SCIENTIFIC REVIEW CURRENT ISSUES OF THEORY AND PRACTICE

Published: August 10, 2023 | Pages: 127-131

ADVANCEMENTS IN RETRANSMISSION STEGANOGRAPHY: AN ENHANCED ALGORITHM AND ITS STEGANALYSIS APPROACHES

Obid Mavlonov

Tashkent University Of Information Technologies Named After Muhammad Al-Khwarizmi

Tashkent, Uzbekistan

ABSTRACT: - Network steganography, also known as a covert communication channel within a network, is a discrete method for secretly transmitting confidential data by exploiting the redundancies found in network protocols. The technique known as retransmission steganography (RSTEG) involves hiding classified information within the payload section of retransmitted packets intentionally generated by the communicating parties. However, this method overlooks the checksum fields in the original packets, resulting in differences between the retransmission packets and compromising its level of secrecy. To address this limitation, we introduce an improved version of the RSTEG algorithm called Enhanced RSTEG (ERSTEG) in this paper. The proposed enhancement ensures that the checksum fields in both the original and retransmission packets are synchronized, thereby significantly enhancing the concealment capabilities of ERSTEG compared to RSTEG.

KEY WORDS: - Synchronized, thereby significantly enhancing, RSTEG.

INTRODUCTION

In 2007, Zandel conducted a scientific study [3] that examined existing covert channels and their corresponding detection algorithms. Over time, the original covert channels have become well-known, and as covert communication occurs within regular traffic, it has resulted in significant alterations to normal network traffic patterns. These changes have inadvertently exposed information from these secret channels. Consequently, current research efforts are directed towards developing new covert channels. Researchers in this field are primarily focused on creating hidden channels that closely resemble normal communication channels. This approach enhances the privacy of these covert channels. Here are some findings from scientific research on methods for creating covert channels.

In a study led by Ji and colleagues [4], they propose the use of a covert channel that utilizes the length of network packets to transmit covert messages. Their algorithm takes into consideration the normal distribution of packet lengths, ensuring that the hidden packet length distribution closely resembles the normal distribution. Yao and his research colleagues [5] introduced an ON/OFF hidden time channel, which relies on network time slot allocation. This approach enables the approximation of the hidden time series to closely resemble normal behavior. Gianvecchio and other researchers [6] proposed a hidden time channel based on a straightforward time slot

Published: August 10, 2023 | Pages: 127-131

distribution model. This method offers high stealthiness and proves to be more efficient than most existing techniques for detecting hidden time channels.

Szczypiorski and his research team[7] introduced the Retransmission Steganography (RSTEG) algorithm. This technique utilizes the payload field of retransmission packets to discreetly transmit secret messages. Typically, network retransmissions occur due to increased network load, excessive delays, or packet reordering, constituting approximately 7% of all Internet traffic[8]. RSTEG capitalizes on the substantial payload capacity of a single packet, leading to high throughput. However, it is essential to note that RSTEG alters the checksum field of retransmission packets compared to the original packets, making it possible for detectors to identify hidden communication based on discrepancies in checksum values. In essence, RSTEG operates as a form of retransmission steganography, and its underlying principles are detailed below. The RSTEG method operates based on the following principles: Given that a significant portion of Internet traffic (approximately 80% to 90%) is conducted using the TCP protocol, integrating RSTEG within a TCP packet is a strategic choice. The RSTEG framework can be visualized as depicted in Figure 1 below. It functions as a steganography algorithm that leverages TCP packet retransmission when a timeout occurs.

Here's how it works: When the receiver successfully receives a TCP segment, it refrains from sending an ACK (acknowledgment) packet. However, if the sender does not receive an ACK packet from the receiver within a specified time, it triggers the retransmission of the last packet. In these retransmission packets, the sender manipulates the payload field to embed hidden messages. Upon receiving these retransmission packets, the receiver extracts the secret messages and sends an ACK packet back to the sender. In the TCP protocol, once one segment is successfully transmitted, the next segment is sent. The RSTEG algorithm essentially mirrors the timeout state of a TCP packet, with the distinction lying primarily in the conditions that trigger retransmission.

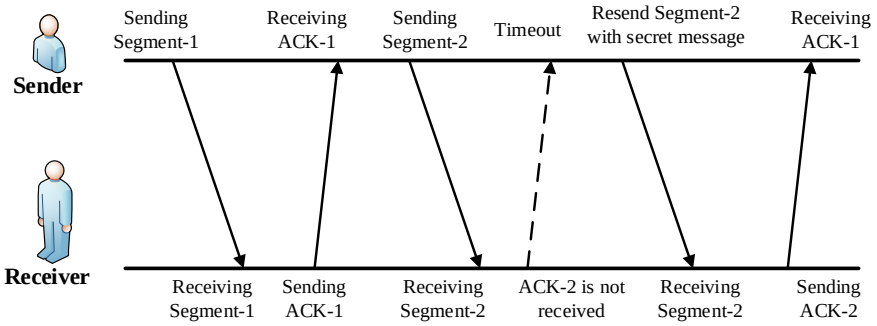

Figure 1. RSTEG framework

As depicted in Figure 1 above, when a TCP segment is transmitted, the receiver withholds an ACK packet to acknowledge message receipt. Consequently, the message sender has the opportunity to modify the segment's content and resend it. By utilizing this approach, the message sender

Published: August 10, 2023 | Pages: 127-131

conceals a secret message within the content of the retransmitted segment, which the receiver subsequently extracts.

Analyzing the RSTEG method reveals three potential detection approaches. The first method involves comparing retransmission probabilities, a proposal introduced by Szczypiorski [9]. In this method, if the probability of retransmission surpasses a specified threshold, the traffic is considered anomalous and potentially indicative of RSTEG. However, this method's effectiveness diminishes when the retransmission probability is low.

The second method involves comparing the payload fields. In TCP retransmissions, the payload fields of the original and retransmitted packets remain identical. This method assesses the payload fields of both the original and retransmitted packets. If they match, the retransmission behavior is deemed normal; otherwise, it is considered anomalous. This approach addresses the drawback of the first method and can detect instances where the sender employs retransmission probabilities that closely resemble normal behavior. However, it comes with its own limitations, notably the requirement for significant cache memory and computing resources. For example, assuming a TCP link speed of 50 packets per second, each packet being 1500 bytes long, a retransmission probability of 5%, and 20 TCP links on the gateway, detecting RSTEG using this method would demand 1.4 GB of cache memory per second. As more TCP links are added, the resource demands increase substantially.

The last method entails comparing checksum values. When the sender inserts secret messages into the payload field, it must recalculate the checksum of the retransmitted packet; otherwise, the packet will be dropped. In most cases, this recalculated checksum value differs from that of the original packet. The detector can compare the checksums of the original and retransmitted packets to identify RSTEG. The effectiveness of this method depends on predefined thresholds for high and low detection rates.

Indeed, among the three potential detection methods discussed, the last method, which involves comparing checksum values, offers the advantage of requiring fewer resources while maintaining high accuracy. Therefore, when enhancing the RSTEG method, it is advisable to prioritize and further refine the checksum value comparison approach. With this in mind, the improved ERSTEG method of the RSTEG technique is developed as described below.

The ERSTEG framework is proposed as shown in Figure 2, which mainly consists of following three steps:

- Embedder;
- Compensator;
- Filter.

Published: August 10, 2023 | Pages: 127-131

In the enhanced ERSTEG method, the covert communication process is structured into three key steps:

1. Message Embedding: Initially, the sender employs an Embedder to convert the secret messages into specific payload fields of the retransmission packets. These secret messages are hidden within the payload of the packets in such a way that they appear like regular data.

2. Checksum Compensation: Following message embedding, a compensator is utilized to allocate 2 bytes (2B) of the payload field. This allocation is dedicated to compensating for the checksum field in accordance with a compensation algorithm that will be detailed shortly. After the compensator's intervention, the checksum field of the retransmission packet becomes identical to that of the original packet.

3. Packet Transmission and Reception: Subsequently, the sender transmits the retransmission packet containing the concealed messages. Upon receiving this packet, the receiver employs a filtering mechanism to differentiate hidden traffic from regular traffic. Once the filter identifies the presence of hidden messages, the receiver proceeds to extract these messages from the payload field of the retransmission packet.

The sequence of these steps ensures the secure and covert transmission of messages within the network traffic, with the compensation algorithm playing a crucial role in maintaining the integrity of the retransmission packets.

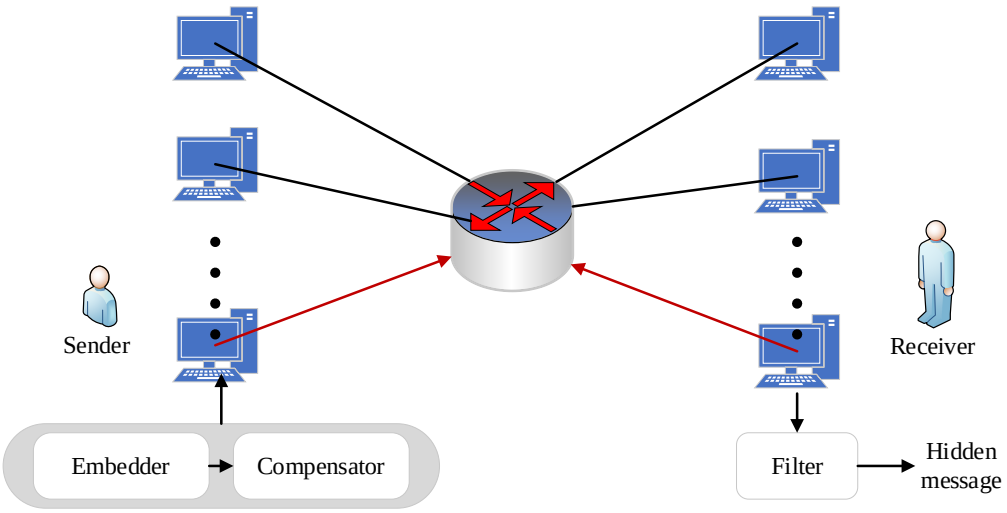

Figure 2. The diagram of ERSTEG

CONCLUSION

In summary, the retransmission steganography algorithm, RSTEG, demonstrates a notable advantage in terms of its high stealth capability. However, a vulnerability of RSTEG lies in the fact that the checksum fields of the original and retransmission packets differ, which can be detected using the checksum value comparison method. The Enhanced RSTEG (ERSTEG) algorithm, introduced in this research, addresses this detection vulnerability of secret communication.

Published: August 10, 2023 | Pages: 127-131

ERSTEG offers enhanced concealment abilities compared to the RSTEG algorithm. Additionally, ERSTEG incorporates an algorithm for comparing payload samples, further bolstering its effectiveness in covert communication. ERSTEG is designed to provide a more robust and covert method for transmitting hidden messages within network traffic, making it a valuable advancement in the field of steganography and data security.

REFERENCES

1. Lampson B. Practical principles for computer security //NATO SECURITY THROUGH SCIENCE SERIES D-INFORMATION AND COMMUNICATION SECURITY. – 2007. – T. 9. – C. 151.
2. Ma B. et al. Enhancing the security of image steganography via multiple adversarial networks and channel attention modules //Digital Signal Processing. – 2023. – C. 104121.
3. S. Zandel, G. Armitage, P. Branch. A survey of covert channels and countermeasures in computer network. IEEE Communications. Surveys and Tutorial. 2007, 9(3), pp.44-57.
4. L. Ji, W. Jiang, B. Dai, X. Niu, A novel covert channel based on length of message. In proceedings of 2009 International symposium on information engineering and electronic commerce. 2009, pp. 445-450.
5. L. Yao, X. Zi, L. Pan and J. Li. A study of on/off timing channel based on packet delay distribution. Computers & Security, 2009,28(8), pp.785-794.
6. S. Gianvecchio, H. Wang, D. Wijesekera. Modelbased covert timing channels: automated modeling and evasion. Lecture Notes In Computer Science, 2008, vol.5230, pp.211-230.
7. W. Mazurczyk, M. Smolarczyk, K. Szczypiorski. Retransmission steganography and its detection. Soft Computing. 2009, 15(3), pp. 505-515.
8. S. Rewaskar, J. Kaur, F. Smith. A Performance Study of Loss Detection/Recovery in Real-world TCP Implementation. In Proceedings of the IEEE International Conference on Network Protocols, ICNP 2007, 2007, pp. 256-265.
9. W. Mazurczyk, M. Smolarczyk, K. Szczypiorski. Retransmission steganography and its detection. Soft Computing. 2009, 15(3), pp. 505-515.
10. Kholdinasab N., Amirmazlaghani M. An adversarial learning based image steganography with security improvement against neural network steganalysis //Computers and Electrical Engineering. – 2023. – T. 108. – C. 108725.
11. Bedi P., Dua A. Network steganography using the overflow field of timestamp option in an IPv4 packet //Procedia Computer Science. – 2020. – T. 171. – C. 1810-1818.