electronics

MDPI

Article

Multilayer Detection of Network Steganography

Milosz Smolarczyk [1], Krzysztof Szczypiorski [1,2,*] and Jakub Pawluk [1]

[1] Research & Development Department, Cryptomage SA, 50-130 Wrocław, Poland; Milosz.Smolarczyk@cryptomage.com (M.S.); jakub.pawluk@cryptomage.com (J.P.)

[2] Institute of Telecommunications, Warsaw University of Technology, 00-661 Warsaw, Poland

* Correspondence: krzysztof.szczypiorski@pw.edu.pl or ksz@tele.pw.edu.pl

Received: 19 November 2020; Accepted: 10 December 2020; Published: 12 December 2020

Abstract: This paper presents a new method for steganography detection in network protocols. The method is based on a multilayer approach for the selective analysis of derived and aggregated metrics utilizing machine learning algorithms. The main objective is to provide steganalysis capability for networks with large numbers of devices and connections. We discuss considerations for performance analysis and present results. We also describe a means of applying our method for multilayer detection of a popular RSTEG (Retransmission Steganography) technique.

Keywords: steganography; network security; steganography detection; steganalysis; machine learning; big data; IoT; pattern mining

1. Introduction

Network steganography has recently gained considerable attention in the scientific community. Many new methods have been developed, and many more will be developed in the near future [1] as new network protocols are constantly being developed. This paper focuses solely on the detection of steganography techniques that operate at the network protocol level.

With the growing number of devices in networks, including IoT, network steganography detection faces new challenges in terms of both accuracy and performance [2]. To be performed effectively, steganography needs to operate:

- In line with analyzed network traffic;
- In near real-time regimes.

If detection is performed off-line or if it causes too much latency, there will be more traffic waiting to be analyzed than can actually be analyzed. Performance optimization is the main focus of the research described here since the main application of network steganography is real-time communication [3,4].

Some of the accurate detection methods tailored for specific network steganography techniques cannot be effectively implemented in real-time regimes because excessive computing and/or memory resources are needed [5]. This makes us question the *overall accuracy* of such methods since they are unable to analyze high-throughput traffic in a multi-host environment.

In this paper, we present a new method to introduce a compromise between detailed packet inspection and optimal detection performance. Our motivation is to provide a generic method that orchestrates network steganography detection in real-time regime, making it possible to implement in multi-host environments that generate high-throughput traffic. As a part of the method, we have presented a steganalysis layer selection method that provides an intelligent selection of steganalysis algorithms, preserving the balance between resource consumption and detection performance. To the authors' best knowledge, this is the first generic network steganography detection method that utilizes a top-down approach for a detection method selection algorithm to ensure optimal computation resource allocation.

2. Related Work

Historically, most network steganography detection methods had been part of research on new steganographic techniques. In recent years, there emerged new detection methods that are not countermeasures for a particular steganographic technique but provide a broader perspective. Based on the literature, we can distinguish two major categories for network steganography detection methods: *technique-specific* and *generic*, as presented in Figure 1.

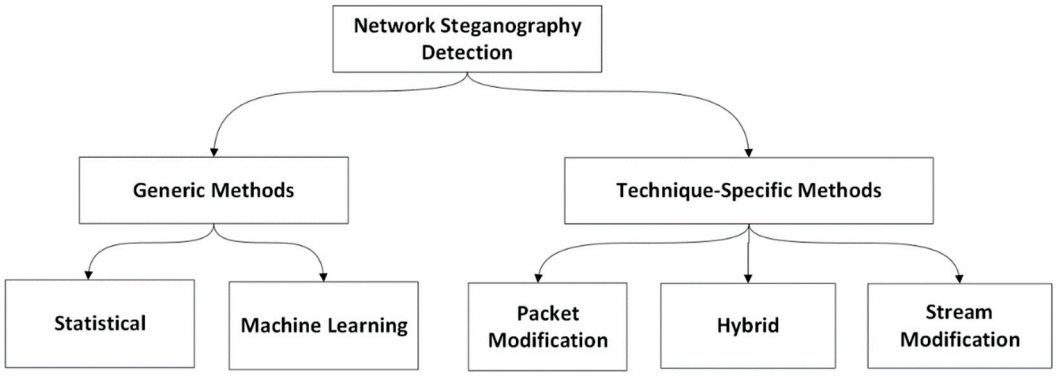

Figure 1. Network steganography detection classification.

The first category: technique-specific, comprises methods proposed as countermeasures for specific steganographic techniques. Methods in this category usually operate on low-level network data, require relatively much computation resources, and are not able to detect other steganographic techniques instead of the one or several for which they are designed.

The second category: generic, comprises methods that are not designed to detect one specific steganographic technique but offer a comprehensive approach to network anomaly detection and categorization of network traffic for potential steganographic utilization. Methods in this category may not provide detailed information on detected suspicious traffic but can label it for further investigation. Most generic methods fall into two subcategories that characterize their approach: statistical or machine learning.

A majority of methods described in the existing literature fall in the first category. Each of those methods is applied to specific steganographic techniques categories, as shown in Figure 2 [6].

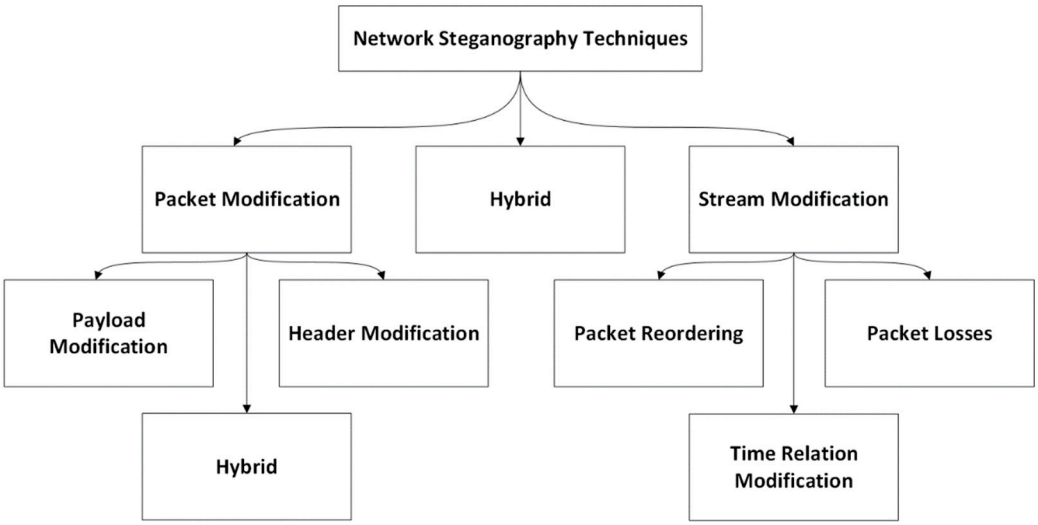

Figure 2. Network steganography classification.

For packet modification techniques, the steganalysis methods presented so far include:

- Header and payload analysis [7], including analysis of Verification Tags values; comparison between values of Maximum Inbound Streams sent by "normal" users (users who do not use steganography) and suspicious users; comparison between values of Stream Sequence Number sent by "normal" users (users who do not use steganography) and suspicious users; checking the value of Payload Stream Identifier; analysis of *a_rwnd* values and sizes of received chunks; analysis of the average number of duplicated chunks; analysis of Shared Key Identifier values; analysis of Padding Data; checking the existence of IP addresses that are sent in these parameters; comparison between values of the Heartbeat Info Parameter sent by a regular user (a user who do not use steganography) and a suspicious user; analysis of RandomNumber; comparison between values of ASCONF-Request Correlation ID sent by a regular user and a suspicious user. The methods presented above are dedicated to all packet modification techniques, including payload modification, header modification, and hybrid techniques.
- Header checksum observation [8], including checksum comparison for retransmitted IEEE 802.11 frames. If the checksum differs for the same payload and header and such observations are frequent, it is likely that a steganographic technique like HICCUPS has been utilized. The method is dedicated to header modification steganographic techniques.
- Observation of selected primary or derived features of header data [9], which includes observation of the least significant bit of the TCP sequence number. The method is dedicated to header modification steganographic techniques.

For stream modification techniques, several detection methods have been described, including:

- A multi-agent approach for observing network traffic time parameters, and intelligent correlation of observed meta-histograms utilizing trained machine learning algorithms [10].
- Analysis of inter-packet delays sequence distribution in multiple dimensions: distribution shape, data variation rule, data statistics. The method proposes an analysis of polarization characteristics, autocorrelation characteristics and clustering characteristics of the above features [11].
- Statistical analysis of selected metrics, header field comparison, and random number analysis [8].

There also exist steganalysis methods designed for hybrid steganographic techniques, including:

- MoveSteg [12], which is a method for detecting an endpoint from which hidden information is transmitted by analyzing a distribution of delay between consecutive packets as well as delay statistical metrics.
- The RSTEG (Retransmission Steganography) detection method [5,13], which is based on outlier detection of selected metrics, such as a retransmission ratio. Detection based on a retransmitted segment payload comparison is also proposed.
- The LACK (Lost Audio PaCKets) detection method [14], which is based on observation and outlier detection of RTP (Real-time Transport Protocol) segment delay.

Some generic methods for steganalysis operating on high-level aggregated metadata have been proposed:

- Data mining and anomaly detection in various metrics for distributed network covert channel detection [15].
- A framework that utilizes a statistical approach for monitoring of selected metrics and anomaly detection in statistical measures, including non-linear chaotic data [2]. The framework analyzes detected outliers and provides a probability of data leakage.
- A deep-learning approach for the detection and classification of covert channels. The method requires a data set comprised of covert communication, which can include a mix of various steganographic techniques [16].
- Detection method based on network traffic visualization [17], in which a fundamental design principle of the anomaly detection approach is the lack of direct, linear time dependencies for the created network traffic visualizations.

In addition, several generic methods for steganalysis have been proposed for steganogram detection in digital media. However, these methods apply for a different range of data-hiding techniques (digital images/media) that are outside the scope of this research. Those methods include:

- A supervised learning-based steganalysis [18], which requires a training phase to learn classification rules to further classify digital data utilizing deep learning algorithms.
- A simple image comparison and its metadata, such as file size, to extract a steganogram [19].
- Utilizing Bayes classifier for observation of peak frequency in audio signals [20],
- Utilizing a sliding window and a convolutional neural network for steganalysis in audio transmission [21].

All told, the existing literature on network steganography detection focuses on countermeasures and methods for the detection of newly described steganography techniques rather than a generic approach, with exceptions described above.

The generic method described in this paper provides a framework for the utilization of various steganalysis methods at once. The method requires the use of other existing network steganography detection methods for optimum effectiveness. The proposed method's main novelty is providing a capability for intelligent selection of best-fit steganalysis methods for analyzed network traffic to maintain optimal resource utilization. While some of the existing methods provide a generic approach to steganography detection, none of those methods provide a unified cooperation model for utilizing other methods.

3. Multilayer Network Steganography Detection

3.1. Method Description

The core concept for our proposed method of network steganography detection is multilayer steganalysis and intelligent detection method selection based on packet classification and optimal resource utilization. We propose a top-down approach for a detection method selection algorithm as it ensures optimal computation resource allocation. In such an approach, we prefer high-layer metrics analysis over methods operating on low-level data (which would require more resources) unless high-level analyzers identify suspicious network traffic.

As shown in Figure 3, the first step is a packet capture (101), which acquires a single network packet from a hardware resource, such as a network card. The next step is feature extraction (102), which is the first stage of building a data model. Extracted features may include protocol headers and other derived data that can be calculated in near real-time. Extracted features serve as an input for metrics aggregation (103) and steganalysis layer selection (104). Metrics aggregation modules provide derived metrics operating on various aggregation layers. The scope of the metrics and calculation algorithms is determined by the steganalysis method(s) for which the method is to be applied. Examples of the metrics aggregation may include aggregated data counters, port utilization, etc. The main assumption for metrics aggregation is that high-layer metrics computation should consume fewer resources and take less time than the computation of low-layer metrics, as shown in Figure 4. We named the lowest-layer metrics "1^{st} *layer* aggregated metrics" and the highest-layer metrics "N^{th} *layer* aggregated metrics."

The calculated metrics and features extracted from each packet serve as input for steganalysis layer selection (104), which determines the optimal steganalysis layer. We discuss the steganalysis layer selection in Section 3.2.

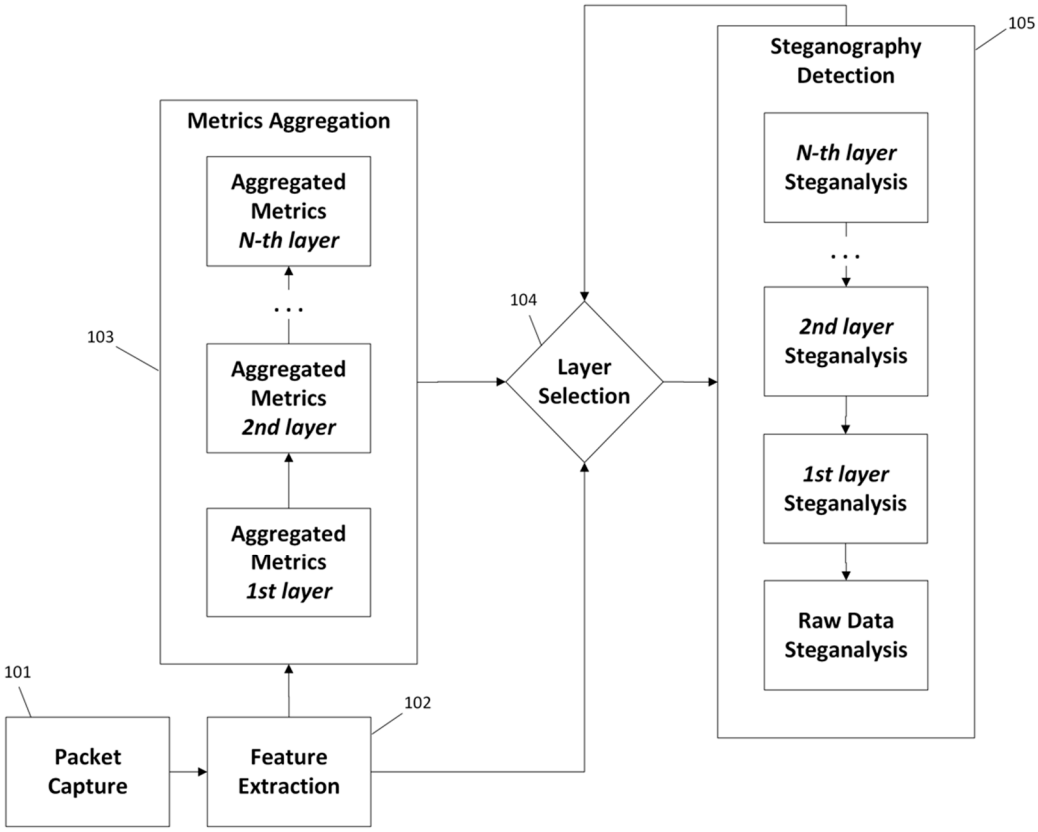

Figure 3. Multilayer detection method description.

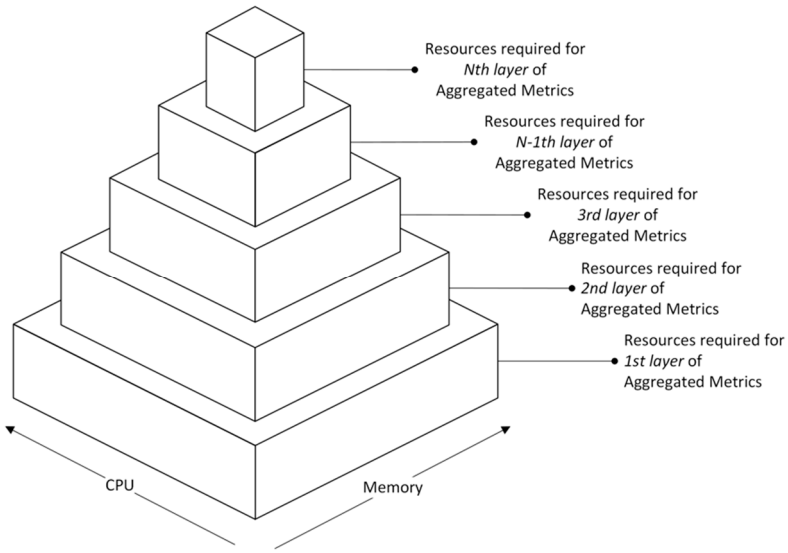

Figure 4. Aggregated Metrics hierarchy.

The Steganography Detection module (105) comprises multiple steganalysis methods. Each steganalysis method is assigned to a specific layer, based on the method's complexity and, in particular, on its resource utilization. Given a maximum of N layers of steganalysis methods, and a function $L(m)$ defining real-time operating resource consumption for each method m belonging to the set of methods M, the following is assumed:

$$\forall m \in M(L(m) < L(m-1)), \text{ provided that } N \geq m > 1 \quad (1)$$

In other words, steganalysis methods in higher layers require fewer resources to effectively detect network steganography in the real-time regime. Steganography detection methods in each layer may, but do not have to, operate on corresponding aggregated metrics layers.

The result of the performed multilayer steganalysis is provided to the steganography layer selection module to update the classification rules.

3.2. Steganalysis Layer Selection

The performance of our proposed method relies on the accuracy of the steganalysis layer selection algorithm and its parameters. In order to achieve better results, the algorithm should be tailored to fit specific performance requirements and at least the anticipated types of steganography technique. We suggest the following selection method, which should suffice for most applications.

As shown in Figure 5, the steganalysis layer selection method can operate in two modes:

1. Rule learning;
2. Packet classification.

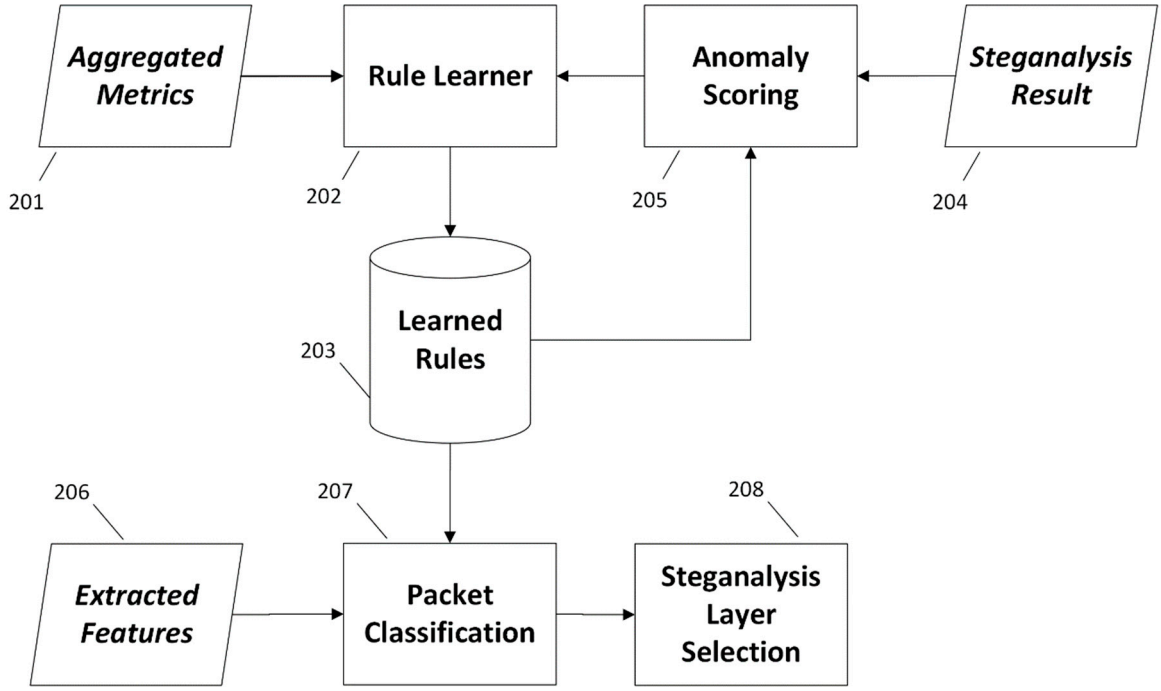

Figure 5. Steganalysis layer selection method.

In the first mode, the method applies various machine learning algorithms for frequent pattern mining, classification, and clustering to the steganalysis result (204) provided by the layered steganalysis module, computed anomaly scoring (205), and aggregated metrics (201). Learned rules are stored in memory (203) for the anomaly scoring module and packet classification.

In the second mode, the layer selection method receives a packet's extracted features (206) to classify the packet (207) for the selection of the optimal steganalysis layer (208). Packet classification (207) operates on previously learned rules and may use various classification methods and metrics, including but not limited to network address classification, network protocol classification, and TCP/UDP port classification.

The selection and application of specific algorithms for frequent pattern mining, classification, and clustering utilized by the rule learner module (202) are beyond the scope of this research work as they are widely discussed in the literature [21,22]. However, we recommend the *k-means clustering*

for mining a predefined number of clusters of network devices, the *FP-growth* algorithm for frequent pattern mining, and an optimized SVM (Support-Vector Machine) trainer [23] for classification.

3.3. Applicability

Our proposed method can be applied to optimize the detection of the most known network steganography techniques shown in Figure 2. The spectrum of detected steganographic techniques relies on network steganography detection methods utilized by the presented multilayer detection method. In Table 1, we outline the potential advantages and disadvantages of applying our multilayer network steganography detection method to each group of techniques.

Table 1. Applicability of detection method.

Group of Techniques	Method Applicability
Packet Modification	Network steganography techniques belonging to this group are relatively easy to detect without utilizing significant resources. Applying our proposed method for this group may introduce unnecessary overhead for high-layer steganalysis.
Stream Modification	Detection of network steganography techniques belonging to this group needs significantly more resources to monitor network traffic. Applying our proposed method for this group provides value by optimizing and narrowing the range of detection methods used in the described top-down approach.
Hybrid	Detection of network steganography methods belonging to this group needs at least as many resources as stream modification methods. Applying our proposed method for this group provides value by optimizing and narrowing the range of detection methods used in the described top-down approach.

Based on the above findings, we suggest limiting the use of our method to stream modification and hybrid network steganography detection.

4. Case Study

4.1. Experiment Scope and Methodology

To measure the crucial features of the proposed method, we decided to perform an experiment by applying the method to a chosen network steganographic technique. The main need was to evaluate steganalysis time and its characteristics. To perform accurate measurements, we needed to choose a steganographic technique that has the following features:

- There exists a detection method that compares raw network traffic;
- There exists a detection method that operates on the *1st layer* of aggregated metrics;
- There exists a detection method that operates on the *2nd layer* of aggregated metrics;
- The method preferably operates under the application layer.

The above set of features ensures that the proposed method application is best utilized and operates on at least three layers. In our opinion, applying the proposed method to any steganographic technique satisfying the requirements above should provide performance gains, depending on the chosen steganalysis methods on each layer. Given the requirements, we chose to apply our method to RSTEG (retransmission steganography) [5,13,24]. The application to RSTEG detection provides us a set of steganalysis methods, presented in the literature, that can operate on aggregated metrics as well as raw data.

The main idea of RSTEG is to not acknowledge a successfully received packet in order to intentionally invoke retransmission. The retransmitted packet carries a steganogram instead of user data in the payload field [5]. Although RSTEG is intended for a broad class of protocols that utilize retransmission mechanisms, we chose to conduct the experiment on hidden communication detection in TCP/IP networks.

The objective of our case study is to document the performance of network steganography detection utilizing steganalysis method(s) individually and in the multilayer approach presented in this paper. Various RSTEG steganalysis methods can be implemented using a passive warden [25] in the architecture we describe in Section 4.2. We proposed detection methods and assigned them to particular layers.

We measured packet processing time to determine the effectiveness of the method. We divided the experiment into two parts:

1. Communication capture;
2. Capture analysis.

Processing time was measured between the times the warden started and finished analyzing captured traffic. All measurements were performed on ~100 MB chunks of ~5 GB of captured network traffic on a virtual machine with a single CPU and 2 GB of RAM. Each measurement was repeated 10 times to provide average results.

4.2. RSTEG Steganalysis Methods

The most effective methods for RSTEG communication in TCP/IP networks are based either on payload comparison or anomaly detection in derived stream metrics, i.e.:

1. Comparison of the retransmitted and original payload;
2. Anomaly detection in the number of retransmissions for an individual connection;
3. Anomaly detection in the number of retransmissions for an individual device.

4.2.1. Comparison of the Retransmitted and Original Payload

The method of detection based on a comparison of retransmitted and original payload operates on the assumption that every retransmitted TCP segment should have a similar payload to the original one. Any outliers can be safely assumed to be carrying steganograms.

Processing and memory requirements for this method are excessive [5] and limit the method's application to selected network connections only. Required resources scale with the amount of transmitted data and the number of network connections.

Based on the above description, we assign this method to the "Raw Data Steganalysis" layer.

4.2.2. Anomaly Detection in a Number of Retransmissions for an Individual Connection

Anomaly detection in a number of retransmissions for an individual connection requires the following operations to be performed:

1. Determining whether an individual packet is retransmitted;
2. Determining the TCP segment retransmission ratio for an individual network connection;
3. Outlier detection in the TCP segment retransmission ratio for an individual network connection.

Based on the fact that all of the above steps operate on a packet's extracted features and aggregated metrics, we assign this method to the first layer.

4.2.3. Anomaly DETECTION in a number of Retransmissions for an Individual Device

The method of anomaly detection in a number of retransmissions for an individual device is similar to the method presented above but operates in a broader scope. In this approach, the retransmission ratio for all network device traffic is determined, and outliers are detected.

Based on the fact that this method operates in a higher layer of aggregated metrics, we assign this method to the second layer.

4.3. Architecture

We conducted the experiment utilizing the following architecture for data capture and further investigation.

The architecture presented in Figure 6 comprises two endpoints: Alice (303) and Bob (311), who have established an RSTEG channel and are exchanging steganograms, among other network traffic. Bob's endpoint resides in a local network (310) in which all network traffic goes through the core router (312). The core router sends a copy of all traffic to the passive warden (313). Communication coming from other network devices (314) not necessarily involved in steganographic communication is also analyzed.

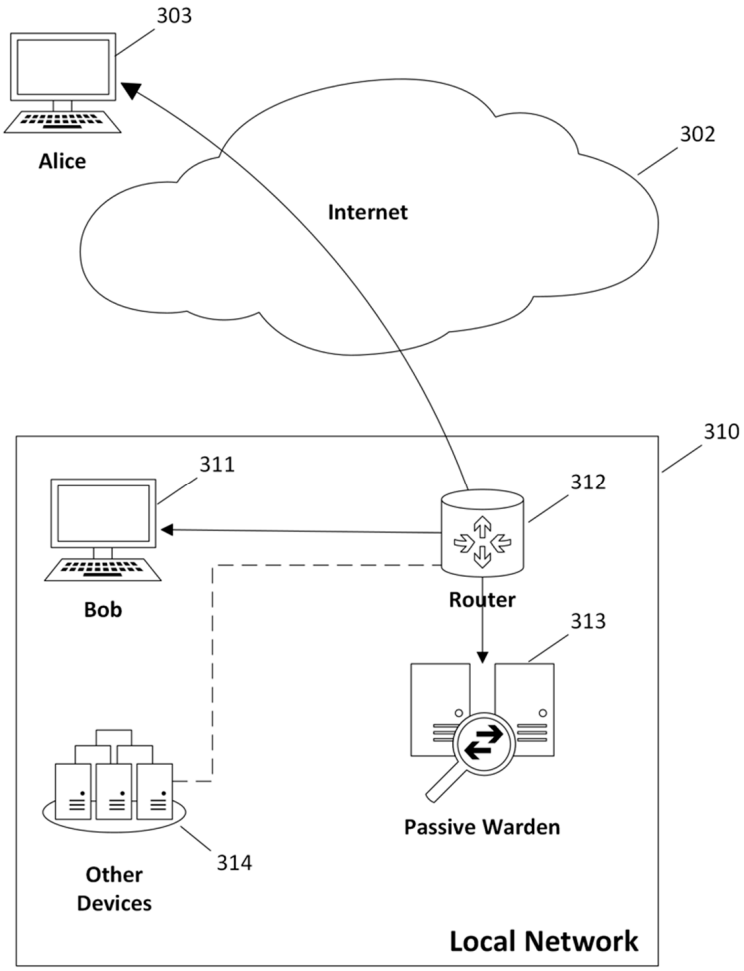

Figure 6. Implementation architecture.

4.4. Results

To provide an overview of multilayer steganalysis method performance, we measured the processing time for the methods applied in each layer as well as the total processing time required by our method. Each measurement was performed using the methodology described in Section 4.1.

As shown in Table 2, an increased ratio of retransmissions in the network causes an increase in processing time despite the chosen method(s). Processing time increases significantly for lower layers of steganalysis methods, including raw data steganalysis.

Table 2. Steganalysis performance.

Ratio of Retransmissions (%)	Raw Steganalysis Time (s)	1st Layer Detection Time (s)	2nd Layer Detection Time (s)
1	2.79	0.53	0.04
2	4.50	0.89	0.12
3	4.63	1.33	0.16
4	5.91	1.04	0.13
5	6.54	2.01	0.14

In Figure 7, we show the steganalysis time for raw data steganalysis in the retransmission ratio domain. As the chart shows, an increase in the network retransmission ratio causes an increase in the processing time; this increase can be approximated by a linear function. Given that raw data steganalysis for RSTEG means storing, iterating, and comparing retransmitted segments with the original ones, the substantial near-linear increase in processing time is fully legitimate.

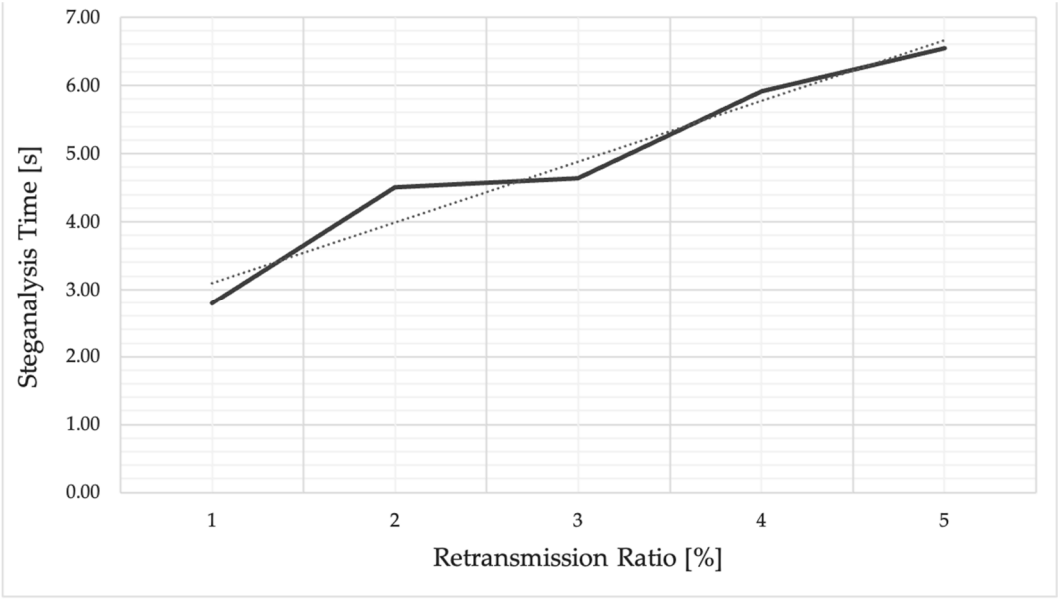

Figure 7. Raw Data Steganalysis time.

In Figure 8, we show the steganalysis time for the first-layer steganalysis in the retransmission ratio domain, which also includes raw data steganalysis for selected traffic. For RSTEG application, the method directs TCP segments belonging to connections that qualified as outliers for further raw data steganalysis, which means payload comparison.

The results also show an increase that can be approximated by a linear function, which makes sense because of the significant overhead required for processing separate connections, anomaly detection, and the potentially higher number of segments directed to lower-layer steganalysis.

In Figure 9, we show the steganalysis time for second-layer steganalysis in the retransmission ratio domain. Second-layer steganalysis involves selectively directing network traffic to first-layer steganalysis as well as raw data steganalysis. In our application, the method analyzes the retransmission ratio in the context of an individual network device, then directs outlier devices to the method that analyzes network connections and directs outlier traffic to payload comparison for retransmitted segments (raw data steganalysis).

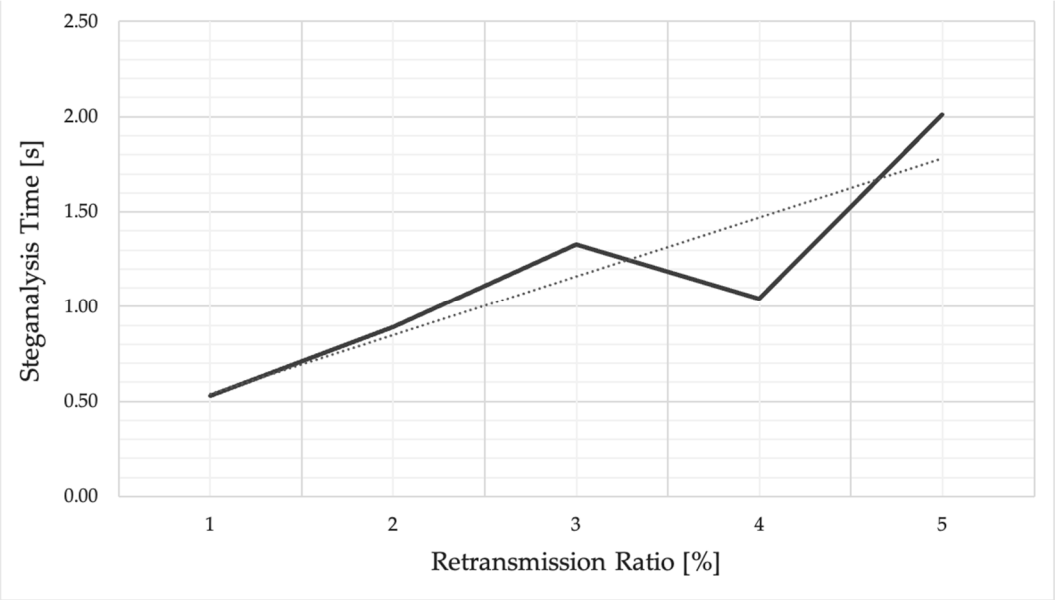

Figure 8. First-layer Steganalysis time.

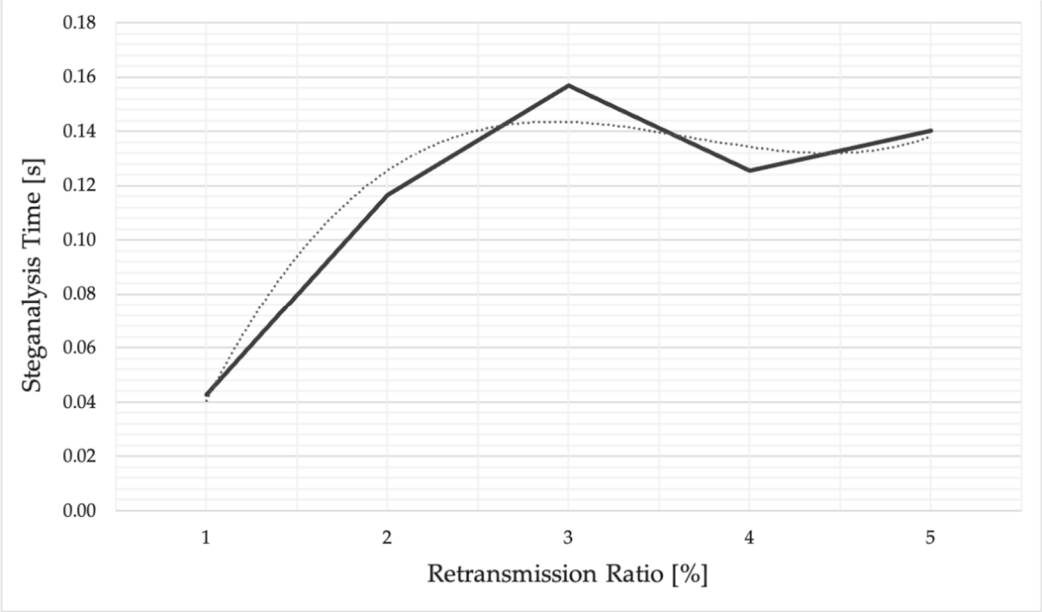

Figure 9. Second-layer steganalysis time.

The results show a non-linear increase in processing time, which can be closely approximated by a third-order polynomial function. Given that the method operates on the highest layer of aggregated metadata, a non-linear increase in processing time is justified. The second-layer method brings the most substantial gain in steganalysis, with an increasing retransmission ratio in our case.

The percentage gain in processing time when multilayer detection is applied is shown in Figure 10 and Table 3. The results show a significant performance gain for higher-layer detection methods (as expected). However, the gain slightly decreases in comparison to the lowest retransmission ratio applied (1%). This is a result of method selection algorithm overhead and aggregation of required metrics.

Table 3. Steganalysis performance gain.

Ratio of Retransmissions (%)	Raw Steganalysis Time (s)	1st Layer Detection Gain (%)	2nd Layer Detection Gain (%)
1	2.79	526%	6552%
2	4.50	506%	3861%
3	4.63	349%	2956%
4	5.91	568%	4716%
5	6.54	325%	4666%

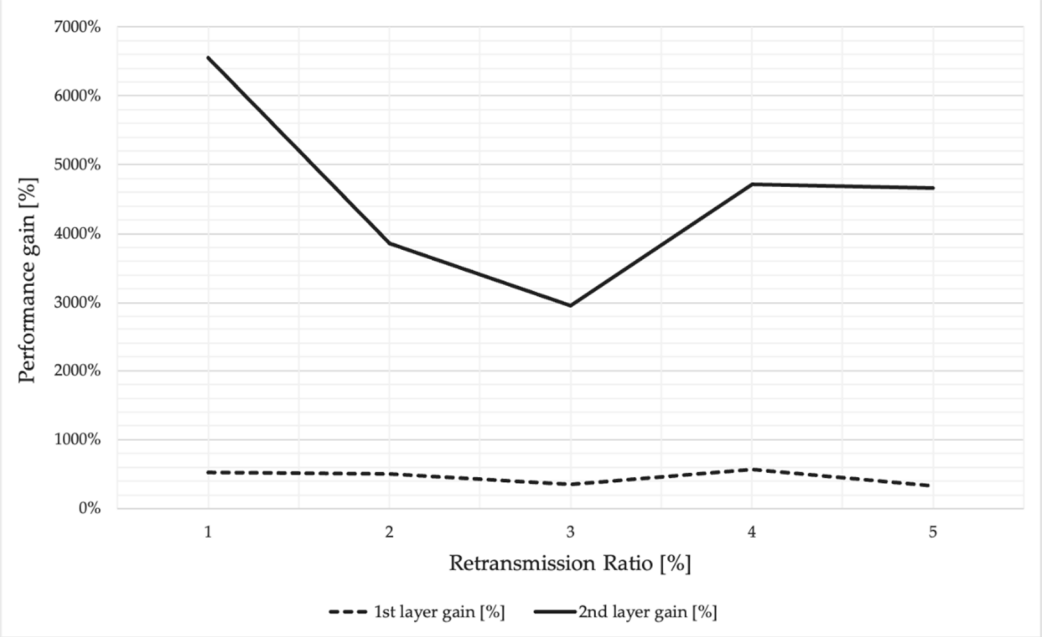

Figure 10. Steganalysis performance gain.

5. Conclusions

Multilayer steganography detection is a method that utilizes a top-down approach for network steganography detection and introduces an intelligent choice of steganographic methods applied to specific network traffic. As a part of the method, we have presented a steganalysis layer selection method that provides an intelligent selection of steganalysis algorithms, preserving the balance between resource consumption and detection performance. To the authors' best knowledge, this is the first generic network steganography detection method that utilizes a top-down approach for a detection method selection algorithm to ensure optimal computation resource allocation.

We have described the method's concept and its key components and discussed the method's applicability for network steganography detection in the context of known data-hiding methods. We also considered steganography detection in real networks in a wider context. The method requires the use of other existing network steganography detection methods for optimum effectiveness. The main novelty of the proposed method is providing a capability for intelligent selection of the best-fit steganalysis method for analyzed network traffic to maintain optimal resource utilization. Other generic detection methods presented so far do not provide orchestration for network steganography detection.

We applied our method for the detection of the RSTEG data-hiding method, presented the proposed detection techniques and assigned them to specific layers. The results demonstrated the method's performance gain over the steganalysis of raw network data. The presented characteristics of performance gain lead us to the conclusion that the method's application for real-time steganalysis is promising as it introduces a non-linear increase in processing time.

We suggest the following areas of future research:

- Performance scaling of required resources;
- Application of the method to other network steganography techniques;
- Application of the method to steganography detection in a broader context not tied to TCP/IP networks.

Author Contributions: M.S. contributed to theoretical formulation, design methodology, dataset development, experiment design and implementation, results interpretation, original draft preparation and revision. The other authors (K.S., J.P.) contributed to project supervision, theoretical formulation, result interpretation, and revision of the initial draft. All authors have read and agreed to the published version of the manuscript.

Funding: This scientific research work was co-financed by the European Union, project name: "The system for identification and monitoring of anomalies and risks in ICT networks". The amount financed by the European Union was EUR 1,044,534.63. The investment outlay value for the entire project was EUR 1,407,526.46. The subsidy was allocated from the European Regional Development Fund, Operational Program "Smart Growth", sub-measure 1.1.1 "Industrial research and development work implemented by enterprises" (grant number: POIR.01.01.01-00-0554/15).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Tanwar, R.; Malhotra, S.; Singh, K. *Future of Data Hiding: A Walk through Conventional to Network Steganography, in Cyberspace Data and Intelligence, and Cyber-Living, Syndrome, and Health*; Springer Science and Business Media LLC: Berlin, Germany, 2020; Volume 1230, pp. 123–132.
2. Nafea, H.; Kifayat, K.; Shi, Q.; Qureshi, K.N.; Askwith, B. Efficient Non-Linear Covert Channel Detection in TCP Data Streams. *IEEE Access* **2020**, *8*, 1680–1690. [CrossRef]
3. Collins, J.; Agaian, S. Trends Toward Real-Time Network Data Steganography. *Int. J. Netw. Secur. Its Appl.* **2016**, *8*, 1–21. [CrossRef]
4. Seo, J.; Manoharan, S.; Mahanti, A. Network steganography and steganalysis—A concise review. In Proceedings of the 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Bengaluru, India, 21–23 July 2016; pp. 368–371.
5. Mazurczyk, W.; Smolarczyk, M.; Szczypiorski, K. Retransmission steganography and its detection. *Soft Comput.* **2009**, *15*, 505–515. [CrossRef]
6. Lubacz, J.; Mazurczyk, W.; Szczypiorski, K. Principles and overview of network steganography. *IEEE Commun. Mag.* **2014**, *52*, 225–229. [CrossRef]
7. Frączek, W.; Mazurczyk, W.; Szczypiorski, K. Hiding information in a Stream Control Transmission Protocol. *Comput. Commun.* **2012**, *35*, 159–169. [CrossRef]
8. Grabski, S.; Szczypiorski, K. Network steganalysis: Detection of steganography in IEEE 802.11 wireless networks. In Proceedings of the 2013 5th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Almaty, Kazakhstan, 10–13 September 2013; pp. 13–19.
9. Goher, S.Z.; Javed, B.; Saqib, N.A. Covert channel detection: A survey based analysis. In Proceedings of the 9 th International Conference on High Capacity Optical Networks and Emerging/Enabling Technologies, Istanbul, Turkey, 12–14 December 2012; pp. 57–65. [CrossRef]
10. Bieniasz, J.; Stepkowska, M.; Janicki, A.; Szczypiorski, K. Mobile agents for detecting network attacks using timing covert channels. *J. Univ. Comput. Sci.* **2019**, *25*, 1109–1130.
11. Lu, S.; Chen, Z.; Fu, G.; Li, Q. A Novel Timing-based Network Covert Channel Detection Method. *J. Phys. Conf. Ser.* **2019**, *1325*, 012050. [CrossRef]
12. Szczypiorski, K.; Tyl, T. MoveSteg: A Method of Network Steganography Detection. *Int. J. Electron. Telecommun.* **2016**, *62*, 335–341. [CrossRef]
13. Mazurczyk, W.; Smolarczyk, M.; Szczypiorski, K. On information hiding in retransmissions. *Telecommun. Syst.* **2011**, *52*, 1113–1121. [CrossRef]
14. Mazurczyk, W.; Lubacz, J. LACK—a VoIP steganographic method. *Telecommun. Syst.* **2010**, *45*, 153–163. [CrossRef]
15. Cabaj, K.; Mazurczyk, W.; Nowakowski, P.; Żórawski, P. Fine-tuning of Distributed Network Covert Channels Parameters and Their Impact on Undetectability. In Proceedings of the 14th International Conference on Availability, Reliability and Security—ARES '19, Canterbury, UK, 26–29 August 2019; pp. 1–8. [CrossRef]

16. Chourib, M. Detecting Selected Network Covert Channels Using Machine Learning. In Proceedings of the 2019 International Conference on High Performance Computing & Simulation (HPCS), Dublin, Ireland, 15–19 July 2019; pp. 582–588.
17. Mazurczyk, W.; Szczypiorski, K.; Jankowski, B. Towards steganography detection through network traffic visualisation. In Proceedings of the 2012 IV International Congress on Ultra Modern Telecommunications and Control Systems, Petersburg, Russia, 3–5 October 2012; pp. 947–954. [CrossRef]
18. Chandramouli, R.; Subbalakshmi, K. Current trends in steganalysis: a critical survey. In Proceedings of the ICARCV 2004 8th Control, Automation, Robotics and Vision Conference, Kunming, China, 6–9 December 2004; pp. 964–967.
19. Krenn, J.R. Steganography and Steganalysis, Internet Publication. Available online: http://www.krenn.nl/univ/cry/steg/article.pdf (accessed on 9 December 2020).
20. Zeng, W.; Ai, H.; Hu, R.; Gao, S. An algorithm of echo steganalysis based on Bayes classifier. In Proceedings of the 2008 International Conference on Information and Automation, Changsha, China, 20–23 June 2008; pp. 1667–1670.
21. Zhao, S.; Chandrashekar, M.; Lee, Y.; Medhi, D. Real-time network anomaly detection system using machine learning. In Proceedings of the 2015 11th International Conference on the Design of Reliable Communication Networks (DRCN), Kansas City, KS, USA, 24–27 March 2014; pp. 267–270.
22. Bieniasz, J.; Sapiecha, P.; Smolarczyk, M.; Szczypiorski, K. Towards model-based anomaly detection in network communication protocols. In Proceedings of the 2016 2nd International Conference on Frontiers of Signal Processing (ICFSP), Warsaw, Poland, 15–17 October 2016; pp. 126–130.
23. Franc, V.; Sonnenburg, S. Optimized Cutting Plane Algorithm for Large-Scale Risk Minimization. *J. Mach. Learn. Res.* **2009**, *10*, 2157–2192.
24. Mazurczyk, W.; Smolarczyk, M.; Szczypiorski, K. Retransmission Steganography Applied. In Proceedings of the 2010 International Conference on Multimedia Information Networking and Security, Nanjing, China, 4–6 November 2010; pp. 846–850.
25. Fisk, G.; Fisk, M.; Papadopoulos, C.; Neil, J. Eliminating Steganography in Internet Traffic with Active Wardens. In *Computer Vision—ECCV 2020*; Springer Science and Business Media LLC: Berlin, Germany, 2002; pp. 18–35.

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).