Stratum based Approach for Securing Multimedia Content Transmission over Large Scale P2P

Ramesh Shahabadkar
Research Scholar
Anna University
Chennai, India

Ramachandra V.Pujeri, Ph. D
KGISL Institute of Technology
Coimbatore, India

ABSTRACT
With the increase of customer base over internet, a large community of the user adopts p2p network because of its potential characteristics of file sharing. From the past decade there has been an extensive research work towards ensuring better security systems over p2p network. However, majority of the security techniques are either highly sophisticated or doesn't yield full fledge security to the user. Hence, the proposed system introduces a security technique for safeguarding the communication channel that is used for multimedia contents sharing. The proposed system uses the potential characteristics of large scale distributed network and scalable coding to perform ciphering process of the multimedia files over P2P. The outcomes of the results are evaluated with respect to PSNR to find that computational overhead is significantly low. Thereby the proposed system ensure cost effective security model in p2p..

Keywords
Cryptography, Key Management, P2P, Security.

1. INTRODUCTION
Peer-to-peer systems have gained more and more momentum over the last years as a means to access multimedia contents, albeit initially in form of file downloads [1]. The evolution to streaming and multicast (e.g., TV) was just a consequence. The P2P (Peer-to-Peer) technology is now well-known by the public, mainly because of the great success of some applications, such as file sharing applications (Kazaa, eDonkey, BitTorrent, etc.) but also more recently such as video streaming applications (PPLive, PPStream, UUSee, SopCast, etc. [2][3]). However, the P2P networks still suffer from bad reputation because of the large number of illegal contents that are distributed by those applications. Social networks [4] provide a wide set of functionality, enabling users to publish and comment private profile pages, create photo albums, join and manage (interest) groups, search for users and groups and communicate with friends and groups through a messaging system. The proposed paper will address the security for the multimedia contents for a p2p-based platform for social networks. Social networking sites are web-based platforms allowing users to publish personal profiles, link each other, post pictures, blog entries, join groups and search for friends. Several hundred millions of users participate in today's social networks like Facebook or MySpace. However, due to the centralized character of this platforms, high server maintenance cost exists. A p2p-based approach solves the load and cost issues but leads to new challenging security issues for secure communication and data access [5]. In these turbulent times, it is assumed that P2P security would be the least of the world's problems. However corporate fraud and loss of revenue due to attacks on their internal networks has brought P2P to the forefront in the IT world [6]. Napster was the headliner but since its high profile court case [7] more and more P2P applications have been causing the corporate world challenges. With better security protocols this headache could be turned into a valuable asset for the corporate world and for the world. The diagram below illustrates the gaps in security when using P2P applications. We can see that we are letting these applications get inside our networks. The security of our "secure" network is now in jeopardy

P2P networking allows the network to be open to various forms of attack, break-in, espionage, and malicious mischief. P2P networks can also allow an employee to download and use copyrighted material in a way that violates intellectual property laws, and to share files in a manner that violates an organisations security policies [7]. Applications such as Napster, Kazaa, Grokster and others have been popular with music-loving Internet users for several years, and many users take advantage of their employers' high-speed connections to download files at work. This presents numerous problems for the corporate network such as using expensive bandwidth and being subject to a virus attack via an infected file download. Unfortunately, P2P networking circumvents enterprise security by providing decentralized security administration, decentralized shared data storage, and a way to circumvent critical perimeter defences such as firewalls and NAT devices. If users can install and configure their own P2P clients, all the network managers' server-based security schemes are out the window.

The proposed system introduces a secure architecture of p2p network that uses scalable coding and some cost effective cryptographic measures to incorporate security over streams of multimedia files using frequently used BitTorrent protocols. Section 2 discusses about some past literatures, while section 3 discusses about the proposed system, while section 4 discusses about the implementation techniques used. The accomplished results were discussed in section 5 where the proposed system has been compared with existing system to check the output efficiency. The efficiency of the proposed system is evaluated using PSNR along with discussion of computational overhead. Finally section 6 concludes the paper discussion.

2. RELATED WORK
Muller e.t. al [8] have presented experiments with efficient Content Based Image Retrieval in a P2P environment, thus a P2P-CBIR system. Although according to the work, peer data summaries can be used within the retrieval process for increasing efficiency, but security aspects are ignored. Jung and Cho [9] have proposed a watermarking platform for protecting unauthorized content distribution in P2P networks. The proposed platform dynamically generates 2D barcode watermark according to consumer's data and inserts the watermark into downloaded audio source in wavelet domain.

However, the proposed watermarking platform is not able to prohibit illegal usage of digital audio content.

Chu e.t. al [10] have investigated the requirements for multimedia content sharing among Peer-to-Peer (P2P) networks and proposed a novel business models along with Digital Rights Management (DRM) solutions. The aim of this DRM research is to set new business models for content owners to benefit from the massive power of content distribution of P2P networks with least intrusion and interference to end consumer's privacy and anonymity.

Kumar and Sivaprakasam [11] have proposed a new encryption mechanism is included in which a message is transformed into a binary image which cannot be identified as a cipher text or stegno object. The approach is very much better for transmitting a confidential data from client to server. However, P2P network reliability is not ensured as the experiments were performed on adhoc network.

Mathieu e.t. al [12] have proposed a P2P system that ensures the security of contents, by controlling that only authorized contents are exchanged between peers and by being able to identify the people that redistribute illegal contents if it happens. This is mostly addressed by the use of watermarking functions in the video contents processing and by the deployment of specific peers that can monitor and detect misbehavior of the peers.

Meddour e.t. al [13] have presented a state of the art study on several solutions, which exploit the power of P2P technique to improve the current multimedia streaming protocol. The author specified that current open issues in multimedia P2P streaming are a) appropriate video coding scheme, b) managing peer dynamicity, c) peer heterogeneity, d) efficient overlay network construction, e) selection of the best peers, f) monitoring of network conditions, and g) incentives for participating peers.

Berson [14] has discussed the security aspects of Skype. Tang e.t. al [15] have presented their experience on a practical P2P-based live video-streaming system called GridMedia, which was employed to broadcast live the Chinese Spring Festival Gala show over the Internet.

Hughes and Walkerdine [16] have presented an ongoing work on the development of the Distributed Video Encoder, a means to utilize the spare computational resources of standard PCs within a P2P network.

Reforgiato e.t. al [17] proposed a multipoint video broadcast framework over a heterogeneous content distribution P2P network. In the proposed system the source generates the video flow by using an MPEG-4/FGS encoder, in such a way that no losses occur at the Base-layer stream even in the presence of short-term bandwidth fluctuations.

Hagemeister [18] has described the framework for a distributed censorship-resistant policy drafting system. By relying on a DTN as well as a P2P network, the system can work even without internet access.

K. Singh et.al [19] described the login screen is successfully made. Key Hand Shake is being implemented. And as a result keys can be generated for a partic-ular session for a particular sender. Hence forth, the encryption of message through the 128 bit AES encryption and decryption of a message is done using in built Java Libraries (JCE).

K. SakthiSudhanet.al [20] investigated application layered protocols to the quality of metric values of H.323 protocol video streaming transmission over peer to peer link in wireless scenario. Video transmission through VoIP from source to destination node in the overall scenario investigate throughput, average delay, jitter, VoIP analysed video traffic from source to destination node and also can be analysed the quality of metric values of traffic pattern in transport layered protocol.

André Filipe et.al [21] described the P2P applications became very popular, not only for content sharing and distribution but also for media streaming. In the last few years an attempt to obscure or even encrypt the traffic generated by those P2P applications has been made in order to increase privacy or to avoid the identification of traffic generated by such applications to escape traffic shaping or blocking.

Heiko Dittrichet.al [22] analyzed the incentive mechanisms of eMule and BitTorrent. They introduced an abstract classification of incentive mechanisms. Further, they have shown that there exists a great number of attacks against P2P file-sharing systems in general and their incentives. Most of these attacks can be countered through improvement or addition of already known incentives.

We have attempted to explore some prior work done towards securing image or video contents over P2P network and examined some attacks and issues with P2P networks. In the multimedia content distribution scenario, this server is usually hosted and maintained by the content providers. This results in peer user's anonymity interference and content provider's efforts in server maintenance. It was found that majority of the work done past is either on cryptography or using DRM or watermarking, where the prime concern is the privacy and anonymity issues of content consumers. Since DRM systems track user transactions, purchases, and access history, end consumers' detail activities are recorded at content retailer's database and thus raise divergences regarding multimedia content protection versus privacy protection. However, a key problem for securing P2P networks is that, because of its inherent decentralized nature, there lacks the means for central administration, and thus control, required to combat security attacks. No much work towards securing image or video content while transmission is explored very recently or even in past. All the issues that has not been addressed in the past are the main focus of implementation in this study.

3. PROPOSED SYSTEM

This section discusses about the secure framework using video coding based approach for safeguarding the communication in peer-to-peer network and mitigates the possible intrusion in P2P network. The proposed system is deployed exclusively for multimedia applications over p2p streams. The proposed framework is deployed on two stratums of multimedia streams e.g. i) the first stratum of the multimedia stream is essentially designed for minimized bit rate termed as bottom stratum that possesses the significant information of the digital multimedia contents, ii) the second stratum of the multimedia stream is termed as augmented stratum targeting at maximized bit rate for enhancing the quality of multimedia streaming. The system will possess the receiver who can make a decision related to the receiving of the chunk information from augmented stratum thereby gradually enhancing the quality of service while streaming multimedia streams by gaining more stemmed augmented stratum. By adopting this process, the heterogeneity and discreteness of the information can be maintained by transmitting only the stratum that a receiver unit can control.

The digital content of the bottom stratum is ciphered by incorporating secure access policies for better security alternatives. The system then applies a discerning ciphering to it that can mitigate illegitimate members by denying their access to the authorized multimedia contents. Once this process is accomplished, the contents of the ciphered bottom stratum are specifically broadcasted to the network along with the messages pertaining to key, while the augmented stratum is sent in the multi-casted system. The entire discussed operation is performed in the secured P2P distributing server.

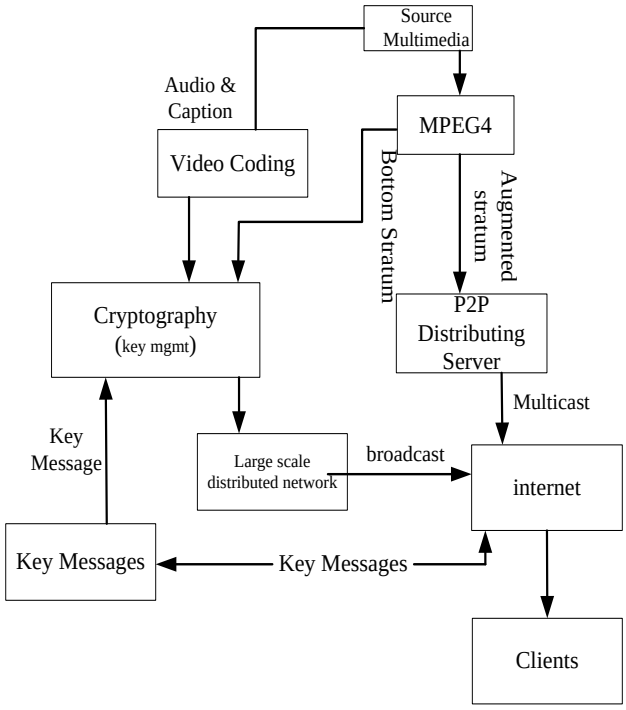

Figure 1: Proposed reputation based P2P security model

The next actor of the system is client module which will the obtain information related to both the stratum (i.e. bottom and augmented stratum). The purpose of deciphering the multimedia content is performed by the bottom stratum thereby furnishing the significant and efficient quality of service in streaming multimedia contents over p2p network. In the similar instant of time, the message incorporated in the key assist to regularly update the session key. The system then performs the phenomenon of re-integrating the security control message as well as multimedia contents for better security where augmented stratum can only be deciphered if the bottom stratum is right way available. This fact can be also highlighted in a way that if the bottom stratum is lost, then the client will not able to access the authorized information. Hence, the proposed system doesn't only ensure secure data transmission but also ensures proper security controls. However, for better flexibility, the augmented stratum may be not obligatory module that primarily enhances the quality depending on the multimedia streams of extreme bit rate. It is possible for client module to obtain the precise quantity of the information in augmented stratum proportionate to channel capacity that leads to enhancement in streaming quality of the multimedia contents.

The phenomenon of the transmission of the multimedia streaming contents can be discussed as following. Initially an encoder M_{enc} maps an instant of the multimedia video using a specific frame F_{mul} into stratum codes S_{code} for bottom stratum S^{i}_{code} for stemmed improvement in the stratum chunk information.

$$M_{enc} \rightarrow F_{mul} \rightarrow \{S_{code} + \sum_{i=1}^{n} S^{i}_{code}\}, \text{(i=1, 2, ..n)}$$

After accomplishing the above process, ciphering process C_{mul} is performed with secure authorization over the bottom stratum S_{code} information and generates the ciphered bottom stratum CS_{code}.

$$C_{mul} : S_{code} \rightarrow CS_{code} \quad (2)$$

The decipher module ($\mathbf{D}_{se}$) Dec in association with the secret key information K_{sec} at the receiving end maps CS_{code}, and all the accomplished augmented stratum $\sum_{i=1}^{p} S^{i}_{code}(p \le q)$ to rebuild the preliminary frame as:

$$Dec : \{CS_{code} + K_{sec} + \sum_{i=1}^{p} S^{i}_{code}\} \rightarrow \Lambda F_{mul}(p \le q) \quad (3)$$

The proposed framework considers integrating the potential charecteristics of p2p network as well as large delivery channels by transmitting the multimedia streaming contents from distributed p2p server in large delivery channels to various other servers and then streaming the multimedia contents using peers. The large delivery network can be thought of as a large distributed system of servers deployed in multiple data centers across the Internet. Using this principle, the proposed system ensures quality of service as well as flexibility of multimedia streaming in p2p network most securely. The broadcasting peer of p2p bottom stratum has highly measurable security management, while maintaining the quality of the service at the same time.

4. IMPLEMENTATION

Figure 2 illustrates the implementation technique of the proposed system. The system uses triple level of large scale distributed network that has web servers and managed servers for the purpose of streaming the video resources to the peer ends. The terminal servers are provided to the proximity of the peer clusters from where the contents belonging to bottom stratum are streamed in broadcasting module in p2p network while the contents belonging to augmented stratum is transmitted in multi-casting module. The system also considered trusted web servers where the multimedia contents are distributed uniformly and then from there it reaches the terminal servers from where the peer users can select to acquire the multimedia contents in p2p network. The web servers can assist the streaming of cumulative traffic with better optimization and also congestion where authentication is done using secret key. Another advantage of the fixed web server is that it permits the peer users to attain the streamed multimedia contents from one of the proximity web server (mirror servers) with minimized latency and cumulative traffic overloading. The quality of the service is ensured by transmitting the multimedia contents of bottom stratum from the large scale distributed network in broadcasting module to get better and refined quality of streaming services eventually in the case of node failures. Moreover the usage of multicasting module in p2p network in the proximity of such servers permit the peer ends to liberally communicate in any p2p protocols to accomplish optimal scalability.

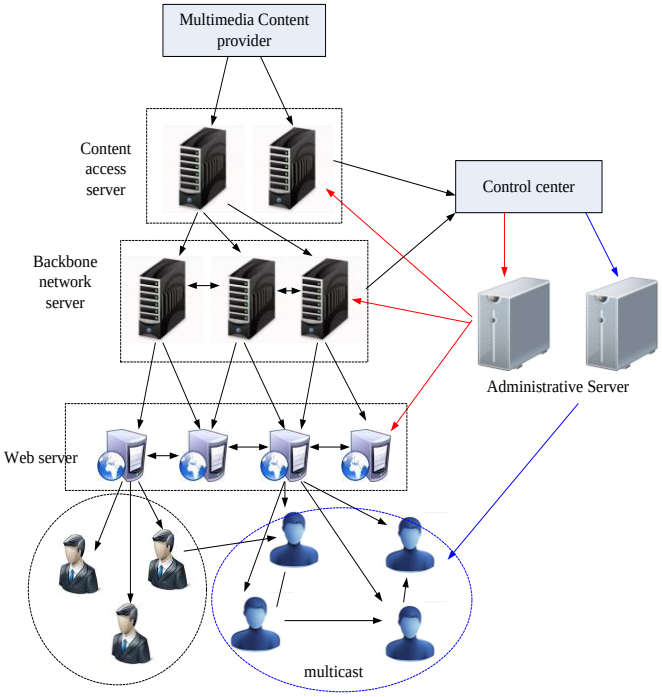

Figure 2: Proposed Test bed for implementation

The proposed system is implemented by designing 4 individual modules e.g. i) multimedia content origin, ii) Peer content control, iii) Traffic management system, and iv) intermediate peers. The source multimedia data that arrives at the cipher module are classified into streams belonging to bottom stratum and augmented stratum. The significant part of the module is also associated with a centralized server that deals with the security authentication and authorization of the peers, performs key management along with ciphering process on the stream belonging to bottom stratum. After this process, the stream belonging to the bottom stratum is transmitted to the authenticated peers in the secured broadcasting module of p2p network and the streams belonging to augmented stratum is transmitted to the basic multicasting module in the p2p network experimented on wireless environment. The architecture that is finalized is shown in Fig. that consists of basic p2p communication function, protocol implementation (BitTorrent), and finally streaming of the multimedia files. The implementation is carried out using control-packets based process that consists of practical control message and inert control message. The practical control message pertains to even clock synchronization and inert control message pertains to incoming request from end peers. The system uses dual types of memory pools for recording the data in both bottom stratum and augmented stratum. Apart from memory management, the proposed p2p protocol also posses relationship management, event information sender, cryptographic module, provisioner module and store event instant. In the streaming process, the peer ends would chooses the data as per synchronization of the elements of multimedia data from bottom stratum or augmented stratum in the memory. The stratum based deciphering process is deployed on the sample multimedia content while the normal deciphering process is applied for audio contents of the multimedia files in p2p networks. During the process of deciphering, the session key is considered as the critical parameter, using which the peer end can decipher the multimedia stream and have an access to the multimedia resources.

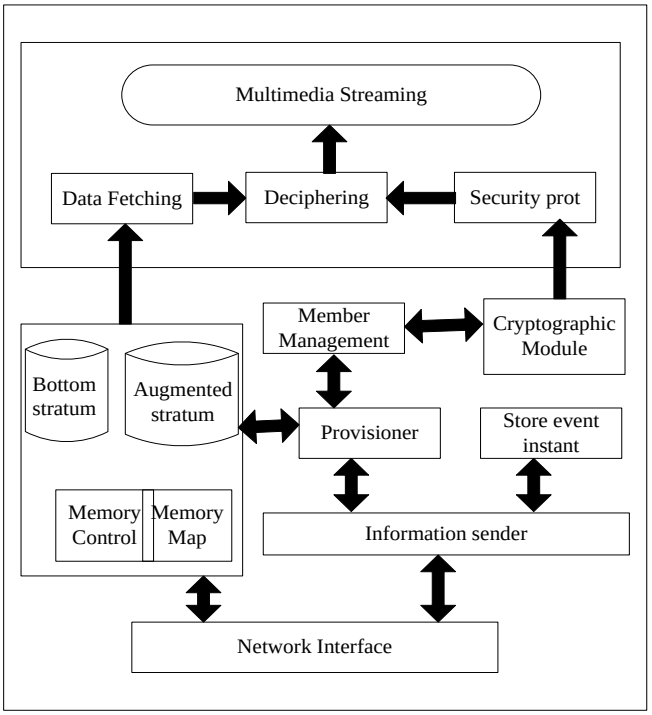

Figure 3: Architecture of proposed implementation

In order to ensure better throughput efficiency and minimize cumulative system overheads, the process considers adopting scalable coding. The scalable coding is usually a coding process of generating contents with reduced quality by directly manipulation the bit streams without using decompression or recompression. The system applies scalable coding for the purpose of encoding and decoding for bottom stratum and augmented stratum.

5. RESULT DISCUSSION

The proposed system uses the dataset of the foreman clip [23], which after performing processing is subjected to evaluation. The emphasis of the evaluation is done on peak signal to noise ratio (PSNR) estimation of the deciphered multimedia file. The outcome of the PSNR is exhibited in Fig.5. After performing a series of experiments by varying parameters, the simulation outcome is exhibited with steady enhancement in the quality with the maximization in the bit rate of the multimedia contents using scalable coding scheme. Therefore, the results exhibited in Fig.4 highlights that scalable multimedia coding on the efficiency of coding is not that better as unsalable multimedia coding that still furnishes the satisfactory quality of the multimedia content and channel capacity requirements. Considering the better stratum based characteristics required by the proposed system that cannot be designed by the existing conventional single stratum coding technique, scalable coding is therefore a better choice for efficiency in the proposed system. The result exhibited in Fig.6 highlights the performance of encoding system as compared to windows media encoder; the proposed system provides better performance.

Table 1 Simulation Parameters

Interval between peers	3-5 seconds
Optimal Buffering time	6-20 seconds
Extent of CPU utilization	<20%
Supported number of peers	10,000 peers
Supported Bitrate	100 kbps-1 Gbps

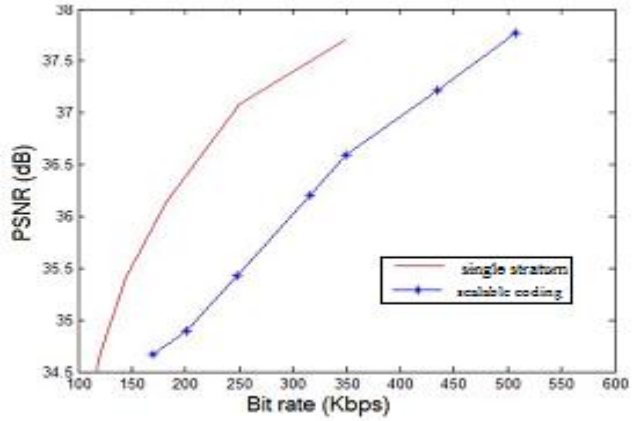

Figure 4: performance of Bit rates of single-stratum and scalable coding

Figure.5: Performance of the foreman clip

The result has also examined quality of service as well as security issues by considering the harmful influence of security management on the quality of the multimedia file. Fig. 5 exhibits another result where increase of frame numbers has been evaluated with accomplished PSNR values estimated in decibel. The results exhibits effects of higher bits of data incorporated in the sample multimedia clip with various cycle of modulation and the PSNR of the individual frames in the peer ends. It can be seen that when the cycle of modulation is 2, the PSNR value ranges between 33.5 to 34.5, which is accepted by the diminished PSNR value when the cycle of the module is equivalent to 4 or 8. Hence, it can be seen that cycle of modulation value of 2 is a problematic factor between optimal quality of the multimedia content and maximum identified precision.

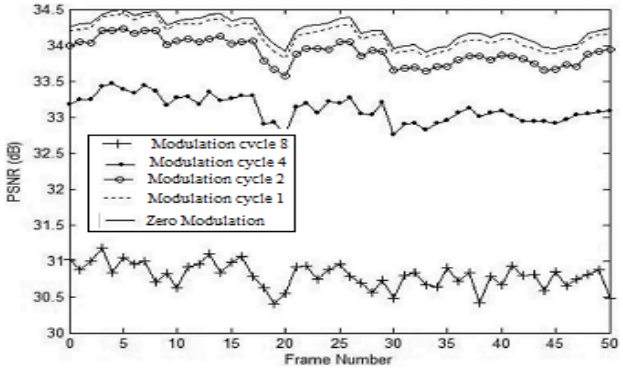

Figure. 6: Performance of quality due to security protocol

The proposed system is therefore capable of maintaining security with better quality of the services. The security protocol is also evaluated with respect to computational overhead owing to application of cryptographic approach. The system ensures better security over the channels as key management servers produces a new cluster key whenever two member attempts to communicate and transmit it via secured channel. Whenever any peer unit of one group attempts to communicate with other, the group key is updated and is securely distributed using the same secure channel thereby thwarting any possibility of intrusion. As the size of the group key is quite less so the computational overhead is also comparably less. In the process of streaming multimedia contents, the session key will be required to be deciphered and re-ciphered by the one peer member between any two group along the route, which drastically ensures minimal re-ciphering process leading to less computational overhead due to session key re-ciphering process. Finally, with smaller number of group size, when any peer unit attempts exchanging information, the computational overhead just for maintaining group itself is very less. These properties of the proposed system thereby ensured better security and optimal streaming quality cost effectively.

6. CONCLUSION

From the increasing demands of p2p network and its associated applications, there is also rise of security threats. Although various algorithm and techniques has been introduced in the past research work, but majority of the studies doesn't establish full fledge security along with better quality of services. Hence, the proposed system has attempted to introduce a novel security protocol that has been tested over foreman clip over p2p network. The proposed system has been evaluated over Bit Torrent protocol considering large number of peers using scalable coding. The evaluation result shows that the proposed system integrates the potential characteristics of large scale distributed network and p2p network by scalable coding to accomplish better security standards.

REFERENCES

[1] http://www.computerworld.com/s/article/69883/Peer_to_Peer_Network, Accessed on 21st Feb, 2014

[2] T.Do., KA. Hua., M. Tantaoui.2004. P2VoD: Providing Fault Tolerant Video-on-Demand Streaming in Peer-to-Peer Environment. the Proc. of the IEEE ICC, France

[3] D. Ciullo., M. A. Garcia., A. Horvath, E. Leonardi, M. Mellia, D. Rossi, M. Telek, P. Veglia.2008.Dissecting PPLive, SopCast, TVAnts, techrep, Polito

[4] http://zeenews.india.com/news/net-news/cyber-criminals-targeting-social-networking-sites-to-steal-money_827996.html, Accessed on 21st Feb, 2014

[5] G.Kalman., M. Patrick., M. Burkhard., H. Daniel., K. Aleksandra., S. Ralf.2009.Practical Security in P2P-based Social Networks, IEEE 34th Conference, pp.269-272

[6] S.Anil., M. Upendra., R. Ajay.2012.A pragmatic analysis of peer to peer networks and protocols for security and confidentiality, IJCCR, Vol.2, Issue. 6

[7] http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p10.html, Accessed on 21st Feb, 2014

[8] M. Wolfgang., E. Martin., H. Andreas.2004.Efficient content-based P2P image retrieval using peer content descriptions, SPIE Electronic Imaging

[9] J. Eui-Hyun., C. Seong-Yun.2006.A Robust Digital Watermarking System Adopting 2D Barcode against Digital Piracy on P2P network, International Journal of Computer Science and Network Security, Vol.6, No.10

[10] C-C, Chu., X, Su., B.S. Prabhu, R. Gadh., S. Kurup.,G. Sridhar., V. Sridhar.2006.Mobile DRM for Multimedia Content Commerce in P2P Networks, IEEE, CCNC

[11] S. Kumar, P. Sivaprakasam.2012.A New Approach for Encrypting and Decrypting Data in Images among users in Ad hoc Network, European Journal of Scientific Research ISSN 1450-216X, Vol. 92, No. 3, pp.425-430

[12] M. Bertrand., G.G.Le., D. Mathieu.2010.Mitigating illegal contents via watermarking in video streaming P2P network, In Proc. IEEE Advanced Networks and Telecommunication Systems, India

[13] M. Djamal-Eddine., M. Mubasher., A. Toufik.2006.Open Issues in P2P Multimedia Streaming, Multicomm

[14] B.Tom.2005.Skype security evaluation, Anagram Laboratories

[15] T.Yun., L. Jian-Guang., Z. Qian., Z. Meng., Y. Shi-Qiang.2007. Deploying P2P Networks for Large-Scale Live Video-Streaming Service, IEEE Communications Magazine

[16] H. Daniel., W. James.2005.Distributed video encoding over a peer-to-peer network, PREP

[17] R. Diego., L. Alfio., S. Giovanni.2009.A P2P Platform based on Rate-Controlled FGS encoding for Broadcast Video Transmission to Heterogeneous Terminals with Heterogeneous Network Access, GTTI

[18] H. Philipp.2012.Censorship-resistant Collaboration with a Hybrid DTN/P2P Network, Masters Thesis

[19] S.A.Kumar., M. Shubham.,Dekar, R.2012.Peer to Peer Secure Communication in Mobile Environment: A Novel Approach, International Journal of Computer Applications, (0975 – 8887) Vol.52, No.9

[20] K.S. Sudhan., G. Thangaraj., P. Deepa.2012. Achieving Quality of Metric for Video Streaming Service in the Warehouse Application with Coexisting of IEEE 802.11 a/b/g Standards, International Journal of Computer Applications

[21] E.A.F.Ferreira.2011.Detection of Encrypted Traf_c Generated by Peer-to-Peer Live Streaming Applications Using Deep Packet Inspection

[22] D. Heiko.2012.Analysing the Security of Incentive Schemes in P2P-based File-sharing Systems

[23] http://trace.eas.asu.edu/yuv/, Accessed on 21st Feb, 2014