

Security issues in multimedia IP networks

Gergő Juhász¹, Róbert Sándor Kovács²

¹Obuda University, Doctoral School of Security Science, József körút 6., Budapest, 1088, HUN, juhasz.gergo@kvk.uni-obuda.hu

²Obuda University, Kandó Kálmán Faculty of Electrical Engineering, Institute of Electronics and Communication Systems, Department of Telecommunications and Infocommunications, Bécsi út 96/B, Budapest, 1034, HUN, kovacs.robert@kvk.uni-obuda.hu

Abstract: One of the most important elements of 21st century communications is multimedia IP communication. These networks enable high-quality content to be delivered cost-effectively from the service provider to users. With the growing popularity of this technology, the number of cyber threats and attacks targeting it has also increased dramatically. Since the IP networks used to transmit media content use the same protocols as those used for data communication, the same potential vulnerabilities exist. Due to the network architecture, vulnerabilities are not limited to home networks and content sources; attacks can also affect the core network and the delivery and distribution network. This means that in order to ensure IT security, procedures and systems must be developed to defend against attacks affecting every layer of the TCP/IP layer model. When implementing these methods, it is also important to keep in mind the principle that the user experience should not be compromised, which is why real-time criteria must be ensured. In the case of multimedia IP networks, it is not only necessary to take into account classic cyber-attacks, but also to implement appropriate rights management (subscription management) on the user side and user data protection on the service provider side. [1] From the above, we can see that these multimedia networks play a significant role in our age, which makes their IT security and research a key priority. In my article, I will discuss these cybersecurity issues and related research.

Keywords: multimedia, IP, IPTV, cybersecurity, communication

1 Introduction

IP-based multimedia content delivery has become one of the most important pillars of global mass communication today. Streaming platforms, IPTV broadcast networks, cloud-based video sharing platforms, and interactive multimedia applications are now the primary means of accessing information worldwide. Users are increasing their consumption of video, audio, and interactive content,

which they access via IP-based networks. The rapid spread of multimedia content delivery is significant not only in economic and technological terms, but also in terms of social and national security.

The primary requirement for modern streaming services is stable, fast, and reliable data transfer, which is ensured by QoS (Quality of Service). However, maintaining QoS is a significant challenge, as real-time multimedia content transfer is highly sensitive to network latency, jitter, and packet loss. Optimizing QoS parameters is therefore one of the most important challenges and a key area of research today, especially for video streaming systems that require high bandwidth and transmission speeds. [2]

Because multimedia IP networks use the same TCP/IP protocols as all other Internet services, they also have their own vulnerabilities. In addition, the specific architecture of streaming and IPTV services, which consists of CDNs, servers, and compression methods, as well as protocols that ensure real-time performance, carries with it additional attack surfaces. The issue of ensuring their secure operation is therefore multifaceted: it affects the layers of the TCP/IP model, content delivery systems, end devices, and user awareness.

The manipulation of multimedia IP infrastructures is especially dangerous in modern information warfare, as streaming systems play a critical role in informing the public. A successful attack (e.g., content replacement, service disruption, disinformation-based news reporting) can cause mass panic or social destabilization. The aim of my article is therefore to review the technological structure of multimedia IP systems, ensure QoS requirements, highlight security challenges, and present my PhD research program, which discusses the protection options for these systems.

2 The evolution of multimedia communication – from analog broadcasting to IP-based platforms

The telecommunications infrastructure of the last century was primarily defined by analog broadcast technologies. Radio and television broadcasting implemented a single-way, centralized content distribution model, which enabled widespread and fast information transfer, but completely lacked interactivity. Users only consumed content provided by the service provider, at specific times, with limited choices.

The appearance of digital broadcasting (DVB-T, DVB-S, and DVB-C technologies) led to significant improvements in quality, but the broadcast model continued to dominate. The breakthrough came with the spread of broadband Internet, which enabled IP-based content distribution. The development of

streaming technologies, improvements in content encoding efficiency, and the expansion of server-side infrastructure gradually replaced traditional broadcasting models.

The foundations of modern multimedia network development are highlighted in numerous studies, which emphasize that IP-based systems are more flexible, efficient, and customizable than traditional broadcast-based solutions. This flexibility has enabled the rapid spread of interactive services (VoD - Video on Demand, rewindable programs, customized program recommendations) and, with it, a complete change in user needs. [3]

3 The workings and architecture of multimedia IP networks

Multimedia IP -based systems are multi-layered, requiring complex infrastructure. After content is produced, server-side systems compress, encode, and upload the video to a CDN (Content Delivery Network) infrastructure, which functions as a geographically distributed network of servers. The purpose of the CDN is to place content close to users geographically, reducing latency and backbone network traffic.

Without CDNs, the quality and performance of streaming services would not be guaranteed, as QoS conditions would be compromised. CDNs provide the core of modern multimedia content delivery, ensuring continuous operation through caching, load balancing, and error management. [4]

Streaming services and IPTV demand a high degree of flexibility. The network structure is often organized in multiple layers:

- Origin servers
- CDN servers
- Local area networks
- User end devices (set-top boxes, smart TVs, mobile devices)

Content distribution takes place in real time and is extremely sensitive to delays and bandwidth allocation. A detailed examination of modern IPTV architectures also shows that integrating security and QoS requirements is a complex task due to the diversity of network devices. [5]

4 The role of QoS in multimedia IP networks

Providing QoS in multimedia IP networks is one of the most important issues in this technology. Streaming services, especially live videos, real-time broadcasts, and high-definition content, are sensitive to any network faults. Unfortunately, this means that minimal delay is necessary to minimize packet loss.

There are several methods for optimizing QoS, among which adaptive resource allocation based on artificial intelligence stands out, as it is capable of reacting to network problems in real time. Predictive, AI-based QoS optimization can significantly reduce packet loss and improve the reliability and speed of multimedia transmission. [2]

The most relevant QoS parameters are:

- Delay – critical in live broadcasts.
- Jitter – particularly important for video and audio synchronization.
- Transmission capacity – important for transferring high-definition content.
- Packet loss – causes quality reduction, especially with high-definition content.

One of the challenges with IP-based multimedia systems is to find the balance between QoS and security. Encryption, authentication protocols, packet verification, and other security procedures can increase latency, degrading the user experience. Service providers must therefore find a compromise that guarantees both network security and high-quality multimedia content. This will be one of the key areas of research in my work.

5 Security challenges in multimedia IP networks

The vulnerabilities of multimedia IP infrastructure can appear on multiple levels: in the layers of the TCP/IP model, in CDNs, in backend systems, in end devices, and in possible illegal user behavior. Due to the popularity of streaming services, the number of cyberattacks against them is also on the rise.

A number of security issues can arise in IPTV and streaming platforms, including::

- Unauthorized access to paid content
- Blocking of information flow (slowing down, interruption)
- Overload attacks

Several studies have reviewed security issues in streaming and IPTV systems in detail, highlighting that these systems are particularly vulnerable due to their complex architecture and real-time operation. [6]

Threats such as content substitution, disinformation manipulation, or service disruption in crisis situations can have extremely serious social consequences. As a result, multimedia IP networks can easily become targets of cyberattacks, affecting the citizens' access to information. [7]

6 The human factor and social vulnerabilities

One of the non-technical aspects of multimedia IP system security that is still one of the most critical factors is human behavior. Users are often unaware of what personal data they enter when registering for streaming services, how profile management and program recommendation systems work, or how important it is to use a strong password and enable two-factor authentication.

One of the key aspects of my PhD research will therefore be a questionnaire survey examining different age groups:

- awareness of the use of multimedia services,
- level of cybersecurity knowledge,
- risky user behavior.

An inappropriate attitude towards our own digital privacy provides a significant attack surface that cannot be completely eliminated by technical measures. Therefore, examining the human factor is an essential part of my research.

7 Technical safety tests

One of the most critical parts of multimedia systems is the CDN, which is directly related to network speed and security. CDNs enable fast access to content, but they can also carry multiple vulnerabilities. Research examining the risks of CDNs highlights that cache manipulation and attacks on geographically distributed server infrastructure represent a serious threat. [4]

Studies of the architecture of streaming systems highlight that real-time content delivery is extremely vulnerable to cyber attacks, and user-side vulnerabilities (e.g., smart TV or set-top box bugs) also represent a significant risk factor. [5][6]

A number of studies analyze in detail the typical parameters and vulnerabilities of IP-based multimedia networks, while research on multimedia processing describes methods for optimizing data stream management and making networks more secure. [8][9]

Based on these, the technological part of my PhD research will include:

- Creating an IPTV test network,
- IP data stream analysis in laboratory and real environments,
- vulnerability tests for user terminal equipment,
- compare encryption and authorization management methods.

8 Structure of my PhD research (2025–2029)

The research is divided into four years and structured as follows:

- Year 1: literature review, questionnaire survey (human factor aspect).
- Year 2: Test network building, IP data stream analysis.
- Year 3: Testing of end devices and analysis of encryption procedures.
- Year 4: development of methodology, recommendations, publications.

The aim is to develop a comprehensive methodology that can examine the safety of all components of multimedia IP systems, applying not only technical but also human factors.

Conclusion

The security of multimedia IP -based systems is of high importance, as these platforms have become the primary channels for information communication. Balancing QoS and security is a complicated task, which is especially challenging for real-time streaming services. Based on the literature reviewed, it can be concluded that multimedia IP networks are vulnerable in several ways and have become targets for cyberattacks due to their significant growth.

The aim of my PhD research is to develop a comprehensive methodology for assessing the security of these systems, applying both technical and human approaches. The results of this research may contribute to increasing the security of multimedia services and reducing social vulnerabilities.

References

- [1] Suliman Mohamed Fati; Saiful Azad; Al-Sakib Khan Pathan, "IPTV Network Security: Threats and Countermeasures," in *IPTV Delivery Networks: Next Generation Architectures for Live and Video-on-Demand Services*, Wiley, 2018, pp.203-224, DOI: 10.1002/9781119397939.ch8
- [2] Qin Xin, Mamoun Alazab, Rubén González Crespo, Carlos Enrique Montenegro-Marin, AI-based quality of service optimization for multimedia transmission on Internet of Vehicles (IoV) systems, *Sustainable Energy Technologies and Assessments*, Volume 52, Part A, 2022, 102055, ISSN 2213-1388, <https://doi.org/10.1016/j.seta.2022.102055>.
- [3] Michael Oche, Rafidah Md Noor, Johnson Ihieh Aghinya, Network centric QoS performance evaluation of IPTV transmission quality over VANETs, *Computer Communications*, Volume 61, 2015, Pages 34-47, ISSN 0140-3664, <https://doi.org/10.1016/j.comcom.2014.12.001>.
- [4] Paul Ganley, Copyright and IPTV, *Computer Law & Security Report*, Volume 23, Issue 3, 2007, Pages 248-261, ISSN 0267-3649, <https://doi.org/10.1016/j.clsr.2007.01.005>.
- [5] Chaeyun Jang, Seongcheol Kim, Kids content as IPTV operator's new differentiator: The Korean case, *Telecommunications Policy*, Volume 48, Issue 6, 2024, 102765, ISSN 0308-5961, <https://doi.org/10.1016/j.telpol.2024.102765>.
- [6] Kristina Irion, Natali Helberger, Smart TV and the online media sector: User privacy in view of changing market realities, *Telecommunications Policy*, Volume 41, Issue 3, 2017, Pages 170-184, ISSN 0308-5961, <https://doi.org/10.1016/j.telpol.2016.12.013>.
- [7] Naoya Sekiguchi, Hidema Tanaka, BGP hijack attack policy against AS topology map, *Internet of Things*, Volume 25, 2024, 101059, ISSN 2542-6605, <https://doi.org/10.1016/j.iot.2024.101059>.
- [8] NianMin Yao, JinZhong Chen, Guaranteed Quality of Service in Multimedia System, *Procedia Engineering*, Volume 24, 2011, Pages 287-291, ISSN 1877-7058, <https://doi.org/10.1016/j.proeng.2011.11.2643>.
- [9] Li Kuang, Zhifang Liao, Wentao Feng, Haoneng He, Bei Zhang, Multimedia services quality prediction based on the association mining between context and QoS properties, *Signal Processing*, Volume 120, 2016, Pages 767-776, ISSN 0165-1684, <https://doi.org/10.1016/j.sigpro.2015.01.013>.