Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 3159-0040
Vol. 2 Issue 5, May - 2015

A Novel Security Protocol for P2P Incentive Schemes

Eludiora Safiriyu I.
Department of Computer Science & Engineering,
Obafemi Awolowo University, Ile-Ife, Nigeria.
safiriyue@yahoo.com

Ayanda Dauda
Kenneth Dike Library,
University of Ibadan
daudayanda@gmail.com

***Abstract*— Incentive mechanism is presently being considered as one of the most critical aspects in the design of Peer-to-Peer (P2P) systems that enforce co-operative and resource sharing among participants. Incentive policies, on the other hand, is a research field that requires specific policies to fight against malicious and selfish behaviour by peers. Encouraging peers to collaborate in resource sharing in a secure P2P system has widely been investigated, however, this issue is yet to be fully explored.**

In this study, we propose a model for mitigating security issues in an incentivized P2P system where unauthorized users are involved. This model presented architecture for the security of the P2P incentive schemes. Coloured Petri-nets was used for the simulations. There are three users. The peer, is a bonafide member of that peer to peer computing cooperative. The user is not a member, but register as a temporary user of the facilities. The free-rider who only benefits from the facilities but add nothing to the group.

The results of the simulation shows that for about 100 requests only 3 may be granted. The remaining 97 requests are denied. The requests are granted based on the availability of the peer that owns the facilities. Some of these requests may be from free-riders and they gain access to any resource.

The model will address the security challenges of the incentive schemes. The proposed study is efficient in terms of fairness to peers and users.

Keywords—P2P Computing, Incentive Mechanism, Security, Resources Allocation, Network, Free Rider

I. INTRODUCTION

Peer-to-Peer (P2P) computing has recently emerged as an attractive distributed computing paradigm as a result of the development of high-speed networks with low cost computational resources. P2P systems allow participants to share their computational, storage and networking resources to benefit the participants. The P2P paradigm is an alternative to the client-server model in Internet computing. Client-server represents single unit solution while P2P model represents the execution of entities with the role of client-server. This shows that P2P enables peers to share their resources with mostly limited or no interation with centralized server [1]. Also, client-server approach leads to bottleneck since a large number of clients are sometimes involve for a single server to deal with huge workload leading to bottlenecks unlike P2P that allow even distribution of workload across the peer in a balanced way.

The P2P technology potentials are yet to be fully explored due to security and some other related challenges. Security issues like trust, privacy, piracy and other attacks are common on the Internet which affects the reliability and availability of services on P2P [12, 9, 2, 11]. Today many devices are becoming ubiquitous, that is anywhere and anytime, in usage. Most of these devices are having resources constraints that do not have enough resources to process some security provisions that can be available on fixed wired or wireless systems. In this study, we examine security issue based on review of existing literature on P2P network in order to come up with an approach that ensure verification of resources being shared among the users. The phenomenon of selfish individuals who opt out of a voluntary contribution to a group's common welfare has been widely studied and is known as the free-rider problem [13, 5, 7]. Free rider is one of the serious problems encountered in P2P because it consumes resources from the network with no compensation nor contribution in return and this has a significant impact on the overall system performance. Free-rider problem is thus considered as an example of social dilemmas which arise from discretionary databases when a user's personal interests are at odds with the collective interest.

Incentive scheme comes as a result of the need and opportunity to improve P2P file-sharing systems to increase the proportion of users that share files. It enables sharing of resources and information at low cost with high scalability. This makes the files readily available and competitive, and increases system's value to its users. Torrento considered incentive techniques as one of the most critical aspects in the design of P2P system in order to enforce co-operation and resource sharing among the participants. The author identified incentive policies in P2P computings as a research field that requires specific policies to fight against malicious and selfish behaviour by peers.

The major contribution in this paper is to model a security solution for incentive mechanism in P2P resources and files sharing schemes. The rest of the paper are outlines as follow: Section 2 reviews related

work on the research; Section 3 system framework; Section 4 discusses proposed P2P security system layers; Section 5 presents resources control, we discuss security protocol in section 6, system model and simulation is presented in section 7 and Section 8 concludes the study with proposition for further study.

II. RELATED WORK

Several studies have been carried out in the area of P2P computing that encourage peers to collaborate and co-operate in resource sharing. However, the identified issues are still at very early stage of research while security has largely been an issue for consideration.

The problem of free-rider in P2P file sharing networks have been presented in literature [4, 1, 6]. The study examined the design implications of the assumptions that users will selfishly act to maximize their own rewards and proposed a simple game theoretic model of agent behaviour in centralized P2P systems. In [6], a peer's EigenTrust score that addressed the problem of free rider on P2P networks was considered. Cost for participation in the sharing were not taken into consideration, except reward for faster download times and bandwidth usage.

Klaas [7] examined the problem of over-contribution in the Usenet file-sharing network based on the effect of free-riders and proposed a game-theoretic model that could mitigate the effects by group self-regulation. The proposed scheme demonstrated that the effect of over-contribution is insufficient for a system's population to self govern on a system-wide level due to partitioning of the population into disjoint communities. A game theoretic framework has also been applied to study the phenomenon of free-riding in P2P systems [3]. In this paper, a user decided whether to contribute or free-ride based on how the current burden of contributing in the system compares to her type. The study presented a mechanism that penalizes free-riders which improve system performance by reducing the burden placed on the contributors.

A further study on BitTorrent was carried out in the context of choking and optimistic unchoking algorithm [8]. The study proposed seed bandwidth allocation based on the uploading rate of peers in the BitTorrent system to effectively guard against free-riding and improves the performance of contributors. The study is limited to homogenous peers while the robustness of the seed bandwidth allocation strategy need further verification.

A new computational economy-based distributed cluster resource management system was proposed by Ranjan et al. [10]. The economy-based Grid Federation systems uses agents that maintain and access a shared federation directory of resource information. Simulation result showed that the system provided an increased ability to satisfy quality of service (QoS) demands over all users and algorithmic output indicated that the resource supply and demand pattern affects resource provider's overall incentive.

Sieka et al [14] presented a protocol that is resilient to the attacks considered in the paper. The proposed protocol [14], enhanced security against various attacks was achieved using smart design and a combination of various techniques such as the use of digital signatures for message. The paper addressed the file sharing security challenges. We addressed the issues of resources sharing in which file sharing is inclusive. In addition, our focus is to make security provision for present and future incentive schemes developers.

III. SYSTEM FRAMEWORK

The security usually consists of provisions and policies adopted to prevent an unauthorized access, misuse, modification or denial of computer network and network-accessible resources. The security is necessary to know the peer identity (identity management) and the users' authentication and authorization. Authentication is a process of verifying the identity of the user usually through the password authentication procedure while authorization ensures that the attribute of the actual users are verified before accessing the resources or information.

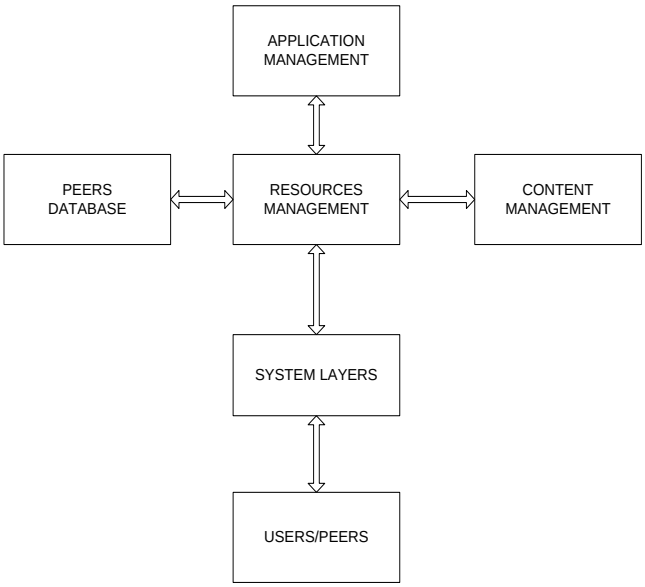

Fig. 1 P2P Security System Architecture

Figure 1 described the architecture of the proposed system. The users/peers send the requests to the resources management via the system layers. The resources management has the files and computing resources that can be available to the peers. The peers' database section manages the peers profile and its interaction with other peers. Peers database maintain the transactions' logs that will provide record of transactions. The peers' databases communicate with content management section via the resources management section. The content management section act as a repository or archive of all files. The application management section determines the peers request approval. This section will consider the peer's right to access the resources. The computing

resources such as: secondary storage (memory space), Random Access Memory (RAM), software etc. Details of the operation are discussed in other sections.

IVPROPOSED P2P SECURITY SYSTEM LAYERS

This study approach is different from the previous studies on P2P systems where security procedure constituted an open challenge. The paper models the P2P network as a line topology that consider different layers from security layer to application layer in a top down approach as shown in Figure 2.

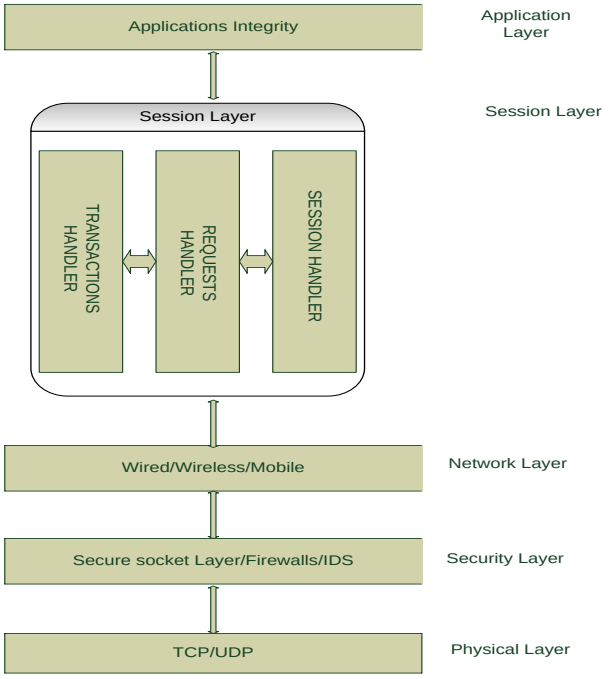

Fig. 2 A Proposed Peer to Peer System Layers

Physical layer: describes the means at which a peer can connect with the Internet. This connection can from different medium, wired or wireless.

Security layer: this layer addresses the security issues and different security tools are put in place. Secure socket, firewalls and different intrusion detection schemes (IDS) are to secure data being transmitted.

Network layer: packet forwarding through the router do take place in this layer. Different networks such as WAP, Broadband are used.

Session layer: this layer is subdivided into three. The session, request and transaction handlers are put together to enhance security of Peers. The session handler provides slot for the peer requests. It will determine when it can access resources available in other peer. The request handler collates all the requests and forwards them to different peers for their attention. Transaction handler takes record of transactions among the peers.

Figure 3 explained what each handler will do on the request(s) before it will leave that layer. The session layer was added to minimize network congestion. All requests would have been filtered before they will leave the layer.

Application layer: the interactions among the handlers are later presented to application layer for validation and integrity check for the peers.

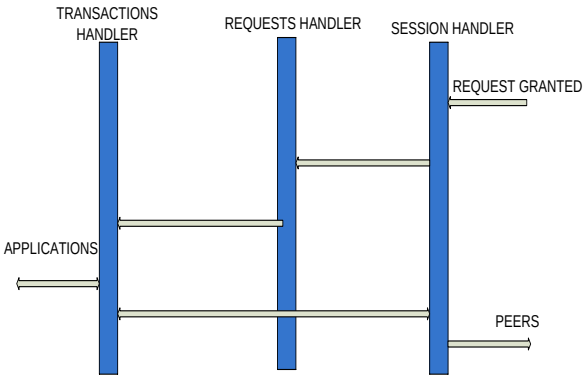

Fig. 3 Session Layer Activities

VRESOURCES CONTROL

The resources control as shown in figure 4 describes the steps required to release any resources to any Peer or user. The identity of user or peer will be attached with the request. The identity (ID) management unit will scrutinize the profile of the peer/user. The details of the peer must include its organization and other verifiable documents. This unit has its own criteria of determine who qualifies and who does not. A qualified peer will be processed to the level of authentication. The authentication management level will authenticate the peer/user whether it belongs to the group or not. The verification will be conducted and benchmarked with set criteria. Some of the criteria are the network security, operating system and bandwidth capacity.

Resources to be used must be authorized by the group. The authorization of such resources will be determined by the rules/principles that guide the resources release. The authorization management unit will issue a certificate for the resources control management unit to release the resources for the peer/user.

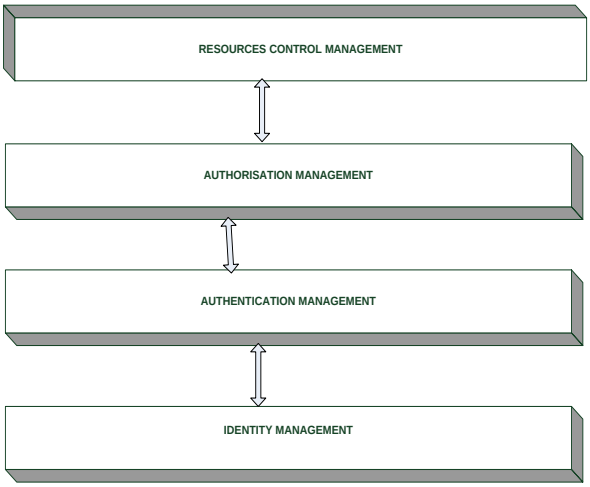

Fig. 4 Resources Control

VI SECURITY PROTOCOL

The security protocol shown in figure 5 explains how any resource transaction will be monitored security wise right from the point at which the request has being made. The membership of the peer/user will be determined before it request could be certified. The peer or user will be authenticated before a peer or user can use the resource(s). An access to a resource by a peer or user will be authorized based on the certification received from the authentication unit. The resources we considered in this paper are RAM, CPU and HARD DISK. These resources are important to peers and need stringent security measures to prevent intruders of free riders.

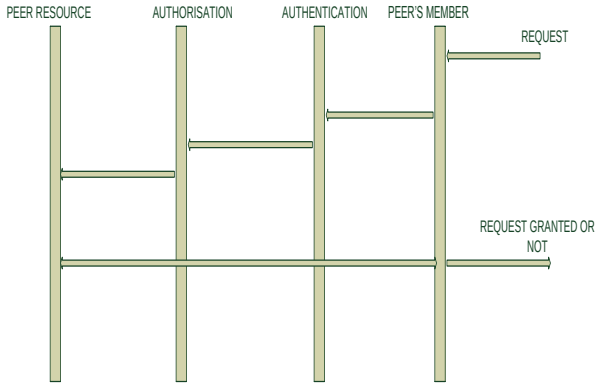

Fig.5 Security Protocol

VII SYSTEM MODEL AND SIMULATION

The modelling and simulation was done using Coloured Petri Nets (CPN). We assumed that there are three major stakeholders; they are the users (who may intend to register for the resources or files he wants), the peers (legitimate members of the group) and the free-riders. This security solution presented intended to minimize the access of free-riders to peer network. We have three transitions, T1, T2, and T3. We have T1=requests, T2=authentication and T3=authorization as in figure 6. From T1 one can select the resources, and the users, peers or the agents. We can fire the transition to determine whether the request will be denied or accepted. A request from a user can be denied if the resources on a peer is in use or such a user does not register. A user can register after it has been denied access. However, a free-rider will not register or sign-up after it has been denied access. A peer request can be granted if the resources or files are available. Otherwise, it can be denied.

We presented a scenario for 100 peers that are collaborating. How many denied and accepted requests. We expected a peer to have hard-disk, random access memory (RAM), network and processor (CPU). Also each peer's system resources will vary in capacities. Figure 7 shows the graph plotted to explain our scenario. It shows that only peers and users could access resources and files.

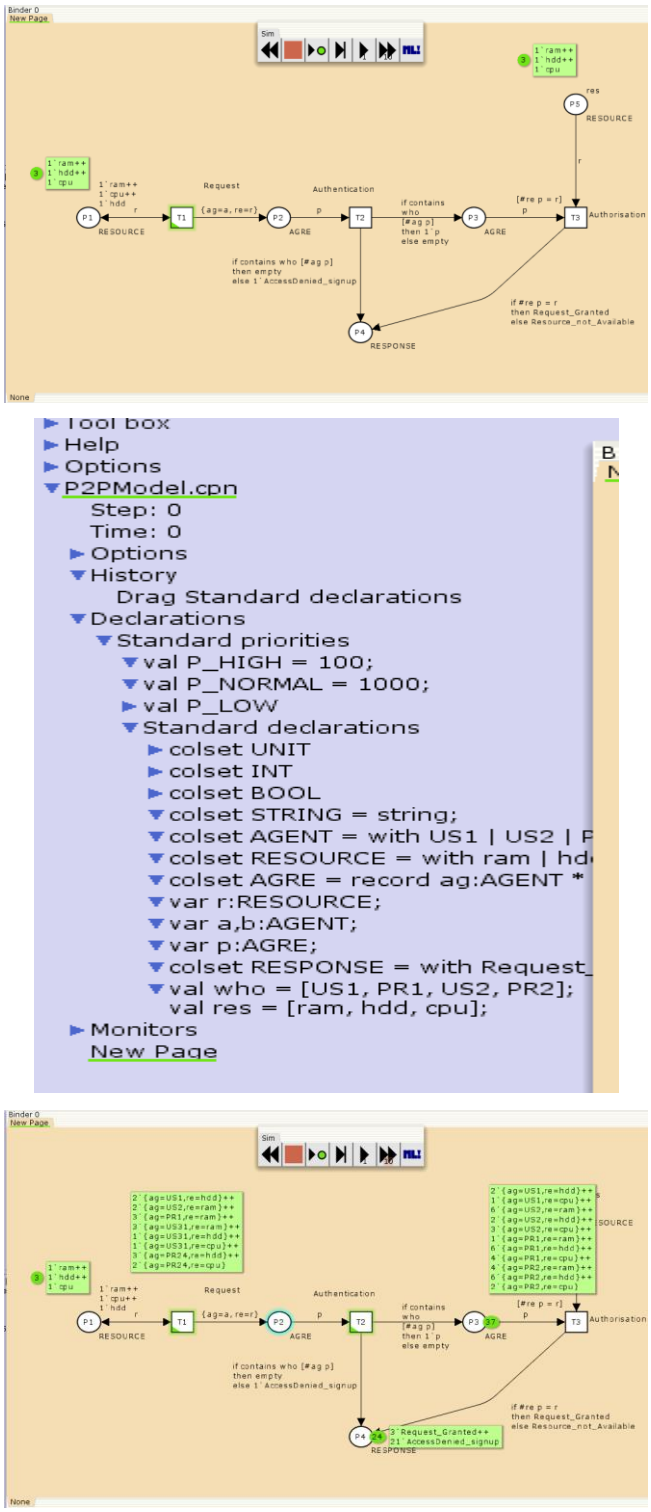

Fig. 6 Simulation of the Model

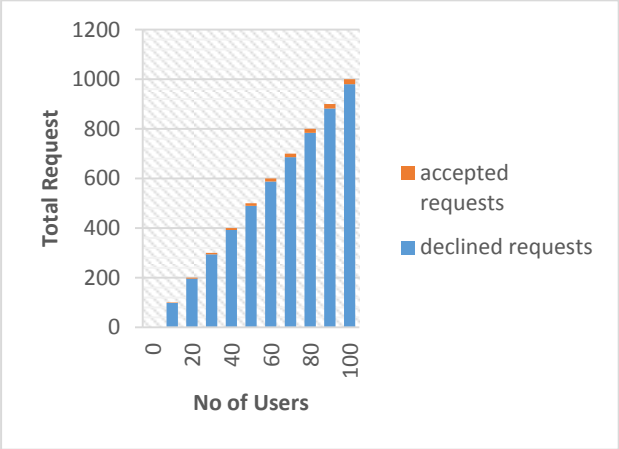

Fig. 7 Peers/Users Requests

VIII RESULTS

We analysed the simulation and the results plotted in figure7 show that, the number of requests accepted and denied has a wide ratio because of many reasons.

Table1 Results of the Simulation

Iteration	Peers Available	Peers or users requests	Requests accepted	Denied requests
1	15	200	15	185
2	42	550	42	508
3	65	778	65	713

From table 1, It implies that the number of available peers will determine the number of requests that will be accepted. The peers attend to the users and other peers that are requesting for one resources or the other.

The proposed security solution has many security mechanisms that will not allow non- collaborative peers to take the advantages of security lapses to benefits without being a contributor. Users that are ready to sign up will benefit, but free-riders will be denied access. The model proposed new P2P security layers to address resources control. The identity management, authentication, and authorization are put in place to eliminate free-riders.

IX CONCLUSION

The P2P security solution proposed in this paper aimed at addressing some incentive schemes that may be proposed in future by the researchers. This security solution consider sharing of resources than file. Individual peers cpu, ram and hard disks can be shared by peers. Therefore, a stringent security protocol system proposed to address the fair of the peers.

X FUTURE WORK

It is our plan to propose an incentive scheme that will be tested with this security solution. The incentive scheme performance will be evaluated.

REFERENCES

[1] Buragohain, C., Agrawal, D. and Suri, S. A Game Theoretic Framework for Incentives in P2P Systems, in *Proc. 3rd Int. Conf. Peer-to-Peer Computing*, 2003, pp. 48–56.

[2] Dumitriu, D., Knightly, E., Kuzmanovic, A., Stoica, I. and Zwaenepoel, W. Denial-of-service resilience in peer-to-peer file sharing systems. In *ACM SIGMETRICS Performance Evaluation Review*, volume 33,2005, pp. 38-49.

[3] Feldman, M., Papadimitriou, C., Chuang, J., Stoica, I. Free-Riding and Whitewashing in Peer-to-Peer Systems, *IEEE Journal of Selected Areas in Communication, Special Issue on Price-Based Access Control and Economics of Networking*, 24(5), 2006, pp. 1010-1019.

[4] Golle, P., Leyton-Brown, K. and Mironov, I.

Incentives for sharing in peer-to-peer networks, in *Proc. 3rd ACM Conf. Electronic Commerce*, Tampa, FL, Oct. 2001, pp. 264–267.

[5] Kalman, M. E.; Fulk, J., Monge, P. and Heino, R. Motivations to resolve communication dilemmas in database-mediated collaboration. *Communication Research*, 2002, 29(2):125–154.

[6] Kamvar, S. D., Schlosser, M. T. and Garcia-Molina, H. Incentives for Combatting Freeriding on P2P Networks, 2003. *Available online at< nlp.stanford.edu/pubs/freerider.pdf>* assessed on 15/02/2012.

[7] Klaas M. Over contribution in discretionary

databases. In *Second Annual workshop in the*

Economics of Peer-to-Peer Systems, 2004.

[8] Li, M., Yu, J. and Wu, J. Free-Riding on BitTorrent-Like Peer-to-Peer File Sharing Systems: Modeling, Analysis and Improvement, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 19 No. 7, 2008, pp. 954-966.

[9] Pretre, B. and Wattenhofer, D. R. Attacks on Peer-to-Peer Networks, 2005.

[10] Ranjan, R., Harwood, A. and Buyya, R. A Case for Co-operative and Incentive-based Federation of Distributed Clusters, *Future Generation Computer Systems (Elsevier)*, 24, 2007, 280-295.

[11] Rowaihy, H., Enck, W., McDaniel, P. and Porta, T. L. Limiting Sybil Attacks in Structured P2P Networks", In *INFOCOM 2007, 26th IEEE International Conference on Computer Communications*, 2007, pp. 2596-2600.

[12]Sit, E. and Morris, R. Security Considerations for Peer-to-Peer Distributed Hash Tables, In *1st International Workshop on Peer-to-Peer Systems (IPTPS)*, 2002.

[13] Sweeney, J. An experimental investigation of the free-rider problem. *Social Science Research* 2, 1973.

[14]Sieka, B., Kshemkalyani, A. D. and Singhal, M. On the Security of Polling Protocols in Peer-to-Peer Systems, url: http://ojs.academypublisher.com/index.php/jnw/article/viewFile/0604607614/2912 [Accessed 7/10/2014].