Nat. Volatiles & Essent. Oils, 2021; 8(4): 15234-15247

NVEO
Natural Volatiles & Essential Oils

Trusted Optimum Path Selection Using Channel And Node Aware Routing In Manet

[1]Dr. M. Saravanan ,[2]Kamjula Lakshmi Kanth Reddy ,[3]Dr. R. Senthilnathan , [4]K. Vasanth Kumar , [5]B. Sundaramurthy , [6]Dr. G. Karthik

[1]Professor, Dept of CSE, Aurora's Technological and Research Institute, Hyderabad, Telagana,

[2]Assistant Professor, Department of Computer Science and Engineering,KKR & KSR Institute of Technology and Sciences -[KITS],Guntur, AndhraPradesh, India

[3]Associate Professor, Dept of CSE, AarupadaiVeedu Institute of Technology, Chennai, India

[4]Research Scholar, Department of computer science and engineering, Sri Satya Sai University of Technology and Medical Sciences,Sehore(MP)

[5]Associate professor, VMKV Engineering College, Salem, India

[6]Professor/CSE, VMKV Engineering College, Salem, India

Abstract

In reactive AOMDV protocol, an existing path fails as intermediate node along the path becomes unavailable due to its low energy level or when the node moves out of coverage .The packet delivery ratio is also affected by external noise interference or malicious behavior of nodes. To overcome this drawbackwe proposeTrusted Optimum Path Selection Using Channel And Node Aware Routingfor packet transmission in multiple path from source to destination. The AOMDV reactive routing protocol is used to find multiple paths from source to destination. Best path from available multiple path is selected based on the following criteria.1)The signal to noise ratio along the path are sensed and noisy channel are avoided. 2) Energy level of the nodes is analyzed and a node with sufficient energy level is alone taken.3) The malicious nodes are identified and removed based on their behavior using watchdog timer technique. 4) Node with high mobility isrejected as it makes link failure when it moves out of coverage. Thusmultiple bestpaths are selected based on channel analyzing, mobility and energy level estimation of nodes and malicious node detection and removal. Then either packets are routed along multiple best path from source to destination or delay factor is calculated among the multiple best path and optimum path with less delay factor is selected of packet transmission. This will increase throughput, packet delivery ratio, reduces delay and also provide security for data transmission.

Keywords: - Trusted Optimum Path Selection Using Channel and Node Aware Routing, AOMDV, channel analyzing, packet delivery ratio

INTRODUCTION

When AODV route discovery process uses same node again and again, its energy level is reduced due to its data transmission and the node becomes unavailable in the near future. This may lead to link failure that causes routing overhead (we initiate reroute discovery process) and reduces the packet delivery ratio.[1]

Sometimes a path may exist and its link may be affected by radio link fluctuation which causes reduction in signal strength. Hence the path becomes unstable for transmission. Since there is no centralized control in MANET, the resources such as energy level, bandwidth availability and load sharing are not effectively utilized and it reduces the network performance.[2]

AODV selects any one of the paths to reach the destination, but it won't check whether it's an optimum path to reach the destination. Only the optimum path may have stable link, node with sufficient energy level (node should not fail during transmission) and less queuing delay (data stored in the queue must be less than average queue level). Then only that data can be processed forwarded quickly. Hence it considerably increases the network performance by increasing throughput, packet delivery ratio, etc.[3]

It is found that the performance of a typical on demand routing protocol sharply decreases as the percentage of unreliable nodes increase. The objective of the researcher's work is to provide reliable path and obtain improved performance in the presence of stable nodes. This research work is mainly motivated the reliable path features are to be incorporated into the popular AODV protocol while limiting overheads.

The following situations involving unreliable nodes are to be taken care of:It reports to the neighbor nodes that the unreliable for expected to fail, the neighbor node overcomes unreliable node during the packet transmission in a reliable path.It reduces the delay and purposefully avoids the dropping of data packets in a reliable path.[4][5]

A load distribution is across the multiple paths to forward information route based on energy level and available bandwidth. Here node energy level is analyzed using consumed energy which is greater than the required energy of each path. The available bandwidth is analyzed using node capacity is lesser than number of packet transfer in each node. This handles of both energy and bandwidth are guaranteed in order increase node lifetime, reduce delay and reliability of route discovered. Uniform and non uniform load distribution across multiple paths forwarding data packets are splitting due to the heavy traffic and less delay[6][7]

The multiple paths are route discovery using AOMDV forwarding packets loop free and link disjoint nodes. To calculate the different parameter as the energy level of each node, improve secure node and channel behavior affected by signal to noise ratio using secure path is found instead of multiple paths. It increases the packet delivery and reliable data transmission. Traffic analysis, such as queuing delay is not performed hence it may result in performance degradation in the best selected path. [8][9]

Based on this analysis node residual life time and link stability is predicted for proper route selection. It improves the packet delivery ratio, throughput and reduces overhead. This paper doesn't consider the load balancing factor for congestion avoidance.[10]

Early Detection-AODV (EDAODV) calculated the queue length in an each and every node to identify the states of the congestion. When a queue length becomes maximum and minimum threshold value is assigned by default. If queue length is greater than the Max threshold value, a node becomes secure zone. If queue length is greater than the Min threshold value and less than to greater than the Max threshold value, a node becomes lightly congestion zone. If queue length is less than the Min threshold value, a node becomes congested zone. This condition is based on early detection of congestion control for route discovery and forwarding data packets in MANET. Performance analysis of simulator in ERAODV increases packet delivery ratio and reduces the end to end delay in comparison with an AODV routing protocol.[11]

Link Breakage Time (LBT-AODV) compared to AODV routing protocol in MANET.LBT-AODV calculates the signal strength and link breakage time.LBT is node1 moves connect the link establishes node2 in which the various samples of transmission range in a time interval. The Received Signal Strength (RSS) is greater with respect time from one node to another. Otherwise, it shows the warning message indicating the link failure. It is applied to evaluate the simulation parameters like a throughput, Packet delivery ratio and End to end delay. To select the reliable node based on received signal strength and prediction of link breakage time. It increases Packet delivery ratio, throughput and reduces the delay pertaining to AODV.[12][13]

The predict link failure in AODV involves replacement of existing node or introducing new neighbors along the path or both can be carried out increasing signal strength. It improves packet delivery and reduces traffic control. It must be addressed for best neighbor node selection for better improvement in QoS.[14][15]

Each node calculates the link failure time, the minimum LFT first, second and third should be exchanged in the backup path. It reduces path failure time and also LFT is greater than PFT. In this each and every node maintains backup path for failure recovery and it leads to additional overhead in path. The best backup nodes are heavy traffic or not sufficient energy level due to some other constraints unavailability.[16][17]

When the paths are route discovery average non fading metric based on the select the stable link. When the fading occurred in the path, the preventive a handoff procedure is applied in the multiple paths and reused in the same path without being affected by fading. It provides improved throughput, reduces the routing overhead and improve network performance due to reuse. If the number of the path is affected by noise then channel fading occurs. It will frequently lead to hand off procedure and reduce the overall performance in MANET.[18][19]

PROPOSED SYSTEM

In our proposed the message packets are routed along multiple paths to reach destination,this will preserve the energy level of transmission nodes. It also reduces transmission time as each packet is individually routed and reaches the destination quickly. Load balancing is used to reduce the traffic. By usingthis techniques, network performance is increased by reducing average delayand increasing the reliability of communication.

CHANNEL SENSING ALONG PATH:

This proposed scheme will isolate and remove the malicious nodes based on the node behavior while transferring the message or routing information by watchdog timer technique. The signal to noise ratio of channel is analyzed. If channel signal strength is very much higher than the noise interference then node is selected in reverse case it is rejected. AOMDV uses predicted signal strength to trigger a hand off before a fade occurs

MALICIOUS NODE IDENTIFICATION AND REMOVEAL:

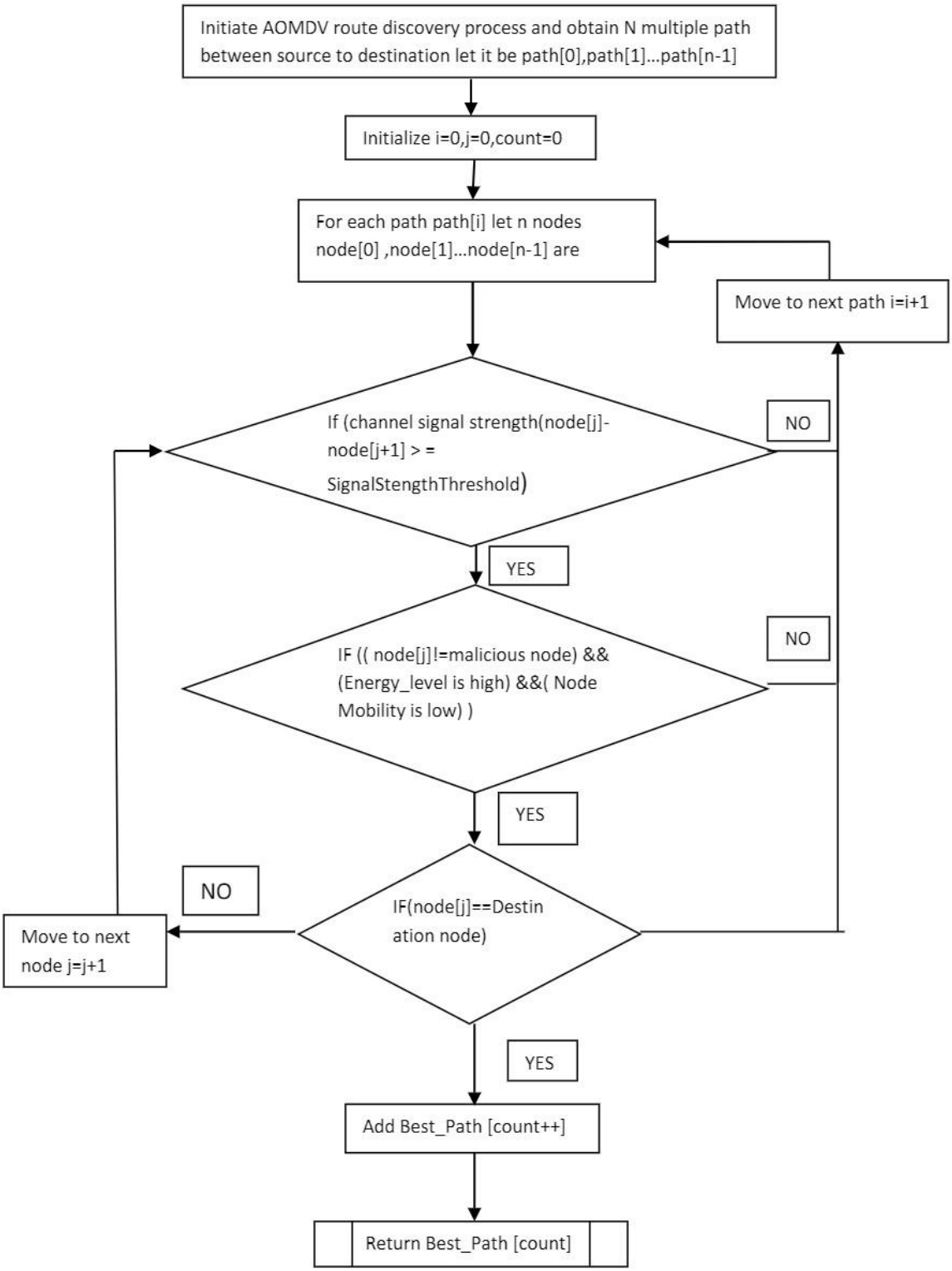
During the message transmissionif anode behaves as a malicious node, then packet drop will occur.Misbehavior node will use some energy costs to create thread in mobile adhoc network. Masquerading and spoofing attacks may be performed by malicious nodes. By performing Fabrication attack amalicious node gains the un privileged accessand also introducesome counterfeet objects into the mobile adhoc network. This will produce false routing messages known as Gray hole attack.This attack will drop packets and behave as malicious node for some timeand later it behaves as normal node. This makes identification of malicious node difficult. Black hole attack also known as Jellyfish attack. The black hole attack is ainner attack, it has two behavior as listed below: A malicious node receives packet but it won't forward to correct destination. Second case, the malicious node will exploits the mobile ad hoc routing protocol, tby announce itself as if it has accurate route to reach destination node, and sends false route information to neighbor node .It will be copied in forwarding group and makes delays in message sending unnecessarily. Thiswillmake end-to-end delay in data transmission.

The malicious nodes are identified and removed based on their behavior using watchdog timer technique

NODE MOBILITY ANALYSIS ALONG THE PATH

The methods in finding the mobility factor of a node are given below.

Figure 1 Flow chart for node Mobility analysis


Initiate AOMDV route discovery process and obtain N multiple path between source to destination let it be path[0],path[1]…path[n-1]
Initialize i=0,j=0,count=0
For each path path[i] let n nodes node[0] ,node[1]…node[n-1] are
Move to next path i=i+1
If (channel signal strength(node[j]-node[j+1] > = SignalStengthThreshold)
NO
YES
IF ((node[j]!=malicious node) && (Energy_level is high) &&(Node Mobility is low))
NO
YES
IF(node[j]==Destination node)
NO
Move to next node j=j+1
YES
Add Best_Path [count++]
Return Best_Path [count]

(1) All the nodes in Mobile adhoc network will estimate their self mobility, i.e. when the mobile node is moving to any new location with respect to the previous location.

(2) Find the neighbors mobility of all the nodes in Mobile adhoc network by considering the neighbor node's self mobility

(3) Each node in the MANET will estimate the mobility factor based on self mobility and neighbors mobility. The mobility factor of a node may be used to establish a path from the source to the destination. The stable nodes in the path will provide higher packet delivery ratio and lower latency.

In best path selection algorithm, initially AOMDV protocol is used to establish multiple path between the source to destination. Then each path is taken and the node as well as channel along the path is examined. If there no noise interference in the channel within the path and each node in the path have sufficient energy level and their mobility is low then path is selected as the best path and other path are rejected.

TRUSTED OPTIMUM PATH SELECTION USING CHANNEL AND NODE AWARE ROUTINGALGORITHM:

Initially AOMDV route discovery isdone to find the available path between senderto receiver and we are going to select the best path among the available path using path selection algorithm.

The signal strength threshold is fixed based on the sensitiveness of receiving information. This can be done by calculating to which extent the noise interference is tolerable by the receiver.

The dynamic queue space are analyzed and their energy level are estimated and are sent to source node through the RREP packet that are sent as response to RREQ in route discovery process.

Best Paths SelectionAlgorithm

Establish N multipath between source to destination using AOMDV reactive protocol

Let available path be AVAIL [N];

Signal Strength threshold value SS_{th};

Initialize count = 0, K = 0, n = Source node;

DO

{

Choose the available path AVAIL [K];

L: Analysis the medium between n and one hop neighbor node (n+1);

IF (medium signal strength between(n-n+1)> = SS_{th})

Choose the n+1 node;

IF (((n+1) node is Malicious_Node)or(Energy level of node is poor) or(Node Mobility is high))

Eliminate the current path;

Proceed with next path K++;

ELSE IF((n+1)node= = Destination Node)

Add toBest_Path [count];

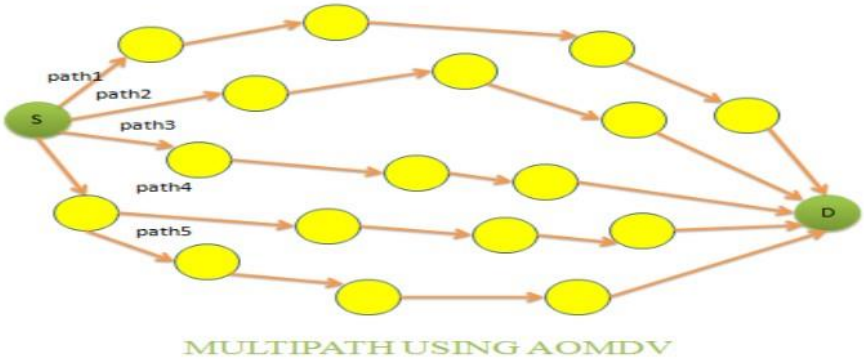
K+ + and count++;

ELSE

n++ ;

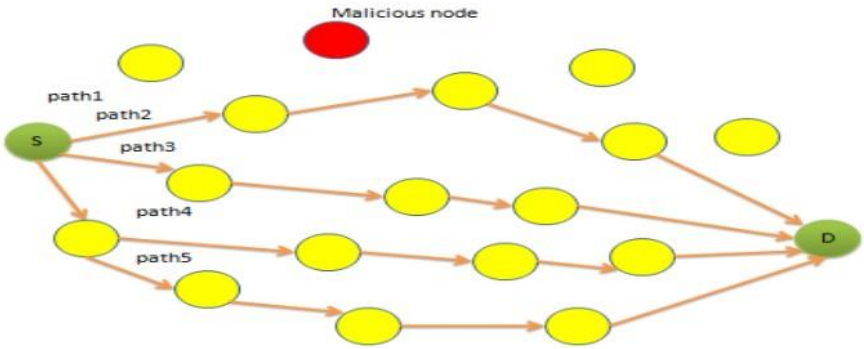
GOTO L;

END IF
ELSE
Eliminate the path;
Proceed with next path K++;
END IF
}
WHILE K< = N



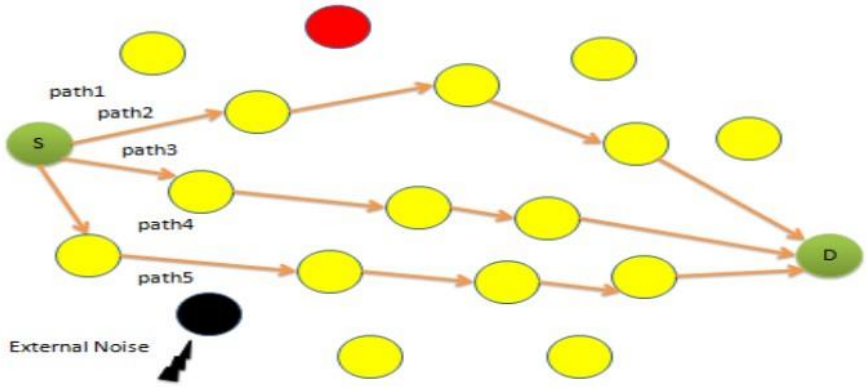
MULTIPATH USING AOMDV

Figure 2 shows the establishment of all multiple paths between sender and receiver using AOMDV route discovery process.



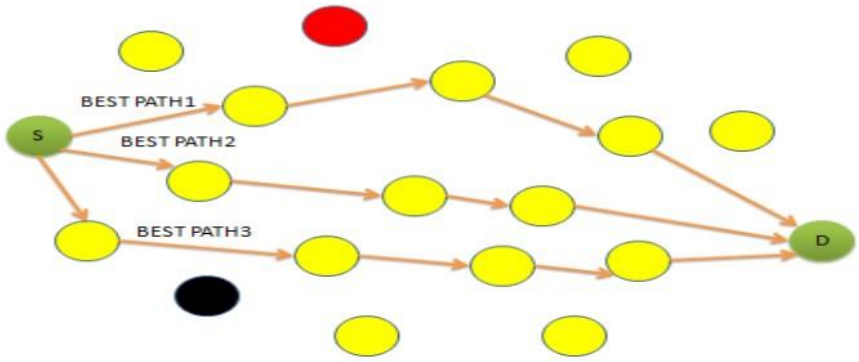
Malicious node path removed

Figure 3 shows the malicious node detection and removal of that particular path.



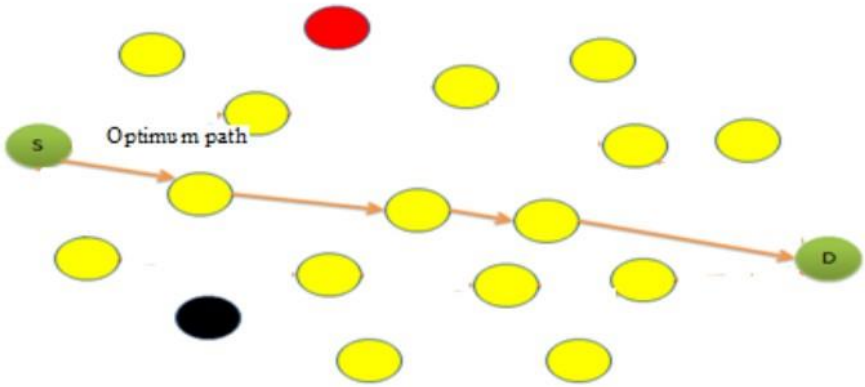
Noise affected path removed

Figure 4 shows the removal of noise affected path from the existing path.



Best path Selection

Figure 5 shows the best path selection among the available multiple path.



Optimum path selection

Figure6 shows the optimum path selection among the multiple best path.

Figures 3,4&5 checks each and every path of AOMDV route discovery process individually and selects the best available paths that involves nodes with residual energy is higher than or equal to signal strength threshold value, mobility of node is less, no malicious behavior of node and channel is noiseless After selecting the best path we are going to send all our packets through the best path from source to destination in round robin fashion using load balancing algorithm.

Multipath Sharing Algorithm

ArrayBest_Path [count]; //array of available best path from Best Paths Selection Algorithm

Array Message_Packet P[packet_count]; //Available message packets
Message_count = number of message packet;
Initialize l = 0, m = 0;
while(l<message_count)
Send p[l] in best_path [m];
l++;

```
IF(there is problem in the path)THEN
  count = count-1; // To remove the path
END IF
m = m +1 mod count;
```

END WHILE

If there is a problem in existing best path or else existing best path fails then the corresponding best path is removed and the best path count is reduced and remaining best path where used to transfer packets. If sufficient number of best path is not available then re route discovery is initiated.

OPTIMUM SINGLE PATH SELECTION ALGORITHM

When a packet arrives a node then it has to wait in queue for some time then it is processed and routed by the node. Thus the transmission delay includes propagation delay ,queuing delay and node processing delay. We cannot reduce the propagation and processing delay but we can select a path with less queuing delay. When the arrival rate is higher than the node processing time then queue size is increased in reverse case the queue size is reduced

In this we examine the available queue spaces in each node of the multipath and calculate the delay factor of each path and select the path that has less delay factor. When only twenty five percentage of queue space is occupied in node then waiting factor is assigned one. If fifty percentage of queue space is occupied in node then waiting factor is assigned two and more than fifty percentage of queue space is occupied in node then waiting factor is assigned three.

Optimum Single path selection algorithm

```
routine Optimum_Single_path_selection( Best_path[n])
    {
    Array Delay_calc_path [n];
    for i=0 to n-1
      Take Best_path[l] path and it has N[0], N[1]... N[K]  Nodes .
      Delay _calc _Path[i] = 0
      for m=0 to k
        if (OccupiedQueue space (N[m])< = 0.25)
    Time_waiting _ Factor (N[m]) = 1;
        else if (OccupiedQueue space (N[m])< = 0.5)
    Time_waiting _ Factor (N[m]) = 2;
        else
    Time_waiting _ Factor (N[m]) = 3;
        End if
```

```
    Delay _calc _Path [l]+ = Time_waiting _ Factor (N[m])
  End for
End for
return(path[minimum(Delay _calc _Path [n])
}
```

SIMULATION RESULT

Simulation parameters for secured multipath load balanced channel awareness routing algorithm

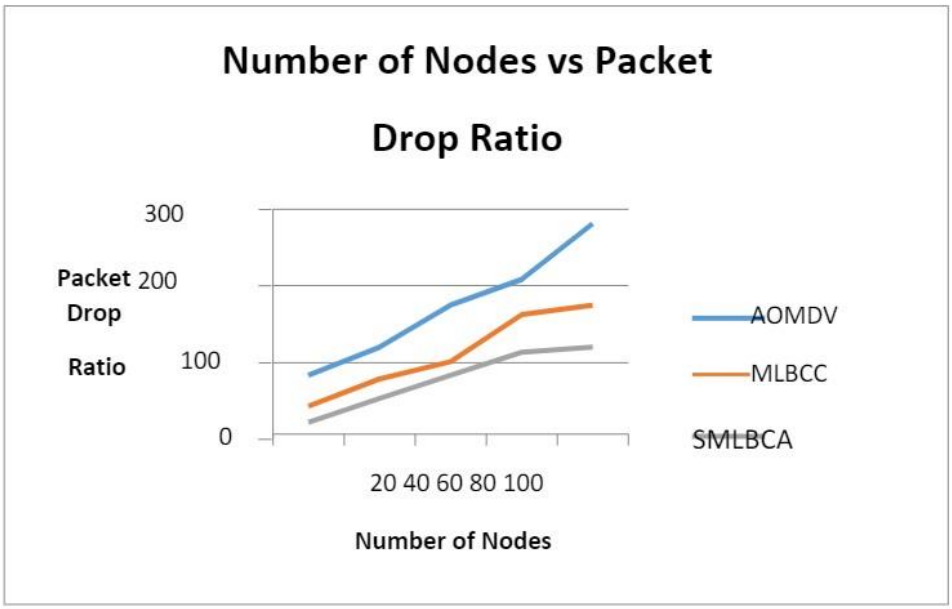
Property	Values
Simulation Time	900 Sec
Number of nodes	500
Network area	1100 X 900
MAC protocol	802.11
Radio Range	300 m
Traffic Source	CBR
Payload Size	1024 bytes
Node Deployment	Random
Mobility Model	Random Way Point
Speed (m/Sec)	3m/Sec
Number of flows	25 flows

Table 1 Simulation Results

Packet Drop Ratio

In our proposed system, initially we are examining whether nodes are not malicious andit have sufficient energy to transmit .Therefore node will not fail and path are maintained throughout the transmission. Hence packet drop ratio drastically and comparative results with AOMDV and MLBCC is shown below.

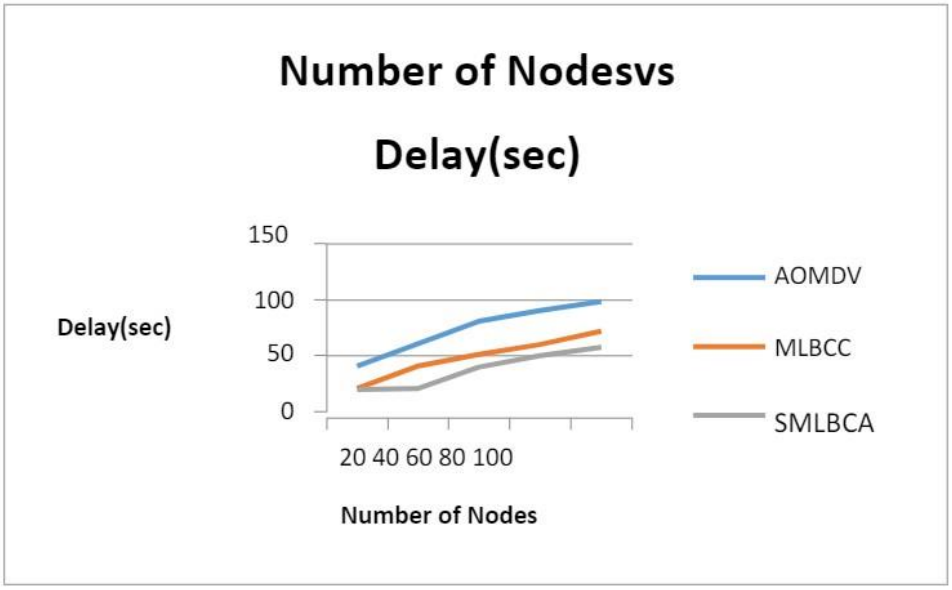
Fig-7 packet drop ratio versus number of nodes



Delay

Since we are going to route packet in multiple path, the packet transmission delay is reduced and energy level of transmission nodes are also preserved. The comparative results with AOMDV and MLBCC are shown below

Fig-8 Delay versus number of nodes



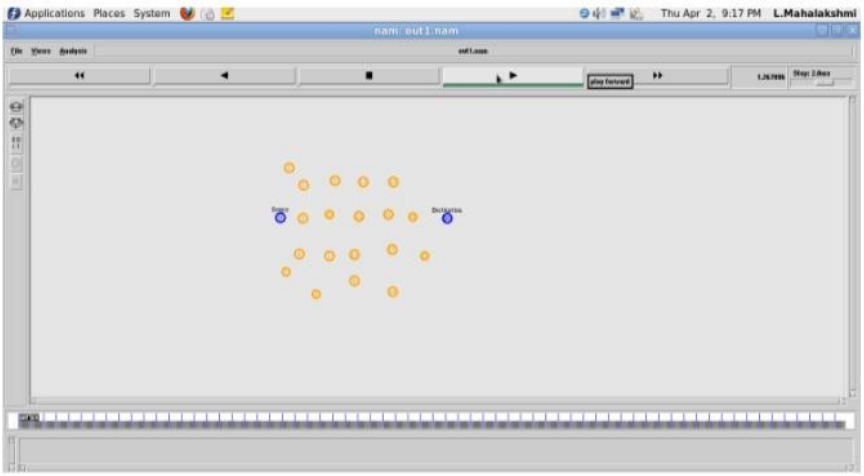


Fig -9 Node creation

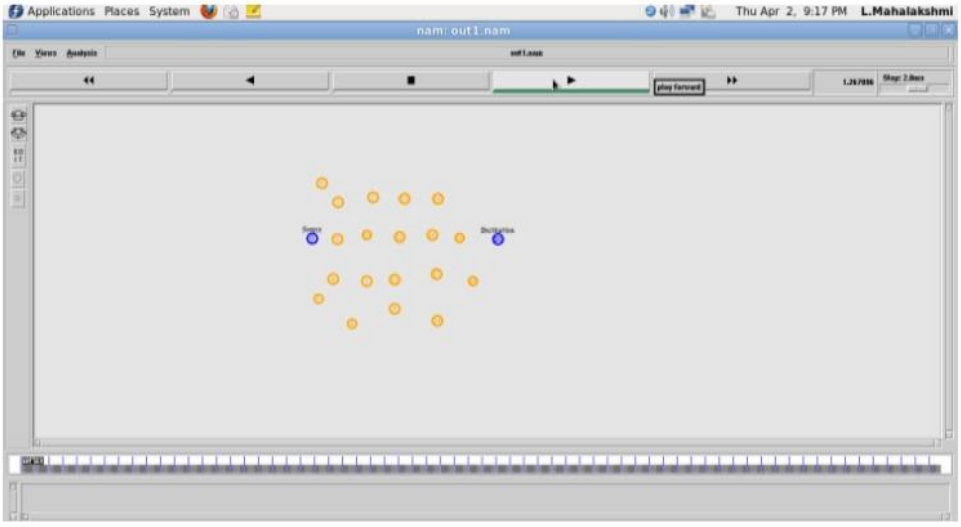


Fig -10 Multiple path establishment using AOMDV

Figure -11 Packet transmission in multiple path

Conclusion

In this paper, we propose a multipath routing that uses available best paths and load balancing algorithm that effectively sends packets among the best path. The selection of best path will include sensing the channel between the neighbor nodes and avoiding the external noise path that affects sending data packets. It is very simple but efficient algorithm to sharing the packet transmission load and alleviates the congestion in mobile adhocnetwork. The algorithm will reduces delay of about 0.65%, transmission overhead of about 0.55%,, minimizes traffic congestion of about 0.85%, in network and increase data transmission speed of about 0.68%, between source and destination with secure manner by avoiding malicious nodes.

REFERENCES

[1] Raju, J. and Garcia-Luna-Aceves, J.J., (1999), October. "A new approach to on-demand loop-free multipath routing". In Proceedings Eight International Conference on Computer Communications and Networks (Cat. No. 99EX370) (pp. 522-527). IEEE.

[2] Dube, R., Rais, C.D., Wang, K.Y. and Tripathi, S.K., (1997). "Signal stability-based adaptive routing (SSA) for ad hoc mobile networks". IEEE Personal communications, 4(1), pp.36-45.

[3] Sharma, N. and Sharma, S., (2011), December. "Provisioning of quality of service in MANETs by performance analysis and comparison of AODV and OLSR". In Proceedings of 2011 International Conference on Computer Science and Network Technology (Vol. 4, pp. 2341-2344). IEEE.

[4] Karthikeyan, B., Kanimozhi, N. and Ganesh, S.H., (2014), October. "Analysis of reactive AODV routing protocol for MANET". In 2014 World Congress on Computing and Communication Technologies (pp. 264-267). IEEE.

[5] Thakkar, P. and Shete, P., (2015). AH-AODV: "adaptive hello messaging based AODV routing protocol ". International Journal of Computer Applications, 124(17).

[6] Devi, S.S. and Sikamani, K.T., (2013), July. "Improved routerror tolerant mechanism for AODV routing protocol in MANET". In 2013 International Conference on Current Trends in Engineering and Technology (ICCTET) (pp. 187-190). IEEE.

[7] Dandotiya, H., Jain, R. and Bhatia, R., (2013), April. "Route selection in MANETs by intelligent AODV". In 2013 International Conference on Communication Systems and Network Technologies (pp. 332-335). IEEE.

[8] Kumar, R. and Gupta, M., (2014), December. "Route stability and energy aware based AODV in MANET". In 2014 International Conference on High Performance Computing and Applications (ICHPCA) (pp. 1-5). IEEE.

[9] Gite, P., (2017), January. "Link stability prediction for mobile Ad-hoc network route stability ".In International Conference on Inventive Systems and Control (ICISC) (pp. 1-5). IEEE.

[10] Prabha, R. and Ramaraj, N., (2015). "An improved multipath MANET routing using link estimation and swarm intelligence ".
EURASIP Journal on Wireless Communications and Networking, 2015(1), p.173.

[11] Alghamdi, S.A., (2015). "Load balancing ad hoc on-demand multipath distance vector (LBAOMDV) routing protocol ".
EURASIP Journal on Wireless Communications and Networking, 2015(1), pp.1-11.

[12] Deva Priya, M. and Priyanka, P., (2015). "Probabilistic prediction coefficient link stability scheme based routing in MANET ". Int. J. Comput. Sci. Eng. Technol, 6(4), pp.246-256.

[13] Zonghua, M. and Xiaojing, M., (2011). "A modified AODV routing protocol based on route stability in MANET".

[14] Gnanasekaran, P. and Vibeeth, B., (2015), March. "Link breakage time based QoS improvement in mobile ad hoc network". In 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015] (pp. 1-4). IEEE.

[15] Maamar, S. and Abderezzak, B., (2016). "Predict link failure in AODV protocol to provide quality of service in MANET". International Journal of Computer Network and Information Security (IJCNIS), 8(3), pp.1-9.

[16] Zadin, A. and Fevens, T., (2013). "Maintaining path stability with node failure in mobile ad hoc networks". Procedia Computer Science, 19, pp.1068-1073.

[17] Chen, X., Jones, H.M. and Jayalath, D., (2010). "Channel-aware routing in MANETs with route handoff ". IEEE Transactions on Mobile computing, 10(1), pp.108-121.

[18] Ahmed, I., Tepe, K.E. and Singh, B.K., (2009), September. "Reliable coverage area based link expiration time (LET) routing metric for mobile ad hoc networks. " In International Conference on Ad Hoc Networks (pp. 466-476). Springer, Berlin, Heidelberg.

[19] Bagwari, A., Jee, R., Joshi, P. and Bisht, S., (2012), May. "Performance of AODV routing protocol with increasing the MANET nodes and its effects on QoS of mobile ad hoc networks". In 2012 International Conference on Communication Systems and Network Technologies (pp. 320-324). IEEE.