An Exploration of Monetary Based Approach (MBA) in Peer-to-peer system Network: A Review

[1] Dr. Faiyaz Ahmad, Assistant Professor, Integral University

[2] Durba Das Gupta, M. Tech. in Computer Science and Engineering, Integral University

Abstract
The major concept of the Monetary Based Approach (MBA) network uses the Label Switch Path (LSP) technique that pro- vides high performance in packet delivery without routing table lookup. Nevertheless, it needs more overhead to rebuild a new path when occurring link failure in the MBA network. MBA (Monetary Based Approach) networks are currently evolving towards a universal and convergent network, capable of flowing multiservice traffic (voice, data and video) over the same IP based infrastructure. Quality of Service (QoS) is more and more becoming a necessity for emerging applications carried by MBA networks. This fact stimulates service providers to improve network planning techniques to adequately provide network resources and overcome all failures. The paper presents typical network failures, which cause path recovery in MBA networks and experimental results of network failures, when MBA is used.

Keyword: Monetary Based Approach (MBA), Label Switch Path (LSP), Quality of Service (QoS)

1. Introduction

The use of Peer-to-peer system has increased at a staggering rate in the last few years because of there is usefulness in the field of sharing like processing power, disk storage or network bandwidth. The main of theses system is that it is directly available to all the users (Peers) without any intermediate medium. But it also has some threat viz. Free-riding, which degrades the performance of the Peer-to-peer system.

MBA (Monetary Based Approach) [14] is being used in many corporate networks and public infrastructures and as a backbone technology of many Autonomous Systems. This is a connection-oriented technology that arises to palliate the problems that current networks have related to speed, scalability and traffic engineering. Most of the time MBA is considered on top of transport networks (SDH or WDM depending on required link speed) [15]. In fact, MBA packets forwarding is based on labels and not in the analysis of encapsulated data from upper levels. It is a multi-protocol technology that supports any network protocol as well as any technology in lower layers (link or physical). MBA is used as a traffic engineering tool [16] to direct traffic in a network in a more efficient way then original IP shortest path routing. Path in the network can be reserved for traffic that is sensitive, and links and router that are more secure and not known to fail can be used for this kind of traffic. However, the question arises whether it is suitable to have MBA nodes just at the edge of the network to collect packet traffic from users, or to introduce also MBA facilities on a subset of the core nodes in order to exploit packet switching flexibility and multiplexing, thus inducing a better bandwidth allocation.

Network requirements in all networks can be separated into components, based on their environment and what is wanted to accomplish with this network architecture. End-to-end characteristics are measured across multiple network devices in the path of one or more traffic flows, and may be extended across the entire network. But MBA recovery provides different levels of service, based on their service requirements. It should give the flexibility to select the recovery mechanism, choose the granularity at which traffic is protected and choose the specific types of traffic that are protected in order to give operations more control over that trade-off. The recovery of the MBA network is based on the algorithm that is applied in order to detect the faults and to route the data flow in an alternative path. MBA recovery may be motivated by the notion that there are limitations to improving the recovery times of current routing algorithms. For a MBA based backbone network, the fault-tolerant issue focuses on how to protect the traffic of a label switched paths (LSP) against node and link failures. In IETF, two well-known recovery mechanisms (protection switching and rerouting) have been proposed, but many researchers create every year some better suggestions, but they have different advantages and disadvantages. All of the models can protect a working path end-to-end in one MBA domain, but there is no protection for node failures on the ingress or egress label switching router (LSR).

Multiprotocol Label Switching (MBA) is the backbone network for IP domain and it is the new fastest growing communication network to enhance the speed, scalability of network. MBA network has feature is that it supports traffic engineering tunnels by avoiding congestion and utilizing all the available network bandwidth with an efficient way. The main functionality of Traffic Engineering of MBA network [17] is resource reservation, fault-tolerance and optimal Resource's utilization. Multiprotocol Label Switching technology (MBA) allows traffic engineering (TE) and enhances the performance of the existing protocols over the traditional IPv4 network. It is foreseen that MBA will be chosen as the bearer of IP network in future large backbone networks. The main focus of MBA network is to attach a short fixed-length label to packets at the ingress router of the MBA domain. The packet forwarding in network depends on the tagged label, not on longest address match, as in traditional IP forwarding. A router or nodes placed on the edge of the MBA network called Label Edge Router (LER) that is associated to a label on the basis of a Forwarding Equivalence Class (FEC). In the MBA network, internal routers that perform swapping and label-based packet forwarding are called Label Switching Routers (LSRs) [18].

Free-riding Effects

P2P networks vary in their architecture and application domain, but one thing they all have in common is that files are transferred directly between peers. By default, when these files are delivered, the user becomes a contributor [3]. In an ideal world, P2P networks provide information to all members, and single-user consumption does not reduce network download capacity.

Applying public goods theory to P2P networks yields two very interesting results. First, free-riding is rampant in P2P networks. Users can choose to share or not share downloaded files. This feature helps them save bandwidth.

The second observed feature of P2P networks is their persistence despite high levels of free-riding.

These facts raise a lot of research questions. Can P2P networks survive high levels of free-riding? Second, does free-riding reduce the network's utility to its peers? Undeniably, economic incentives can improve network performance.

The model shows that P2P networks can withstand free-riding issues. Moreover, the model predicts that without external incentives, free-riding will exceed socially optimal levels. A network operator can achieve a socially optimal outcome by differentiating the quality of service provided to sharers and non-sharers. Before examining various anti-free-riding strategies, let us consider two common P2P scenarios.

Assume that out of N peers, the majority are free riders. All files in the system are shared by a few users. Assume a P2P system has 2000 files, of which one peer Pi has contributed 1000. The 1000 files contributed by other users are the system's utility to peer Pi. Pi will lose interest in the system if no new files are added after he downloads some of these 1000 files. His withdrawal would mean the loss of all his files. The system then loses a lot of files. As a result, the system will crumble.

This issue has another facet. Consider N peers, Nf of whom have uploaded files for sharing. Let the system download R requests per second. So, each Nf peer must serve R/Nf requests per unit time. If Nf is small, each Nf peer must serve many requests. This may cause network overload. This may cause users to leave the system to avoid frequent congestion.

Consider the second scenario, where all users share the same file count. Since Nf =N, each peer can only serve a small number of requests at a time. This will alleviate network congestion. In an equal sharing environment with M files, each peer would have (M-N/M) files that he could download. Thus, each node has nearly the same number of unowned files. Thus, free riding reduces the lifespan and evolution of P2P file-sharing systems.

2. Background

Xu et al. (2010) multi-domain networking is an important focus area and crank back signaling strategies offer much potential for post-fault recovery. However, most studies in this space have not addressed multi-failure scenarios, e.g., correlated failures such as those resulting from weapons of mass destruction attacks. Hence this paper proposes a novel solution for intra/inter-domain post-fault crank back restoration in IP/MBA networks (also extendible to optical DWDM networks). Specifically, inter-domain path/distance-vector routing state information is integrated with dynamic node/link failure and intra-domain link-state information to improve the recovery process. The performance of the proposed solution is then analyzed for a range of multi-failure scenarios. This paper proposes novel crank back solution for postfault restoration in large multi-domain backbone networks under multiple failures, i.e., WMD-type attacks. The scheme uses an enhanced next-hop domain selection strategy and incorporates full crank back history tracking to improve the effectiveness of the recovery process. In addition, a dual crank back counter approach is introduced to limit the number of intra/inter-domain retry attempts and both end-to-end and intermediate restoration modes are supported. The detailed performance results show very high post-fault recovery rates for correlated failure events with varying severity levels, particularly for E2E crank back. Future studies will look at extending this work with analytical modeling of restoration behaviors as well as integration with protection strategies.

Capone et al. (2015) The proposed mechanism is based on Open State, an OpenFlow extension that allows a programmer to specify how forwarding rules should autonomously adapt in a stateful fashion, reducing the need to rely on remote controllers. They present the scheme as well as two different formulations for the computation of backup paths. In this paper they have presented a new failure management framework for SDN and a mathematical modeling approach specifically designed to exploit the capabilities of Open State. The framework considers both single link and single node failure. The protection scheme is based on the idea that, upon failure detection, packets can be tagged and backtracked along the primary path to signal the failure to the first convenient reroute node, automatically establishing a detour path. Such scheme aims at having zero packet loss after failure detection, and doesn't require controller intervention. The models were tested on three well-known topologies and comparative results were obtained, showing the superiority of the scheme with respect to a classic end-to-end path protection scheme and with respect to an approach based on the OpenFlow fast-failover mechanism. They are currently working on the dimensioning problem and developing the Open State application to experimentally validate the proposed solution.

Almandhari & Shiginah (2015) Monetary Based Approach (MBA), which was introduced by Internet Engineering Task Force (IETF), is widely used in communication networks to provide QoS guaranties to traffic. In this connection-oriented protocol, network failures can cause a serious disruption to critical data traffic which is unacceptable for customers who require highly reliable services. To guarantee high QoS and enhance network performance during failures, researchers have developed different recovery mechanisms for MBA to ensure rerouting traffic from original faulty paths to alternate paths. In this paper, a comprehensive study is carried out on MBA recovery mechanisms for protecting and restoring traffic after failure occurrence. In order to model the recovery mechanisms in MBA networks, a new modeling framework for MBA recovery was developed on a multi-layer approach. The new framework was designed to be generic and flexible in order to easily model network topologies with different MBA recovery mechanisms and simulate variable parameters/scenarios for performance analysis purposes. Multiprotocol Label Switching (MBA) recovery mechanisms aim to restore traffic during network failures and provide a high delivery performance. This work has focused on the performance evaluation of MBA recovery mechanisms by developing a new generic modeling framework as a layered approach on top of OMNeT++ simulation tool. The proposed framework had been tested in order to validate the response of the four recovery models namely: Best Effort, Makam, Local Rerouting and Fast Reroute. The tests concluded that the newly introduced framework is able to model the MBA recovery mechanisms (i.e., the selected mechanisms as well as the ones to be added in the future) on any network topology with a node/link failure.

Attar et al. (2018) The optimal load distribution over a set of independent paths for Monetary Based Approach for Traffic Engineering (MBA -TE) networks is regarded as important issue; accordingly, this paper has developed a mathematical method of optimal procedures for choosing the shortest path. As a criterion for choosing the number of paths, a composite criterion is used that takes into account several parameters such as total path capacity and maximum path delay. The mathematical analysis of using the developed method is carried out, and the simulation results show that there are a limited number of the most significant routes that can maximize the composite quality of service indicator, which depends on the network connectivity and the amount of the traffic. The developed technological proposals allow increasing the utilization factor of the network by 20%.

Hanshi & Al-Khateeb (2010) MBA recovery mechanisms are increasing in popularity because they can guarantee fast restoration and high QoS assurance. In fact, QoS is important for interactive voice and video application and for specific clients. However, link failure always incurs delay and packet losses of the traffic passing through the failed link. Therefore, network has to restore the traffic by switching the affected traffic to alternative path. In this paper, QoS objectives are concerned in this study to redirect the protected traffic with acceptable levels of quality before failure take place. The proposed scheme setup more than one alternative path in advance in order to introduce fast rerouting and the selecting criteria is based on the required bandwidth and end-to-end delay. In this work, they proposed the traffic splitter to split the protected traffic after failure, in case the available bandwidth in the alternative path is not enough to deliver the traffic. Finally, alternative path selection is updated based on current network resource availability. To verify the efficiency of the proposed algorithm, the MBA network simulator MNS-2 has been used as the test platform. In this study, the network has to restore the traffic by switching the affected traffic to another path. Therefore, QoS objectives are concerned in a recovery scheme to redirect the protected traffic with the same quality as before failure takes place. To support high quality service, several parameters must be guaranteed, such as bandwidth, fast rerouting mechanisms and rerouting should be based on updated information of network. The proposed QoS scheme is used to serve the traffic based on information of network resources; therefore, alternative path decisions will be made according to changes in the current network resources availability at failure time. The proposed protection scheme introduces a significant contribution in the field of recovery schemes in terms of alternative path decision parameters and the rerouting method.

Hassan et al. (2011) Failure of backbone nodes/links can have catastrophic consequences unless they are addressed in a timely manner. Monetary Based Approach, is an increasingly popular technology that employs various recovery mechanisms from such failures. In addition to failure recovery these mechanisms minimize downtime, data loss and convergence time while also avoiding inefficient bandwidth utilization. The aim of this survey paper is to provide an overview of the recovery and bandwidth sharing techniques used by MBA. They discuss the recovery mechanisms, as well as merits and demerits, of global and local recovery. They also present the bandwidth sharing potential of each recovery technique and discuss different protocols proposed for bandwidth sharing. Their work will be valuable to networking researchers who want to get an insight into the operation mechanism, as well as design tradeoffs, of various MBA recovery techniques.

Ridwan et al. (2019) Multiprotocol label switching (MBA) networks are packet-based networks that offer considerable advantages, including improved network utilization, reduced network latency, and the ability to meet the quality of service and strict level agreement requirements of any incoming traffic. A vast number of applications are now migrating to packet-based conditions that cause increased pressure on network providers to change their systems. Innovations and improvements on MBA are still on going to ensure that such networks can cater to the ever-increasing bandwidth demand whenever required. This study provides a review of MBA networks and their promising technologies, such as traffic engineering, protection and restoration, differentiated services, and MBA -transport profile (MBA -TP) and its applications. This work also reviews recent issues on MBA networks and discusses the implementation of MBA -TP networks in the power grid. A review of recent literature shows that researchers should be careful in proposing new protocols or designs for MBA to ensure that it achieves the most efficient and optimal performance. Furthermore, they can conclude that although MBA is a promising technology for future networks, there are challenges to overcome with regards to security and network flexibility, especially as far as migration to MBA -TP is concerned.

Karakus & Durresi (2019) Failures are inevitable in an operational network. They can happen anytime in different sizes and components of a network. They impact the network economics regarding CAPEX (Capital Expenditure), OPEX (Operational Expenditure), revenue lost due to service provisioning cut and so on. In order to mitigate the damages resulting from these failures, reactions of network architectures and designs are crucial for the future of the network. Recently, Software Defined Networking (SDN) has got the attention of researchers from both academia and industry as a means in order to increase network availability and reliability due to features, such as centralized automated control and global network view, it promises in networking. To this end, they explore the effects of programmable network architectures, i.e., SDN technology, and traditional network architectures, i.e., MBA (Multiprotocol Label Switching) technology, on network economics by exploiting Number of Satisfied Service Requests and their predefined Unit Service Cost Scalability metrics under network failure scenarios: i) a random single data plane link failure and ii) a random controller (i.e. control plane) failure. To the best of their knowledge, this study is the first to consider a comparison of a programmable network architecture, i.e., SDN, along with different control plane models, Centralized (Single) Control Plane (CCP), Distributed (Flat) Control Plane (DCP), and Hierarchical Control Plane (HCP), and a non-programmable network architecture, i.e. MBA, regarding network economics in case of network failures.

Li & Liang (2011) This paper puts forward a model of path fault recovery of MBA VPN, which is DR-PFR (Double Recovery-Path Fault Recovery), for the failure on the path of MBA VPN. DR-PFR can solve the failures in both the working path and the backup path. Experiments show that under the condition of using the resources effectively, when the network fails, DR-PFR can enable the network recover timely and effectively reduce the impacts on users. DR-PFR model makes MBA VPN more robust. If the working path fails, on account of local backup path, data loss rate is lower than global recovery; when both the working path and the local backup path fail, the model can still ensure that the network recovers promptly.

Lin, J. W., & Liu, H. Y. (2010) To provide a reliable backbone network, fault tolerance should be considered in the network design. For a multiprotocol label switching (MBA) based backbone network, the fault-tolerant issue focuses on how to protect the traffic of a label switched paths (LSP) against node and link failures. In IETF, two well-known recovery mechanisms (protection switching and rerouting) have been proposed. To further enhance the fault-tolerant performance of the two recovery mechanisms, the proposed approach utilizes the failure free LSPs to transmit the traffic of the failed LSP (the affected traffic). To avoid affecting the original traffic of each failure-free LSP, the proposed approach applies the solution of the minimum cost flow to determine the amount of affected traffic to be transmitted by each failure-free LSP. For transmitting the affected traffic along a failure-free working LSP, IP tunneling technique is used. They also propose a permission token scheme to solve the packet disorder problem. Finally, simulation experiments are performed to show the effectiveness of the proposed approach.

Qiu et al. (2010) Researching on use of new real-time connection-oriented services like streaming technologies and mission critical transaction-oriented services and more reliable network become inevitable trends presently. MBA is a next generation backbone architecture; it can speed up packet forwarding to destination by label switching. However, if there exists no backup LSP when the primary LSP fails, MBA frames cannot be forwarded to destination. Therefore, fault recovery has become an important research area in MBA Traffic Engineering. At present, two famous methods, Makam and Haskin are belonging to Protection Switching, and other methods basically come into being on base of them. But these two famous methods both have its disadvantage. In order to solve their drawback, the thesis tries to do some exploration on the MBA -based recovery model. This new model in the thesis using the Reverse Backup Path to solve the wrapping of data back to the path is too long, and using the simulation tool NS-2 to do some experiments. Finally, the simulation experiments show that new method of MBA -based recovery has less packet disorder and much lower delay and packet losses than the two famous methods.

Cascone et al. (2017) When dealing with node or link failures in Software- Defined Networking (SDN), the network capability to establish an alternative path depends on controller reachability and on the round-trip times (RTTs) between controller and involved switches. Moreover, current SDN data plane abstractions for failure detection, such as OpenFlow "Fast-failover", do not allow programmers to tweak switches' detection mechanism, thus leaving SDN operators relying on proprietary management interfaces (when available) to achieve guaranteed detection and recovery delays. They propose SPIDER, an Open Flow-like pipeline design that provides i) a detection mechanism based on switches' periodic link probing and ii) fast reroute of traffic flows even in the case of distant failures, regardless of controller availability. SPIDER is based on stateful data plane abstractions such as OpenState or P4, and it offers guaranteed short (few milliseconds or less) failure detection and recovery delays, with a configurable tradeoff between overhead and failover responsiveness. They present here the SPIDER pipeline design, behavioral model, and analysis on flow tables' memory impact. They also implemented and experimentally validated SPIDER using OpenState (an OpenFlow 1.3 extension for stateful packet processing) and P4, showing numerical results on its performance in terms of recovery latency and packet loss.

Wang et al. (2019) Link failure is a major problem that must be addressed, which occurs frequently in large networks. In a software-defined network, the recovery scheme for single link failure can be divided into two categories: proactive and reactive. For reactive scheme, it takes a long time to recover due to the controller participation. Though the proactive scheme can achieve faster recovery, it may consume a large number of forwarding rules, which is typically limited on switches due to expensiveness and power hungry. Therefore, this paper proposes a proactive recovery scheme for single link failure based on segment routing with less forwarding rules. In the proposed scheme, they regard the affected flows through the same link as an aggregated flow and use the link protection methods to achieve link failures recovery. The link protection methods calculate backup paths for each link of the working path, so they propose the backup paths calculation problem and formulate it as a mixed integer non-linear programming model. To solve the problem and avoid link congestion, they design an efficient algorithm to select the most appropriate backup path. In addition, due to the limitation of the maximal number of MBA labels that the packet header can hold, they design an algorithm to divide the working and backup path into segments to meet the hardware requirements. The simulation results show that the proposed algorithms outperform CAFFE and SPR by 14.7% and 77.1% on recovery time, and outperform CAFFE by 21.5% on forwarding rules consumption. Moreover, the proposed scheme does not cause congestion in post-recovery network.

3. Structured P2P systems: In these systems, overlay connections are fixed. It uses distributed hash table-based indexing. Examples of systems which support distributed hash table functions are: -Tapestry, Pastry, Chord and Content Address Network. In these systems, contents are stored and retrieved according to strict rules. The current Node ID and content name of each node is hashed to a key. Content is stored in the node whose key is closest to the content key and query routing processes forward queries to neighboring nodes whose keys are closer to the query object keys.

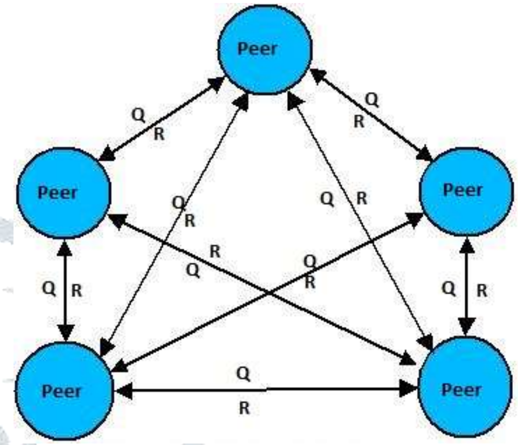

Fig. 1: Peer to peer network

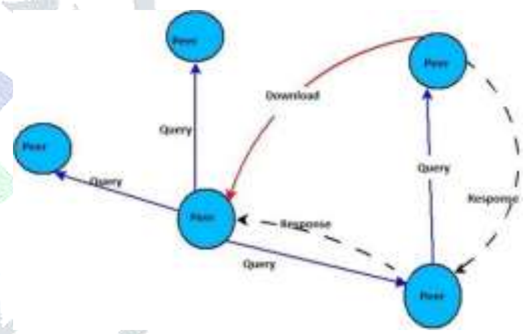

Fig. 2: Deentralized P2P Network

Figure 1: MBA Architecture [21]

Free-riding Problem in P2P network

The Free-Riding problem affects the system in two ways. Firstly, it affects the growth of files in the system. The number of popular files becomes smaller by the day. This, consequently, affects the user's interest in system and eventually he pulls out of the system. When popular file sharers pull out of the system, it becomes poorer in terms of number of files shared. It may eventually lead to the collapse of the system. Secondly, if the number of file sharers is limited, all the downloading requests are directed towards them. This causes overloading of these peers and congestion of the networks. Peers experiencing frequent congestion may eventually pull out of the system.

In game theoretic terms, it is a dominant strategy for users to download without any contribution to the system. As a result, all individuals can reason in this way and free ride on the contribution of other 'benevolent users', ultimately resulting in overall system performance degradation and making everyone a loser, a situation referred to as the "tragedy of the digital commons". The prevalence of free-riding problem in P2P systems can be attributed to specific characteristics viz. decentralization, high churn rate (users joining and leaving the system), availability of cheap identities (pseudonyms), hidden actions and collusion (groups to maximize benefits).

2.2 Impact of Free-riding

P2P networks vary in their architectural designing and application domain but the one thing common in all P2P networks is that files are transferred directly between the peers connected to the network. Also, as these files are delivered, the user becomes a contributor of that file by default [3]. In the ideal case, P2P networks will provide information to all members of the network and consumption by one user does not decrease network downloading possibilities in the absence of free-riding.

If we apply the public goods literature to P2P networks, we can make two very interesting observations. First, researchers have observed high levels of free-riding in P2P networks. Users have the option to either share the downloaded files or not. This feature helps them to economize on their own private allocation of bandwidth.

The second observed characteristics of P2P networks are that they appear to persist in spite of high levels of free-riding.

These facts tend to raise many empirical research questions. First, can P2P networks persist in spite of high levels of free-riding? Second, how much does free-riding reduce the utility of the network to its peers? And third, can network designers improve network performance by using economic incentives.

The analytical model shows that P2P networks can weather the free-riding problems. Also at the same time, the model shows that in the absence of external incentives, the level of free-riding will be above the socially optimal levels. Finally, the model shows that by differentiating the quality of service provided to sharers and non-sharers, network operators can achieve the socially optimal network outcome.

Before taking a look at the various schemes of combating the free-riding problem, let us take a look at two different scenarios prevalent in P2P systems.

In the first scenario, let us consider that out of a total of N peers, majority are free riders. All the files available in the system are shared by a small number of users. Suppose in a P2P system there are 2000 files, out of which a single peer Pi has contributed 1000 files. Here, the utility of the system to peer Pi is the 1000 files that are being contributed by other users. After Pi downloads some of these 1000 files, he will start losing interest in the system as no new files are being added and he is likely to withdraw from the system. His withdrawal would lead to loss of all the files owned by him. The system then becomes poorer in terms of number of files by a large amount. Consequently, it will lead to the downfall of the whole system.

There is another dimension to this problem. For this let us consider N peers and out of them Nf have uploaded some files for sharing. Let there be R downloading requests per unit time for the system. Then each of the Nf peers would have to serve R/Nf requests per unit time. If N_f is small, then each of these Nf peers would have to serve a large number of requests. This may cause overloading and network congestion. This may prompt the users to leave the system in order to protect themselves from frequent congestions.

Now, consider the second scenario where all users share equal number of files. Here, N_f =N, so each peer will have to serve only a small number of requests at a time. This will take care of the problem of network congestion and overloading. Also, if there are M files in such an equal sharing environment, each peer would have (M-N/M) files not owned by him, which the peer might be interested in downloading. In this scenario, each node will have almost equal number of un-owned files. Therefore, it can be concluded that free riding has a negative impact on the lifetime and evolution of P2P file-sharing systems.

Approaches to combat free-riding

Most of the P2P systems lack effective mechanism to provide cooperation among the peers. This results in the free-riding problem. To address this problem many approaches have been proposed to make P2P networks" contribution-aware" and thus combat free-riding. The study of these approaches makes our mind to think about how to control the behavior of free-riding in the network. The approaches proposed can be categorized into four main groups [4]:

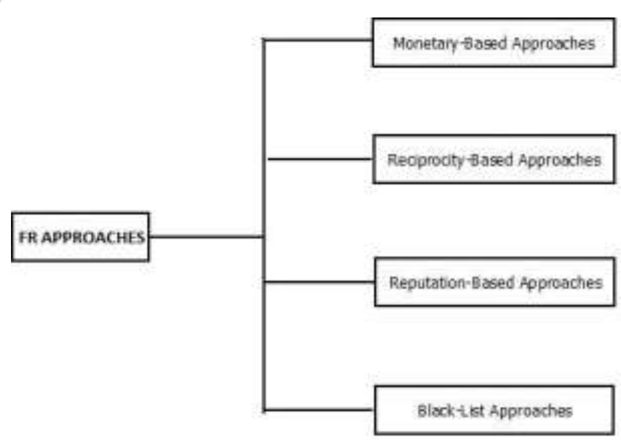

Fig. 5: Free Riding Approaches

Monetary Based Approach

As the name suggests, this approach is based on charging peers for the services they receive. This approach is also called micropayment-based solution, because the services are provided at a very low cost. This system has two basic components: an accounting module to securely store the peers' virtual currency and a settlement module to exchange virtual currency for services. These components are implemented by centralizing their functions within a single authority, which manages each peer's balance and transactions by tracking accounts and distributing and cashing virtual currency.

Most of the proposed solutions use Public Key Infrastructure (PKI) to protect from frauds and errors. Since these system deals with only micro payments, the security mechanisms must also be lightweight. Most monetary-based systems do not guarantee a totally safe exchange of goods and payments. But they require only "good enough" security mechanisms in which fraud is detectable, traceable and unprofitable while preserving high efficiency.

The monetary-based system can be implemented in two ways: online payment and offline payment. In online payment system virtual currency exchange and services occur simultaneously. To implement this, the central authority must be online at the time of transaction. This solution prevents most frauds.

In offline system, P2P system can exchange currency after the services have been received whenever the central authority is present. This requires user to use permanent identification. The problem here is that since the payment is offline, the P2P system will not be able to ascertain whether the coin is fraud or not.

Researchers tend to favor the offline payment because of its lower computational and communication costs and lower latency. Some examples of monetary-based approaches are PPAY and online and offline Karma.

The various limitations of Monetary based approaches are: -

Centralization and communication overhead: The solutions require some centralized authority to track every peer's balance and transactions. This causes scalability and single point failure problem. Also, distributing virtual currencies, managing transactions and applying auditing mechanisms increases the communication overhead of the network.

Persistent Identifiers: The P2P systems require persistent user identifiers to store peer balances and monitor transactions. But this is complicated by users anonymity, wide range and ease of identity spoofing.

Mental transaction costs: Since this a micro-payment system, the user has to decide before each service whether it is worth the expenditure or not, leading to confusion and mental decision costs.

4. Conclusion

With more applications requiring different QoS treatments on the same core network, MBA in P2P networks is a promising solution. MBA is one of the best technologies for dynamically managing traffic with varying SLA requirements and quickly resolving issues so that consumers can continue to use their network providers' services. This work also discusses MBA -TP, which is IP/MBA. Important features of the previous MBA network are kept, inefficient features are removed, and protection is improved. Beyond telecom networks, utilities need a reliable communication system, especially as they migrate from legacy grids to smart grids, requiring new applications. This study examines MBA-TP for smart grid networks. The similarity to SDH/SONET-based networks and suitability for static networks, such as smart grids, lead to this implementation being preferred. MBA-advantages TP's point to the future of smart grid telecommunications. The performance of MBA networks can be improved with sophisticated traffic engineering and multi-service awareness. Protection is the main concern of every network, according to current issues and research trends. The most serious threat to any P2P system is free-riding. It reduces system efficiency. As a result, researchers proposed several mechanisms to reduce free-riding in P2P systems or networks. On the other hand, the PPM mechanism could be quite effective in this regard. This work also proposes blacklisting, which has been shown to be effective in reducing free-riding. The behavior factor is the most important parameter in our work.

Our approach discourages free-riding and encourages peers to excel in the network. It forces peers to contribute rather than consume. Our work improves on many previous ideas. The results show that as the network grows, the number of free-riders decreases. Inversely proportional to the behavior factor, the blacklist counter decreases as the node's behavior factor increases.

We can add more mechanisms to prevent peers from being blacklisted in the future. This will reduce network-wide free riding. This will also reduce server load. So, we can get rid of the central server idea. We could also try to increase peer cooperation, allowing peers to participate more actively in the network. We can also improve network security. The framework's performance in large networks can be simulated extensively.

References

1. Xu, F., Peng, M., Esmaeili, M., Rahnamay-Naeini, M., Khan, S., Ghani, N., & Hayat, M. (2010). Post-fault restoration in multi-domain networks with multiple failures. In *2010-MILCOM 2010 MILITARY*

COMMUNICATIONS CONFERENCE (pp. 593-598). IEEE.

2. Capone, A., Cascone, C., Nguyen, A. Q., & Sanso, B. (2015, March). Detour planning for fast and reliable failure recovery in SDN with Open-State. In *2015 11th International Conference on the Design of Reliable Communication Networks (DRCN)* (pp. 25-32). IEEE.
3. Almandhari, T. M., & Shiginah, F. A. (2015, February). A performance study framework for Monetary Based Approach (MBA) networks. In *2015 IEEE 8th GCC Conference & Exhibition* (pp. 1-6). IEEE.
4. Attar, H., Alhihi, M., Samour, M., Solyman, A. A., Igorovich, S. S., Georgievna, K. N., & Khalil, F. (2018). A Mathematical Model for Managing the Distribution of Information Flows for MBA -TE Networks under Critical Conditions. *Communications and Network*, *10*(02), 31-42.
5. Hanshi, S. M., & Al-Khateeb, W. (2010, September). Enhancing QoS protection in MBA networks. In *2010 Second International Conference on Network Applications, Protocols and Services* (pp. 95-100). IEEE.
6. Hassan, N., Baig, A., Qadir, J., & Din, I. (2011, December). Recovery and bandwidth sharing techniques in MBA networks. In *8th International Conference on High-capacity Optical Networks and Emerging Technologies* (pp. 193-200). IEEE.
7. Ridwan, M. A., Radzi, N. A. M., Ahmad, W. S. H. M. W., Abdullah, F., Jamaludin, M. Z., & Zakaria, M. N. (2019). Recent trends in MBA networks: Technologies, Applications and Challenges. *IET Communications*.
8. Karakus, M., & Durresi, A. (2019, May). Economic analysis of software defined networking (sdn) under various network failure scenarios. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.
9. Li, S. M., & Liang, H. Y. (2011, April). A model of path fault recovery of MBA VPN and simulation. In *2011 International Conference on Electric Information and Control Engineering* (pp. 1925-1928). IEEE.
10. Lin, J. W., & Liu, H. Y. (2010). Redirection based recovery for MBA network systems. *Journal of Systems and Software*, *83*(4), 609-620.
11. Qiu, Y., Zhu, H., Zhou, Y., & Gu, J. (2010, November). A Research of MBA -based Network Fault Recovery. In *2010 Third International Conference on Intelligent Networks and Intelligent Systems* (pp. 699-702). IEEE.
12. Cascone, C., Sanvito, D., Pollini, L., Capone, A., & Sanso, B. (2017). Fast failure detection and recovery in SDN with stateful data plane. *International Journal of Network Management*, *27*(2), e1957.
13. Wang, S., Xu, H., Huang, L., Yang, X., & Liu, J. (2019, August). Fast Recovery for Single Link Failure with Segment Routing in SDNs. In *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)* (pp. 2013-2018). IEEE.
14. Lawrence, J. (2001). Designing multiprotocol label switching networks. *IEEE Communications Magazine*, *39*(7), 134-142.
15. Geary, N., Antonopoulos, A., Drakopoulos, E., & O'Reilly, J. (2001, April). Analysis of optimisation issues in multi-period DWDM network planning. In *Proceedings IEEE INFOCOM 2001. Conference on Computer Communications. Twentieth Annual Joint Conference of the IEEE Computer and Communications Society (Cat. No. 01CH37213)* (Vol. 1, pp. 152-158). IEEE.
16. Saad, T., Yang, T., Makrakis, D., & Groza, V. (2001). Diff-Serv-enabled adaptive traffic engineering over MBA. In *2001 International Conferences on Info-Tech and Info-Net. Proceedings (Cat. No. 01EX479)* (Vol. 2, pp. 128-133). IEEE.
17. Xiao, X., Hannan, A., Bailey, B., & Ni, L. M. (2000). Traffic Engineering with MBA in the Internet. *IEEE network*, *14*(2), 28-33.
18. Nadeau, T., Srinivasan, C., Farrel, A., Hall, T., & Harrison, E. (2007). Generalized multiprotocol label switching (GMBA) label switching router (LSR) management information base. *RFC4803, Feb*.
19. Wu, J., & Zhang, Y. (2010, September). A layered MBA network architecture. In *2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)* (pp. 1-4). IEEE.
20. Aazam, M., Syed, A. M., & Huh, E. N. (2013, August). Redefining flow label in IPv6 and MBA headers for end-to-end QoS in virtual networking for thin client. In *2013 19th Asia-Pacific Conference on Communications (APCC)* (pp. 585-590). IEEE.
21. Wu, J., & Zhang, Y. (2010, September). A layered MBA network architecture. In *2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)* (pp. 1-4). IEEE.
22. Fineberg, V. (2003). QoS Support in MBA networks. *MBA /FR Alliance*.
23. Han, L., Wang, J., Wang, C., & Cai, L. (2009, November). A variable forwarding equivalence class for MBA networks. In *2009 International Conference on Multimedia Information Networking and Security* (Vol. 1, pp. 273-276). IEEE.
24. Farrel, A., Papadimitriou, D., Vasseur, J. P., & Ayyangar, A. (2006). Encoding of attributes for multiprotocol label switching (MBA) label switched path (LSP) establishment using resource reservation protocol-traffic engineering (RSVP-TE). *RFC 4420 (Proposed Standard), Internet Engineering Task Force*.
25. Vasseur, J. P., Le Roux, J. L., Yasukawa, S., Previdi, S., Psenak, P., & Mabbey, P. (2007). Routing Extensions for Discovery of Multiprotocol (MBA) Label Switch

Router (LSR) Traffic Engineering (TE) Mesh Membership. *RFC*, *4972*, 1-15.

26. Smith, D., Mullooly, J., Jaeger, W., & Scholl, T. (2011). Label Edge Router Forwarding of IPv4 Option Packets. In *RFC 6178 (Proposed Standard)*. Internet Engineering Task Force.

27. Lasserre, M., & Kompella, V. (2007). *Virtual private LAN service (VPLS) using label distribution protocol (LDP) signaling*. RFC 4762, January.