OPTIMIZATION OF OPEN SHORTEST PATH FIRST ROUTING

P.Anu [1] Dr.S.Vimala*[2]
[1] Research Scholar, [2]Associate Professor Department of Computer Science, Mother Terasa Women's University, Kodaikanal, India

Abstract: Optimization of Open Shortest Path First (OSPF) routing is investigated by various preceding exploration worksby decreasing congestion as well as shortest path.The performance of the network is affected by the flooding perception in OSPF. It results in additional congestion besides further propagation time.Commonly, maximum of the nodes will conversein the Flooding in addition to Packet Forwarding mechanism. If the packet forwarding is not done then it is branded as selfish node.The throughput and performance in the communication is declined by Selfish node. Malicious nodesamend the path in addition it drops the packetwith determination. The decreases in the throughputand performance of the network as well as the escalation of the delay is occurred by malicious nodes. The decrease Flooding, Selfish nodes and malicious nodes in the network is the stimulus behind the recommended effort. This in turn increases the Throughput as well as Routing Optimization of the network.

Keywords: clustering; OSPF, Selfish Node, Flooding, Malicious Node

INTRODUCTION

In modern years, trend of consuming Internet as communication infrastructure for diverse Telecom Communication applications is on the rise considerably [1].In the present-day situation, the widely used routing protocol is Open Shortest Path First (OSPF) [2]. To forward packets, OSPF uses shortest path always which leads to escalation in traffic. Despite the fact, there are supplementary paths that exist are less congested than the shortest path, OSPF continuously inclines to use the shortest path.

As a consequence, it clues to additional traffic [9]. The entire routers retain the comprehensive network topology. OSPF responses to its neighborhood through the periodic Hello messages.Link State Database (LSDB) is preserved by all routers and the neighbors' LSDB is coordinated with the database. The topology facts are notified by the Link State Advertisement (LSA) to the nodes. LSA is sent by the Router to all the nodes excluding the source through which it receives it. Flooding of LSA took place as a result. [10].

2. Open Shortest Path First Protocol

OSPF is a link state protocol. In the beginning in its init state, OSPF enabled router directs hello packets so that it is aware of their links of neighboring routers as well as it pauses for their answers. It will acquire the sender's address also when it accepts its response in the form of hello packets from the neighbors. Link State Routing's elementary ideologies are: 1.All router launches an association with its neighbors; 2.Link state advertisements (LSAs) are produced by every single router which are circulated to all routers.

LSA = (link id, cost,state of the link, neighbors of the link)

A selfish node is solitary node that attempts to make use of the resources of the network for its own yield without distribute its own resources to other nodes. Selfish node will positively evade itself from the routing paths. The selfish node can partake in routing messages on the other hand forward the data packets are not done by selfish nodes.

The malicious node responses to every single route request by misleadingly demanding that it has a renewed route to the destination. In this fashion completely the traffic of the network are readdressed. So that malicious node which at that juncture dumps them altogether.

3. Proposed Methodology

The research progression in one piece is elucidated phase by phase, which notice ably portrays the research breaches and the vital impact made by the contemporary research effort. The different steps of the suggested effort take account of the following:

1. LSA Flood Reduction in OSPF

2. Selfish Node Recognition in addition to Dismissal in OSPF

3. Malicious Node Detection as well as Exclusion in OSPF

3.1. LSA Flood Reduction in OSPF

The exploration is carried with the target of reducing the LSA flooding.

The suggested algorithm is divided into four stages:

- Distance calculation between nodes,
- Cluster formation phase,
- Cluster head selection phase and
- Data Transmission phase.

Cluster formation phase

A cluster isa gathering of multiple nodes which converses with each other. Bring togetherproximate nodes into clusters make it suitable to proficientlyaccomplish each cluster as well as the overall network. [6]

Cluster head selection phase

Clustering pattern is proposed here where cluster head node will perform the part of communicating packet from one cluster to the other. This algorithm encompassesconsortium of nodes into clusters and choosing cluster heads for all the clusters. For competent flooding, certain nodes are nominated as Cluster Heads with exceptionaltasks. Only Cluster heads has the responsibility of flooding the messages. [4]

Cluster head formation

In our recommendedprocedure, all clustersmust have its separate Cluster Head (CH). Cluster Heads only learnt the modification in topology by the nodes through LSA. In case of router failure the substitute path can be confirmed by the Cluster Heads. This leads to decrease in Convergence time. In the midst of the nodes,LSA flooding is also reduced and in turn, the congestion is reduced. [5]

The subsequent are the steps for each & every cluster (C).

Cluster-head Selection (C, CH)

```
Begin:
Step 1: Quantity of clusters, C and quantity of nodes n in a cluster should be quantified
Step 2: Compute the distance of a node with all other nodes in the cluster
fori=1 to n do
for j=1 to n-1 do
$HL_{ij}$ = using Hierarchical length algorithm distance from i to all other nodes is estimated.
Endfor
Endfor
Step 3: Step 2 must be iterated for all the nodes in the cluster.
Step 4: Distance evaluation of every single node to all other nodes is prepared.
Step 5: Nominate the node which is without difficulty approachable by all the nodes in the cluster as cluster head.
```

Data transmission phase

Cluster Heads play a significant part if the Source and Destination belong to diverse clusters. The categories of Data communication is pointed out below:

Data communication between source to destination is estimated as the data communication from source to cluster head1 and data communication from cluster head1 to cluster head2 and data communication from destination to cluster head2.

Cluster Heads and node Interactions

The communication sin the middle of Cluster heads and Router are as follows:

1. Directing a LSA from cluster Head
2. In receipt of a LSA at cluster Head
3. Transfer a LSA from node to cluster head
4. Delivery a LSA at node from cluster head

By means of this recommended algorithm the intra traffic message flow is reduced.[7]

3.2. Recognition and Eradication of Selfish Node in OSPF

A selfish node only converses to other nodes if its data packet is mandatory to send to some other node and discards to cooperate other nodes on every occasion if some data packets or routing packets are received by it that it has no interest in it. Henceforth data packets are either declined to retransmit or else are dropped for being received by a selfish node. [3]

Selfish node is recognized with the aid of Watchdog. Operationalcode of watchdog is to conserve a buffer of in recent timesdirected packets and associating each overheard packet. If the packet has persisted in the buffer for elongated than a certain timeout, the watchdog increments a failure count for the node accountable for not dispatching the packet. If the scoresurpasses a certain threshold, it concludes that the node is misbehaving and spread the note to the source that it is a misbehaving node. Even if the node is the destination, it has to acknowledge. The formulae for watchdog “Amount of incoming communication is equal to

Amount of departingcommunication”.

Previous service time is the time in which precedingperiod the node delivered service to the network, providing services comprisesdirecting/forwarding data packets. If the node is it is source then it is not considered.

Previous hello time is the time loggedas soon as the node has last sent the hello packet. Status is the node present behavior chronicled. At the outset status of the all the nodes is reset to zero, which is the behavior of the node is anonymous.

3.3 Discovery and Elimination of Malicious Node in OSPF

The support is stretched outextra to contemporary one more procedure to become aware ofas well asto eradicate malicious nodes in OSPF.[10]

In our projectedtechnique, Two Threshold is defined 1. Suspect_threshold 2. Acceptance_threshold.If Suspect node drips the packet , then the Suspect node counter is added by 1 besides if it surpasses the Suspect_threshold then suspect node is characterized as MALICIOUS Node and it is included to queue of malicious node and it is conversed by the cluster head to other nodes and quarantined from the network else if the packet is forwarded by Suspect_node with in the restricted time limit then the suspect_node Acceptance level is added by 1, at that juncture after approved period and the MALICIOUS Node is acknowledged as trusted Node.

4. Performance Analysis

The performance of the recommended model is estimated through simulations. At this point the enhancement in network optimization through suggestedapproachesin excess oforthodoxstratagems are appraisedin addition toassociated.

4.1 Packet Delivery Ratio

In the exploration, the Network Packet Delivery Ratio of the OSPF is examined with the projectedeffort. The graph (Figure-1) portrays the enhancement of the projectedpractice over OSPF

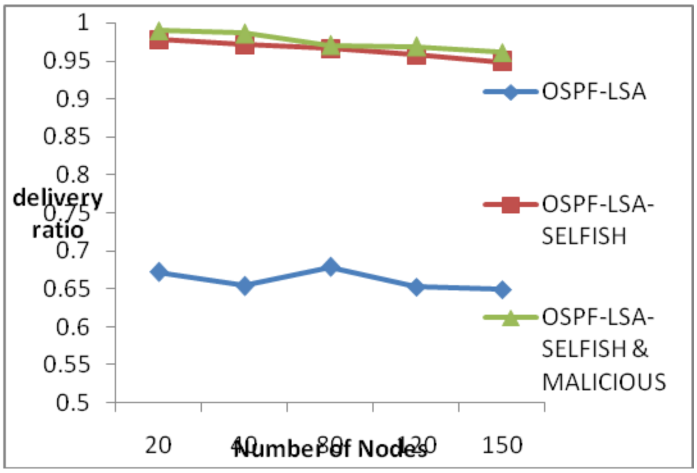

Figure 1: Delivery Ratio in OSPF-LSA algorithm as well as OSPF-LSA-SELFISH Algorithm and OSPF-LSA-SELFISH & MALICIOUS algorithm

4.2 End to End Delay

End-to-End Delay is estimated for the OSPF-LSA algorithm in addition to OSPF-LSA-

SELFISH procedurealso OSPF-LSA-SELFISH & MALICIOUS process by changing the number of nodes to 20, 40, 80, 120 and 150. The above values are portrayed pictorially. The End-To-End delay is reducedsubsequentlyeradicating malicious nodes.

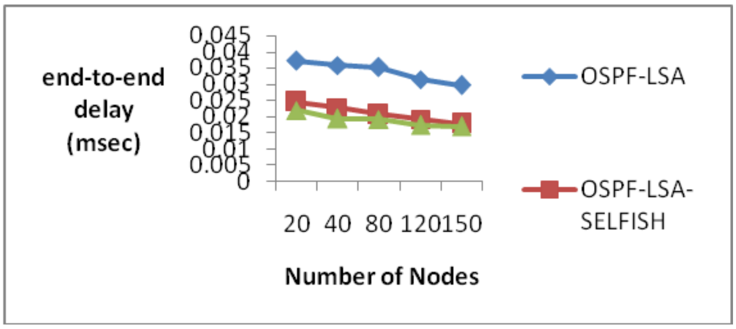

Figure 2: Delay in OSPF- LSA algorithm in addition to OSPF-LSA-SELFISH algorithm and OSPF-LSA-SELFISH & MALICIOUS algorithm

4.3 Throughput

Throughput is calculated for the procedures OSPF-LSA, OSPF-LSA-SELFISH algorithm besides OSPF-LSA-SELFISH & MALICIOUS process for the nodes 20, 50, 80,110 and 150.

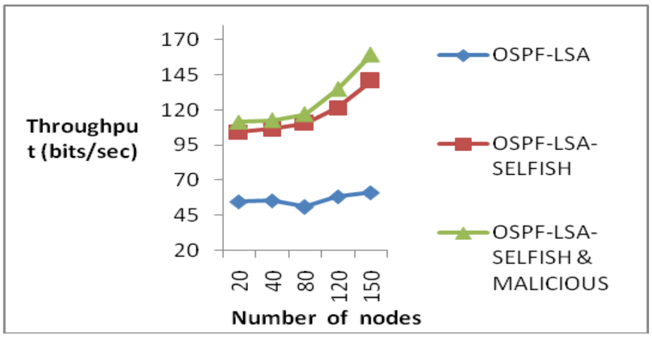

Figure 3: Throughput in OSPF-LSA algorithm with respect to OSPF-LSA-SELFISH algorithm and OSPF-LSA-SELFISH & MALICIOUS algorithm

5. Conclusion

The OSPF takes additional time for convergence owing to LSA Flooding. In order to decrease the LSA flooding, clustering method is announced.

In the principaleffort, a proficient flooding algorithm is recommended to decrease LSA flooding through cluster concept.

The subsequentstages sense as well as eliminate the selfish in addition to malicious node from the route. In the projectedmethodology, the selfish as well as malicious nodes are penalized for their selfish activity then the non-selfish nodes are remunerated for their assistance in routing functionality..

REFERENCES

1. Kyriakos M., V.T. McAuley and R. Morerav, J. Baras, International Conference on Wireless Networks, Communications and Mobile Computing, Using Multiobjective Domain Optimization

for Routing in Hierarchical Networks, Maui, HI, USA 2005

2. Chandra W., Performance Analysis of Dynamic Routing Protocol EIGRP and OSPF in IPV4 and IPv6 Network, 1st International Conference on Informatics and Computational Intelligence, Bandung, Indonesia ,2011
3. N. Ramya, Dr. S. Rathi, Detection of Selfish Nodes in Manet- A Survey, 2016 3rdInternational Conference on Advanced Computing and Communication Systems (ICACCS - 2016), Jan. 22 – 23, 2016,Coimbatore, INDIA ,
4. Masashi Honma, Shunichi Tsunoda, Eiji Oki, Load-Balanced Shortest-Path-Based Routing With Even Traffic Splitting, 2012 18th Asia-Pacific Conference on Communications (APCC), IEEE, Jeju Island, South Korea
5. David Hock, Matthias Hartmann, Tim Neubert, Michael Menth ,Loop-Free Convergence Using Ordered FIB Updates: Analysis And Routing Optimization, 2011, 8th International Workshop on the Design of Reliable Communication Networks (DRCN),IEEE, Krakow, Poland
6. M. Pitkanen, M. Luoma OSPF Flooding Process Optimization, HPSR. 2005 Workshop on High Performance Switching and Routing, 2005, IEEE, Hong Kong, China.
7. P.Anu, Dr. S. Vimala, Optimization of OSPF LSA Flooding Process Using Clustering Technique, Intelligent Systems and Control (ISCO ’16)” on 7 - 8 January 2016 at Karpagam College of Engineering, Coimbatore. Paper was Published and Indexed in IEEE Explorer
8. P.Anu, Dr. S. Vimala, Detection and Elimination of Selfish Nodes in OSPF in International Journal of Pure and Applied Mathematics, ISSN: 1314-3395, Volume 119, 2018.
9. P.Anu, Dr. S. Vimala, Efficient LSA flooding process to optimize OSPF routing, in Pakistan Journal of Bio Technology, PISSN: 1812-1837, EISSN: 2312-7791, Volume 15, 2018
10. P.Anu, Dr. S. Vimala, Reputation based Malicious Node Detection and Elimination in Open Shortest Path First, Journal of Advanced Research in Dynamical & Control Systems, ISSN: 1943-023X Vol. 11, 11-Special Issue, 2019.