Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:01:2022
DOI 10.17605/OSF.IO/NWVEB

A DOS ATTACK RESILIENCE FRAMEWORK FOR MULTIMEDIA STREAMING OVER P2P NETWORKS

REDDEMMA YAGA[1] and Dr. CH. D. V. SUBBA RAO[2]

[1]Research Scholar, Computer Science & Engineering, Sri Venkateswara University College of Engineering, Tirupati, Andra Pradesh, India

[2]Professor, Department of Computer Science & Engineering, Sri Venkateswara University College of Engineering, Tirupati, Andra Pradesh, India

Abstract

Peer-to-Peer networks have inspired many applications that work in distributed environments. One such application is multimedia streaming which exploits the P2P network. However, Denial of Service (DoS) attacks may deny the services causing deterioration of video streaming quality. Therefore, resilience against DoS attacks is indispensable for multimedia content distribution systems. In this paper, proposed a framework known as DoS Resilient-Optimal P2P Topology Construction (DR-OPTC) framework. It strives at arriving at optimally stable topologies at runtime dynamically to defeat DoS attack strategies and ensure desired QoS. An algorithm known as DoS Resilient Topology Construction (DRTC) is proposed. The algorithm constructs stable P2P topologies dynamically by performing cost analysis in presence of DoS attacks. The empirical study revealed that the proposed framework ensures QoS in the multimedia streaming of Application Level Multicast applications. Besides, it outperforms previous approaches as it provides optimally stable topologies against worst-case node failures and DoS attacks.

Keywords –Resilient Topology, Multimedia Streaming, Attack Resilience

1. INTRODUCTION

Overlay P2P networks are widely used for video streaming. However, the problem with it is that the topologies are highly dynamic and Quality of Service (QoS) is to be given high importance. In addition to this, Denial of Service (DoS) an important concern as it will deteriorate QoS [1]. There are many security issues when multimedia streaming applications run on P2P overlay networks. Consideration of QoS and also security with equal importance is essential in such networks. Thus it will have benefits of QoS and also attack resiliency [8]. When overlay networks are constructed for multimedia streaming or when multimedia streaming applications run on existing P2P systems, it is an important observation that the nodes involving in the content dissemination may fail. There might be physical network disruption for any reason. Withstanding such situations is indispensable to have reliable content streaming over overlay P2P networks [9]. In the same fashion, there might be Sybil attacks on P2P networks. Computational puzzles are exploited in [10] to safeguard networks from Sybil attacks. When attacker uses large number of attacker nodes and perform such attacks including DoS, it is important to have defence against such attacks. Typical DoS attack is illustrated in Figure 1.

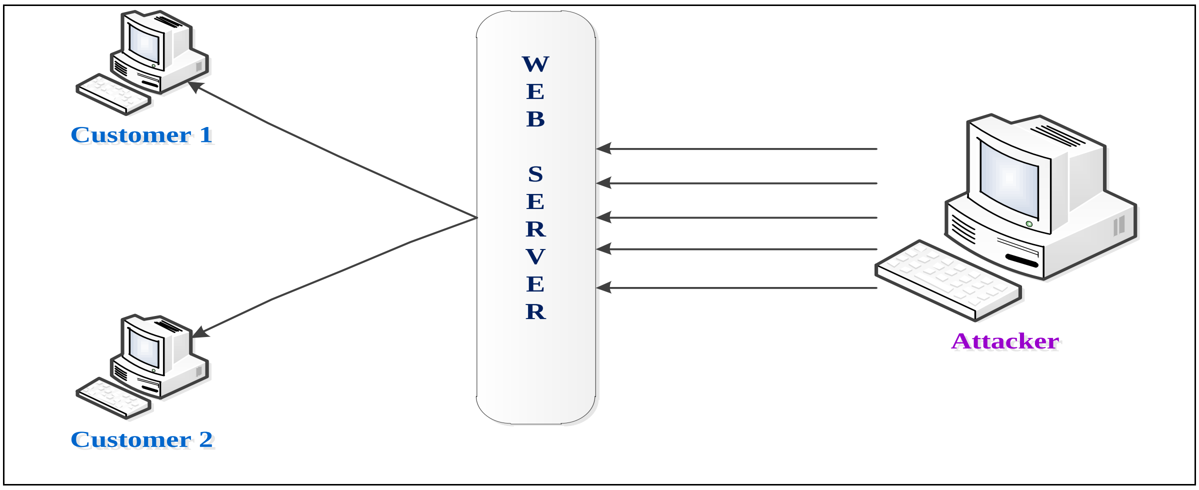

Figure 1: Illustrates a typical DoS attack

Web server is rendering services to number of genuine users or customers. However, an attacker sends fake requests to web server in large scale, it causes the server to be too busy to answer those fake requests and cannot give any sort of service to genuine users. This is known as Denial of Service (DoS). In the literature, many solutions came into existence to ensure that P2P overlays run even in the presence of DoS attacks. More information on the architectures of P2P networks are found in [15]. P2P networks, security issues in different kinds of P2P networks and counter measures are discussed in [16]. DoS resilient topology construction is explored in [1], [3] and [12].

In [1] optimal topology construction to be DoS resilient is studied. In [3] also overlay P2P network is used to have DoS and churn resistant solution for content streaming. In [13], the concept of bandwidth exhaustion attack is explored to have optimal topologies. The commonality in all these solutions is the usage of alternative topologies that can withstand DoS attacks. However, there is no extensive analysis on the effect of high churn rate and high rate of node failure. In this paper we proposed a framework to overcome these drawbacks. The contributions of the paper are as follows.

1. A framework named DoS Resilient - Optimal P2P Topology Construction (DR-OPTC) is proposed to have different modules like cost analysis, churn analysis, node failure analysis and optimal topology construction.
2. An algorithm by name DoS Resilient Topology Construction (DRTC) is proposed and implemented to reduce cost of all outgoing nodes and optimize topology to leverage performance of multimedia streaming over P2P overlay network.
3. An analytical model is made and then simulated with NS-2, a widely used discrete event simulator, for proof of the concept.

The remainder of the paper is structured as follows. Section 2 reviews prior works that are close to the work in this paper. Section 3 presents the proposed framework with details. Section 4 presents experimental results. Section 5 presents evaluation of different methods. Section 6 concludes the paper and provides directions for future scope of the research.

2. RELATED WORK

This section reviews literature on the present state of the art of P2P overlay networks helping in multimedia streaming. It also throws light into DoS attacks and prevention measures found in the prior works.

2.1 P2P Video Streaming vs. DoS Attacks

The concept of network reconfiguration is employed by Drees *et al*. [3] for considering churn and DoS-resistant overlay. Node sampling primitives and reconfiguration algorithms are used to achieve resiliency against DoS attacks and churn. They evaluated their model with three overlay networks. Suganya and Mummoorthy [5] investigated message delay issues in smart grids. They focused on jamming as a kind of DoS attack in wireless networks. Brinkmeier [6] proposed a mechanism to have un-exploitable construction of P2P streaming systems based on the concept of multiple-trees. Different types of internal attacks are used to know the robustness of the system. They opined that their model needs further refinement with more format attack models. Dos and other attacks are studied with different protocols in [13]. There has been research found on P2P networks for security with the help of Virtual Private Networks (VPNs). It is investigated in [14] and found that secure communications in P2P networks is possible with VPN.

Zhu *et al*. [21] proposed a protocol known as Secure Deep Throat (SDP) for achieving witness anonymity. It supports DoS attacks in order to demonstrate resiliency and tracing of attack source. Attacks are restrained in presence of active adversary launching attacks. Lin *et al*. [22] proposed cooperative strategies for improving performance of multimedia streaming in P2P networks. With incentives, it is designed in such a way that the peers do not play selfish and participate in communication genuinely. They used game theory with Pareto optimality and Nash equilibrium. Selfish and attacking behaviours of peers will be controlled with this approach. P2P video streaming is with specific architecture is studied in [27]. Heterogeneity and dynamic playback are the two important issues in video streaming. Since video streaming over P2P overlay networks should provide required quality to end users, it is challenging to ensure the quality in the presence of security issues like DoS attacks [28]. Liao *et al*. [29] proposed a P2P live streaming system known as AnySee which improve resource utilization globally, assign resources optimally, guarantee service quality and balancing load while streaming. In presence of scaling laws and trade-offs, it is important to ensure high quality video streaming with P2P networks.

2.2 DoS Resistant P2P Topologies

P2P overlay networks used for multimedia content dissemination are subjected to DoS attacks. Brinkmeier*et al*. [1] proposed a methodology that will bring about stability to overlay network in spite of DoS attacks. It exploits distributed procedures and global knowledge to have stable topologies that can serve the purpose in presence of DoS attacks. In other words, it focuses on DoS resilient topology construction dynamically. However, it does not focus on the situations where there is high churn rate and high rate of node failures. Suto*et al*. [2] on the other hand proposed a P2P network known as THUP which is said to be robust to DoS attacks and also churn. They used the concept of bimodal degree distribution to achieve this. Stability and communication efficiency were achieved. Wang *et al*. [6] on the other hand modelled DoS attacks in content-centric networks and provided a solution based on content caching. Binary tree topology is employed in their empirical study with NS-2 simulator.

Nguyen *et al*. [11] proposed a system known as Resilient Backbone Construction Scheme (RBCS) for supporting multimedia streaming in hybrid P2P systems. It is made resilient against DoS attacks. It is able to identify stable peers in secure fashion and considers node churn to some extent. Rossberg *et al*. [12] adapted topologies to have minimum impact of DoS attacks on P2P networks. They proposed novel metrics to have approximate estimation of impact of attack. They considered different strengths of attacks like random, greedy and optimal. They simulated both affected and unaffected connections to understand impact of the attacks. Finding optimal topologies, understanding DoS-resilient topology properties and constructing homogenous graph structures are involved in the solution. File sharing with P2P systems with attack resiliency is proposed by Dumitriu*et al*. [17]. They differentiated file-targeted and network-targeted attacks. They found that DoS attacks were causing potential issues with file sharing. They modelled resiliency to network targeted attacks and found stable topologies for file sharing.

Finite Departure Problem (FDP) in investigated in [18] as it is the problem associated with overlay networks. Safely excluding the nodes that leave network is very important issue addressed. It is essential in the presence of DoS attacks. Mainly P2P network topologies can be built dynamically to have effective data transmission systems [19]. Ideal topology construction is possible in presence of DoS attacks with super-peer based overlay P2P network that is used to have large scale data transmission. Overlay P2P with resilient topologies are explored to have better performance and resiliency against attacks. Brinkmeier *et al*. [23] explored a class of P2P topologies that are stable and provide efficient means of multimedia streaming. The topologies are optimally stable against greedy DoS attacks. Monteiro *et al*. [24] on the other hand studied different approaches in which P2P video streaming is achieved.

Srikanth*et al*. [25] made an explicit study on security issues in P2P networks where video streaming is involved. Different problems are identified with respect to security. They include selfishness, DoS attacks, malicious payload insertion attack, whitewasher’s attack, free rider’s attack, Pareto optimality, Nash equilibrium, bandwidth fluctuation, legal contents, privacy, scalability, media streaming, and so on. Different solutions are found in the literature such as Digital Rights Management

(DRM), game theoretic frameworks, multi-objective optimizations etc. From the review of literature, it is understood that P2P networks with dynamic topologies could perform well even in presence of DoS attacks. However, it is important to explore high churn rate and large scale node failures with a comprehensive framework. Such study is the main focus of this paper.

3. PROPOSED FRAMEWORK

We proposed a framework that takes care of DoS attack resiliency while performing video streaming over P2P networks. Live streaming of multimedia content over such networks is challenging in presence of DoS attacks. System stability is important ensuring quality of streaming. Application Layer Multicast (ALM) refers to such streaming phenomenon. ALM has become an important research area especially with overlay networks like P2P. Overlay streaming needs stability which is challenging in presence of churn and node failures besides the DoS attacks. The following sub sections provide more details of the proposed framework to have DoS attack resilient multimedia streaming over P2P network.

3.1 Problem Definition

P2P networks are widely used for multimedia streaming. Multimedia content providers found it suitable platform for their business. However, there are many considerations for successful streaming over such networks. Between sender and receiver nodes, there exists multiple intermediate nodes. In a distributed environment, there are many participating nodes with set of links. Such links may result as a spanning tree which is routed at the source of the stream being rendered over overlay. It comes under cooperative streaming. The content provider cannot deliver the streaming to end users directly. Instead, the streaming takes place with cooperative participation of multiple peers that come in between source and destination. In this context, there are many problems that may arise at runtime. First, arrival of new nodes and departure of existing nodes. This problem is known as churn problem. Due to churn, some links will fail and alternative links are to be chosen for consistent streaming. Second, there are chances of node failures. When a one of more nodes fail among participating nodes, it causes issues and alternative links are to be chosen. Third, there is problem with DoS attack that disturbs the network and participating nodes will not be able to help in streaming. The three problems identified are to be addressed in order to have quality in streaming multimedia content over P2P networks.

3.2 DoS Resilient - Optimal P2P Topology Construction Framework

We proposed a framework known as DoS Resilient - Optimal P2P Topology Construction (DR-OPTC) for solving aforementioned problems in multimedia streaming over P2P networks.

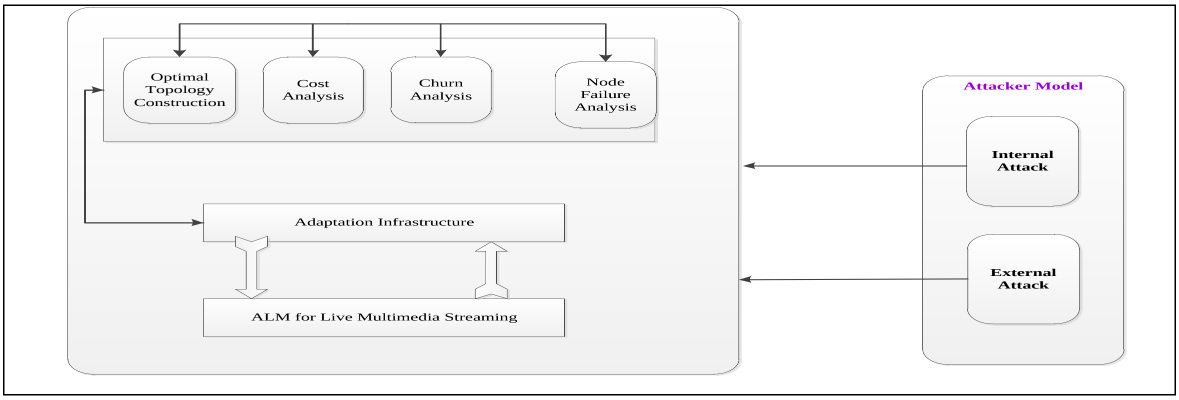

Figure 2: Overview of DR-OPTC framework

The framework enables P2P network to have optimal topologies that are DoS attack resilient. Besides the framework considers cost analysis, churn analysis and node failure analysis. The framework is adaptive in nature. It has different modules to ensure that the streaming quality is not deteriorated and there is DoS attack resilience. It is achieved by considering stable topologies that remain stable even in presence of DoS attacks, churn and node failures. Figure 2 provides an overview of the proposed framework. ALM for live multimedia streaming is the important application considered by the framework. The aim of the framework is to ensure DoS resilient streaming by dynamically building stable topologies. There is adaption infrastructure that closely monitors the ALM application. An attack model is considered with internal and external attacks. In presence of an efficient attack model, how the proposed framework caters to the needs of ALM application to have DoS resilient performance in video streaming is the important research carried out. Different modules available in the framework are cost analysis, churn analysis and node failure analysis. These three modules provide required knowhow to optimal topology construction module which in turn provides adaptation decisions to adaptation infrastructure. Thus adaptation infrastructure finally lets P2P network to have stable and optimized topologies to make the ALM attack resilient over overlay network.

3.3 Cost Analysis for Optimal Stable Topology Construction

Creating optimal and stable topologies of P2P networks is a tedious task. Optimal topologies exhibit three distinct characteristics. First, every node needs to forward data in P2P network in a single spanning tree. Second, source node can have number of direct and distinctive child nodes of source and all heads are maximized. Third, all heads can have number of successors and the difference cannot be more than 1.

Table 1: Shows the notations used in the paper

Parameter	Description
$fanout_{T_i}(v)$	The number of outgoing edges of node v in the spanning tree T_i
$c^+(v)$	The bandwidth capacity available for outgoing stripes
v	Node
T_i	Spanning tree
$succ_{T_i}(v)$	Amount of successors of node
$fanout_T(v,u)$	The number of stripes in which v directly forwards the stripe to u.
K	Total cost function

A distributed procedure is needed to have these properties realized. It is based on tree-first approach that exploits local knowhow. The aim of the distributed procedure is to balance topology in such a way that each node forwards in a single spanning tree. Assuming that the whole stream is split into k stripes and lead to k spanning trees to be created.

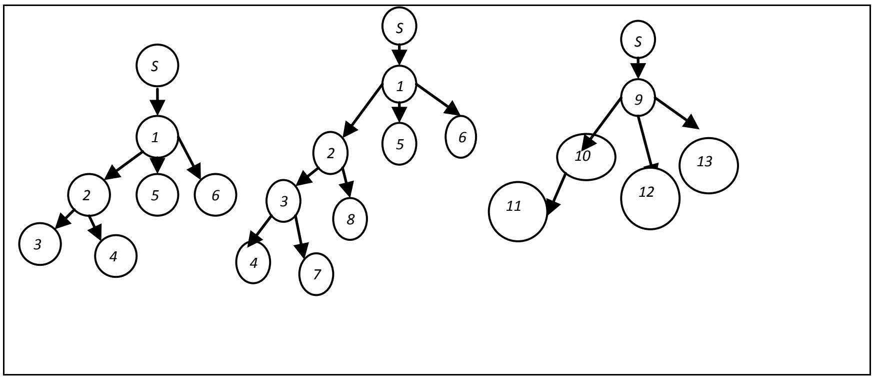

Figure 3: Shows three different stripes

As discussed earlier different stripes may lead to different spanning trees. When a node chooses a stripe to forward data, it has to determine it properly as there are bandwidth constraints. In order to have better optimization four cost functions are used as defined in [base paper]. The cost functions are named as K1, K2, K3 and K4 respectively. The first cost function is defined as in Eq. (1).

$$K_1(v,i) := 1 - \frac{fanout_{T_i}(v)}{c^+(v)} \qquad (1)$$

Every node selects the strip and forward to the most child nodes. We find out cost function of all nodes and find assign higher cost to most preferred stripe

$$K_2(v,w,i) := \{0, neighbor\ can\ forward\ in\ stripe\ i, 1, else \qquad (2)$$

Nodes can forward data in more than one spanning tree to avoid this problem, Eq.(2) is used. Nodes can forward data to only which stripe we select. The Eq. 3 shows that selected stripe path assigned to lower cost i.e.0, different stripe path assigned to higher cost i.e. 1.

$$K_3(v,w,i) := \frac{\left(\frac{succ_{T_i}(v)}{fanout_{T_i}(v)} - 1\right) - succ_{T_i}(w)}{\left(\frac{succ_{T_i}(v)}{fanout_{T_i}(v)} - 1\right)} \qquad (3)$$

In distributed environment we calculate cost function using above equation.

$$K_4(v,w) := \frac{fanout_T(v,u)}{K} \qquad (4)$$

In case a node has to forward data in more than one of the spanning trees, it is important that the direct dependency to each child node is kept to a minimum. In that case to find cost function Eq. 4 is used.

3.4 DoS Resilient Topology Construction (DRTC) Algorithm

This algorithm is meant for constructing optimal and stable topologies that are resilient against DoS attacks. It works in two important phases. First, it tries to minimize the cost of outgoing nodes. Towards this end, it makes use of total cost function K which has four individual cost functions as explained in Section 3.3. Thus parent nodes are capable of understanding the gain if dropping a link and thus balance tree. Balancing does mean making it more robust to DoS attacks and does not allow deterioration of video transmission quality. Second, parent node notifies children about the situation and help them to make steps with respect to successors. However, new node's arrival and departure of existing nodes (churn) will have effect on the network. Complete churn analysis is not in the scope of this paper as we defer it for future work.

Algorithm: DoS Resilient Topology Construction

Inputs: Node *v*, stripe *i*, child nodes of *v* in spanning tree ChT_i

Output: DoS resilient topology

```
initialize the link to drop dlink
initialize alternative parent altp
compute degree of v
i=preferred stripe
gain=true
while gain is true
gain=false
  find link which costs more using cost functions
find alternative link suitable
if new links bandwidth > threshold then
    drop the link and use alternative link
gain=true
  end if
end while
while degree of v< capacity of vdo
find alternative link
  use alternative link
  Increase degree by 1
end while
```

Algorithm 1:DoS Resilient Topology Construction Algorithm

As shown in Algorithm 1, two important functionalities are carried out. First, minimization of cost for all outgoing links is done. Towards this end the gain of dropping a link which costs highest is computed. As far as there is gain, the cost function is minimized by using alternative links. After completion of this, in the second phase, further exploration is made to reduce the levels of topology. Thus the proposed algorithm is able use cost functions described in section 3.3 to have optimal topology construction. The threshold used in the algorithm is the function of available bandwidth of the node which is not constant

4. RESULTS OF ANALYTICAL AND SIMULATION MODEL

This section presents results of the analytical model and simulation model. The analytical model is made mathematically based on the stripes considered for video streaming over P2P networks. The simulation model is where actual real time scenario is modelled and simulated. However, the 4 cost functions used are same for both models.

4.1 Results of Analytical Model

Considering stripe 1 shown in Figure 4 and the four cost functions, results are mathematically derived and presented here. The cost for each function 1.function 2, function 3 and function 4 is computed with equation (1), equation (2), equation (3) and equation (4) respectively. The cost function values for node1 to node 6 can be found table 2.

Table 2: Cost analysis for nodes in stripe 1

Node	K_1	K_2	K_3	K_4	TOTAL
Node1	0.96	2	-0.02	0.66	3.63
Node2	0.979	1	0	0	1.979
Node3	1	0	0	0	1
Node4	1	0	0	0	1
Node5	1	0	0	0	1
Node6	1	0	0	0	1

There are six nodes in stripe 1. For each node cost functions such as K1, K2, K3 and K4 are computed according to Eq. (1), Eq. (2), Eq. (3) and Eq. (4) respectively. The cost analysis results for stripe 1 are visualized in Figure 4.

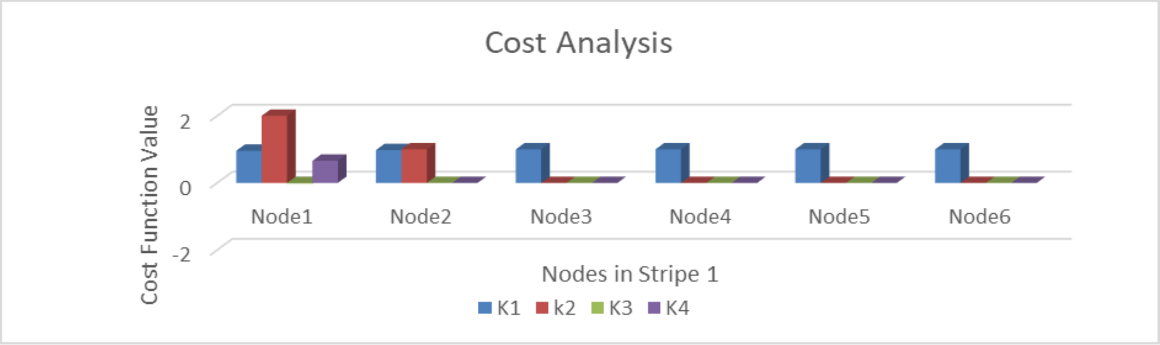

Figure 4: Results of cost analysis for Stripe 1

As presented in Figure 4, there are six nodes shown in horizontal axis. The vertical axis shows the cost function values. At each node of the stripe, four cost functions such as K1, K2, K3 and K4 are computed besides the total. Cost function 2 (K2) showed zero from node 3 to node 6. Similarly, cost function 3 (K3) values are in zeros for all nodes except node 1 which has a negative value -0.02. In case of cost function 4, the cost value of all nodes is zero except node 1.

Table 3: Cost analysis for nodes in stripe 2

Node No	K1	K2	K3	K4	Total
Node 1	0.98	1	0	1	2.98
Node 2	0.97	2	1.8	0.67	3.44
Node 3	1	0	0	0	1
Node 4	1	0	0	0	1
Node 5	0.97	1	2	0	3.97
Node 6	1	0	0	0	1
Node 7	1	0	0	0	1
Node 8	1	0	0	0	1

There are eight nodes in stripe 2. For each node cost functions such as K1, K2, K3 and K4 are computed according to Eq. (1), Eq. (2), Eq. (3) and Eq. (4) respectively. The cost analysis results for stripe1 are visualized in figure5.

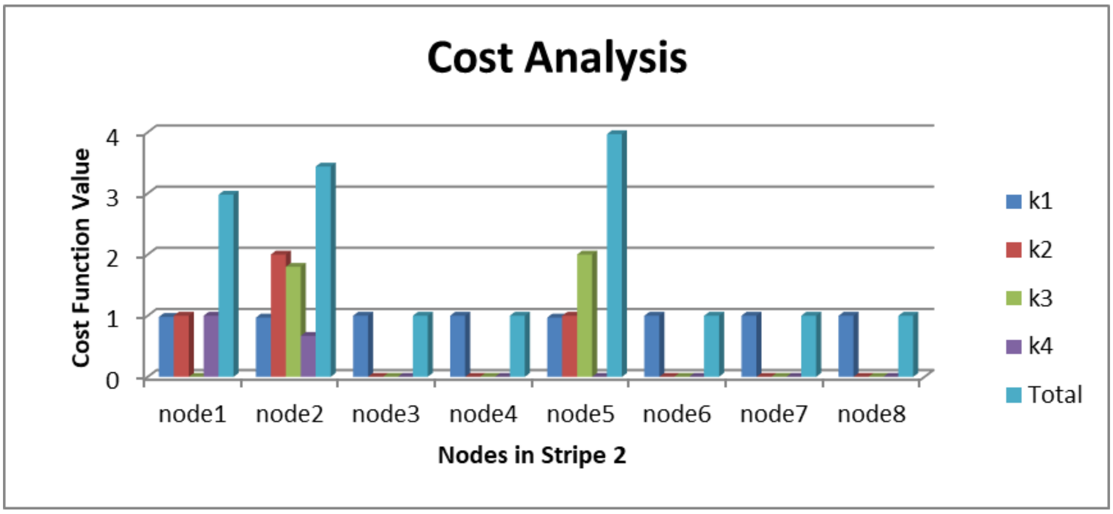

Figure 5: Results of cost analysis for Stripe 2

Table 4:Cost analysis for nodes in stripe3

Node	K1	K2	K3	K4	Total
Node9	0.97	1	0	0.67	2.64
Node10	0.96	1	2	0	3.96
Node11	1	0	0	0	1
Node12	1	0	0	0	1
Node13	1	0	0	0	1

As presented in Figure 5, there are eight nodes shown in horizontal axis. The vertical axis shows the cost function values. At each node of the stripe, four cost functions such as K1, K2, K3 and K4 are computed besides the total. Cost function 2 (K2) showed zero from node 3 to node 8 except at node 5. Similarly, cost function 3 (K3) values are in zeros for all nodes except node 2 and node 5. In case of cost function 4, the cost value of all nodes is zero except node 1 and node 2.

There are five nodes in stripe 3. For each node cost functions such as K1, K2, K3 and K4 are computed according to Eq. (1), Eq. (2), Eq. (3) and Eq. (4) respectively. The cost analysis results for stripe 2 are visualized in Figure 6.

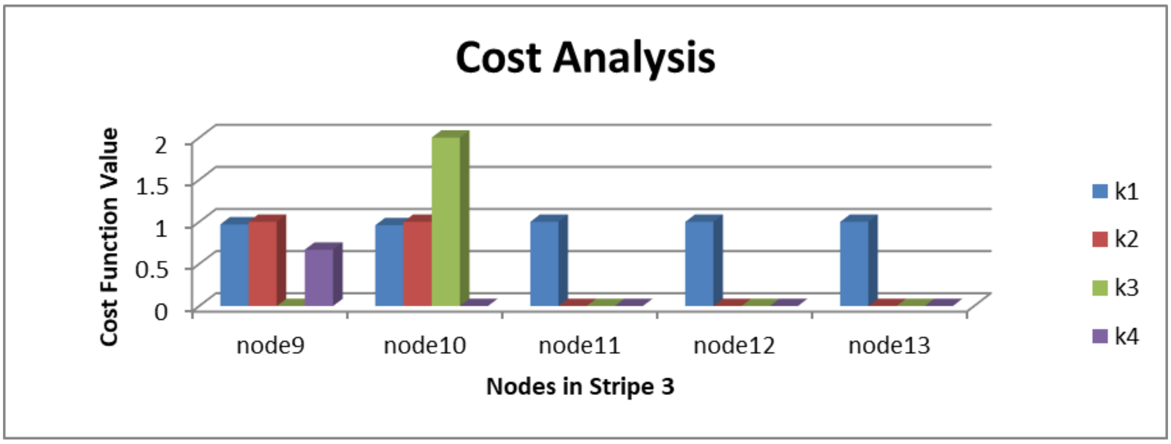

Figure 6: Results of cost analysis for Stripe 3

As presented in Figure 6, there are eight nodes shown in horizontal axis. The vertical axis shows the cost function values. At each node of the stripe, four cost functions such as K1, K2, K3 and K4 are computed. Cost function 2 (K2) showed zero from node 11 to node 13.Similarly, cost function 3 (K3) values are in zeros for all nodes except node 10. In case of cost function 4, the cost value of all nodes is zero except the node 1 and node 2.

4.2 Results of Simulation Model

NS-2 simulation is used to evaluate the proposed model. The environment used for the same is as in Table 4. The simulation setup is described here. A generator program is used to have optimal topologies for video streaming in overlay networks.

Then the cost based approach discussed in this paper is used in the simulation model in order to evaluate the approach. NS-2 is the discrete event simulator that is used to study the performance of the proposed framework.

Table 5:Simulation environment

Parameter Name	Parameter Value
Channel Type	Wireless Channel
Radio-Propagation	Propagation/TwoRayGround
Network Interface	WirelessPhy
Interface Queue Type	DropTail
Antenna Model	NS2
Interface Queue Length	50
Routing Protocol	DEXRSSMAC
No.of Nodes	35
rxPower	1.08918e-9
txPower	4.4613e-10 (250W)
RXThresh	1.4613e-10 (160m)
CPThresh_	10
CSThresh_	1.559e-11
RXThresh_	3.652e-10
CTSThreshold_	2000
RTSThreshold_	5000

As shown in Table 5, the simulation environment set for experiments using NS-2 is provided. Figure 7 shows an excerpt of the simulation made to demonstrate proof of the concept. The cost functions discussed in this paper in Section 3 are used to model the topologies and make observations. The results are captured and compared with that of analytical model.

The results of analytical model and simulation model nicely matched. The analysis is made with 3 stripes. The proposed framework in this paper is realized with regard to cost analysis and creating optimal and stable topologies in presence of DoS attacks. The reason behind using 4 different cost function is to have completeness in the estimation of cost. Choosing one or two cost functions shows bias towards cost computations. The cost analysis is made for each node in the given stripe. Thus at runtime, decisions are made to have optimal topologies that ensure video transmission without being affected by DoS attack. The implementation in this paper has limitations as the churn analysis and node failure analysis are deferred to our future work.

5. PERFORMANCE EVALUATION

Different ALM approaches are compared to evaluate the proposed approach. Greedy global attacks [1] is used for attack model. When such attack is made, it results in removal of some nodes. The fraction of removed nodes and the fraction of remaining packet reception are observed.

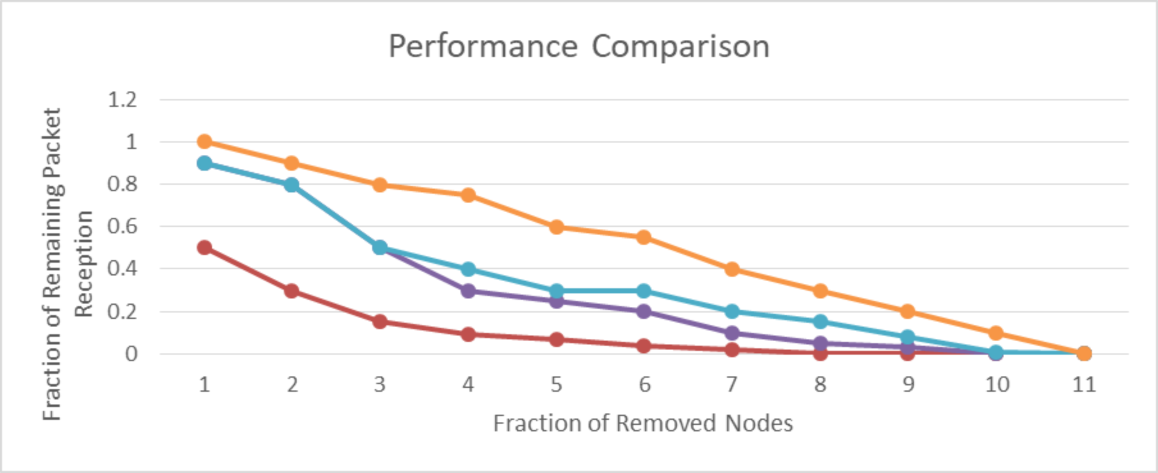

Figure 7:Performance comparison

As presented in Figure 7, the fraction of removed nodes is presented in horizontal axis while the vertical axis showed the fraction of remaining packet reception. The proposed method achieved better performance when compared with the previous methods such as Optimal, Stable and DAG . The rationale behind this is that the proposed method uses 4 cost functions in order to have more stable and optimal topologies.

6. CONCLUSION AND FUTURE WORK

Application layer multicast overlay P2P network is modelled and characterized with graph theoretic model. The nodes between source of multimedia content dissemination and the destination nodes are considered to have strips or spanning trees. It is understood that the data transfer takes place from source to destination through a single spanning tree. In presence of DoS attacks, the data transfer will result in packet loss and delay in transmission. These problems are overcome by proposing a framework that has infrastructure for adaptation with the help of different mechanisms like content analysis and optimal topology construction. The stable and optimal topology construction is made by computing cost functions. In each stripe where data is travelled, 4 cost functions are used to have unbiased estimation of the cost. Based on the cost, dynamic topology construction is made possible. Thus in presence of DoS attack, the dynamically constructed optimal topology will be resilient to the effects of such attacks. This will help to ensure QoS in multimedia streaming over P2P overlay networks. An algorithm named DoS Resilient Topology Construction (DRTC) is proposed to construct optimally stable topologies. The analytical model is evaluated with simulations made using NS-2. The results revealed that the simulation model nicely matched with the analytical model. However, the proposed framework is not yet fully realized. The present implementation has two drawbacks. First, it has not considered large churn rate which will help improve the stability of P2P topologies. Second, it has not explored the condition where large number of nodes fail in the path of video transmission over P2P network. In future, therefore, we focus on the churn analysis and node failure analysis modules of the DR-OPTC framework for leveraging resiliency against DoS attacks further.

REFERENCES

1. Michael Brinkmeier et al. (2009). Optimally DoSResistant P2P Topologies for Live Multimedia Streaming. Ieee Transactions On Parallel And Distributed Systems, p1-14.
2. KatsuyaSuto et al (2013). THUP: A P2P Network Robust to Churn and DoS Attack based on Bimodal Degree Distribution. IEEE, p1-11.
3. Maximilian Drees et al. (2016). Churn- and DoS-resistant Overlay Networks Based on Network Reconfiguration. ACM, p1-11.
4. Tara Small et al. (2006). Scaling Laws and Tradeoffs in Peer-to-Peer Live Multimedia Streaming. ACM, p1-10.
5. K. Suganya et al. (2016). Adaptive Packet Transmission in Smart Grid to Minimize the Message Delay. International Journal of Computer Science and Engineering Communications, 4 (2), p1393-1396.
6. Kai Wang et al. (2012). Content-Centric Networking: Effect of Content Caching on Mitigating DoS Attack. IJCSI International Journal of Computer Science Issues, 9 (6), p43-52.
7. Michael Brinkmeier et al. (2009). Towards the design of un exploitable construction mechanisms for multiple-tree based P2P streaming systems, p1-12.
8. B. Lalitha et al. (2013). Security and QOS centric protocols for P2P networks: current state of the art. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET). 2 (2013), p1055-1064.
9. KatsuyaSuto et al. (2014). An Overlay Network Construction Technique for Minimizing the Impact of Physical Network Disruption in Cloud Storage Systems. IEEE, p1-6.
10. Nikita Borisov et al. (2006). Computational Puzzles as Sybil Defences, p1-7.
11. Giang Nguyen et al. (2015). RBCS: A Resilient Backbone Construction Scheme for Hybrid Peer-to-Peer Streaming. 40th Annual IEEE Conference on Local Computer Networks, p261-269.
12. Michael Rossberg et al. (2012). Analyzing and Improving the Resistance of Overlays against Bandwidth Exhaustion Attacks. IEEE, p1-8.

13. J. JAYASANTHI et al. (2014). Exigent Life from Wireless ad-hoc Signal Networks. International Journal Of Computer Engineering In Research Trends, 1 (6), p 397-404.

14. Michael Rossberg et al. (2012). A Survey on Automatic Configuration of Virtual Private Networks, p1-16.

15. Kaushik Adhikary et al. (2011). Survey on Architecture of Peer-to-Peer Network. Int.J.Comp.Tech.App. 2 (6), p3089-3096.

16. Naohisa Ohta et al. (2013). Emerging Technologies in Communications. IEEE Journal On Selected Areas In Communications/Supplement. 31 (9), p1-5.

17. D. Dumitriu, et al. (2005). Denial-of-Service Resilience in Peer-to-Peer File Sharing Systems. ACM, p38-49.

18. Christian Scheideler et al. (2018). Relays: A New Approach for the Finite Departure Problem in Overlay Networks, p1-30.

19. Sebastian Jeckel et al. (2009). Benchmarking of P2P Technologies from a SCADA Systems Protection Perspective, p1-54.

20. Hung-Yi Teng et al. (2014). A self-similar super-peer overlay construction scheme for super large-scale P2P applications. InfSystFront, p45–58.

21. Bo Zhu et al. (2006). Providing Witness Anonymity in Peer-to-Peer Systems. ACM, p6-16.

22. W. Sabrina Lin et al. (2009). Incentive Cooperation Strategies for Peer-to-Peer Live Multimedia Streaming Social Networks. IEEE Transactions On Multimedia. 11 (3), p396-412.

23. Michael Brinkmeier et al. (2007). A Class of Optimal Stable P2P-Topologies for Multimedia-Streaming, p1-9.

24. Jânio M. Monteiro et al. (2014). Peer-to-Peer Video Streaming, p1-3.

25. Srikanth T.N. et al. (2012). Explicit Study On Security Issues in Multimedia Streaming in Peer to Peer Network. International Journal of Computer Engineering and Technology (IJCET), 3 (2), p588-602.

26. W. Sabrina Lin et al. (2009). Incentive Cooperation Strategies for Peer-to-Peer Live Multimedia Streaming Social Networks. IEEE Transactions On Multimedia. 11 (3), p396-412.

27. Sabu M. Thampi et al. (2013). A Review on P2P Video Streaming, p1-47.

28. Bo Li et al. (2007). Peer-to-Peer Live Video Streaming on the Internet: Issues, Existing Approaches, and Challenges. IEEE Communications Magazine, p94-99.

29. Xiaofei Liao et al. (2006). AnySee: Peer-to-Peer Live Streaming. IEEE, p1-10.

30. Tara Small et al. (2006). Scaling Laws and Tradeoffs in Peer-to-Peer Live Multimedia Streaming. ACM, p1-10.