DOI: https://doi.org/10.57233/ijsgs.v11i2.842 ISSNp: 2488-9229; ISSNe: *3027-1118*

IJSGS FUGUSAU VOL. 11 (2) WEBSITE: https://fugus-

INTERNATIONAL JOURNAL OF SCIENCE FOR GLOBAL SUSTAINABILITY
(A PUBLICATION OF FACULTY OF SCIENCE, FEDERAL UNIVERSITY GUSAU, NIGERIA)

Hybrid Defense against Pollution Attacks in P2P Live Video Streaming

[1,2]Firdausi Umar Kaita, [2]Dr. Umar Iliyasu, [2]Ahmad Jamilu Bashir, [2]Yusuf Surajo

[1]Department of Computer Science, Federal University Gusau, Nigeria
[2]Department of Computer Science, Federal University Dutsin-Ma, Katsina Nigeria.

Corresponding Author's Email & Phone No.: fukaitas05@gmail.com, +2348037995768

Received on: April, 2025 **Revised and Accepted on:** May, 2025 **Published on:** July, 2025

ABSTRACT

Pollution attacks present a serious risk to the integrity and reliability of peer-to-peer (P2P) live video streaming networks, negatively impacting video quality and user experience. This paper introduces a combined security strategy that merges blacklisting and traffic encryption techniques to counter these attacks. We assessed the effectiveness of Blacklisting, Traffic Encryption, and Hybrid methods using the OMNeT++ simulation environment across networks ranging from 1,000 to 5,000 nodes. The findings revealed that the Hybrid method consistently surpassed the others, achieving a detection rate of 90% and a pollution rate of 9% at 5,000 nodes, compared to 72%/20% for Blacklisting and 65%/23% for Traffic Encryption. This research work shows that the hybrid approach provides a more robust, scalable, and effective means of protecting P2P video streaming from pollution attacks

Keywords: Peer-to-Peer Streaming, Pollution Attack, Traffic Encryption, Blacklisting.

1.0 INTRODUCTION

The swift progress of multimedia technologies has transformed how digital content is consumed, with Peer-to-Peer (P2P) live video streaming becoming a scalable and effective method for delivering content in real time. In contrast to conventional client-server systems, P2P networks utilize a decentralized framework where each user serves as both a provider and a consumer of content (Kumar et al., 2024). This setup improves fault tolerance and lessens dependence on centralized infrastructure, making it particularly well-suited for high-traffic situations like live video streaming. The decentralized structure of peer-to-peer (P2P) systems makes them vulnerable to significant security threats, particularly pollution attacks. These attacks involve the introduction of corrupted or harmful data into the network, leading to poor video quality, playback issues, and a decline in user trust (Hernández-Oregón et al., 2023). While various mitigation strategies have been suggested, such as blacklisting and traffic encryption, each comes with notable drawbacks. Blacklisting depends on recognizing known malicious nodes, which can be ineffective against new or evolving threats. On the other hand, traffic encryption protects data during transmission through protocols like HTTPS, but it does not prevent content manipulation after the data has entered the stream.

Recent research highlights the necessity for a hybrid approach that merges different security mechanisms to overcome the shortcomings of individual strategies (Safaei et al., 2023). For instance, integrating blacklisting with dynamic encryption keys and real-time buffer table analysis can improve the detection and prevention of pollution attacks. Additionally, sharing threat intelligence among streaming platforms can lead to more proactive measures against new attack methods (Hwang et al., 2022).

This study introduces an innovative hybrid solution that combines blacklisting and traffic encryption techniques, further enhanced by dynamic key exchange and intelligent packet verification. The model is implemented using OMNeT++ simulation, which offers a realistic setting for assessing security performance in a P2P video streaming network. Key performance metrics include pollution detection and mitigation rates, with simulations conducted using the User Datagram Protocol (UDP) across various attack scenarios and up to 5,000 nodes.

By addressing the shortcomings of existing mitigation techniques, this research aims to advance the field of cybersecurity for multimedia applications. It offers a comprehensive, adaptive, and scalable solution that ensures the seamless delivery of high-quality video content while safeguarding against sophisticated pollution attacks in P2P live streaming networks.

DOI: https://doi.org/10.57233/ijsgs.v11i2.842 ISSNp: 2488-9229; ISSNe: *3027-1118*

IJSGS FUGUSAU VOL. 11 (2) WEBSITE: https://fugus-

2.0 RELATED WORKS

Several studies have explored the severity of pollution attacks in peer-to-peer (P2P) live video streaming networks and proposed various countermeasures. However, many of these approaches suffer from notable limitations, including dependence on centralized architectures, high memory overhead, and limited scalability.

Kumar and Chand (2020) introduced SecP2PVoD, a secure P2P video-on-demand system leveraging an Escrow-Free Identity-Based Signcryption (EF-IDSC) scheme. Their model enhances privacy, confidentiality, and authentication using asymmetric cryptography and theoretical security analysis. Despite its strengths, the approach is constrained by its lack of real-world deployment and narrow focus on a single threat vector. In a separate study, the same authors proposed a Pairing-less Identity-Based Blind Signature with Message Recovery (IDBS-MR) tailored for cloud services, which improves efficiency and bandwidth use through elliptic curve cryptography. However, its practical integration into large-scale cloud systems remains underexplored (Kumar & Chand, 2020).

Tang et al. (2020) conducted a comprehensive analysis of Peer-Assisted Delivery Networks (PDNs), exposing critical vulnerabilities such as segment pollution, free-riding, and IP leakage. They developed an automated detection framework, but their work lacks formal security models or concrete mitigation strategies. Fakis et al. (2020) focused on WebRTC-based privacy leaks, proposing countermeasures through browser extensions and HTTP gateways. While effective under controlled scenarios, their solutions face challenges in browser compatibility and long-term usability.

Decouchant et al. (2020) developed P3LS, a privacy-preserving P2P live streaming model incorporating *k-anonymity* and *plausible deniability*. The system offers enhanced user privacy and bandwidth efficiency but introduces added complexity and potential latency due to fake stream handling. Similarly, Fantacci (2019) examined pollution vulnerabilities in Kademlia (KAD) and Rolan protocols, suggesting cryptographic defenses. Yet, the reliance on centralized systems and high memory requirements limits scalability and practical deployment.

Overall, while these works contribute significantly to understanding and addressing security in P2P video streaming, most focus on singular techniques and lack holistic, scalable, and real-time solutions to pollution attacks. This highlights the need for a hybrid approach—such as combining traffic encryption with blacklisting—to ensure robust and adaptable protection mechanisms. Numerous studies have investigated the impact of pollution attacks in peer-to-peer (P2P) live video streaming networks and have proposed various solutions. However, many of these methods have significant drawbacks, such as reliance on centralized systems, excessive memory usage, and limited scalability.

3.0 METHODOLOGY

This research utilized a simulation-based method with OMNeT++, a modular C++ discrete event simulator, to create a model of a peer-to-peer (P2P) live video streaming network and examine the effects of pollution attacks and their mitigation strategies. OMNeT++ was selected for its scalability, flexibility, and compatibility with both wired and wireless network protocols, along with its ability to integrate video streaming modules. The simulation environment was set up with varying numbers of nodes—1k, 2k, 3k, 4k, and 5k—to replicate real-world P2P streaming situations under different traffic loads and network conditions. Each node was configured to reflect real peer characteristics, including bandwidth, processing power, and latency.

The simulation was conducted in stages. The first stage involved creating a baseline P2P streaming system without any malicious activity. In the second stage, pollution attacks were introduced by setting specific nodes to inject corrupted or altered video segments into the network. These segments spread throughout the network, impacting legitimate nodes and diminishing streaming quality. A mathematical model was developed to illustrate the behavior and dissemination of polluted content, considering the number of malicious nodes and the attack rate.

To counteract the attack, two primary techniques were implemented: blacklisting and traffic encryption. The blacklisting approach employed a trust-based model that assigned a dynamic trust value to each node, which decreased when suspicious behavior (such as repeated transmission of corrupted segments) was detected. Nodes that fell below a certain trust threshold were blacklisted and barred from further content exchange. This collaborative trust assessment system enabled nodes to share and disseminate blacklist information across the network, effectively isolating malicious peers.

The traffic encryption method was used to secure content transmission between nodes. Each node was provided with symmetric keys for real-time encryption

DOI: https://doi.org/10.57233/ijsgs.v11i2.842 ISSNp: 2488-9229; ISSNe: *3027-1118*

and public-private key pairs for secure key exchange. Video segments were encrypted using AES-128, and keys were exchanged using RSA. At the receiving end, encrypted segments were verified using hash functions (like SHA-256) to ensure content integrity. The system also included periodic key rotation to bolster security and minimize the risk of long-term key exposure.

Ultimately, a hybrid model was created that combined both blacklisting and traffic encryption. This model provided a multi-layered security approach by isolating attackers through trust evaluation while simultaneously encrypting data to prevent unauthorized alterations. In this configuration, nodes continuously monitored content validity, updated trust scores, and enforced blacklist rules while ensuring secure communication through dynamic encryption protocols. Simulation results were gathered and analyzed using OMNeT++'s built-in tools and Excel graphs to assess pollution and detection rates in various scenarios.

4.0 RESULTS AND DISCUSSION

The simulation assessed the effectiveness of three security techniques—Blacklisting, Traffic Encryption, and a Hybrid Method—using two main metrics: Detection Rate and Pollution Rate. The results indicated that the Hybrid Method consistently delivered the highest detection rate, beginning at 75% with 1,000 nodes and increasing to 90% with 5,000 nodes. In contrast, the Blacklisting Method improved from 60% to 72%, while Traffic Encryption had the lowest performance, rising from 55% to 65%, as illustrated in Figure 1. This suggests that the Hybrid Method provides stronger detection capabilities due to its combination of behavioral trust assessment and secure data transmission.

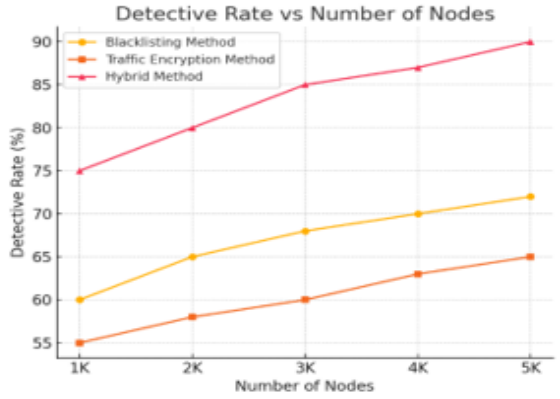

Figure 1: Detection rate for the three methods

Likewise, the pollution rate decreased for all methods as the network expanded, with the Hybrid Method again showing the best results—lowering polluted content from 15% to 9% as the number of nodes increased from 1,000 to 5,000. The Blacklisting and Traffic Encryption Methods exhibited higher pollution rates, decreasing from 25% to 20% and from 28% to 23%, respectively, as shown in Figure 2. These findings underscore the superior resilience of the

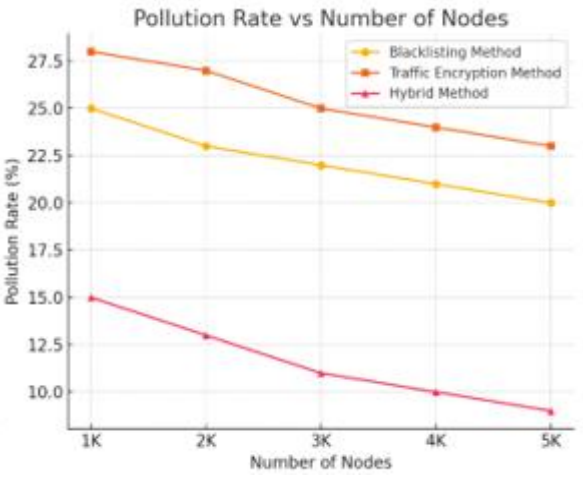

Figure 2: Pollution rate for the three methods

Hybrid Method in preserving data integrity and ensuring a higher Quality of Service (QoS) in large-scale P2P live video streaming networks. The results demonstrate that combining multiple security mechanisms significantly improves both detection accuracy and defense against pollution attacks.

5.0 CONCLUSION

This study introduced a hybrid approach that merges blacklisting and traffic encryption to combat pollution attacks in P2P live video streaming networks. Simulation results from OMNeT++ indicated that the hybrid method achieved the best performance, with a 90% detection rate and a 9% pollution rate at 5,000 nodes. In comparison, blacklisting attained a 72% detection rate and a 20% pollution rate, while traffic encryption recorded a 65% detection rate and a 23% pollution rate. The findings validate the hybrid method as a more effective and scalable solution for securing P2P video streaming.

REFERENCES

Decouchant, J., Ding, A. Y., & Tarkoma, S. (2020). P3LS: Privacy-preserving peer-to-peer live streaming. *Computer* Networks, 170, 107077. https://doi.org/10.1016/j.comnet.2020.107077

Fakis, M., Vassilakis, C., & Papadopoulos, A. (2020). Countermeasures to WebRTC privacy leaks via STUN/TURN protocols. Journal of Information Security and Applications, 52, 102471. https://doi.org/10.1016/j.jisa.2020.102471

Fantacci, R. (2019). Pollution attack mitigation in KAD and Rolan using trusted cryptographic mechanisms. International Journal of Computer Networks & Communications, 11(1), 15–28.

Hernández-Oregón, E., González, M., Guzmán, J., & Navarro, J. (2023). Securing decentralized video streaming networks against advanced threats. Journal of Network and Computer Applications, 205, 103493. https://doi.org/10.1016/j.jnca.2022.103493

Hwang, J., Kim, D., & Park, S. (2022). Privacy and security in modern live streaming platforms: A comprehensive review. Multimedia Tools and Applications, 81, 19581–19604. https://doi.org/10.1007/s11042-022-12514-5

Kumar, P., & Chand, S. (2020). Pairing-less identity-based blind signature with message recovery for cloud-assisted services. Future Generation Computer Systems, 107, 972–987. https://doi.org/10.1016/j.future.2019.12.053

Kumar, P., & Chand, S. (2020). SecP2PVoD: Secure peer-to-peer video on demand system using escrow-free identity-based signcryption. Multimedia Tools and Applications, 79(5), 3245–3266. https://doi.org/10.1007/s11042-019-08366-y

Kumar, T., Sharma, P., Tanwar, J., Alsghier, H., Bhushan, S., Alhumyani, H., Sharma, V., & Alutaibi, A. I. (2024). Cloud-based video streaming services: Trends, challenges, and opportunities. CIT Transactions on Information and Communication Technology, Published online March 14, 2024. https://doi.org/10.1049/cit2.12299

Safaei, M., Khalaj, B. H., & Goudarzi, H. (2023). A survey on pollution attack prevention techniques in peer-to-peer streaming networks. Computer Networks, 224, 109623. https://doi.org/10.1016/j.comnet.2023.109623

Tang, J., Zhang, Y., & Zhang, K. (2020). Large-scale measurement and security analysis of peer-assisted delivery in video streaming platforms. IEEE Transactions on Dependable and Secure Computing, 19(1), 288–301. https://doi.org/10.1109/TDSC.2020.2966890