

Security Considerations and Techniques for Video Streaming Distribution in Home ISPs

Iliyan Iliev ^{1,*}, Ivan Blagoev ¹ and Krassimira Stoyanova ¹

¹ Institute of Information and Communication Technologies at the Bulgarian Academy of Sciences, Acad. G. Bonchev St., 1113 Sofia, Bulgaria; ivan.blagoev@iict.bas.bg, krassimira.stoyanova@iict.bas.bg

*E-mail of corresponding author: iliyen.iliev@iict.bas.bg

Abstract: The increasing adoption of Internet live-streaming services and high-resolution video formats generates significant network traffic and requires stable high-bandwidth Internet connectivity. However, many regional Internet service providers (ISPs) still face practical limitations in delivering high-quality live-streaming services to subscribers, particularly in environments with limited external Internet capacity. This paper proposes an architectural approach for secure redistribution of Internet live-streaming services within local ISP infrastructures based on passive optical network (PON) environments. The proposed model combines multicast-oriented traffic distribution with encrypted HTTP Live Streaming (HLS), conditional access mechanisms, certificate-based authentication, and dynamic cryptographic key management for IPTV set-top boxes. In addition, the paper discusses security considerations related to authentication, encrypted key delivery, band-width optimization, and protection against unauthorized redistribution of multimedia content.

Keywords: cybersecurity; live streaming; IPTV; FTTH; PON; multicast; HLS; video encryption; conditional access; authentication; content protection.

Received 30 March 2026

Accepted 5 July 2026

Published 23 September 2026

1. Introduction

The rapid growth of Internet-based live-streaming services and over-the-top (OTT) platforms has significantly increased the demand for reliable high-bandwidth multimedia delivery [1]. Modern high-resolution video formats, including 4K and High Frame Rate (HFR) streaming, require stable network connectivity and efficient traffic distribution mechanisms despite improvements in video compression technologies [2]. In regional and remote areas, Internet service providers (ISPs) may still experience limitations related to external Internet capacity and scalability of multimedia delivery infrastructures.

Passive optical network (PON) technologies are increasingly deployed in ISP environments due to their efficient bandwidth utilization and scalability [3]. Such infrastructures create opportunities for implementing local redistribution mechanisms for live-streaming services in order to reduce external traffic consumption and improve quality of service for end users. In this context, multicast-based delivery models are particularly suitable because they minimize unnecessary traffic replication during simultaneous distribution of identical multimedia streams to multiple subscribers [4,5].

At the same time, redistribution of protected multimedia content introduces important cybersecurity

and content-protection challenges. Modern streaming platforms rely on encryption, authentication, and conditional-access mechanisms to prevent unauthorized access and illegal redistribution of copyrighted content. HTTP Live Streaming (HLS), one of the most widely adopted streaming technologies, supports encrypted MPEG Transport Stream delivery using AES-based protection mechanisms defined in RFC 8216 [7].

This paper proposes an architectural approach for secure redistribution of Internet live-streaming services within local ISP environments. The proposed model combines multicast-based distribution in PON infrastructures with encrypted HLS delivery, external authentication services, and dynamic cryptographic key management for IPTV set-top boxes (STBs). The paper additionally discusses practical considerations related to conditional access, authentication workflows, encrypted key delivery, and protection against unauthorized redistribution of multimedia content.

1.1. Main Contributions

This paper proposes an architectural approach for secure redistribution of Internet live-streaming services within ISP-operated passive optical network environments. The proposed model combines multicast-oriented traffic distribution with encrypted HTTP Live Streaming (HLS), certificate-based authentication, and dynamic cryptographic key management for IPTV set-top boxes [6–8].

Particular attention is given to the separation between content distribution, authentication services, and key-management infrastructures in order to reduce direct



exposure of protected multimedia content and sensitive user information. The proposed workflow additionally addresses practical considerations related to bandwidth optimization, secure key delivery, and prevention of unauthorized redistribution in local ISP environments [3–5].

The presented architecture is intended as a practical engineering framework that may support future implementation and performance evaluation of secure live-stream redistribution systems in real ISP infrastructures.

2. Proposed Architecture for ISP Live Streaming Redistribution

The proposed approach is based on the deployment of a local streaming node within the infrastructure of an Internet service provider (ISP) for the purpose of redistributing Internet live-streaming content to end users independently of limitations in their external Internet connectivity. Such an architecture aims to improve the accessibility of high-quality protected multimedia services in regional ISP environments while simultaneously reducing the amount of external traffic generated by multiple subscribers consuming identical live-streaming content.

The implementation of local redistribution mechanisms may provide several practical advantages for Internet service providers and their subscribers. By maintaining local synchronization of multimedia streams and redistributing them through the ISP infrastructure, subscribers may access high-quality protected video content with improved stability and reduced dependence on external network conditions. At the same time, the reduction of replicated external traffic may improve bandwidth efficiency for the provider, particularly during large-scale live broadcasts involving a significant number of simultaneous viewers. In addition, the deployment of local redistribution platforms may create opportunities for promoting regional multimedia initiatives and locally distributed video services.

The proposed architecture is primarily focused on deployment within passive optical network (PON) environments, as PON technologies are increasingly replacing traditional copper-based access infrastructures such as ADSL, VDSL, and copper Ethernet networks. Modern PON deployments provide scalable bandwidth distribution models and support efficient integration of multimedia services within ISP infrastructures [3]. In such environments, multicast-oriented traffic distribution mechanisms become particularly suitable because they minimize unnecessary replication of identical multimedia traffic and improve scalability during simultaneous delivery to multiple subscribers.

The implementation of secure local redistribution of protected multimedia content requires consideration of several key technical aspects. These include efficient traffic distribution techniques capable of avoiding unnecessary concentration of traffic at a single network point, secure authentication and encryption mechanisms for protecting multimedia streams, and additional measures intended to reduce the risk of unauthorized redistribution of copyrighted content.

Modern web-streaming services typically rely on separate protocols for upstream media contribution and downstream content delivery, with RTMP and HTTP Live Streaming (HLS) being among the most widely adopted protocol combinations. This architectural separation has evolved as a practical response to the characteristics of consumer Internet connectivity and the requirements of adaptive multimedia delivery. Within the HLS protocol, multimedia streams are divided into encrypted video segments accompanied by periodically updated M3U playlists describing the available media fragments and corresponding decryption parameters [7]. To achieve service reliability, low latency, and efficient load balancing, modern streaming platforms are commonly deployed using content delivery network (CDN) architectures consisting of geographically distributed streaming nodes.

In the proposed model, the local ISP streaming node operates as an intermediary redistribution component between the external streaming platform and the local subscriber network. The node continuously synchronizes encrypted multimedia segments from the original streaming service while simultaneously redistributing the content to local subscribers through the ISP infrastructure. This approach allows optimization of external bandwidth consumption while preserving compatibility with existing streaming technologies, authentication workflows, and content protection mechanisms.

3. Distribution techniques

3.1. Unicast Combined with Server–Client Communication

Unicast server–client communication remains the most widely used approach for Internet video streaming due to its simplicity, reliability, and compatibility with existing web infrastructures. Modern streaming platforms commonly rely on unicast delivery because it allows straightforward session management and efficient integration with adaptive streaming technologies such as HTTP Live Streaming (HLS) and content delivery network (CDN) architectures [7]. However, in local ISP redistribution environments, pure unicast delivery leads to repeated transmission of identical multimedia traffic between the streaming source and the local redistribution node. As a result, the approach is less suitable in scenarios where minimization of replicated external traffic and bandwidth optimization are primary objectives.

3.2. Peer-to-Peer (P2P)

Peer-to-Peer (P2P) communication represents a distributed traffic-delivery approach intended to reduce concentration of network traffic at a single distribution point. P2P mechanisms have historically been applied in file-sharing systems, multimedia distribution platforms, device discovery protocols, and decentralized communication services. In multimedia streaming environments, P2P architectures may improve scalability by distributing traffic generation among participating client devices instead of relying exclusively on centralized streaming servers.

Despite these advantages, large-scale P2P redistribution is less suitable for passive optical network (PON) infrastructures operating in Point-to-Multipoint (P2M) environments. In such networks, multiple optical network terminals (ONTs) share common downstream and upstream bandwidth resources associated with a single optical line terminal (OLT) port. Consequently, uncontrolled peer-generated traffic may introduce additional network congestion and reduce the efficiency of bandwidth utilization, particularly in scenarios involving high-bitrate live-streaming services.

3.3. Multicast

Multicast communication provides an efficient mechanism for distributing identical multimedia traffic simultaneously to multiple subscribers without unnecessary replication at a single network point. For this reason, multicast technologies are particularly suitable for live-streaming services deployed within modern passive optical network infrastructures [4,5]. In multicast environments, a single multimedia stream may be transmitted through the network and replicated only at the appropriate distribution points, thereby significantly reducing bandwidth consumption compared to traditional unicast delivery models.

The application of multicast delivery in PON environments extends traditional multicast concepts used in enterprise and carrier-grade networks by introducing additional mechanisms associated with multiplexed optical transmission and GEM frame processing [5,6]. In such architectures, multicast frames may contain identifiers corresponding to the destination optical network terminals, allowing efficient distribution of multimedia traffic between the optical line terminal and multiple subscriber devices. The general multicast distribution model in a GPON environment is illustrated in Figure 1:

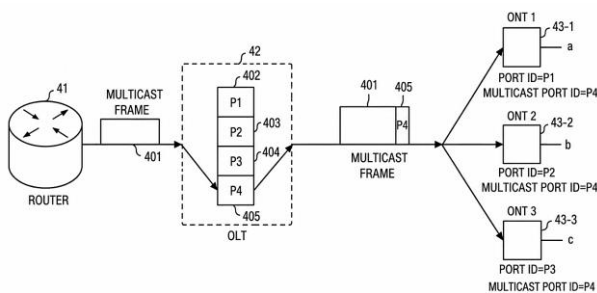


Figure 1. Multicast GPON transmission and GEM frame processing method multicast frame transmitted in PON (adapted from [6]).

4. Security Considerations

4.1. Communication security

Communication security in multimedia streaming systems is traditionally implemented through conditional-access architectures similar to those used in Digital Video Broadcasting (DVB) ecosystems. In such systems, cryptographic key exchange procedures and content scrambling mechanisms are logically separated, while specific conditional-access implementations, including

Conax, Irdeto, VideoGuard, and Viaccess, integrate these functions into unified content-protection frameworks [8,9]. The primary objective of these mechanisms is to restrict access to protected multimedia content exclusively to authorized client devices and authenticated subscribers.

A comparable security model may be applied to HTTP Live Streaming (HLS)-based infrastructures. The HLS specification defined in RFC 8216 supports encryption of MPEG Transport Stream (TS) video segments using AES-based cryptographic protection mechanisms [7]. In this approach, multimedia content is encrypted on the streaming server before distribution, while authorized client devices obtain the information necessary for decryption through standardized M3U playlists and associated key-delivery procedures. The playlist metadata specifies the encryption method, cryptographic parameters, and the location of the corresponding decryption keys required for processing protected video segments.

Such an architecture allows encrypted multimedia traffic to be distributed through intermediate network infrastructures, including ISP-operated redistribution nodes, without exposing the original video content in unencrypted form. As a result, the streaming infrastructure may maintain compatibility with existing CDN and multicast-oriented delivery models while preserving secure conditional access to protected multimedia services.

4.2. Authentication

In encrypted multimedia streaming environments, the protection of video segments alone is insufficient without reliable mechanisms for authenticating authorized client devices and subscribers. Since encrypted HLS segments cannot be decrypted without access to the corresponding cryptographic keys, authentication procedures may be focused primarily on controlling secure access to key-delivery services rather than to the multimedia traffic itself [8,10]. Such an approach allows encrypted video content to be distributed through intermediate infrastructures while restricting decryption capabilities exclusively to authorized playback devices.

Previous research has demonstrated that conditional-access mechanisms for web-based video streaming may be implemented through authenticated user sessions and cryptographic token exchange between client devices and streaming services [10]. A similar approach may be applied within the proposed ISP redistribution architecture, where authentication procedures are integrated directly into the cryptographic key-delivery workflow instead of the multimedia segment delivery process itself. In this model, the streaming infrastructure distributes encrypted multimedia traffic independently of the authentication subsystem, while access to decryption keys remains protected through authenticated sessions and authorization tokens.

The proposed authentication architecture relies on interaction between IPTV set-top boxes (STBs), external trust-service providers, and key-management infrastructures responsible for distributing authorized cryptographic material. After successful user authentication, the client device obtains temporary

authorization credentials that allow secure retrieval of the corresponding decryption keys required for processing protected multimedia segments. Such separation between encrypted multimedia delivery and authentication procedures improves scalability of the streaming infrastructure while reducing direct exposure of protected content and sensitive authentication information.

In practical ISP environments, encrypted HLS playback is expected to be performed primarily through dedicated IPTV set-top boxes rather than general-purpose web browsers. Consequently, the authentication workflow must support automated session establishment, secure token management, and controlled cryptographic key distribution within consumer multimedia devices. The overall architecture of the proposed redistribution model, including streaming infrastructure, authentication services, and cryptographic key management, is illustrated in (Figure 2).

4.3. Example Workflow for System Operation

The proposed redistribution architecture relies on integration between IPTV set-top boxes (STBs), external trust-service providers, and cryptographic key-management infrastructures responsible for authorizing access to protected live-streaming services. Initially, the subscriber registers with a trust-service provider integrated into the streaming ecosystem and creates a user profile accessible through a mobile application or similar authentication platform. In practical deployments, such identification procedures are typically performed remotely through secure online verification mechanisms.

When a protected live-streaming event becomes available, the subscriber selects the corresponding streaming service and associated trust-service provider directly from the IPTV set-top box interface. The STB subsequently generates an asymmetric cryptographic key pair, where Elliptic Curve Cryptography (ECC) is

recommended because it provides comparable security strength with substantially shorter key sizes than RSA [14]. The device additionally generates a PKCS#10 Certificate Signing Request (CSR) containing a randomly generated identifier, such as a UUID-based common name, intended to minimize direct exposure of user-identifiable information.

To establish the authentication workflow, the STB encodes a dedicated authorization URL as a QR code displayed on the television screen. In parallel, the device transmits the generated CSR to the trust-service provider and waits for certificate issuance. The subscriber scans the QR code using the authentication provider's mobile application and confirms authorization for access to the selected live-streaming service. Following successful authentication and authorization, the trust-service provider signs the CSR, issues a temporary X.509 certificate with limited validity corresponding to the duration of the live event, and forwards the certificate information to the streaming infrastructure.

After certificate issuance, the IPTV set-top box downloads the corresponding X.509 certificate and initiates the protected streaming workflow. The streaming platform encrypts the AES decryption keys associated with the multimedia stream using the public keys of authorized subscriber certificates and stores the encrypted key material within a dedicated key repository. To retrieve the required decryption keys, the STB establishes an HTTPS connection to the key-management service using mutual TLS authentication with the issued client certificate and associated private key. Following successful authentication, the key-management infrastructure issues a temporary cryptographic authorization token allowing the device to retrieve the encrypted AES keys required for multimedia playback.

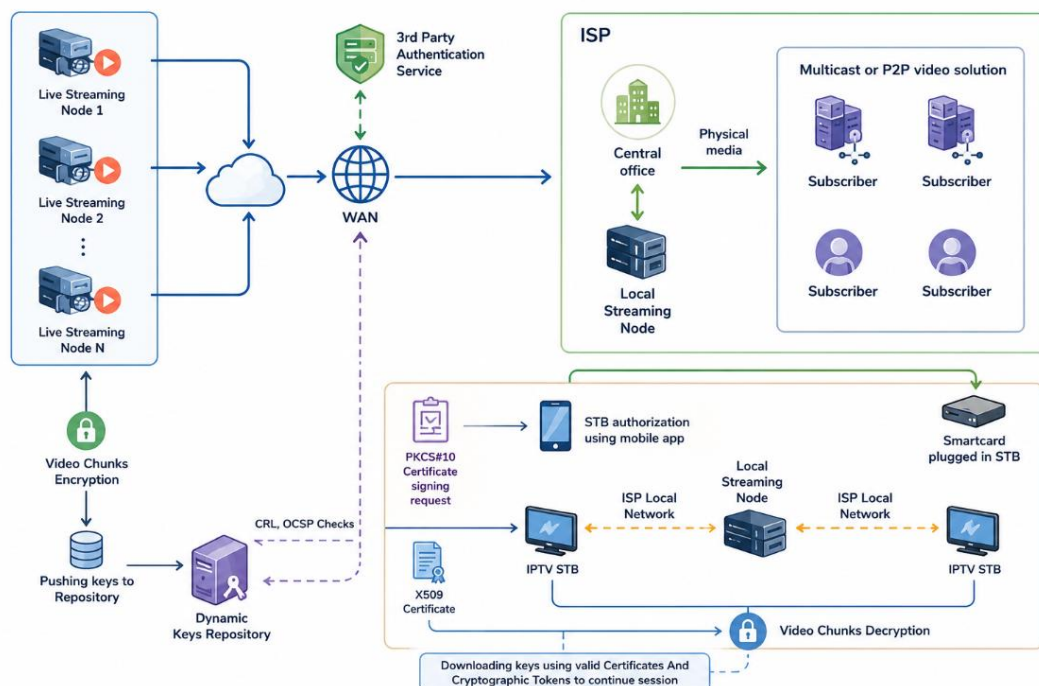


Figure 2. General scheme for Live Streaming redistribution in a local ISP environment.

The IPTV set-top box decrypts the retrieved AES keys locally using its private key and subsequently applies the decrypted symmetric keys to process the encrypted HLS video segments. Once the authenticated session has been established, repeated client-certificate authentication is not continuously required during active playback. Instead, temporary authorization tokens may be periodically renewed within the active session lifecycle, while prolonged inactivity or token expiration requires re-establishment of the authenticated TLS session.

The proposed workflow is designed to minimize unnecessary exposure of personal information and sensitive cryptographic material within the ISP infrastructure. Personal-data processing operations remain isolated within the systems of the external authentication provider, while the ISP infrastructure primarily operates as a transport and redistribution environment for encrypted multimedia traffic. Similarly, the key-management repository may operate as an independent service separated from both the authentication provider and the multimedia distribution infrastructure, thereby reducing direct exposure of decryption capabilities within intermediary network components.

In the presented scenario, X.509 certificates issued by the trust-service provider are used as authentication credentials for multimedia access control. Since typical multimedia streaming services do not require qualified electronic identification procedures, the generated certificates are not necessarily qualified certificates within the meaning of formal electronic identification frameworks. Consequently, private cryptographic keys may be generated and stored directly on consumer devices rather than exclusively within specialized hardware security modules or smart-card environments. While such an approach simplifies deployment and improves usability, it also introduces potential security considerations associated with unauthorized extraction or replication of cryptographic material from compromised playback devices, which remains relevant in the context of illegal redistribution of protected multimedia content.

4.4. Limitations and Performance Overhead

Despite the advantages of the proposed architecture regarding bandwidth optimization and secure redistribution of live-streaming content, several practical limitations and performance considerations must be taken into account during implementation. The integration of authentication services, encrypted key delivery, and conditional access mechanisms inevitably increases the complexity of the overall streaming infrastructure and introduces additional processing and communication overhead.

One of the primary factors affecting system performance is the authentication and session establishment procedure between IPTV set-top boxes, the trust service provider, and the local streaming infrastructure. The proposed workflow relies on asymmetric cryptographic operations, certificate issuance, HTTPS communication, and token-based session management. These mechanisms introduce additional computational work associated with asymmetric cryptographic operations, certificate processing, secure

communication exchanges, and token management during session establishment. In large-scale deployments involving simultaneous authentication requests from numerous subscribers, the trust service provider and key management infrastructure may become a bottleneck if appropriate load-balancing and scaling mechanisms are not implemented.

Additional session-establishment latency may also occur during the initialization phase of live-stream playback. Before receiving decryption keys, the client device must complete authentication procedures, establish secure communication channels, and obtain valid authorization tokens. Although the amount of control traffic associated with these procedures is relatively small compared to the video stream itself, the additional communication exchanges and cryptographic operations may increase playback startup time, particularly during high-demand live events with a large number of concurrent users.

Another important consideration concerns the secure storage and management of cryptographic material within IPTV set-top boxes. In the proposed architecture, private keys may be generated and stored directly on client devices. Although this approach simplifies deployment, secure management and storage of cryptographic keys become critical implementation requirements, since compromise of keying material may undermine the protection of encrypted content [11]. Consequently, unauthorized extraction of cryptographic material from compromised devices remains a potential risk factor for illegal redistribution of protected content.

The multicast-based distribution model additionally introduces synchronization and network-management challenges in passive optical network environments. Efficient multicast delivery requires proper configuration of Internet Group Management Protocol (IGMP) mechanisms, multicast forwarding policies, and traffic isolation procedures between optical network terminals [5]. Improper multicast configuration may lead to packet duplication, unnecessary bandwidth consumption, or instability during large-scale live-stream distribution. Furthermore, encrypted HLS delivery combined with multicast redistribution may require careful balancing between segment duration, synchronization intervals, and caching strategies in order to minimize playback interruptions and buffering delays.

The proposed architecture also depends on the availability and reliability of external trust-service providers responsible for authentication and certificate issuance. Temporary unavailability of such services may prevent subscribers from establishing new playback sessions even if the streaming infrastructure itself remains operational. For this reason, practical deployments should consider redundancy mechanisms, distributed authentication infrastructures, and fallback procedures for maintaining service continuity during network failures or maintenance periods.

Finally, although encryption and authentication mechanisms significantly improve protection against unauthorized access, they cannot fully eliminate the possibility of illegal redistribution of multimedia content after successful playback authorization. Once decrypted

video reaches an authorized endpoint device, various recording and retransmission techniques remain technically possible despite the use of watermarking, HDCP, and conditional access technologies [11,12]. Therefore, practical protection of copyrighted multimedia content continues to require a combination of technical safeguards, legal enforcement mechanisms, and operational monitoring procedures.

5. Prevention against Illegal Redistribution

Protection against unauthorized redistribution remains a major challenge in modern multimedia streaming systems. Unlike analogue broadcasting, digital technologies allow multimedia content to be copied and redistributed without degradation of the original quality, creating favorable conditions for large-scale digital piracy [11].

Modern content-protection strategies therefore combine legal and technical mechanisms intended to limit unauthorized redistribution of protected multimedia services. Legal approaches typically rely on contractual agreements and copyright regulations restricting unauthorized copying and retransmission of multimedia content [11].

In addition, streaming infrastructures employ technical protection mechanisms such as digital watermarking and hardware-based content protection. Watermarking techniques embed identifying information into multimedia streams in order to trace unauthorized redistribution, although practical watermarking schemes must remain robust against various manipulation and removal attacks [12]. Another content-protection mechanism is High-bandwidth Digital Content Protection (HDCP), which protects encrypted digital content transmitted between source and receiver devices. Earlier HDCP protocol versions have been shown to contain authentication and key-exchange weaknesses, including impersonation-related attacks [13].

Consequently, complete prevention of illegal redistribution remains technically difficult even in infrastructures implementing encryption, authentication, watermarking, and hardware-based protection simultaneously. Practical multimedia security architectures must therefore balance usability, deployment complexity, and content-protection effectiveness while acknowledging that no existing solution can fully eliminate the risk of unauthorized redistribution after legitimate playback access has been granted.

6. Discussion

Despite the deployment of modern encryption, authentication, and conditional-access mechanisms, complete prevention of unauthorized redistribution of multimedia content remains technically challenging once protected content reaches an authorized playback device. Consumer environments inherently allow various recording and retransmission techniques, including external capture and screen-recording methods.

Consequently, practical multimedia protection architectures must balance security, usability, deployment complexity, and economic feasibility. Excessively complex protection mechanisms may negatively affect

scalability, infrastructure costs, and user experience without fully eliminating the possibility of unauthorized redistribution.

For this reason, contemporary streaming ecosystems typically rely on a combination of technical safeguards, contractual restrictions, monitoring procedures, and legal enforcement mechanisms rather than on a single isolated protection technology.

7. Conclusion

This paper presented an architectural approach for secure redistribution of Internet live-streaming services within local ISP environments. The proposed model combines multicast-based distribution in passive optical network infrastructures with encrypted HTTP Live Streaming delivery, external authentication services, and dynamic cryptographic key management for IPTV set-top boxes. The approach aims to reduce external ISP traffic consumption while maintaining secure access to protected multimedia content.

The presented architecture demonstrates how encrypted video delivery, certificate-based authentication, and conditional-access mechanisms may be integrated into a unified streaming ecosystem while preserving separation between content distribution, authentication services, and cryptographic key management. At the same time, the implementation of such systems introduces practical challenges related to authentication latency, session management, scalability, and protection against unauthorized redistribution of multimedia content despite the use of encryption, watermarking, and hardware-based protection technologies.

Future work may include experimental validation of the proposed architecture in real ISP environments, analysis of multicast scalability in large PON deployments, and evaluation of authentication overhead, key-distribution performance, and quality-of-service parameters during live-streaming delivery.

References

- [1] Tefertiller, A. & Sheehan, K. (2019). TV in the Streaming Age: Motivations, Behaviors, and Satisfaction of Post-Network Television. *Journal of Broadcasting & Electronic Media*, vol. 63, pp. 595–616. doi: 10.1080/08838151.2019.1698233.
- [2] Mackin, A., Zhang, F. & Bull, D.R. (2019). A Study of High Frame Rate Video Formats. *IEEE Transactions on Multimedia* 2019, vol. 21, 1499–1512. doi: 10.1109/TMM.2018.2880603.
- [3] Arpaci, M., Ho, E. & Yen, W. (2001). Providing Integrated Services with Broadband PON. *Proceedings of SPIE*, Vol. 4583, Metro and Access Networks, pp. 20–30. doi: 10.1117/12.445133.
- [4] AMX by HARMAN. (2015). Multicast for Enterprise Video Streaming. White Paper, v.01.2015. Official AMX white-paper page: <https://adn.harmanpro.com/>.
- [5] Yang, W. & Zhang, L. (2011). An Application Research on IPv6 Multicasting Testing Method. *Procedia Engineering*, vol.24, 143–151. doi: 10.1016/j.proeng.2011.11.2617.
- [6] Lim, S.-Y.; Song, J.-Y.; Kim, J.-H.; Kwon, S.-W.; Lee, Y.-S. & Lee, J.-H. (2011). Multicast GPON Transmission and GEM Frame Processing Method. European Patent EP1499155A1, 19 January 2005. <https://patents.google.com/patent/EP1499155A1>.
- [7] Pantos, R. & May, W. HTTP Live Streaming. RFC 8216. Available online: <https://www.rfc-editor.org/info/rfc8216>.

-
- [8] ITU-R. Conditional-Access Systems for Digital Broadcasting. Recommendation ITU-R BT.1852-1, January 2017. Available online: <https://www.itu.int/rec/R-REC-BT.1852-1-201701-I/en>.
- [9] Weinmann, R.-P. & Wirt, K. (2005). Analysis of the DVB Common Scrambling Algorithm. In *Communications and Multimedia Security*; Springer: Boston, MA, USA, 2005; pp. 195–207. doi: 10.1007/0-387-24486-7_15.
- [10] Iliev, I.; Blagoev, I. (2022). An Approach to Improve Web Video Streaming Security and Prevent Personal Data Leakage. *Information & Security: An International Journal*, vol. 53, pp. 78–88. doi: 10.11610/isij.5306.
- [11] Qureshi, A. & Megías, D. (2021). Blockchain-Based Multimedia Content Protection: Review and Open Challenges. *Applied Sciences*, 11, 1. <https://doi.org/10.3390/app11010001>.
- [12] Malanowska, A., Mazurczyk, W., Koohpayeh Araghi, T., Megías, D. & Kuribayashi, M. (2024). Digital Watermarking—A Meta-Survey and Techniques for Fake News Detection. *IEEE Access*, 12, 36311–36345. doi:10.1109/ACCESS.2024.3374201.
- [13] Zhao, J.; Gu, D.; Li, Y. & Cheng, W. (2012) On weaknesses of the HDCP authentication and key exchange protocol and its repair. *Mathematical and Computer Modelling*, 55(1–2), 19–25. <https://doi.org/10.1016/j.mcm.2011.01.005>.
- [14] Barker, E. (2020). Recommendation for Key Management: Part 1—General. NIST Special Publication 800-57 Part 1, Revision 5; National Institute of Standards and Technology: Gaithersburg, MD, USA. doi: 10.6028/NIST.SP.800-57pt1r5.