Vitaliy Danylov
MET Department of Computer Science, Boston University, Boston, USA
E-mail: vitaliy_danylov@ukr.net
ORCID: https://orcid.org/0009-0004-8919-3378

Peer-to-Peer Audio Streaming Using the Tor Network: Problems, Opportunities and Development Prospects

Abstract

This article analyses the potential and challenges associated with the implementation of audio streaming in the anonymous Tor network and the use of peer-to-peer (P2P) technologies. The main focus is on discussing the technical and conceptual issues that arise when integrating audio streaming services with the Tor network, including delays, limited bandwidth and other limitations that affect audio quality. The aim of the study is to find practical solutions to the problem of anonymous audio streaming using Tor technologies or other means to preserve anonymity. By analysing different approaches and tools, it becomes apparent that peer-to-peer broadcasting offers a flexible solution that allows audio to be transmitted over P2P networks, reducing the load on individual nodes and optimising bandwidth usage. This solution offers opportunities for scalability, fault tolerance, bandwidth optimisation and latency reduction, making it an attractive option for audio streaming setups. Meanwhile, the Utopia ecosystem, with its decentralised structure and high level of privacy protection, is another potential solution. Not only does it allow bypassing censorship and firewalls, but it also ensures anonymity in communication and data exchange. With its built-in audio and video communication tools, as well as the ability to create private channels and share files, Utopia can become a reliable platform for streaming audio. Thus, based on the analysis, the solution to the problem of anonymous audio streaming may lie in the integration of technologies such as Peercasting and Utopia, which provide not only the technical capability for streaming, but also a high level of privacy protection for users. It is also important to consider the flexibility of these solutions and the ability to adapt to the specifics of anonymous networks and user requirements. The practical significance of the study of audio streaming over Tor using P2P technologies is to develop methods to increase the anonymity and security of audio communications, which is critical in the face of growing threats to privacy on the Internet. This allows to overcome censorship and Internet restrictions in repressive regimes, providing users with freedom of thought and access to information.

Keywords

audio streaming, peer-to-peer, Tor, onion

JEL: D85, L86, O33, O34, C88

DOI: https://doi.org/10.30525/2500-946X/2024-1-2

1 Introduction

In today's digital landscape, privacy and anonymity in online communications are increasingly critical issues, particularly in the realm of audio streaming. Users not only want to share and consume content in real time, but also want to protect their privacy from external surveillance. However, mainstream audio streaming solutions often fail to provide adequate levels of anonymity and security, prompting users to explore alternative approaches.

In this context, the community is actively researching and discussing options that could meet the demand for anonymity and security. Decentralised P2P networks have a unique position among such solutions, offering a high level of privacy and security to users. This exploration of different approaches to anonymous audio streaming aims to examine both the technical aspects and the potential for developing and integrating these technologies into the broader context of Internet privacy. The aim is not only to ensure anonymity and security for users, but also to expand the possibilities for free and uncontrolled exchange of information in the global digital space.

The purpose of this research is to identify practical approaches to solving the problem of anonymous audio streaming by using Tor or other anonymity-preserving technologies.

The analysis of recent scientific research and publications on the topic of anonymous audio streaming shows that this area remains relatively underexplored. Most existing works focus on general aspects of peer-to-peer (P2P) technologies and audio streaming, as well as the use and limitations of the Tor network

(Segura et al., 2019). However, specialised studies that directly address anonymous audio streaming over Tor or similar networks are quite rare.

The work of Vu, Lupu and Ooi, along with the work of Mello and Duarte (2022), which focuses on P2P principles and strategies for multimedia streaming, may provide valuable technical foundations, but do not directly address anonymity issues in the context of audio streaming.

Research by Dingledine and colleagues (2004) provides an in-depth analysis of the Tor network, but focuses primarily on its architecture and operating principles, without directly examining audio streaming. Similarly, other sources such as The Windows Club and Tails provide information about Tor and its applications, but do not mention audio streaming. A source from YouTube by Info Sec Hub discusses the possibility of using P2P over the Tor network, but lacks specific examples or use cases for audio streaming. This suggests that the implementation of audio streaming in anonymous networks requires further research.

The Utopia ecosystem, mentioned in one of the sources, is an interesting case of a decentralised platform with facilities for anonymous communication and file sharing, including audio, but specific aspects of audio streaming within this system are also not thoroughly explored.

Therefore, to investigate anonymous audio streaming over anonymous networks such as Tor, it is necessary to collect information from various sources, including forums, expert blogs and other informal publications. This underscores the need for further research and development of specialised solutions that would provide a high level of anonymity and security for users engaged in audio streaming.

2 Tor Features

Tor, short for The Onion Router, is open-source software designed for anonymous Internet communication. Its core principle, onion routing, involves encrypting data at multiple layers in the communication protocol stack, similar to the layers of an onion (Dingledine et al., 2004). Tor routes Internet traffic through a global network of volunteer relays, making it difficult to trace a user's Internet activity by masking their location and usage from anyone doing traffic analysis. In this way, Tor protects the privacy of its users by hiding their IP addresses through Tor exit nodes (The windows club, 2023; Alwis et al., 2006).

Tor works by routing Internet traffic through its network of nodes. The user first establishes an encrypted connection to a Tor server and then sets a path through the Tor network that routes traffic between multiple Tor servers. This path is random and changes every 10 minutes. Tor encrypts traffic using a multi-layered encryption scheme that resembles peeling an onion, with each node in the Tor network removing a layer of encryption.

A key advantage of this network is that it is available as free software that is easy to download and install. It is a modified version of Firefox for Windows, Mac OS X and Linux, and the Orbot app for Android provides mobile browsing capabilities.

The main ways to use the Tor network include the following:

– Protection of the privacy of online activity. Tor helps users keep their online activities private from websites or advertisers by preventing unwanted targeting of information.
– Counteracting cyber surveillance. Using Tor helps to avoid individual surveillance and the collection of personal data.
– Circumventing censorship and government surveillance. Tor is often used to circumvent internet access restrictions and government monitoring in countries with limited freedoms.

In general, this network allows maintaining privacy when using various online services through a browser.

This study takes a closer look at the potential of using Tor for audio streaming, given its ability to provide anonymity and privacy. It also facilitates the circumvention of geographical restrictions and censorship, providing access to audio content that may be blocked in certain regions.

3 Features of Audio Streaming Implementation

Streaming audio is the process of transmitting audio content in real time over the Internet, allowing users to listen to music, podcasts and other audio files without having to download the entire file to their device. This gives access to a huge array of audio content without the need to store files locally.

Peer-to-peer (P2P) audio streaming is a method of streaming audio in which data is transferred directly between users (nodes) of a network without relying on a centralised server. This approach allows for increased scalability and reduced dependence on central infrastructure, potentially increasing efficiency and resilience to single points of failure.

In a P2P audio streaming scenario, each participant on the network acts as both a client and a server, sharing portions of the audio files with each other. This decentralised nature of P2P networks can contribute to more robust and distributed audio streaming services, where users benefit from shared resources and bandwidth, leading to potentially better performance and scalability, especially in high demand situations (Figure 1).

In P2P networks, each node can act as both a client and a server at the same time, sharing resources such as audio files with other nodes. The main advantage of P2P audio streaming is that it reduces the load on a single central server by distributing traffic across many nodes. This improves network efficiency and

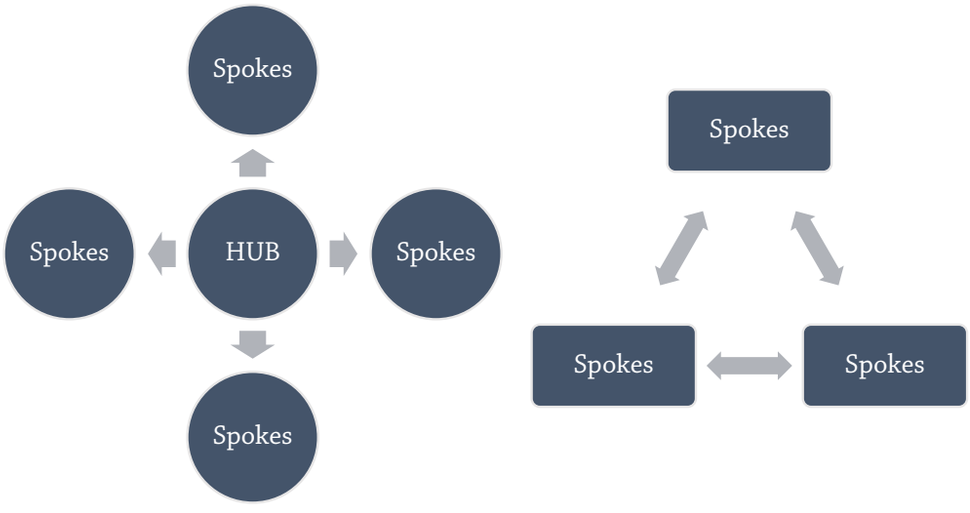

FIGURE 1 Peer-to-peer streaming features

Source: (Vu et al., 2010)

can provide a more stable and faster connection for users, especially in the case of high demand for certain content. In addition, P2P networks can help circumvent geographical restrictions and censorship, as data is transferred directly between users rather than through centralised servers located in a particular location. However, the use of P2P technologies can raise privacy and security concerns, as data is transmitted directly between users and can be vulnerable to interception or abuse. This is where Tor becomes relevant.

To use Tor for peer-to-peer (P2P) audio streaming, there are several technical aspects to consider:

1. Setting up Tor Browser. The Tor Browser, a free browser based on Firefox, must first be installed and configured to provide an anonymous connection to the Internet. Users should ensure that their connection to Tor is via a secure and reliable route. Although Tor Browser is specifically designed to work with the Tor network, other popular web browsers such as Chrome or Firefox do not have built-in Tor support, which means that additional tools or proxy server settings are required to connect these browsers to the Tor network.

2. Selection of a compatible P2P application. It is necessary to choose a P2P file sharing application that is compatible with Tor. File sharing applications such as BitTorrent clients often do not support direct connection to the Tor network, making it difficult to use Tor for anonymous file sharing. Additionally, instant messaging or VoIP applications such as Skype or WhatsApp are not typically configured to use Tor, making it difficult to use them anonymously over this network.

3. Configuration of the P2P application. The P2P application must be configured to route all traffic through Tor, which may involve changing the proxy settings in the application to a local Tor proxy.

4. Additional security measures. To ensure complete anonymity, additional security measures, such as a VPN, must be taken to guarantee complete anonymity (Info Sec Hub, 2022).

It is to be expected that the speed of P2P exchanges over Tor may be slower due to anonymous routing.

4 Problems of Using Peer-to-Peer Audio Streaming via the Tor Network

The use of peer-to-peer audio streaming over the Tor network is subject to certain obstacles due to technical limitations inherent in the Tor network. Some of the key aspects that can affect the streaming experience include the following:

Lack of Support for UDP and WebRTC. UDP (User Datagram Protocol) is the main transport layer protocol used on the Internet, offering a connectionless service. This makes it faster and more efficient for applications that require fast data transfer, such as streaming video, online gaming, or VoIP (Voice over Internet Protocol), but less reliable because packet delivery is not guaranteed.

WebRTC (Web Real-Time Communication) allows for the direct exchange of multimedia (video, audio) and data between browsers and mobile applications in real time. Many modern applications for video calls, chats and conferences use WebRTC. A key feature of WebRTC is its peer-to-peer nature, which reduces latency and improves connection quality. Tor's incompatibility with these protocols limits its use for many network applications and services.

Lack of End-to-End Encryption. While data is encrypted when it enters the Tor network, it is not encrypted before or after it passes through the network. An external observer can see unencrypted data in transit, such as usernames and passwords.

Reduced Browsing Speed. The expected slowdown due to the data going through a more complex and longer route makes Tor impractical for streaming high-quality video or torrents.

Complexity in Connecting Applications to the Tor Network. While there are methods to overcome these limitations, such as using a VPN with Tor, this does not solve the problem of slow browsing. A VPN provides end-to-end encryption and supports application traffic, but does not make the user truly anonymous as the VPN provider could technically monitor the user's activity (Tails, 2023).

Below is a summary of the critical problems with using Tor for peer-to-peer audio streaming presented in Table 1.

Given these limitations, Tor is not an ideal solution for streaming, especially for applications that require a high-speed and stable connection.

5 Solution Search for Anonymous Audio Streaming

The online community is actively discussing the issue of maintaining stable audio broadcasts through Tor. They have identified several solutions that take into account the unique requirements of anonymous networks, such as low latency and the variability of network paths.

One of the first solutions to this problem was StreamerP2P, which supports all audio/video codecs and transfer protocols. However, the lack of updates and feedback from the developer may indicate that it is no longer supported.

Peercasting is a hybrid between peer-to-peer (P2P) networks and traditional streaming, allowing users to act as both clients and servers, distributing audio or video streams. This significantly reduces the load on individual network nodes and optimises bandwidth usage (Mello, 2022). The essence of peercasting is that each participant in the network, upon receiving a stream, simultaneously forwards it to the next listeners. This dynamically distributes content to many users without relying on a single central server, making distribution more efficient and scalable.

Peercasting is used for audio streaming in web applications and services that allow users to broadcast live audio performances, radio shows or podcasts. An example of such a service is Peercast, which provides a user-friendly tool for creating one's own audio and video broadcasts using P2P technologies (Wiki, 2023).

The potential and prospects of using Peercasting for peer-to-peer audio streaming include several key benefits:

1. Scalability. As each participant distributes the content further, the network can efficiently scale to accommodate large numbers of listeners without significantly increasing the load on the source of the stream. This distributed approach to content delivery allows for a more resilient and flexible system that can adapt to growing audiences without the need for significant infrastructure investment.
2. Fault Tolerance. Peercasting reduces reliance on individual servers or nodes, making streaming more reliable in the event of network component failures. By distributing the streaming load across multiple nodes, the network ensures that the failure of one node doesn't necessarily disrupt the entire streaming service, making the system more resilient.
3. Bandwidth Optimisation. The use of P2P technologies enables efficient use of available bandwidth, reducing traffic costs for broadcasters. Each node on the network contributes its bandwidth, resulting in a more efficient distribution of resources. This collective sharing of bandwidth not only optimises the capacity of the network, but also helps to manage the costs associated with data transmission.
4. Reduced Latency. Peercasting can offer lower latency in content distribution compared to traditional centralised servers, especially in cases where geographically distributed nodes are used. The peer-to-peer nature of the network means that content can be relayed over the shortest possible path between peers, potentially reducing the time it takes for data to travel from source to end user (HandWiki, 2023).

The adoption of such technologies opens up new opportunities for application developers and

TABLE 1 The main problems with using Tor for peer-to-peer audio streaming

Limitations	Description	Impact on P2P Audio Streaming
No support for UDP	UDP is a transport protocol that provides fast transmission without delivery confirmation.	Restricts the use of applications that require UDP for fast audio/video transmission.
No support for WebRTC	WebRTC allows direct data exchange between browsers in real time.	Makes it complicated to use browser-based applications for P2P audio and video communication.
No end-to-end encryption	Tor does not provide encryption after leaving the network.	The risk of interception of unencrypted data at the exit from the Tor network.
Transmission speed	Data transmission via Tor passes through several nodes, which reduces the speed.	It degrades streaming quality, especially for high-quality video.
Difficulty in connecting applications	Connecting conventional applications to Tor can be difficult.	Makes it difficult or impossible to use multiple applications for Tor streaming.

Source: (Tails, 2023)

online event organisers, allowing them to reach large audiences with minimal infrastructure investment. This democratisation of content distribution empowers smaller content creators and event organisers to deliver high-quality streaming experiences previously only achievable by larger organisations with significant resources.

In fact, alternative approaches to the problem may be more appropriate, especially given the limitations of traditional tools such as Tor for streaming purposes. One such innovative solution is the Utopia Ecosystem, a groundbreaking decentralised P2P system that operates without the need for a central server to transmit or store data. This system is specifically designed to protect the privacy of communications, confidentiality and security of personal data.

Designed for users who value privacy above all else, Utopia provides the means to bypass online censorship and firewalls, ensuring freedom of communication. It ensures that a user's physical location is not revealed and that communications and data cannot be intercepted by third parties. All account data is stored on the user's local device in an encrypted file using 256-bit AES encryption.

With Utopia, users can send text and voice messages, transfer files, create group chats and channels, news feeds and have private discussions. Channels can be geolocated using integrated uMaps, making it easier to find Utopia channels and adding an extra layer of security. This eliminates the need for public mapping services, which are notorious for collecting user data. uMail provides a decentralised alternative to traditional email, without the need for servers to transmit or store mail. A uMail account allows an unlimited number of messages to be sent and attachments to be stored (Babatunde, 2022).

Utopia could serve as an alternative solution for anonymous audio streaming, thanks to its ability to decentralise data transmission without central servers and its high level of privacy protection. This system could be particularly beneficial for audio streaming, where a high level of anonymity and security is required (Chainkong- Crypton, 2023).

Further use of Utopia for audio streaming can include creating private channels to stream music or podcasts, securely sharing audio files, and holding anonymous audio conferences. With built-in tools such as uMail and uWallet, Utopia can also facilitate content monetisation and donations for content creators, thus opening up new opportunities for audio content providers to work in an anonymous, privacy-respecting environment (Utopia, 2023).

6 Conclusions

In conclusion, solving the problem of anonymous audio streaming, especially in environments that require a high level of privacy and security, requires exploring alternative solutions that take into account the nuances of anonymous networks. Experience shows that Tor may not meet all the requirements due to its limitations related to connection speed and stability.

An analysis of various approaches and tools shows that Peercasting offers a flexible solution that allows streaming audio over P2P networks, reducing the load on individual nodes and optimising bandwidth usage. This solution offers opportunities for scalability, fault tolerance, bandwidth optimisation and latency reduction, making it an attractive option for streaming audio.

Simultaneously, the Utopia Ecosystem, with its decentralised structure and high level of privacy protection, represents another potential solution. Not only does it allow users to bypass censorship and firewalls, but it also ensures the anonymity of communication and data exchange. With built-in tools for audio and video communication, as well as the ability to create private channels and share files, Utopia could become a reliable platform for audio streaming.

Therefore, based on the analysis, the solution to the problem of anonymous audio streaming may involve the integration of technologies such as Peercasting and Utopia, which provide not only the technical capability for streaming, but also a high level of privacy protection for users. It is also important to consider the flexibility of these solutions and their ability to adapt to the specifics of anonymous networks and user requirements.

References

[1] Alwis, H. A., Doss, R., Chowdhury, M., & Hewage, P. S. (2006). A performance evaluation of Route Based Packet Marking (RBPM) for IP trace back. DOI: https://doi.org/10.1109/inmic.2006.358193
[2] Babatunde O. (2022) Utopia P2P – The Ecosystem for cutting-edge Privacy Protect, anonymous cryptocurrency trading, and much more. Listed on CMC and CG. Linkedin. E-source: https://www.linkedin.com/pulse/utopia-p2p-ecosystem-cutting-edge-privacy-protect-much-babatunde/
[3] Chainkong-Crypton (CRP). E-source: http://chainkong.com/currency/utopia
[4] Devi, A. (2023). What Is Audio Streaming? Ventuno Technologies. E-source: https://blog.ventunotech.com/glossary/audio-streaming/
[5] Dingledine, R., Mathewson, N., & Syverson, P. F. (2004). Tor: The second-generation onion router. In Proceedings of the 13th USENIX Security Symposium (pp. 303-320). USENIX Association. E-source: https://www.researchgate.net/publication/2910678_Tor_The_Second-Generation_Onion_Router

[6] EveryMundo. (n.d.). Newsletter Subscription for multiple industries Websites. E-source: https://marketplace.everymundo.com/products/newsletter-subscription
[7] HandWiki (2023). Peercasting. E-source: https://handwiki.org/wiki/Peercasting
[8] Info Sec Hub (2022). Can You Run P2P over the TOR network? E-source: https://www.youtube.com/watch?v=zsQenUipryI
[9] Limitations of the Tor network. Tails, 2023. E-source: https://tails.net/doc/about/warnings/tor/index.en.html
[10] MacMyanmar. (2023). MacMyanmar Mac 4K YouTube to MP3 Pro 4.12.1 Download. E-source: http://macmyanmar.com/mac-4k-youtube-to-mp3-pro-4-12-1-download/
[11] Mello S., Duarte E. (2022). A Hybrid Peer-to-Peer and Client-Server Strategy for Multimedia Streaming. E-source: https://www.researchgate.net/publication/359202633_A_Hybrid_Peer-to-Peer_and_Client-Server_Strategy_for_Multimedia_Streaming
[12] Segura, F. R., & Roca, J. B. (2019). La formación lectora y literaria de los futuros maestros mediante la metodología de trabajo por proyectos para el desarrollo de un aprendizaje integrado basado en competencias [Literacy and literary training in pre-service teacher education through project-based learning in a competency-based model]. *ENSAYOS. Revista de la Facultad de Educación de Albacete,* 34(2). DOI: https://doi.org/10.18239/ensayos.v34i2.1589
[13] The Tech Journal (2023). iPad Apps Archives – Page 7 of 7. E-source: https://thetechjournal.com/tag/ipad-apps/page/7
[14] The windows club (2023). What is Tor Network and what is it used for? E-source: https://www.thewindowsclub.com/what-is-tor-network
[15] TutorialsPoint (2023). Breaking the Chains: Overcoming Limitations of Distributed Systems. E-source: https://www.tutorialspoint.com/breaking-the-chains-overcoming-limitations-of-distributed-systems
[16] Utopia Ecosystem. E-source: https://u.is/en/faq.html#faq2
[17] Vu, Q., Lupu, M., Ooi, B. C. Peer-to-Peer Computing. Principles and Applications. Springer-Verlag Berlin Heidelberg 2010. E-source: file:///Users/oksanakostiuk-pukaliak/Downloads/P2p_computing.pdf
[18] Wiki (2023). Peercasting. E-source: https://en.wikipedia.org/wiki/Peercasting

Received on: 08th of February, 2024
Accepted on: 25th of March, 2024
Published on: 12th of April, 2024