Reliable Positioning-Based Routing Using Enhance Dream Protocol In Manet

Leena Jadhav, Dr. Jitendra Sheetlani, Harsh Pratap Singh

Abstract: The nodes in MANET continuously moves in a limited area with random mobility speed. MANET forming dynamic topology and nodes are only aware of the nearby nodes if they are in radio range. If the node/s is out of range then it is not possible to communicate with that node in the network. The dynamic topology formation is also possible in decentralized MANET. The routing protocols of MANET are not same as traditional wireless routing protocols. One major issue on this network is security. The routing protocols are sending information to destination from particular source and the routing strategy is provides the better way of delivery in the network. The DREAM protocol is improving the performance of multipath routing by sustaining the location information of mobile nodes. The DREAM protocol reduces the overhead of routing packets flooding in MANET by that reduces the delay in the network also the performance is better than the existing AODV-Line, AODV-Selfwd, DYMO-Line, DYMO-Selfwd. The proposed Reliable DREAM performance is better than normal AODV routing. The DREAM is to sustain the location information with the mobility speed of nodes. The expected possibility of node movement is calculated and also the flooding of routing packets is minimized. The flooding of packets is towards at expected location of the destination. The number of nodes position continuously changes and the DREAM is work on each and every node. Every node is preserving the location information of all nearby nodes in the network. The proposed Reliable DREAM protocol is improves routing performance and provides better data delivery in a dynamic network.

Index Terms: MANET, DREAM, AODV, Security, Location, Mobility, Routing.

1 INTRODUCTION

A Mobile ad hoc networks (MANETs), a class of flexible and self-autonomous wireless networks that can be rapidly deployed and reconfigured without infrastructure support or centralized management, are highly promising to provide communication support [1]. The mobile nodes can move from one location to another. The mobile nodes are formed as a network without help of central management [1, 2, 18]. The Nodes in networks make use of an equivalent random access channel, cooperating in an especially friendly manner to contributing themselves in multihop forwarding. The node in the network not solely acts as hosts however conjointly as routers that route information to/from different nodes in network. Each device in an exceedingly in MANET is liberated to move severally in any direction, and therefore modification its links to other nearby nodes normally. When a source node wishes to find the location of a destination it will query these location servers. Location services allow routing to the destination using either a conventional forwarding mechanism such as flooding or a geographic one. Where flooding is used it is usually only partial flooding, restricted to a geographic area such as that used by DREAM [3], or a strategy more specific to geographic routing such as geocasting. Greedy forwarding and face routing are two of the earliest geographic routing strategies and have together formed the basis of numerous subsequent approaches. Of the two approaches, greedy is the earliest and most basic; tracing its routes back to an approach known as Cartesian routing which was introduced for routing in large-scale internets [4]. Greedy forwarding is a conceptually simple form of geographic routing in which packets are forwarded to the neighbour located closest to the destination at each hop.

- *Leena Jadhav, Research Scholar, SSSUTMS, Sehore, E-mail: leenavishal83@gmail.com*
- *Dr. Jitendra Sheetlani, Associate Professor, SSSUTMS, Sehore, E-mail: dr.jsheetlani@gmail.com*
- *Harsh Pratap Singh, Assistant Professor, SSSUTMS, Sehore, E-mail: singhharshpratap@gmail.com*

Although MANET have the potential for use in a wide range of application scenarios as diverse as battlefield communications and smart home environments, they also have some drawbacks. In addition to the general challenges of wireless communications such as interference, path loss, and fading that are also present in infrastructure wireless networks, the unique characteristics of MANET lead to some unique challenges [5]. While a lack of centralisation can be seen as an advantage, it can also be a disadvantage as there is no means of ensuring all devices are operating using the same standards (especially if they are all under the control of different entities). Similarly, ad-hoc networks are typically more dynamic, being formed to fulfil a particular goal and terminated when that goal has been achieved. In addition, most of the nodes allow to join and leave the network at will, so that the topology is constantly changing. Depending on the application, some or even all nodes may be battery powered which presents the possibility of nodes 'dying' during operation. This means that conventional wired and wireless network protocols are not suitable for use MANET. This has led to both the adaptation of conventional routing protocols and (more commonly) the design of new ones. Generally MANET routing protocols fall into one of two categories; proactive or reactive [6, 7]. Proactive protocols store and maintain topology information through a series of regular update (hello) messages sent between network nodes. Reactive protocols do not regularly share network information and instead send out route request messages to other nodes when they need to reach a particular destination (although they will typically store routes found during this process for later use). While proactive protocols guarantee that where a network is connected every node will have a route to a particular destination in advance, they also require the storage and transmission of frequent update messages which can cause problems in the wireless medium. In this research we use the AODV[8] routing protocol with DREAM protocol. The security mechanism is reliable and also identified the malicious presence. The attackers or malicious nodes are simply distressful the initial routing performance [9,19]. If the sender is started the data sending at that instant offender is activated and drop or corrupt all valuable information [10]. a number of the malicious nodes also are flooding unwanted info in large

quantity.

2 DREAM (DISTANCE ROUTING EFFECT ALGORITHM FOR MOBILITY)

In DREAM protocol, every node maintains location info that stores position data relating to each other node that is a district of the network. it'll thus be classified as an all-for-all approach. an entry among the position info includes a node image, the direction of and distance to the node, still as a time value that indicates once this info was generated. an entry within the position information includes a node identifier, the direction of and distance to the node, still as a continuance that indicates once this info was generated. Of course, the accuracy of such an entry depends on its age. every node frequently floods packets to update the position info maintained by the opposite nodes. S forwards the packet to all one hop neighbours that are lying in the direction of destination Di. To determine the forwarding zone in the direction of Di, the source node Si calculates the region that is likely to hold Di, called the Expected Region (ERe) as shown in Fig. 1.

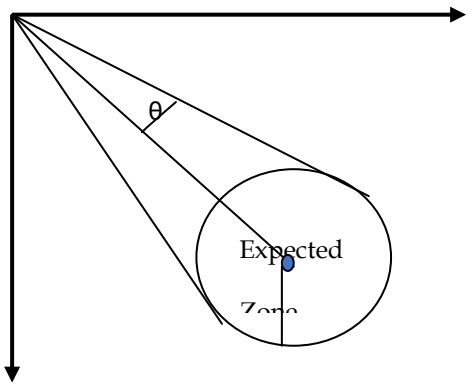

Fig.1 *Region finding with DREAM*

The radius r of this expected region is set to the value (t1 − t0)vmax, where t0 is the time stamp of the position information that S has concerning D, t1 is the current time, and vmax is the local known speed that the node Di may travel in ad hoc network. The line between Si and Di with the angle θ represents the direction towards Di. When the source node Si wishes to send a message to a destination node Di, the position table is checked to retrieve information about its geographical position. If the direction of Di is valid, the message is forwarded by Si to the all one hop neighbors in the forwarding zone using that direction. If case no one hop neighbor is found in the required direction i.e. no location information is available for Di, then a recovery procedure is started by flooding partly or totally the network in order to reach Di. When any node receives the data packet and it itself a destination Di, an acknowledgement is replies back to the source node regarding message receiving otherwise all other nodes except Di replicate the same method by sending it to all one hop neighbors that are in the direction of Di. This method is replicated by each of these nodes, until destination Di is reached [9].

3 LITERATURE SURVEY

The previous work that has been done in this field is explained in this section. Here the current research is observed to find the new routing scheme in location-based routing. In this paper [11] is to assess the impact of the error associated with the position of the nodes in LB routing protocols for MANETs. Specifically, DYMOselfwd and AODV-Line has been used for the performance evaluation, as they both have been proposed to reduce the routing overhead in AODV/DYMO routing protocols. The aim of this work is to assess the impact of the position accuracy on the performance of location-based routing protocols that have been recently proposed. The goal of DYMOselfwd is to reduce the overhead of the legacy DYMO protocol, extending hence the network lifetime and optimizing the bandwidth usage.

Research Drawbacks:-

Sudhir K et al. [12], Reinforcement Learning (RL) based solutions are proposed for routing in dynamically changing node location scenarios. It is shown that RL based solutions provide better outcome in comparison to the static algorithms. Static algorithms fail to adapt the changing situations while the RL based solutions are able to adapt to these changes and minimize the average packet delivery time. The RL based algorithm works according to the rewards and penalties it gets from the performed steps. A rewarded step is kept in memory for future actions. However, exploration is done for new cases and accordingly the learning algorithm is updated. Least busy paths are normally chosen as the first step of the proceeding. Gradually from learning outcomes, the least busy paths may be avoided for optimal performances. Sultanuddin S. et al. [13] proposed a secure routing protocol STMR(Secure Token Multipath Routing). STMR is a hybrid approach of clustering and path selection algorithm. In STRM clustering is performed using triangle optimization algorithm with balanced set. Based on the performance metrics the highest trust degree node is selected as cluster head (CH). Finally the multi favor decision making algorithm selects the optimal path. Waheb A et al. [14] proposed a protocol assigning rank to nodes based on multi criteria node rank metric(MCNR). The metrices for assigning the rank to the nodes are nodes lifetime, idle time of node, node speed, enduring battery and queue length. These multiple parameters are aggregated by MCNR into comprehensive metric. For multiple route computation these metrics are utilized by MCNR using a function new link quality assessment. This function is also used for of multipoint relay (MPR) clustering of nodes for topological information flooding based on QoS and Energy aware MPR selection mechanism. It reduces the complexity of multiple constrained considerations and avoids the control overhead due to separately broadcasting multiple parameters. Sudhir K et al. [15] proposed a strong secure mysterious location based routing (S2MLBR) protocol for MANET using optimal partitioning and trust inference model. In S2MLBR protocol, first partitions a network into sectors using optimal tug of war partition (OTW) algorithm. Then, compute the trustiness of every mobile node using the constraints received signal strength (RSS), mobility, path loss and cooperation rate. RSS is cost-effective metric used to estimates the distance between the mobile nodes for localization objectives. RSS is the most widely used benchmark because it is easy to measure and is directly related to the provision excellence.

4 PROBLEM STATEMENT

The discovery and recovery procedures are time and resource

overwhelming. Once the trail breaks, data packets can get lost or be delayed for a protracted time till the reconstruction of the route, inflicting transmission interruption. Pre-determination of an end-to-end route are made before knowledge transmission also no guarantee the info can send to destination. Without knowing location needs longer and energy to discovery and recovery the route to send data. Mobile Ad Hoc network are maintained dynamic topology with random mobility by that we can't identify the location of nodes. Multipath protocols have definitely sort the problem of single path by providing alternative route in between sender and receiver. It means, if the existing route is break than in that case the alternative route is available but it is not providing the location of mobile nodes. AODV has more message overheads during route discovery due to increased flooding and since it is a multipath routing protocol, the destination replies to the multiple RREQs those results are in longer overhead. The overhead enhancement are increases the delivery of routing packets in network by that the data delivery are affected and end to end delay in the is also increases.

5 PROPOSED APPROACH

In future we identified that the behavior of attackers behind initiation either packet dropping or routing misbehavior is to achieve a certain goal such as attack (i.e. making certain resources or services, such as applications, web access, printing, or routing, unavailable to the intended users). By controlling the early depletion of the battery, adjust the energy to decide the proper energy level of a node and integrate the low power strategies into the protocols used in various layers of protocol stack. In addition, other goals of attackers might include partitioning the network, creating routing loops, or generating multiple identities discovering valuable information, or theft of resources. It's assumed that the attacker joins the network with its single identity, and that malicious nodes do not collide with one another. It also assume that nodes do not increase or decrease their transmit power because power consumption issue of attack is in different categoryThe multipath concept is to flooded RREQ (Route REQuest) packets in network and waits for the RREQ (Route REPly packets) from the nearby nodes and these packets are also flooded by number of intermediate nodes till the packets are not reaching to destination. If the nodes that are for able to forward packets or other nearby nodes then generate RERR (Route ERRor) message to sender. The reasons of route error are of many not limited in network. The location of mobile nodes in MANET is not found by normal or traditional routing protocol. In dynamic network the link establishment is more difficult as compare to other protocols like wireless network and sensor network. Send Connection Confirmation with extra field of (Nodes Speed and Algorithm: Secure and Reliable hybrid AODV-Dream Routing in MANET

Input:
£ = Network Field 1000*1000
K_n = Mobile node
T_x: Transmitter node ∈ K_n
R_x: Receiver node ∈ K_n
I_l: intermediate node ∈ K_n
M_P = AODV; //Routing protocol
l_k: location of k node
d_k: direction of k node
δ_k: Speed of k node
ψ= 550 m^2 radio range
r_s: receiving signal strength
Dream: Location aware protocol
S_p: suspicious node ∈ I_l
P_i: activity watcher and protector node

Output: Data send, receives, packet delivery ratio, position error, throughput, delay

Procedure:

K_n is in £
T_x, R_x ∈ K_n generate route for communication
T_x Request M_P for route execution
Generate (T_x, R_x, M_p)
While I_l is ψ && I_l != R_x do
I_n ← route-table(T_x, R_x, M_p)
I_l← Store (r_{s_i}, use Dream) // r_{s_i}: signal strength of i^{th} respect of T_x
Forward (T_x, R_x, M_p)
I_l← I_l + 1
End do
If I_l is ψ && I_l == R_x && path > 1 then
If $path_i(r_{s\_i})$ > $path_j(r_{s\_j})$ then
Select $path_i(r_{s\_i})$
R_x create reverse path
T_x send(data, R_x)
Else
Select $path_j(r_{s\_j})$
R_x create reverse path
T_x send(data, R)
Else if I_l is ψ && I_l == R_x && path ==1 then
Select $path_j(r_{s\_j})$
R_x create reverse path
T_x send(data, R_x)
Else
R_x not found or R_x not reachable
End if
// If Suspicious node in network
P_i is in £
P_i watch neighbour node
If path active from T_x to R_x then
Watch all I_l by P_i
If I_l receive data & I_l != R_x & I_l not forward to i_{l+1} | data != tcp || udp | M_p header then
P_i set i_l as S_p
P_i send control message to S_p
If S_p work as normal then
S_p further in path
Else if S_p work as abnormal then
S_p block by P_i
Else
Send periodically S_p information to T_x
End if
Else
Activity is normal
P_i generate log file all active neighbour I_l
End if
Else
Path not active for data communication
End if

The attacker presence is loss the data packets. The presence of attacker is conform after identified its abnormal behavior. Distance of nodes estimate is only possible if the nodes are in

radio-range and also the communiqué procedure is possible. Due to the absence of position service in dynamic network, required an proficient method to estimate the distance or direction up to the destination. Thus, the combination of multihop features of AODV and DREAM position based routing and propose Reliable DREAM protocol improve the route discovery mechanism in MANET.

6 SIMULATION PARAMETERS

Table 1 are represents the following simulation parameters to make the scenario of routing protocols. The detailed simulation model is based on network simulator-2 (version 2.31) [16], is used in the evaluation. The NS instructions can be used to define the topology structure of the network and the motion mode of the nodes, to configure the service source and the receiver etc.

Table 1 *Simulation Parameters for Case Study*

Network Area	*800*800*
Network Type	*MANET*
Nodes/Devices	*70*
Physical Medium	*Wireless*
Simulation Time	*100 seconds*
Protocol	*AODV, DYMO, AODV-Dream*
Traffic Type	*CBR, FTP*
Number of Connection	*20*
Propagation radio model	*Two ray ground*
Rate	*Random*

7 SIMULATION RESULTS

The performances of both the protocols are measured here on the basis of performance matrices and the performance of Transport layer protocols like User Datagram Protocol (UDP).

7.1 Average Route Overhead Analysis

In MANET sender and receiver both are the continuously change their location. Then for finding the destination the source is flooded the RREQ (Route REQuest) packets in network and also the number of nodes is receive RREQ packets is replied through RREP(Route REPly) packets. In this graph the routing performance of proposed reliable DREAM is better in network as compare to AODV-Line, AODV-Selfwd, DYMO-Line, DYMO-Selfwd protocols. The routing overhead in proposed scheme is provides better results in dynamic network. The routing packets flooding in case of AODV-Line (pos-error) is less but packet receiving is also minimum. The high overhead is not produces loss, it produces more lightweight efforts to improve packets receiving.

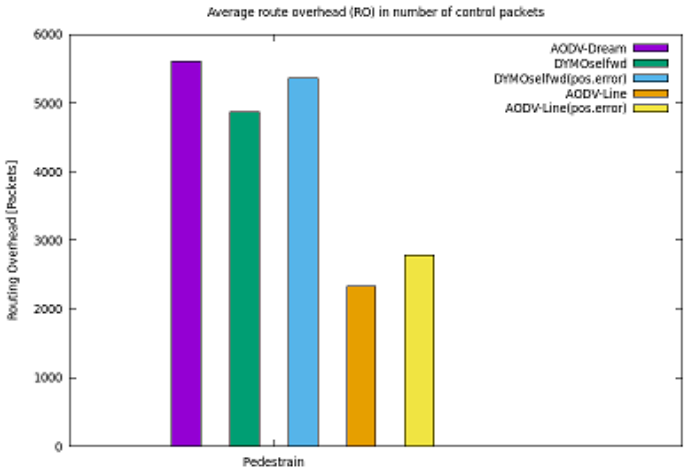

Fig.2 *Average Route Overhead Analysis*

7.2 Average Packet Delivery Ratio Analysis

The number of packets better receiving is represents the better network performance in dynamic network. If the numbers of packets lost in network then the routing performance of protocol is also degrades in network. The Packet Delivery Ratio (PDR) is measure the percentage of data packets send by sender and the packets received by receiver in dynamic network. In this graph the percentage ratio of multipath and proposed reliable DREAM is handle load more efficiently. The proposed scheme is improves the packets receiving, that's why continuously enhancement in performance up to end of simulation time. The performance of packets receiving is more as compare to AODV-Line, AODV-Selfwd, DYMO-Line, DYMO-Selfwd protocols.

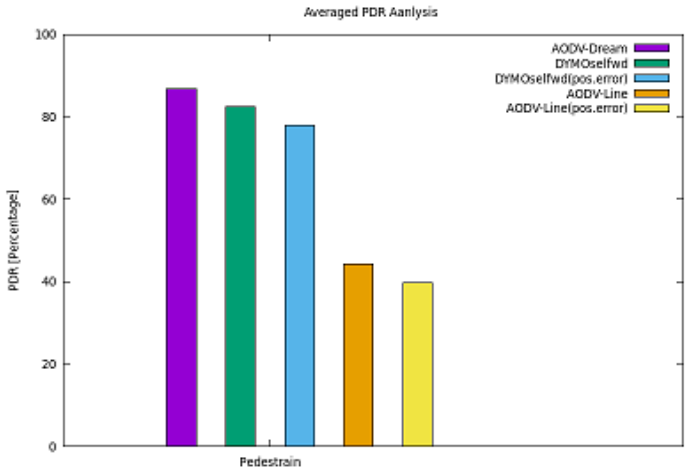

Fig.3 *Average PDR Performance Analysis*

7.3 Mean Route Discovery Delay

In dynamic network routing performance criteria is the major issue. The symmetric link possibility in the network up to destination is not sure available. The location based Reliable DREAM routing protocol is able to resolve such kind of problems to establish strong link in between sender and receiver. In this graph the delay performance of proposed Reliable DREAM and AODV-Line, AODV-Selfwd, DYMO-Line, DYMO-Selfwd protocols is measured. In this graph the

performance of proposed protocol is reduces delay because of awareness of mobile nodes location. The delay performance of proposed protocol is minimum, that shows the overhead is contain the information of mobile nodes and it is light weighted.

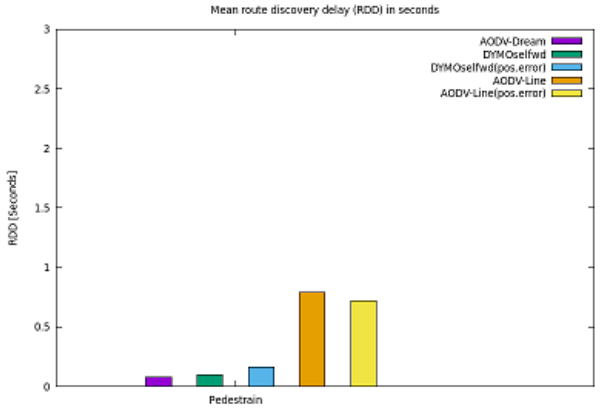

Fig.4 *Mean Route Discovery Delay Analysis*

7.4 Mean Route Life-Time Analysis

The data packets in network are passes from network layer to transport layer. In this graph the performance of Route Lifetime is measured. The performance of proposed Reliable DREAM is better because it establish the strong link in between sender and receiver. The packet loss is almost negligible due to better receiving. The AODV-Line, AODV-Selfwd, DYMO-Line, DYMO-Selfwd protocols performance are also better but they not measure the expected region of communication with destination.

7.5 Average Hops Analysis

In this graph the hop counts are examining in dynamic environment and observe that proposed Reliable DREAM is provides the better results as compare to the AODV-Line, AODV-Selfwd, DYMO-Line, DYMO-Selfwd protocols. The proposed approach aim is to reduces the overhead in presence of reactive protocol that also reduces delay. In proposed scheme the location based routing is really provides better performance to enhance packets receiving and definitely reduced packet loss.

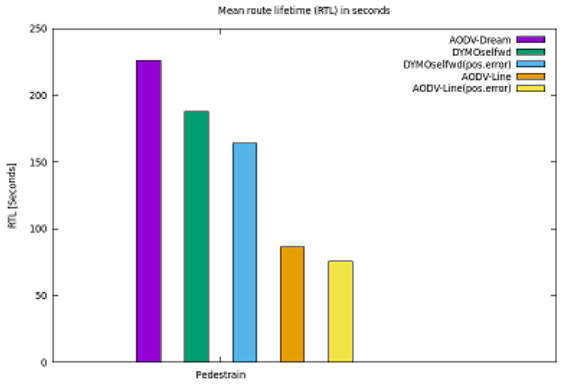

Fig.5 *Route Lifetime Analysis*

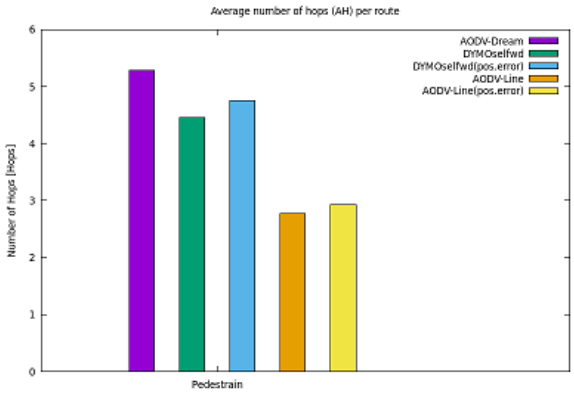

Fig.6 *Average Hop Analysis*

7.6 Mean NRL Analysis

The number of nodes are flooding route request for sending data to destination. The DEAM protocol has reduces the overhead in network by maintain the record of each node with respect to other node. In this graph the performance analysis of proposed reliable DREAM and rest of the AODV-Line, AODV-Selfwd, DYMO-Line, DYMO-Selfwd protocols is measured. The performance of DREAM is not satisfactory but the packets count in overhead is location information. The high overhead of DREAM with AODV is again receives highest number of packets.

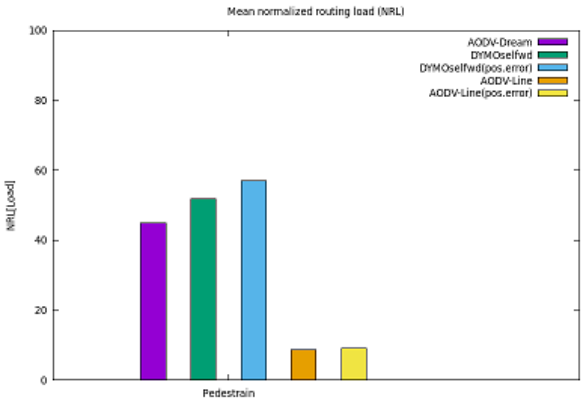

Fig.7 *Mean NRL Analysis*

7.7 Overall Performance Analysis

The overall performance of all the protocols are mentioned in table 1. The performance of The AODV-Line, AODV-Selfwd, DYMO-Line, DYMO-Selfwd protocols are not bad but Reliable DREAM with AODV is really produces the better routing approach . The overall delay is minimized and the packet receiving is more. The average number of hops count is maximum and also the link expiration time is also improved. The proposed approach is improves routing performance and also malicious actions are reduces due to better security approach.

Table 2 *Overall Analysis*

Parame-ters	*Avg Hops*	*PDR*	*NRL*	*Route Pkts*	*Delay*	*Lifetime*
AODV-Line	*2.78*	*44.26*	*8.61*	*2327*	*0.79*	*86.48*
AODV-	*2.93*	*39.83*	*9.04*	*2792*	*0.72*	*75.67*

Selfwd						
DYMO-Line	*4.46*	*82.43*	*51.91*	*4875*	*0.1*	*187.84*
DYMO-Selfwd	*4.75*	*77.95*	*57.1*	*5362*	*0.16*	*164.36*
AODV-Dream	*5.29*	*86.89*	*44.84*	*5616*	*0.08*	*226.31*

8 CONCLUSIONS

The location-based routing is really improved the routing performance and also finding the destination in minimum overhead. The use of location is also helpful for finding the malicious nodes or attacker nodes in network. If the attacker node/s is identified by security scheme then it is possible to find the attacker location in network. Then location based routing is also helpful for securing and finding attacker nodes in MANET. In this work the performance of AODV and proposed Reliable DREAM is evaluated through performance metrics PDR, Throughput and routing overhead. The multihop protocol is no doubt much better for the communication in dynamic network. The performance of proposed Reliable DREAM is compare with AODV-Line, AODV-Selfwd, DYMO-Line, DYMO-Selfwd. The proposed reliable DREAM solution enhance the throughput, reduces packet loss and reduces routing load we combines the approach of DREAM and AODV. Also apply the reliable security mechanism to reduce the loss of data in network. This approach will depends on the results analysis of normal routing and Location based energy efficient routing protocols The routing overhead and packet loss in network is minimized and data packets receiving is improves. The nodes in MANET is aware about the location of another nodes that's why the overhead in network is minimizes and also the nodes are directly send data packets instead of flooding routing packets. The throughput performance is improved, PDR is improves because the packet receiving in network is improves. The performance of routing is provides better results and reduces the unnecessary overhead in multipath routing.

9 REFERENCES

[1] Jochen Schiller. Mobile Communications. Addison-Wesley, 2000.

[2] C. Siva Ram Murthy, B. S. Manoj, "Ad Hoc Wireless Networks, Architectures and Protocols", Second Edition, Low price Edition, Pearson Education, 2007.

[3] S. Basagni, I. Chlamtac, V.R. Syrotiuk, B.A. Woodward, "A distance routing effect algorithm for mobility (DREAM)", MobiCom 98' Proceedings of the 4th annual ACM/IEEE International Conference on Mobile Computing and Networking, Pp. 76–84, October 1998.

[4] G. Finn, "Routing and addressing problems in large metropolitan-scale internetworks," 1987, technical paper.

[5] G. S. Mamatha, Dr. S. C. Sharma, "Analyzing the MANET Variations, Challenges, Capacity and Protocol Issues", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.1, August 2010.

[6] Rajesh Yadav, Dr. Srinivasa Rao, "A Survey of Various Routing Protocols in MANETs", International Journal of Computer Science and Information Technologies, Vol. 6 (5), pp. 4587-4592, 2015.

[7] Changling Liu, Jörg Kaiser, "A Survey of Mobile Ad Hoc network Routing Protocols", MANIMA, the University of Magdeburg, 21 October 2005.

[8] S. Das, C. Perkins, E. Royer, "Ad Hoc On Demand Distance Vector (AODV) Routing", IETF RFC3561, July 2003.

[9] Mohammad O. Pervaiz, Mihaela Cardei, and Jie Wu, "Routing Security in Ad Hoc Wireless Networks", Mohammad O. Pervaiz, Mihaela Cardei, and Jie Wu Springer pp.1-32, 2005.

[10] B. Sun, L. Osborne, Y. Xiao, and S. Guizani, "Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks," IEEE Wireless Communications Magazine, special issue on Security in Wireless Mobile Ad Hoc and Sensor Networks, Vol.14, No.5, pp. 56-63, October 2007.

[11] M Israel Martin Escalona, Fabio Perrone, Enrica Zola, Francisco Barcelo Arroyo "Impact of Unreliable Positioning in Location-based Routing Protocols for MANETs", pp. 1534-1539, 2017.

[12] Sudhir K. Routray, Sharmila K. P., "Routing in dynamically changing node location scenarios: A reinforcement learning approach", Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), 2017.

[13] 15 S. J. Sultanuddin, Mohammed Ali Hussain, "STMR - Secure Token Based Multipath Routing Protocol for Manets Using Hybrid Clustering and Path Selection Algorithm", International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-8, Issue-6, April 2019.

[14] Waheb A. Jabbar, Wasan Kadhim Saad, and Mahamod Ismail, "MEQSA-OLSRv2: A Multicriteria-based Hybrid Multipath Protocol for Energy-Efficient and QoS-Aware Data Routing in MANET-WSN Convergence Scenarios of IoT", Vol. 6, Pp. 76546-76572, IEEE Access 2018.

[15] Swetha M. S, Thungamani M, "A Novel Approach to Secure Mysterious Location Based Routing For MANET", ,International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-8 Issue-7 May, 2019

[16] Network Simulator-ns-2 Tutorial Available on link, http://www.isi.edu/nsnam/ns/tutorial/index.html.

[17] Harsh Pratap Singh, itendra Sheetlani,, Nagesh Salimath and K. Murali Gopal, "Design and Implementation of an Algorithm for Mitigating the Congestion in Mobile Ad Hoc Network", International Journal on Emerging Technologies 10(3): 472-479(2019) ISSN No. (Print) : 0975-8364 (pp. 472-479).

[18] Singh, H. P., & Singh, R. (2017). Exposure And Avoidance Mechanism of Black Hole and jamming attack in mobile Ad hoc Network. International Journal of Computer Science, Engineering and Information Technology, 7(1), 14-22.