ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 3, Issue 1 (Jan. - Mar. 2015)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2015)

Video Streaming Techniques and Issues

[I]Sunny Taksande, [II]Kiran Joshi, [III]Vishwanath Chikaraddi, [IV]Sowmiya Raksha
[I,II,III,IV]Department of Computer Engineering and Information Technology
Veermata Jijabai Technological Institute, Mumbai, India

Abstract
The Video Streaming as opposed to downloading enables an end user or consumer to play the video without being needed to download the whole video file. Video streaming in recent times has become important part of the Internet and is still going to play significant role in unforeseen internet applications to come. This paper presents some basic techniques in video streaming like use of suitable video coding standards, video encryption schemes, video delivery schemes through different protocols and related issues.

Keywords
Streaming, Compression, Encryption, Security, Mutlicast, Peer-To-Peer

I. Introduction

In the past decade there has been consistent increase in the amount of network traffic carrying video content. Amongst these video streaming applications have significant share. Streaming means the video content are streamed and watched even before the whole file is downloaded at the client side. Numerous applications like video conferencing, video telephony, Video on demand (VOD) and live TV and Internet protocol television (IPTV) use video streaming. Video might is streamed directly from streaming servers on the internet and might be consumed on different end devices like computers or mobiles. Like most of the internet applications video streaming applications are faced with issues like bandwidth and security.

Different networks have different bandwidth capacities. A high quality video requires high bandwidth. In some case where bandwidth availability is less a poor quality video might be acceptable for viewing by dropping some few video frames. Video compression along with transrating can be used to fit the available bandwidth. In transrating video is coded to lower bitrate without changing video format and thus limiting the bandwidth requirements.

Securing video content in streaming is another challenge required by applications like video conferencing, VOD and Pay-TV. In each case the user or the clients need to be authenticated and authorized before streaming. Video conferencing requires high security whereas VOD and Pay-TV need conditional access to whatever the content is being subscribed by the end user. The destination device through which the content will be consumed is unknown and therefore it is must that the decryption process should have less computational complexity to meet the real time requirements. Meeting computational requirements and desirable security simultaneously is a challenge.

In recent years, the multimedia storage grows and the cost for storing multimedia data is cheaper. So there is huge number of videos available in the video repositories. It is difficult to retrieve the relevant videos from large video repository as per user interest. Hence, an effective video and retrieval system based on recognition is essential for searching video relevant to user query from a huge collection of videos [13].

The paper is organized as follows. In section II we discuss some of the video coding standards followed by video encryption schemes in section III. In section IV we discuss multicast streaming and key management issues and end with section V discussing the issues with peer-to-peer streaming.

II. Video Coding Standards

Raw or uncompressed video is neither suitable for transmission nor for storage and distribution. Different bandwidth is supported by different networks. Even with good increase in the bandwidth capacity in the last decade the current transmission rates are insufficient to transmit uncompressed video in real time for applications like video conferencing and live video streaming. Similarly an uncompressed video takes more space as compared to compressed video. Video compression algorithms operate by removing redundancy in the temporal, spatial and frequency domains. The growing popularity of high definition TV and related services means growing need for efficient coding techniques for compression. We will discuss the two of the most widely used video coding standards MPEG-4 Visual and H.264.

MPEG-4 Visual (Part 2 of ISO/IEC 14496) helps to deal with a wide range of visual data including rectangular frames ('traditional' video material), video objects (arbitrary-shaped regions of a visual scene), still images and hybrids of natural (real-world) and synthetic (computer-generated) visual information [1]. MPEG-4 Visual classes of profiles include 'simple' profiles (coding of rectangular video frames), object-based profiles (coding of arbitrary-shaped visual objects), still texture profiles (coding of still images or 'texture'), scalable profiles (coding at multiple resolutions or quality levels) and studio profiles (coding for high-quality studio applications).

The Moving Picture Experts Group and the Video Coding Experts Group (MPEG and VCEG) developed 'Advanced Video Coding' (AVC) standard. It is published jointly as Part 10 of MPEG-4 and ITU-T Recommendation H.264 [2]. In contrast with MPEG-4 Visual, H.264 provides high compression as compared to previous standards. It has features like Video Coding Layer (VCL) and Network Abstraction Layer (NAL) to support reliable, robust transmission over multiple channels and networks like ISDN, cable modem, DSL, UMTS, wireless networks, LAN etc. Only three profiles are currently supported. The Baseline profile (for "conversational" applications such as video conferencing or video telephony), the Extended profile (for video streaming across networks) and the Main profile (for consumer applications such as video broadcast and storage).

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

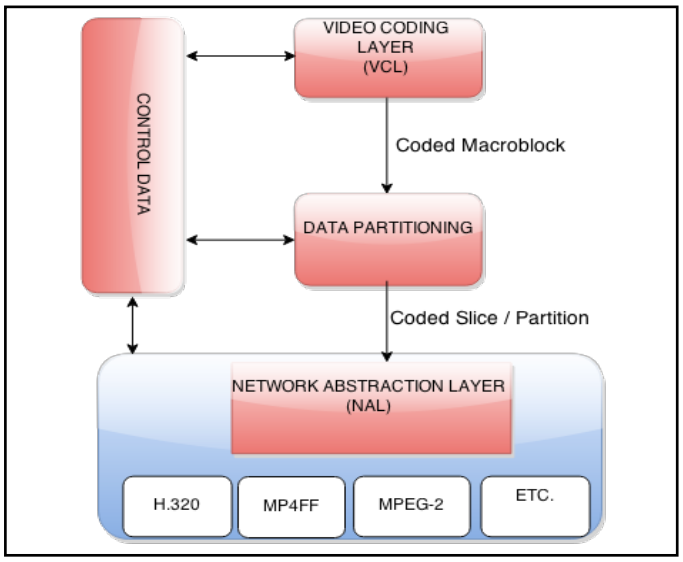

Figure1: Structure of H.264/AVC encoder

The scalable video coding (SVC) extension of H.264/AVC enables a decoder to selectively decode a part of the bit stream. The SVC bit stream consists of a base layer and one or more enhancement layers. This can be useful for low complexity or limited resources decoder like in mobile devices to decode only the base layer for a low quality version. A low-rate bit stream may be extracted for transmission over a network channel with limited capacity. The enhancement layers increases the bit rate compared to H.264/AVC [3] and thus there is a bandwidth overhead.

There are different container formats for storage and transmission of the encoded pictures. MPEG-PS or Program stream is used for reliable media like DVDs. MPEG-TS or Transport stream is designed for less reliable transmission such as terrestrial or satellite broadcast. Unlike program stream that can carry one program, a transport stream can carry different programs which are multiplexed in the stream. MPEG-TS format is also used in IPTV. These two container formats are specified in the MPEG-2 Part 1 document [4].

Real time protocol (RTP) is an application layer protocol that can be used to stream audio and video data over IP networks. The packet header provides detection of out of sequence messages. It also provides facilities for jitter compensation generally found in IP networks. RTP packets can be multicasted for video streaming to multiple destinations. The MPEG-4 Part 8 document specifies method to carry MPEG-4 data in RTP payloads.

III. Video Encryption Schemes

The suitability of an appropriate video encryption scheme depends on the application in which it is going to be used. Different degree of security may be required for different applications. Low security may not be a problem for pay-TV or Video on Demand (VOD) applications. It may be desirable that a consumer be able to watch low quality resolution picture (transparent encryption) [5]. High security is required in case of video telephony or video conferencing applications. Video can be consumed by heterogeneous devices like low powered and limited resources capacity mobiles. Hence computational efficiency of the encryption or decryption plays an important factor especially in case of real time applications such as live TV. It may also be required that the chosen video encryption scheme preserves functionalities such as format compliance, transcodability and watermarking [5].

Encryption of the video can take place before compression, during compression or after compression. Encryption before compression techniques are mainly used for privacy preservation or encrypting region of interest. However, these techniques can reduce compression efficiency [5]. Joint or integrated compression and encryption algorithms are codec specific and require modifications to the standard codec. Thomas St¨utz and Andreas Uhl [5] discussed different techniques in detail. These algorithms maintain format compliance and can preserve transcodability. Many approaches scramble the signs of the DCT coefficients and the MVD (motion vector differences). Some techniques use secret scan order to scan the DCT coefficients. But compression efficiency is degraded by permuting or scrambling the DCT coefficients. Numerous approaches also encrypt the intra and interprediction modes that are signaled in the bitstream. Modes are encoded using exponential Golomb codes and then encrypted. In case of compressed domain encryption algorithms (encryption after compression) the entire encoded bitstream can be encrypted or only a part of it. Payload of the Network Abstraction Layer (NAL) units in H.264 can be encrypted without losing any structure and syntax requirements. Partial encryption techniques (encryption of I or B frame types or parts of NAL units) can reduce the amount of data to encrypt and thus need less resource by reducing computational complexity.

Symmetric encryption algorithms like AES, DES and others can be use to secure the video content and can provide block or stream based encryption modes. DES is insecure for many applications mainly because of the 56-bit key size being too small. AES is more secure (128, 192 and 256 bit key sizes) and supersedes DES. Wail S. Elkilani and Hatem M. Abdul-Kader [6] demonstrated the performance of AES in encrypting MPEG-4 video compared to two symmetric encryption techniques RC4 and XOR. The encryptions delay overhead using AES is less compared to the overhead using RC4 and XOR algorithm.

Watermarking can complement video encryption to protect copyrights and help in content tracking by embedding signal of ownership information or identities of buyers.

In some case if video is not encrypted and still we may need to block the video content. One such approach has been discussed by Devani et al. to block videos on the fly using GPU based system [14].

IV. Multicast Streaming

Many applications in the Internet like video conferencing, live video streaming, IPTV… require simultaneous communication between groups of computers. IP multicast routing permits a single IP datagram to be routed to multiple hosts simultaneously. Thus compared to traditional unicast communication multicast communication reduces significant bandwidth requirements by reducing the network traffic.

Each multicast group is identified by a group address. Internet Group management protocol IGMP in IPv4 and MLD in IPv6 are used to keep track of hosts in a group. A host uses protocol like IGMP to join a multicast session by informing the routing system that it should deliver packets for a particular multicast group to this host. A host can join or leave a multicast group at any time it wishes to do so. Thus joining and leaving a multicast group is dynamic.

A host in a multicast group can send or receive multicast messages to or from neighbors. Thus securing the message or the content becomes very important. This requires a group key

management technique to distribute and maintain cryptographic keys with registered group members. It must not be possible for a host that joins a group in the middle of the communication to read past messages or data and similarly a host that leaves a group must not be able to read future messages or data. The above two requirements are called as forward and backward secrecy. To maintain forward and backward secrecy a new group key is generated whenever a member joins or leaves the group. This entails large number of key update messages if the group size is huge and members join and leave frequently.

Multicast group key management techniques can be characterized into Centralized, Decentralized and Distributed solutions [7]. Centralized solutions are simple but don't scale well with a big size and dynamic group. In addition to that this mechanism is highly unreliable. Decentralized and distributed key management solutions overcome these drawbacks. They reduce the dependency on a single key distribution server and also reduce the number of key update messages that need to be sent whenever a host joins or leaves a group.

Yu-Lun Huang et. al. [8] proposed three key distribution schemes for pay-TV systems. A four level key hierarchy is used for subscription channel protection and a three level key hierarchy for pay per view channels. Only one message is needed to renew key in the key distribution schemes for subscription channel protection. One-way hash function and exclusive-OR operation are used for key updates to reduce the computation cost.

Sungoh Hwang et. al. [9] proposed an approach to key management, called 2-way Hash Chains Scheme (2HCS). The proposed scheme maintains forward and backward secrecy. In comparison with the 3G Multimedia broadcast/ Multimedia service and OMA BCAST standards for group key management the method shows reduction in the number and the size of keying messages.

Table 1. Group key management schemes [7]

1.	Centralized Solutions	Naive Key Management Scheme Pairwise Keys Group Key Management Protocol Logical Key Tree
2.	Decentralized Solutions	Scalable Multicast Key Distribution Iolus System
3	Distributed Solutions	Distribution Registration and Key Distribution Baal

IPTV delivers television services using Internet or LAN. IPTV content can be viewed using set-top box or any other customer premise equipment given by the service provider. Generally H.264 is used as a video codec to deliver the multimedia content. Compressed video packets are encapsulated in MPEG-TS or RTP packets. MPEG-TS is primarily used in traditional satellite and cable broadcast communications. Conditional access system (CAS) is used to deliver secure content to subscribed viewers. A conditional access system facilitates the charge for video subscription in a pay-TV system However, since IPTV uses multicast for Live TV video streaming it also faces the problem of group key management.

V. Peer-to-Peer Streaming

Peer-to-peer (P2P) networking is a distributed architecture in which the participating nodes share the work loads. In contrast to multicast architecture it does not require support from Internet routers and network infrastructure. Each newly joined node not only downloads a portion of the content but also uploads to other peers in the network. Thus scaling becomes easy as more nodes or peers mean more resources. It has become the most popular architecture for file sharing systems like BitTorrent. File sharing systems are not real time dependent as compared to applications like video streaming or broadcast that need stringent realtime deadlines to be met. The job becomes further complicated as video broadcasting means more bandwidth and the need to keep track of large number of peers participating and leaving.

Ammar Waysi AITuhafi et. al. [10] discussed a comparison of Peer-to-peer topologies for video streaming. Tree and mesh are the basic P2P networking topologies. In Tree topology source is at the root of the tree, broadcasting the video stream. Each peer receives stream from its parent in the tree. The video stream is then push down to its children. The drawback of this topology is that the peers or leaves will not help in uploading any data and thus only downloading will take place at the bottom of the tree. Failure of nodes that are at a higher level in the tree means disruption of stream to the whole subtree.

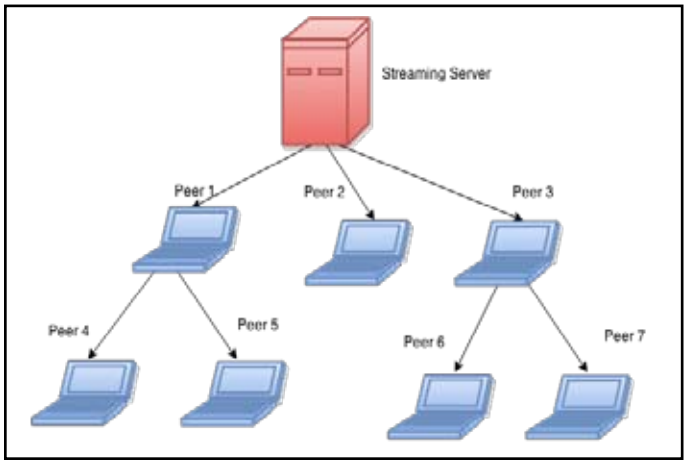

Figure 2 : Tree topology for Peer-to-peer streaming

In Mesh topology a peer can download data or stream from number of nodes and can upload to other nodes in turn. The advantage is that the failure of some single source node has less effect since other nodes are available as source. Thus it is more reliable. It is also shown to have a better performance than tree topology. However, it is more difficult to create and maintain as compared to tree topology.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

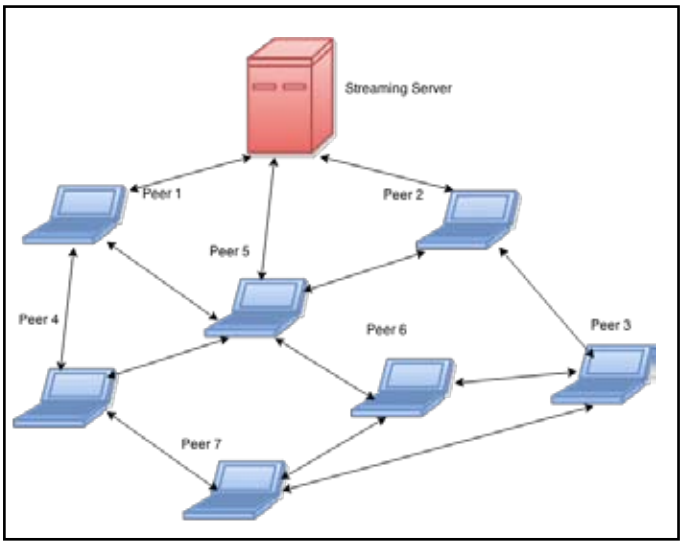

Figure 3: Mesh topology for Peer-to-peer streaming

All P2P topologies face attacks like free riding and data pollution. Free riding is the case when a peer doesn't contribute to uploading of any data but only downloads it. In data pollution attack malicious node can mix some unwanted or corrupt data chunks with the original data chunks. Thus receiving peers will in turn forward this data to other peers in the network polluting the whole data or stream. Dhungel et. al. [11] discussed different defenses against such an attack like blacklisting, traffic encryption, hash verification, and chunk signing. Chunk signing in which the source signs all the data chunks was shown to be more effective than others.

Jeff Seibert et. al. [12] discussed vulnerabilities and attacks in data delivery in a mesh topology for video streaming. The authors proposed a reputation scheme in which each peer computes the reputation scores of the other known peers. The reputation score helps in deciding which peer to admit as neighbor as well as which peer should remain as neighbor. The scheme is shown to be resistant to attacks such as slandering, white-washing and self-promotion.

VI. Conclusion

H.264/AVC codec achieves more compression efficiency and is widely used for streaming video as compared to MPEG-4 Visual Part 2. Encryption during compression techniques help to reduce computational complexity but can lead to less compression efficiency as compared to encryption after compression schemes. Multicast streaming can preserve the bandwidth as compared to unicast streaming. It needs infrastructure support like routers and also suffers from large rekeying messages if group size is large and dynamic. Peer-to-peer streaming scales efficiently compared to multicast but it is prone to attacks like free riding, data pollution and data availability from malicious neighbor nodes.

References

[1] *I. E. G. Richardson, H.264 and MPEG-4 Video Compression: Video Coding for Next Generation Multimedia. New York: Wiley, 2003.*

[2] *T. Wiegand, G. J. Sullivan, G. Bjontegaard, and A. Luthra, "Overview of the H.264/AVC video coding standard," IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 7, July 2003.*

[3] *Heiko Schwarz, Detlev Marpe and Thomas Wiegand, "Overview of the Scalable Video Coding Extension of the H.264/AVC Standard," IEEE Transactions on Circuits and Systems for Video Technology, vol. 17, no. 9, Sep. 2007.*

[4] *ISO/IEC 13818-1, ITU-T Recommendation H.222.0, "Information technology – Generic coding of moving pictures and associated audio information: Systems", Feb. 2012*

[5] *T. Stütz and A. Uhl, "A survey of H.264 AVC/SVC encryption," IEEE Transactions on Circuits and Systems for Video Technology, vol. 22, no. 3, March 2012.*

[6] *Wail S. Elkilani, Hatem M. Abdul-Kader, "Performance of Encryption Techniques for Real Time Video Streaming," IEEE International Conference on Networking and Media Convergence (ICNM), 2009.*

[7] *Youssef Baddi and Mohamed Dafir, "Key Management for Secure Multicast Communication: A Survey," IEEE, 2013.*

[8] *Yu-Lun Huang, Shiuhpyng Shieh, Fu-Shen Ho and Jian-Chyuan Wang, "Efficient Key Distribution Schemes for Secure Media Delivery in Pay-TV Systems," IEEE Transcactions on Multimedia, vol. 6, no. 5, Oct. 2004.*

[9] *Sungoh Hwang, Sergey Seleznev, and Jae Yong Lee, "New Key Management Approach for Broadcast and Multicast Services," IEEE Communications Letters, vol. 15, no. 2, Feb. 2011.*

[10] *Ammar Waysi AITuhafi, Sureswaran Ramadass and Yung-Wey Chong, "Concepts and Types of Peer-to-Peer Network Topology for Live Video Streaming," IEEE International Conference on RFID Technologies and Applications, 2013*

[11] *P. Dhungel, X. Hei, K. Ross, and N. Saxena, "The pollution attack in p2p live video streaming: Measurement results and defenses," ACM SIGCOMM P2P-TV Workshop, 2007.*

[12] *Jeff Seibert, Xin Sun, Cristina Nita-Rotaru, Sanjay Rao, "Towards Securing Data Delivery in Peer-to-Peer Streaming," IEEE conference on Communication Systems and Networks (COMSNETS), 2010.*

[13] *Vilas Naik, Vishwanath Chikaraddi, Prasanna Patil, "Query clip genre recognition using tree pruning technique for video retrieval," International Journal of Computer Engineering and Technology (IJCET), ISSN 0976 – 6367(Print), ISSN 0976 – 6375(Online) Volume 4, Issue 4, July-August (2013), pp. 257-266 ISSN 09766367(Print).*

[14] *Urvesh devani, V.B.Nikam and B.B.Meshram, "On the fly porn video blocking using distributed Multi-GPU and data Mining approach," International Journal of distributed and parallel system Vol.5 No.4 July 2014*