Modern technologies for marking network flows: from classical methods to innovations

L.Y. Molkova, K.Z. Biliatdinov, M.L. Gluharev

***Abstract* — Stream watermarks are a key tool in information security, enabling the tracking and identification of data in network streams. This article discusses various methods of stream watermarking, including technologies based on traffic flow speed, packet synchronization, packet numbers, transmission intervals, interval centroids, packet length, and their order of sequence. It also analyzes hybrid methods, Flow Fingerprinting technology, and the Patch-based Flow Marking method, which combines the advantages of various approaches. The article examines the advantages and disadvantages of each method, as well as their applicability in modern network environments.**

***Keywords* — stream watermarks, data security, network traffic analysis, Patch-based Flow Marking, Flow Fingerprinting, network technologies.**

I. Introduction

With the rapid growth of network traffic and the increasing number of cyber threats, data protection has become a top priority in the field of information security. Streaming watermarks are one of the promising methods for ensuring the integrity and authenticity of transmitted data. They enable the embedding of hidden information into network traffic parameters, making it possible to track and identify data without significantly affecting its transmission [1-3].

To date, numerous methods for creating streaming watermarks have been developed, utilizing various network traffic characteristics. These include technologies based on flow rate, packet synchronization, packet numbers, time intervals, interval centroids, packet length, and packet order. Additionally, hybrid approaches exist, combining multiple methods to enhance reliability and resistance to attacks. One of the key research directions is Flow Fingerprinting, a technology that enables the identification of network flows based on their unique characteristics.

This paper analyzes existing methods of embedding streaming watermarks, examines their advantages and disadvantages, and discusses the prospects for further development of this technology.

II. Fundamentals of research and problem statement

The relevance of this research topic is driven by the growing security threats to modern information systems and networks, including cyberattacks, data leaks, and traffic manipulation. As network traffic volume and complexity continue to increase, the importance of data protection becomes evident. One of the promising tools for ensuring security is the use of streaming watermarks. These technologies enable the embedding of identification markers into data flows, helping to track and identify changes while ensuring the integrity of transmitted information.

However, despite the active development of streaming watermarking methods, many existing approaches face challenges related to their resistance to various attacks, network load, and computational overhead. This creates a need for the development of new methods and technologies capable of effectively addressing these issues while adapting to the constantly evolving network environment.

The goal of this study is to analyze existing streaming watermarking methods, examine their advantages and limitations, and propose new approaches that enhance the protection of network flows.

The primary objective of this research is to conduct a comprehensive analysis of existing streaming watermarking techniques, including methods based on transmission rate modifications, packet order changes, time intervals, interval centroids, Flow Fingerprinting technology, and data fragmentation. Based on this analysis, a new Patch-based Flow Marking method will be proposed, combining the benefits of various approaches to offer innovative solutions for improving resistance to attacks and reducing computational costs.

Research Objectives:

1. Examine existing streaming watermarking methods and their shortcomings.
2. Develop the Patch-based Flow Marking method for embedding markers into data streams.
3. Describe the advantages of the Patch-based method, including protection against trace removal attempts, flexibility, minimal network load, and resistance to manipulation.
4. Explore potential application scenarios for this method in modern network environments and its integration with intelligent algorithms, including machine learning.

The Patch-based Flow Marking method represents a promising approach to data protection, and this study focuses on its theoretical justification and analysis. Evaluating the effectiveness of this method in real-world conditions and comparing it with existing approaches will be the subject of future research.

L.Y. Molkova, K.Z. Biliatdinov, M.L. Gluharev – Emperor Alexander I St. Petersburg State Transport University, 190031, Moskovsky pr.9, Saint Petersburg, Russia (email: lolita-molkova@mail.ru, k74b@mail.ru, mlgluharev@yandex.ru).

III. METHODS OF APPLYING STREAMING WATERMARKS

3.1. Main carriers of streaming watermarks

Streaming watermarking technologies are based on various characteristics of network packets, including their payload, traffic rate, transmission time intervals, sequence number, length, and order [1-5]. In most cases, a single carrier is used; however, combined approaches are also possible, such as embedding markers based on both timing characteristics and packet structure.

A promising direction in this field is Flow Fingerprinting, which utilizes unique network traffic features for data marking. Additionally, researchers are actively exploring the potential of adaptive watermarks, which leverage machine learning to dynamically select the optimal embedding method.

3.2 Packet payload-based methods

Technologies that utilize packet payloads embed watermarks by modifying the content of data within transmitted packets. This approach establishes a link between data flows, enabling their identification and tracking [4,5].

One example of such a method is Sleepy Watermark Tracking (SWT), proposed by Wang et al. In this approach, when suspicious activity is detected, the system inserts watermarks into the attacker's return traffic, allowing the identification of its source. However, this method has limitations, as it relies on specific network protocols and cannot be applied to encrypted connections [4,5]. This makes it vulnerable to detection and blocking by attackers.

3.3 Traffic flow rate-based watermarking technologies

Traffic rate-based watermarking methods enable the integration of information into network flows by adjusting their speed. These technologies are widely used for tracking target data flows and identifying transmission sources.

Fu et al. proposed a method that utilizes frequency domain transformation for watermark encoding. The watermark is then integrated into the network flow through electromagnetic interference, which helps reduce anonymity in wireless networks based on traffic mixing [6].

Yu et al. developed a method based on Direct-Sequence Spread Spectrum (DSSS), which enables the tracking of anonymous users by varying traffic transmission rates. This method is particularly effective in fixed-bandwidth flows [7,8].

Research by Huang and Pan introduced streaming watermarking using long pseudo-noise (PN) codes. In this approach, each watermark bit is encoded using a fragment of a long PN code, enhancing reliability and enabling multi-flow tracking without significant interference [9].

However, the application of traffic rate-based watermarking requires the deployment of traffic control units, which can affect network availability. Additionally, the need to generate auxiliary data streams may impose extra load on the target network. Another limitation is the relatively high probability of detection, reducing the resilience of such watermarks against attacks.

3.4 Packet synchronization-based streaming watermarking technologies

Packet synchronization-based streaming watermarking methods utilize modulation of temporal network traffic characteristics, such as inter-packet delays (IPD), for covert data embedding. These technologies establish a link between data flows, enabling identification and tracking.

To enhance resilience against timing disturbances, Wang and Reeves proposed a probabilistic watermarking scheme, where watermark bits are embedded by making small random adjustments to IPD.

Park and Reeves developed an adaptive method that adjusts watermark parameters based on the temporal characteristics of the target traffic, increasing its robustness against external interference [10].

Another approach, introduced by Pan et al., is based on packet clustering, where the target flow is divided into several clusters, which are further split into pairs to improve embedding accuracy [9].

Wang et al. proposed a method for tracking anonymous VoIP calls, in which modifications to the mean IPD distribution allow for watermark bit embedding [11].

To counter packet insertion attacks, Peng and his team introduced a packet matching and IPD balancing technique, which optimizes the trade-off between detection accuracy, false positives, and computational complexity.

Houmansadr et al. developed the RAINBOW method, which significantly reduces delays, improving watermark stealthiness. Later, Borisov and Houmansadr applied repeat-accumulate coding, increasing the detection efficiency of watermarks in this technology [12].

Gong et al. implemented a quantization-index modulation (QIM) approach, incorporating an error correction layer to enhance resistance against desynchronization [13].

Zhang et al. introduced a multiple-matching synchronization method, improving both detection speed and accuracy [14].

The DropWat method, proposed by Jacovazzi, is based on controlled packet dropping, simulating natural data loss in the network to embed a watermark. This improves the stealthiness of the method and enhances its resistance to external interference [15].

Compared to payload-based or traffic rate-based watermarking techniques, packet synchronization-based technologies offer wider applicability, do not require specialized protocols, and are relatively easy to implement. However, they are vulnerable to multi-flow attacks, root mean square autocorrelation attacks, and timing distortions, which may reduce their reliability.

3.5 Streaming watermarking technologies

Packet number-based streaming watermarking methods use information about the number of transmitted packets within specific time intervals. This approach includes technologies based on time intervals and interval centroids.

3.5.1 Interval-based streaming watermarking technologies

Interval-based methods involve dividing the target flow into multiple fixed-length time segments, where packet transmission regulation enables watermark embedding. This approach is effectively used for tracking malicious flows and detecting unauthorized traffic modifications.

Pyun et al. proposed the Interval-Based Watermarking (IBW) technique, which allows for network flow tracking even when data undergoes repackaging [16].

Houmansadr and Borisov developed SWIRL, a scalable and covert watermarking method resistant to packet loss. This method serves as an efficient tool for traffic analysis in large-scale networks, as it minimizes latency while remaining invisible to users and potential attackers [17].

Wang et al. introduced the Sequential Watermark Detection Model (SWDM), which incorporates three sequential detectors for efficiently tracking malicious flows. Using sequential probability ratio testing, they proposed two optimized approaches: Pairwise Optimal Watermark Detection (POWD) and Single Interval Optimal Watermark Detection (SOWD). These methods provide high-precision watermark detection based on time intervals, assuming that the parameters of the observed traffic are known in advance [18,19].

To detect and track botnets, Houmansadr and Borisov developed BotMosaic. This technique captures multiple bots in a honeynet environment and embeds coordinated watermarks across several flows directed toward the botnet's command-and-control (C&C) server. A honeynet is a specialized network designed for cyber threat research and monitoring. This approach enables botnet tracking and interaction analysis, significantly enhancing network security against automated threats [20].

3.5.2 Interval centroid-based streaming watermarking technologies

An interval centroid represents the balance point of the number of transmitted packets within a given time interval, allowing for effective correlation of network flows through its modulation.

To counter changes in flow structure, Wang et al. developed the Interval Centroid-Based Watermarking (ICBW) method, which assigns a unique identifier to flows of any length. This method demonstrates resilience against various types of attacks, such as mixing, splitting, packet deletion, and timing disturbances [21].

Lin and his colleagues proposed a network flow watermarking method – Network Flow Watermarking Method – Centroid Matching in Interval Groups (NFWM-CMIG), which uses the IPD centroid and a secret key to make changes to the temporal characteristics of the flow [22].

Packet number-based watermarking methods offer high resistance to interference and can be applied in various network environments without being tied to specific protocols or encryption mechanisms. However, they are vulnerable to timing analysis attacks, and their capacity for storing information is limited by the need to process large amounts of packets.

3.6 Packet length-based streaming watermarking technologies

Packet length-based watermarking methods allow embedding identification tags into data streams by modifying the size of transmitted packets.

Ramsbrook et al. proposed Length-Based Watermarking (LBW) – a technology that enables embedding watermarks in command-and-control (C&C) messages used by botnets. This method is effective for detecting bot-master activities operating through Internet Relay Chat (IRC), as identifying them requires analyzing only a few dozen packets [23].

Ling et al. developed a method that transforms web traffic into virtual objects, and then embeds hidden messages in their final packets, altering their size. To enhance stealth, they use a Monte Carlo sampling method [24].

Despite their effectiveness, packet length-based methods have several limitations. Their implementation is hindered by low data storage capacity, limited applicability, and a high likelihood of detection by attackers.

3.7 Packet order-based streaming watermarking technologies

The method of watermark embedding through packet reordering allows for the identification and analysis of data flows by intentionally altering their sequence.

Zhang et al. developed a flow watermarking technology based on packet reordering, called Packet Reordering-Based Flow Watermarking (PROFW), where controlled permutation is used to embed watermarks. To improve resistance to packet order changes, the encoding process utilizes error correction theory. The method is based on stochastic modulation, which regulates the degree of packet reordering while maintaining a high level of watermark stealth [25].

Compared to traditional methods of embedding flow watermarks, the PROFW technology demonstrates increased watermark capacity and has a high resilience to synchronization failures and disruptions in packet transmission order.

3.8 Hybrid methods for embedding streaming watermarks

To enhance the reliability and accuracy of watermark detection, hybrid techniques that combine multiple embedding mechanisms are sometimes used.

One such method is the hybrid length-timing watermarking (HLTW) technology, proposed by Wang et al. This method combines packet length modification and timestamp control, achieving nearly 100% detection accuracy during experiments on the PlanetLab platform [23].

Lei et al. proposed a hacker-resistant digital fingerprinting method for network flows, based on multidimensional orthogonal carriers. This technology uses two mutually orthogonal carriers to form attack-resistant watermarks. The approach combines interval properties of centroids with decoding algorithms based on Markov models, ensuring high levels of stealth and reliability in embedding [25].

3.9 Flow fingerprinting technology

Compared to the Flow Watermarking method, the Flow Fingerprinting technology has several distinguishing characteristics: (i) uniqueness – the attributes of the flow fingerprint are unique values that allow for the unambiguous identification of a network flow; (ii) increased capacity – from an information theory perspective, Flow Fingerprinting technology enables the transmission of more data compared to Flow Watermarking. Additional bits of information can be used to transmit data such as the traffic source in the network or the identifier of the organization performing the flow analysis [12].

To identify hidden servers in anonymous networks, Elices and Perez-Gonzalez proposed an attack using flow fingerprints, which matches incoming server flows with the flow generated by the malicious client. They also developed

an optimal detector based on the Neyman-Pearson lemma [26].

Houmansadr and Borisov were the first to formulate the problem of flow fingerprinting, suggesting the use of encoding to create identification schemes. In their study, they developed the Fancy Non-Blind Fingerprinting method, which enables high-reliability tagging of network flows, involving only a few dozen packets from each flow [27].

Lei and his colleagues presented a network flow fingerprinting model based on optimization theory. This approach defines unified criteria for analyzing reliability and stealth, and converts the problems of reliability and stealth into mathematical constraints [28].

Rezaei and Houmansadr developed the first blind flow fingerprinting system, named TagIt. This method embeds fingerprints by minimally delaying packets within specific time intervals, known only to the parties conducting the fingerprinting. This helps increase the stealth of the fingerprints and minimizes the likelihood of their detection by attackers. In this context, fingerprinting refers to the technology of creating «digital fingerprints» of network traffic for identification and tracking purposes. It is not related to physical fingerprints but to Flow Fingerprinting technology, which links specific characteristics to particular data flows [29].

3.10 Patch-based flow marking method

After analyzing existing methods, a proposal can be made to create a new approach. This section introduces the Patch-based Flow Marking method. The Patch-based Flow Marking method is an innovative approach where markers are embedded in the data flow by altering its structure. This method is used to create distinctive «spots» or «patches» in the flow that allow the identification of changes, leaks, or attempts to manipulate data. The main idea is to subtly introduce markers that can be used to verify the integrity of transmitted data.

Advantages of the Patch-based Flow Marking method:

1. Protection against trace hiding attempts: Even with partial changes to the flow, the basic structure remains protected.

2. Flexibility and adaptability: The method can be applied in various network environments and adapted to specific tasks.

3. Minimal network load: Unlike cryptographic methods, patch-based marking requires minimal computational resources.

4. Resilience to manipulation: The flow remains identifiable even in the case of packet order changes or packet substitution.

5. Effective leak and attack detection: The method allows unauthorized data changes to be detected and network activity to be analyzed.

6. Resilience to interference: Preserving the structure of the flow allows identification of changes even under noise attacks.

7. Integration with intelligent algorithms: The ability to use machine learning for automatic detection of suspicious changes in the flow.

The Patch-based Flow Marking method is especially effective for protecting data in high-risk attack and manipulation environments, making it a promising direction for the development of flow watermarking technologies.

VI. Conclusion

The article provides a detailed analysis of various methods of applying flow watermarking techniques used for data protection and network traffic monitoring. It examines technologies based on traffic flow speed, packet synchronization, packet numbers, time intervals, interval centroids, packet length, and packet order. Hybrid methods, Flow Fingerprinting technology, and the proposed Patch-based Flow Marking method have been analyzed. The key advantages and limitations of each method are identified, including their resilience to attacks and their integration potential in modern networks.

Promising directions for future research include the development of more reliable and stealthy methods of embedding flow watermarks, as well as the integration with machine learning algorithms to enhance the accuracy of network traffic analysis. Future work should focus on creating adaptive solutions capable of functioning effectively in dynamically changing networks and addressing emerging cybersecurity threats. Special attention should be given to the development of self-learning systems that can adapt to new attack methods and the evolution of network technologies.

References

[1] Yuan Y., Ge J., Cheng G. DeMarking: A defense for network flow watermarking in real-time //Computers & Security. – 2025. – С. 104355.

[2] Feng W. et al. Ip-pealing: a robust network flow watermarking method based on ip packet sequence //Chinese Journal of Electronics. – 2024. – Т. 33. – №. 3. – С. 694-707.

[3] Li T. et al. HeteroTiC: A robust network flow watermarking based on heterogeneous time channels //Computer Networks. – 2022. – Т. 219. – С. 109424.

[4] Wang X. et al. Sleepy watermark tracing: An active network-based intrusion response framework //IFIP International Information Security Conference. – Boston, MA : Springer US, 2001. – С. 369-384.

[5] Feng W. et al. HSTW: A robust network flow watermarking method based on hybrid packet sequence-timing //Computers & Security. – 2024. – Т. 139. – С. 103701.

[6] Fu X. et al. On flow marking attacks in wireless anonymous communication networks //Journal of Ubiquitous Computing and Intelligence. – 2007. – Т. 1. – №. 1. – С. 42-53.

[7] Yu W. et al. DSSS-based flow marking technique for invisible traceback //2007 IEEE Symposium on Security and Privacy (SP'07). – IEEE, 2007. – С. 18-32.

[8] Karnani S., Agrawal N., Kumar R. A comprehensive survey on low-rate and high-rate DDoS defense approaches in SDN: taxonomy, research challenges, and opportunities //Multimedia Tools and applications. – 2024. – Т. 83. – №. 12. – С. 35253-35306.

[9] Pan X. et al. Long PN code based traceback in wireless networks //International Journal of Performability Engineering. – 2012. – Т. 8. – №. 2. – С. 173.

[10] Park Y. H., Reeves D. S. Adaptive timing-based active watermarking for attack attribution through stepping stones //Proc. Second Int. Workshop on Security in Distributed Computing Systems, Washington, DC, USA. – 2005. – С. 107-113.

[11] Wang X., Chen S., Jajodia S. Tracking anonymous peer-to-peer voip calls on the internet //Proceedings of the 12th ACM conference on Computer and communications security. – 2005. – С. 81-91.

[12] Houmansadr A., Kiyavash N., Borisov N. Non-blind watermarking of network flows //IEEE/ACM Transactions on Networking. – 2013. – Т. 22. – №. 4. – С. 1232-1244.

[13] Gong X., Rodrigues M., Kiyavash N. Invisible flow watermarks for channels with dependent substitution, deletion, and bursty insertion

errors //IEEE transactions on information forensics and security. – 2013. – Т. 8. – №. 11. – С. 1850-1859.
[14] Zhang L. et al. Synchronization in inter-packet delay based flow correlation techniques //J. Comput. Res. Dev. – 2011. – Т. 48. – №. 9. – С. 1643-1651.
[15] Iacovazzi A. et al. DropWat: An invisible network flow watermark for data exfiltration traceback //IEEE Transactions on Information Forensics and Security. – 2017. – Т. 13. – №. 5. – С. 1139-1154.
[16] Pyun Y. J. et al. Interval-based flow watermarking for tracing interactive traffic //Computer Networks. – 2012. – Т. 56. – №. 5. – С. 1646-1665.
[17] Houmansadr A., Borisov N. SWIRL: A Scalable Watermark to Detect Correlated Network Flows //NDSS. – 2011.
[18] Wang X., Yang M., Luo J. A novel sequential watermark detection model for efficient traceback of secret network attack flows //Journal of network and computer applications. – 2013. – Т. 36. – №. 6. – С. 1660-1670.
[19] Yu L. et al. Dynamic interval-based watermarking for tracking down network attacks //2021 IEEE 21st International Conference on Software Quality, Reliability and Security (QRS). – IEEE, 2021. – С. 52-61.
[20] Houmansadr A., Borisov N. BotMosaic: Collaborative network watermark for the detection of IRC-based botnets //Journal of Systems and Software. – 2013. – Т. 86. – №. 3. – С. 707-715.
[21] Wang X., Chen S., Jajodia S. Network flow watermarking attack on low-latency anonymous communication systems //2007 IEEE Symposium on Security and Privacy (SP'07). – IEEE, 2007. – С. 116-130.
[22] Lin M. et al. Network flow watermarking method based on centroid matching of interval group //2015 IEEE International Conference on Progress in Informatics and Computing (PIC). – IEEE, 2015. – С. 628-632.
[23] Ramsbrock D., Wang X., Jiang X. A first step towards live botmaster traceback //International Workshop on Recent Advances in Intrusion Detection. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2008. – С. 59-77.
[24] Ling Z. et al. Novel packet size-based covert channel attacks against anonymizer //IEEE Transactions on Computers. – 2012. – Т. 62. – №. 12. – С. 2411-2426.
[25] Zhang L. et al. Survey on network flow watermarking: model, interferences, applications, technologies and security //IET Communications. – 2018. – Т. 12. – №. 14. – С. 1639-1648.
[26] Elices J. A., Pérez-González F. Fingerprinting a flow of messages to an anonymous server //2012 IEEE International Workshop on Information Forensics and Security (WIFS). – IEEE, 2012. – С. 97-102.
[27] Houmansadr A., Borisov N. The need for flow fingerprints to link correlated network flows //Privacy Enhancing Technologies: 13th International Symposium, PETS 2013, Bloomington, IN, USA, July 10-12, 2013. Proceedings 13. – Springer Berlin Heidelberg, 2013. – С. 205-224.
[28] Lei C. et al. Net-flow fingerprint model based on optimization theory //Arabian Journal for Science and Engineering. – 2016. – Т. 41. – С. 3081-3088.
[29] Rezaei F., Houmansadr A. Tagit: Tagging network flows using blind fingerprints //Proceedings on Privacy Enhancing Technologies. – 2017.