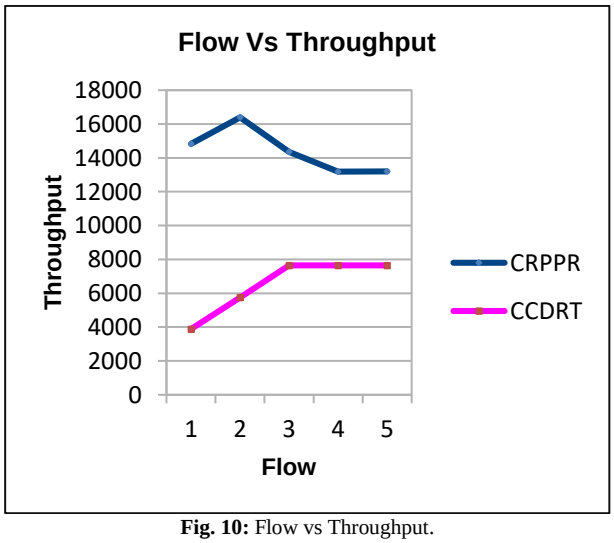

Fig. 10: Flow vs Throughput.

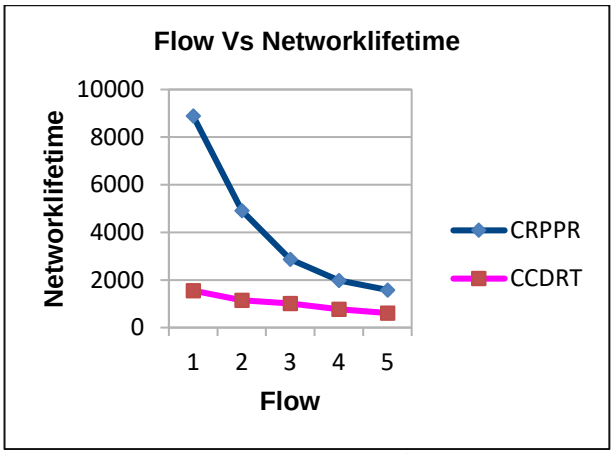

Fig. 11: Flow vs Network Lifetime.

4.2. Performance based on rate

The performance metrics of the proposed work is calculated by varying rates 100, 200, 300, 400 and 500. For each performance metric, the proposed work CRPPR is compared with the existing work CCDRT. Fig. 12 and Fig. 13 show the packet delay and energy consumption of our proposed work respectively and when compared with the existing work, delay of our proposed work is reduced to 29 % as shown in Fig. 12. Although energy consumption of our proposed work is reduced to 9 % than the existing work, it increases when the number of flow increases as shown in Fig. 13. Fig. 14 shows the packet drop of our proposed algorithm. Compared to the packet drop of existing work, our proposed work has 32 % less drop. Delivery ratio and throughput of our proposed work are shown in Fig. 15 and Fig. 16 respectively and those are increased to 42 % and 98 % than that of existing work respectively. Life time of our network is also increased by 96 % than existing work as shown in Fig. 17.

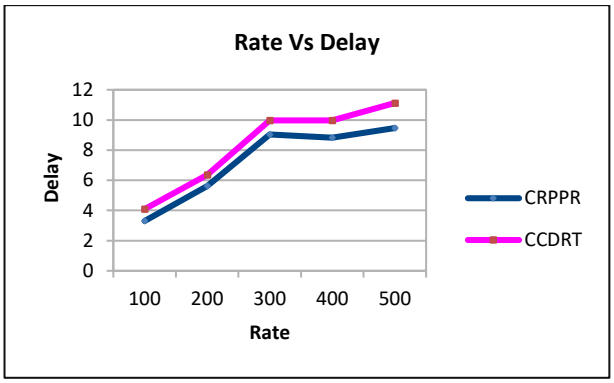

Fig. 12: Rate vs Delay.

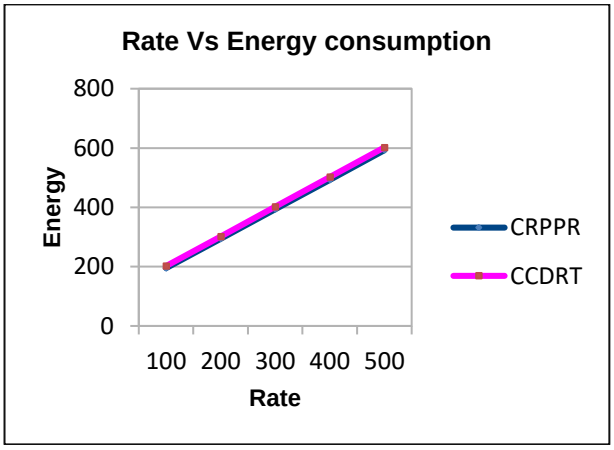

Fig. 13: Rate vs Energy Consumption.

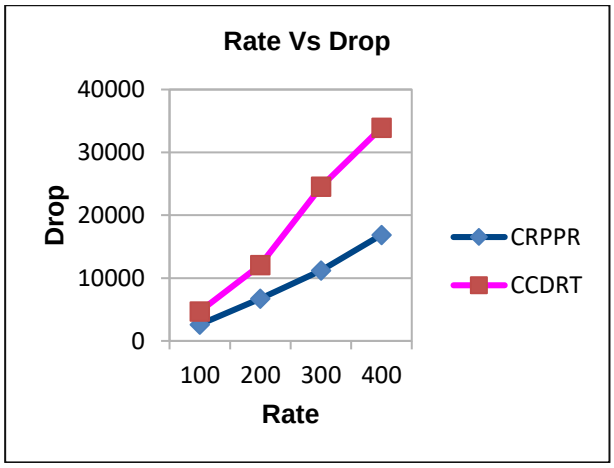

Fig. 14: Rate vs Packet Drop.

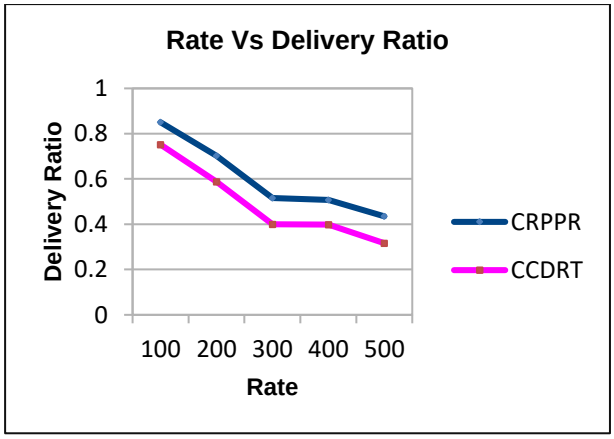

Fig. 15: Rate vs Delivery Ratio.

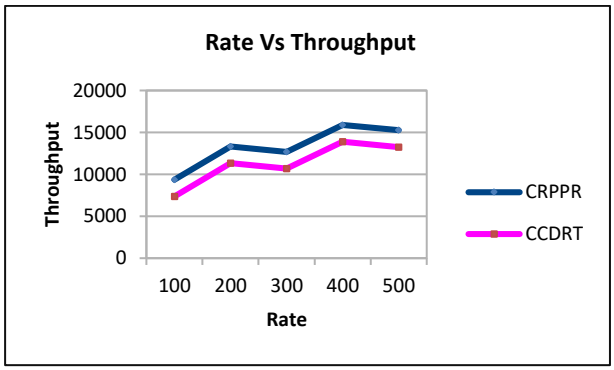

Fig. 16: Rate vs Throughput.

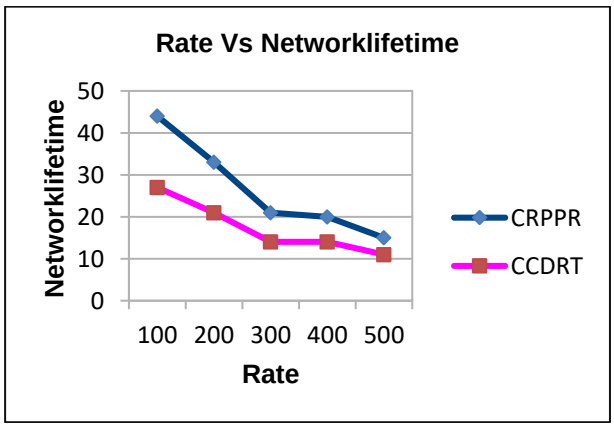

Fig. 17: Rate vs Network lifetime.

5. Conclusion

Cross Layer Based Routing Protocol for Packet Reordering is proposed for MANETs. Network simulator ns2 is used to implement the proposed work. Trust aware routing protocol is used for increasing the quality of the link. Simulation results are compared to the previous work, and throughput and network lifetime of our proposed work has been improved.

References

[1] M. Sakthivel and V. Palanisamy, "Enhancement of accuracy metrics for energy levels in MANETs", *Computers & Electrical Engineering*, Vol. 48, pp. 100 – 108, 2015.https://doi.org/10.1016/j.compeleceng.2015.04.007.

[2] S. Basurra, M. De Vos, J. Padget, Y. Ji, T. Lewis and S. Armour, "Energy efficient zone based routing protocol for MANETs", *Ad Hoc Networks*, Vol. 25, pp. 16 – 37, 2015.https://doi.org/10.1016/j.adhoc.2014.09.010.

[3] E. Daly and M. Haahr, "The challenges of disconnected delay-tolerant MANETs", *Ad Hoc Networks*, Vol. 8, No. 2, pp. 241 – 250, 2010.https://doi.org/10.1016/j.adhoc.2009.08.003.

[4] M. Conti and S. Giordano, "Mobile ad hoc networking: milestones, challenges, and new research directions", *IEEE Communications Magazine*, Vol. 52, No. 1, pp. 85 – 96, 2014.https://doi.org/10.1109/MCOM.2014.6710069.

[5] V. Attada and S. PallamSetty, "Cross Layer Design Approach to Enhance the Quality of Service in Mobile Ad Hoc Networks", *Wireless Personal Communications*, Vol. 84, No. 1, pp. 305 – 319, 2015.https://doi.org/10.1007/s11277-015-2609-6.

[6] W. Kenny and S. Weber, "Below Cross-Layer: An Alternative Approach to Service Discovery for MANETs", *Ad Hoc Networks*, pp. 212 – 225, 2013.

[7] Y. Qin, L. Li, X. Zhong, Y. Yang and C. Gwee, "A Cross-Layer QoS Design with Energy and Traffic Balance Aware for Different Types of Traffic in MANETs", *Wireless Personal Communications*, Vol. 85, No. 3, pp. 1429 – 1449, 2015.https://doi.org/10.1007/s11277-015-2849-5.

[8] C. Gu and Q. Zhu, "A Minimum Interference Cross-Layer Routing Protocol for Mobile Ad Hoc Networks", *Wireless Personal Communications*, Vol. 72, No. 4, pp. 2741 – 2760, 2013.https://doi.org/10.1007/s11277-013-1178-9.

[9] M. Thaalbi, N. Tabbane, T. Bejaoui and A. Meddahi, "A Cross Layer Balanced Routing Protocol for Differentiated Traffics over Mobile Ad Hoc Networks", *Internet of Things, Smart Spaces, and Next Generation Networking*, pp. 407 – 419, 2013.

[10] D. Kampitaki and A. Economides, "Simulation Study of MANET Routing Protocols Under FTP Traffic", *Procedia Technology*, Vol. 17, pp. 231 – 238, 2014.https://doi.org/10.1016/j.protcy.2014.10.233.

[11] M. Anuradha and G. Anandha Mala, "Cross-layer based congestion detection and routing protocol using fuzzy logic for MANET", *Wireless Networks*, 2016.

[12] H. Chang, H. Kan and M. Ho, "Adaptive TCP congestion control and routing schemes using cross-layer information for mobile ad hoc networks", *Computer Communications*, Vol. 35, No. 4, pp. 454 – 474, 2012.https://doi.org/10.1016/j.comcom.2011.11.008.

[13] T. Carvalho, J. JailtonJúnior and R. Francês, "A new cross-layer routing with energy awareness in hybrid mobile ad hoc networks: A fuzzy-based mechanism", *Simulation Modelling Practice and Theory*, Vol. 63, pp. 1 – 22, 2016.https://doi.org/10.1016/j.simpat.2016.02.003.

[14] C. Gu and Q. Zhu, "A Minimum Interference Cross-Layer Routing Protocol for Mobile Ad Hoc Networks", *Wireless Personal Communications*, Vol. 72, No. 4, pp. 2741 – 2760, 2013.https://doi.org/10.1007/s11277-013-1178-9.

[15] A. Shafigh, B. Veiga and S. Glisic, "Cross layer scheme for quality of service aware multicast routing in mobile ad hoc networks", *Wireless Networks*, 2016.

[16] M. Hawa, S. Taifour, M. Qasem and W. Tuffaha, "A dynamic cross-layer routing protocol for Mobile Ad hoc Networks", *AEU - International Journal of Electronics and Communications*, Vol. 66, No. 12, pp. 996 – 1005, 2012. https://doi.org/10.1016/j.aeue.2012.05.002.