[1] **Elham Haseli**

An Improved Method for Detecting Covert Channels in the Transport Layer

JES Journal of Electrical Systems

Abstract: - Steganography is one of the techniques used both to leak information and to prevent theft and distortion of confidential information. Covert channels in the network are one of the platforms for information steganography in the network. Often, this method is realized using the network's protocols. Network protocols are used as an information transfer medium. Network protocols can contain critical information and carry them into the network without attracting consideration. Covert channels are evaluated with three different criteria including capacity, robustness, and insensitivity. Also, the methods to deal with it include removing, limiting, and diagnosing the channel. By definition, covert channels are used to realize covert communication. Steganography methods are safe if the stego has no detectable signatures. Put differently, the stego statistical properties (audio, image, and video) should be similar to the cover properties. The ability to discover the message in the stego depends on the length of the hidden message. The proposed method in this study is to consider the amount of redundant information in a repository, explore the discoverable signs of the covert channel, and check the packet length in the checksum field in the UDP protocol at the transmission layer.

Keywords: Steganography, cryptography, steganography in the network, covert channel, packet length, UDP protocol, suspicious network traffic, checksum field

I. INTRODUCTION

Nowadays, security in the process of sending information is extremely important. Mankind has always looked for a way to securely transmit its information while knowing the enemy's secrets. One of these conventional methods to achieve this goal is called cryptography. In cryptography, strong mathematical calculations are used to convert plain text into cipher text and send it to the receiver through a channel. However, in another approach called steganography, the existence of data is covered [14].

Steganography means the knowledge of data transmission in media such as image, sound, and video. The use of image formats, especially JPEG, is particularly popular in this field. Over the past few years, many computer science researchers have developed numerous methods and algorithms to strengthen security in sending information and revealing hidden information in communications [15]. Along with the development of information steganography methods, the efforts to know the hidden information have also increased. Therefore, researchers have developed and improved methods of steganalysis. Two scenarios are proposed in the steganalysis process. If the steganography algorithm is known, studying it may lead to a way to reveal the hidden message. This method is called specific steganalysis, which is very difficult to implement. The reason is that usually, covert recording methods remain confidential [16]. Even if the kernel of these methods is made available, it seems complicated to detect the method used for steganalysis. It is desirable to detect the presence or absence of a message in the transmission medium without detecting the steganography method. This method is called blind steganalysis. In steganography methods, packet length is used to send covert data [17].

In computer security science, the covert channel is a type of attack with the ability to transfer information objects between unauthorized processes. The term covert channel was proposed by Lampson in 1973. Virtual space or cyberspace as a new phenomenon in the information age has brought many phenomena, each of which has its threats and opportunities. Communication protocols with different structural features, communication methods, communication capacity, security levels, and diverse applications suffer from much vulnerability [18].

One of the critical threats to cyberspace is the leakage of confidential or sensitive information through the network protocol. Information leakage has won second place in the ranking of threats and attacks. One of the main ways of information leakage of organizations in cyberspace is through covert channels [19]. Covert channels form hidden communication under the cover of legitimate and open communication. However, the nature of the relations and the parties remain covert. Generally, covert channels lead to information leakage from a user with a high level of access to another user with a lower level of access. Steganography methods are safe if the stego has no detectable signatures. Put

[1]Department of software engineering - software orientation, Lahijan Branch, Islamic Azad University, Lahijan ,Iran

differently, the stego properties (audio, image, and video) should be similar to the cover properties. The ability to discover the message in the stego depends on the length of the hidden message [20].

One of the ways used by attackers to extract data from the organization's network is to transfer information under the cover of authorized communications and traffic. This type of communication is called a covert channel. The concept of subtly transmitting information under the guise of an authorized communication channel has existed for a long time. The emergence of cyberspace with complex layers and protocols has created a new medium for covert data transmission [21].

The performance of network protocols is directly related to the lifetime and coverage of individual packets that make up the network. As a result, all levels of the network must be designed with full knowledge of how to detect and identify unauthorized channels [13]. One of the most effective things in extending the lifetime of the network is the discovery of covert channels in the transmission layer. Many actions have been taken by network experts to provide different methods to discover covert channels, and at the same time, different protocols have been proposed in this field.

Nicole Tayla et al. (2020) in their study titled "detection selected network covert channels using machine learning" used ML methods to detect network covert channels. The dataset is made up of 9 standard covert tools and covert channels. Subsequently, the data has been categorized and labeled as a pattern. Half of the generated data set has been used to train three ML algorithms. The second part of the data was used to verify the performance of the algorithm. The tested algorithms are support vector machines (SVM), K-nearest neighbors (KNN), and deep neural networks (DNN) [1].

Ovadya (2019) in his study entitled "Cross-router covert channels" showed that the logical separation of the network based on the host and guest networks can be achieved using router covert channels [2].

Sohn et al. (2003) in their study entitled "Detecting covert channels in ICMP using vector machines" showed that ICMP traffic is pervasive in TCP/IP networks. As a result, many network devices consider ICMP traffic to be harmless and allow it to pass. Therefore, attackers can include any information they want in the payload of packets. Researchers used SVM to detect a covert channel in ICMP. The SVM method has excellent performance in pattern classification problems. The findings proved that the proposed method can detect ICMP covert channels from normal ICMP traffic using SVM [3].

Fadlalla et al. (2018) in their study entitled "Packet Length Covert Channel: A Detection Scheme" showed that the hidden path of the packet can create a covert traffic very similar to normal traffic. Researchers proposed a tracking scheme based on machine learning with high detection accuracy to solve this challenge [4].

Alain Rumi et al. (2011) realized the detection of covert channels by presenting a framework based on information theory. The results showed that the usual concept of interference cannot define the concept of conscious information flow of covert channels. At the same time, an advanced idea cannot register the interference of streams with a capacity of less than one bit per channel. Subsequently, they specified and calculated the capacity of covert channels using control flows for a class of systems [5].

Anarita Giani et al. (2005) in their study entitled "Covert Channel Detection: A Survey-Based Analysis" showed that including a table of queries in the network can track covert channels [6].

Zerafshan et al. (2012) in their research entitled "Covert Channel Detection: A Survey" showed that through covert channel tracking techniques, it is possible to track storage covert channels and scheduled covert channels [7].

Dehghani and Saleh Esfahani (2013) investigated covert cyber channels to create safe and inconspicuous communication in hidden networks. The results showed that encryption of information before sending can be desirable to improve the security level of the channel [8].

Dehghani and Saleh Esfahani (2014) conducted research titled "Design and Evaluation of hybrid coding method for the scheduled covert channel on the Internet". The results showed that in reordering the network, selecting three to five bases in the code word table has increased the capacity from 10% to 300%. Also, the imperceptibility has been improved to an acceptable level and the strength of the channel has been maintained [9].

In research entitled "covert channel over social networks", Selvi (2012) showed how the ways of separating data in these networks affect organizational and personal security. As a proof of concept, a tool called Facecat has been introduced. Using this tool, you can chain the ports using the Facebook wall. Therefore, the network can be protected through proxy and other attached tools [10].

Koka (2006) developed a set of experimental tools using C# to detect and analyze covert channels in the application layer to monitor HTTP. This programming language is becoming a trend in the networking industry. Analysis of current trends in channel detection methods and statistics collected about current implementations of the protocol have led to the proper design and implementation of HTTP covert channel detection [11].

Brown et al. (2010) in their study entitled "Covert Channels in the HTTP Network Protocol: Channel Characterization and Detecting Man-in-the-Middle Attacks" showed that the HTTP transport protocol accounts for almost half of all Internet traffic and becomes a standard for hiding network covert channels. This article defines a common set of features. According to these features, several covert channels in HTTP were identified and classified. This article suggests that the detection of network covert channels has useful applications such as the detection of attacks and network penetration [12].

Velijon et al. (2018) conducted a study titled "a study on the Detection of covert channels based on deep learning". A new idea for covert channel detection based on deep learning algorithm is proposed and a new detection model is proposed. This algorithm-based model can identify more complex covert channels. Also, the accuracy of detection has been greatly improved due to the application of a new deep-learning model [13].

The main issue of this research is what communication solutions and protocols exist to discover covert channels in the network. How much can these solutions meet the real communication needs of covert network detection? Which communication protocol has the appropriate capacity and acceptable security with the ability to pass the defense barriers of computer networks? In this study, a network steganography identification scheme is presented. By calculating the checksum field of the UDP protocol, this method can detect the presence of steganography and covert channels. The main question of this research is formulated as follows. Is the improved method of discovering covert channels by calculating the length of the packet in the checksum field considered a suitable solution for solving the problem of hidden network steganography?

First, we start by gathering information and reviewing the available methods to discover covert channels in the transport layer. Then, by comparing these methods with each other and specialized examination of transmission layer protocols, we achieve an improved method to discover covert channels in the fourth layer of the standard OSI model. This research is placed in the class of applied studies. The collection of research resources is done with the library method of using databases accessible through the Internet. Also, the collected information is analyzed by various reasoning methods. Then, using the existing models and conceptual working frameworks in other applications, a new conceptual framework is proposed for recognizing and studying covert channels. Important techniques for performing preprocessing operations should be considered. It seems very necessary to prepare the transport layer protocol for the pattern recognition process. The inputs to the preprocessing stage are transport layer protocols. Also, the key output is the discovered channel-covert. This procedure includes the following steps, each of which performs a specific task to process data and control network traffic.

1) Network traffic control

2) Channel detection (suspicious traffic)

3) Monitor the observed channel

4) Complete route discovery

In discovery operations, these steps are completed in a standard and transparent manner. The output information is finally stored as a transaction.

II. PROPOSED METHOD

The general logic of the proposed method is discussed in this section. In packet length-based network steganography, the packet length is changed to embed the covert data. Using experience and statistical analysis of different packet lengths, it is possible to detect the presence of covert data and subsequently the presence of covert channels. In this proposal, statistical analysis is done in a specific program. The detector monitors a large set of packets for a particular application to detect possible steganographic embeddings. The proposed identification scheme focuses on the steganography of a UDP-based network. Length-based steganography embedding is more appropriate because the packet length distribution should be random.

Package length analysis

Our proposed program reads the packet length field. For each packet number, the corresponding packet length is determined. Packet length statistics are randomly distributed in UDP data. Due to this random distribution, existing analyzers cannot be used to detect the presence of covert data in packet lengths.

Simple example: calculate the 8-bit matching set for the 16-bit block 1010100100111001 and prove that there is no error.

First step: divide the 16-bit code into two 8-bit codes.

Second step: aggregate the numbers in 8-bit groups

10101001 + 00111001 = 11100010

Step 3: Calculate the ones' complement of the resulting number.

00011101

Add the result to the end of the code.

101010010011100100011101

To prove the absence of errors, divide the obtained 24-bit receiver into three 8-bit parts. Add the numbers together and calculate the one's complement of the result.

If the final result is equal to 0, it means no error occurred.

10101001 + 00111001 + 00011101 = 11111111

Ones' complement calculation is done.

00000000

The equipment used in the implementation of this scenario includes the following.

- Default analyzer program (installed on Kali Linux operating system)
- Two Cisco 2960 switches
- Two computers with Windows 7 operating system

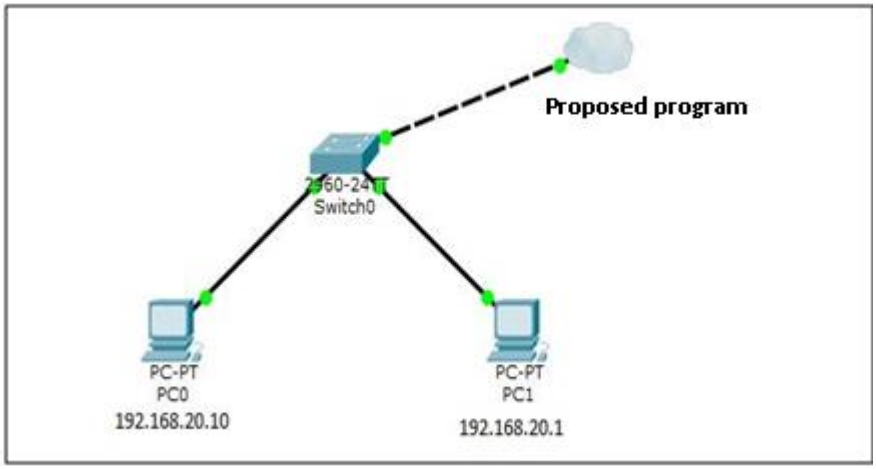

Figure 1: Network implementation scenario diagram

Steganography detection with checksum algorithms

The checksum algorithm is used to check the completeness of the information at the destination and has many applications in the network. All the data in a message are added together and the result is called a checksum. Some simple checksum algorithms include 8, 16, 32, 64-bit, CRC16, and CRC32 algorithms. The number of bits in the checksum algorithm divided by 8 is the number of bytes. If the checksum is equal to the 8-bit Checksum algorithm, the checksum is equal to 1 byte. At the same time, if the checksum is based on the 16-bit Checksum algorithm, the checksum

is equal to 2 bytes. Each bit of the file has its checksum calculated based on a standard and absolute algorithm. If in a file, the checksum is based on the 16-bit CRC algorithm, then the value of our checksum is equal to 2 bytes. This is because every 8 bits is equal to 1 byte. Checksum should be placed at which point in the program? Finding the answer requires complex mathematical calculations and reverse engineering. Access to the program source is also required.

Procedure

Suppose two parties in a network want to exchange messages. The network is always monitored by network analyzers. However, we are going to discover the hidden message on this platform. In this scenario, we want to examine the UDP protocol in the transport layer as a transmission platform and find the length of the covert message.

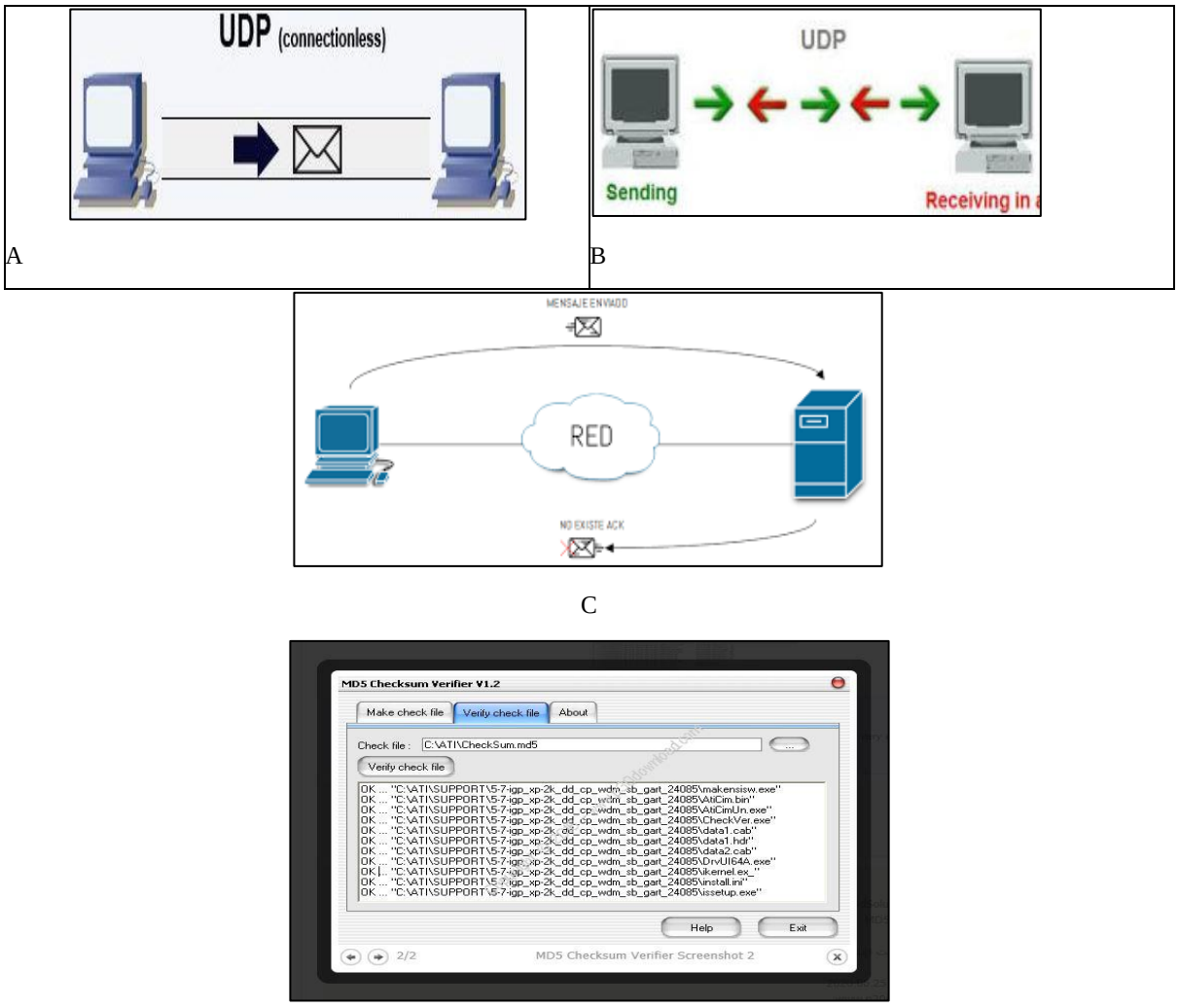

Figure 2: a) sending encrypted message b) receiving message c) comparing the length of the sent data packet with the length of the received data packet

In this research, a tool has been designed with Python programming language to create a covert channel. This software contains two sides: sender and receiver. The sender side using Scapy library functions enables the user to hide and send his secret message in a channel inconspicuously. After receiving the UDP packets, the receiving side compares the required data with the checksum. If the size of the sent data is equal to the received data, it extracts the desired data. The analysis of implementation outputs has also been realized by Python code in Scapy. The evaluation process has been done with Wireshark and MD5 Checksum Verifier. The obtained results and numbers have been converted into graphs using Python's plot function.

III.RESULTS

Checking the traffic of the entire network

First, the packet length vector (X) is calculated for normal traffic. Then, the center of mass resulting from the fixed length vector (X) and the distortion metric (∂) is also determined for normal traffic. Subsequently, the center of mass vector (COM) is also calculated from packet length (X) and distortion metric (∂) for stegano traffic. To reduce the 2D feature space, FLD is performed on dimensions. Using this reduced feature space, a classification method based on linear discriminant analysis (LDA) is trained. ROC curves are used to evaluate the performance of the proposed design. ROC is used to evaluate the classification performance. A steganographic classifier is trained using a two-dimensional feature space to distinguish between normal traffic and extreme traffic. The proposed detector can detect the presence of steganography with high accuracy.

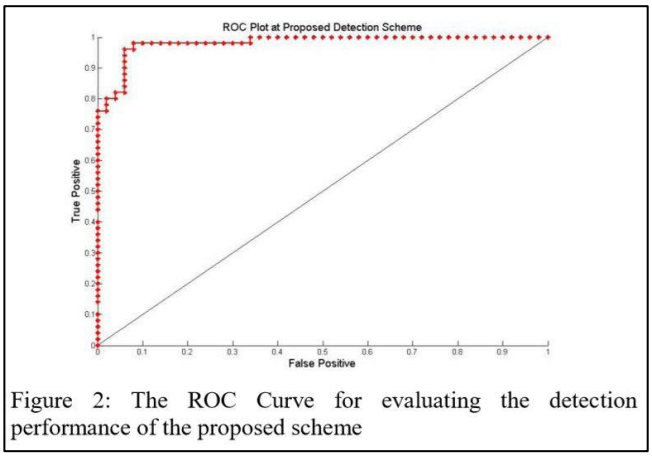

Figure 2: The ROC Curve for evaluating the detection performance of the proposed scheme

Figure 4: ROC plot

According to the results, we check the source and destination addresses of the current UDP traffic in our implementation. The packet length field value of suspicious traffic is compared with Wireshark software. If the message length of both sides is equal, the traffic is normal. Otherwise, the traffic is considered suspicious and a covert channel is declared.

Comparison of other models with the proposed model

Table 1: Comparison of different models

Model	Advantages	Disadvantages
SR	▪ Identification of electronic information based on the first computer file ▪ Comparison of at least one characteristic from the file of the second computer with the first computer ▪ Matching the resolution of the first image with the second image of the file	▪ Failure to check the value of the checksum field
LSB	▪ Packet length detection in low-value bits of signals ▪ Detection of digital signals such as images and sound ▪ Simple and fast detection algorithm	▪ Vulnerability to possible attacks

The proposed method is represented in the form of a confidential information discovery scenario using the covert channel platform based on the packet length comparison technique in the checksum field in the UDP protocol in the figures below.

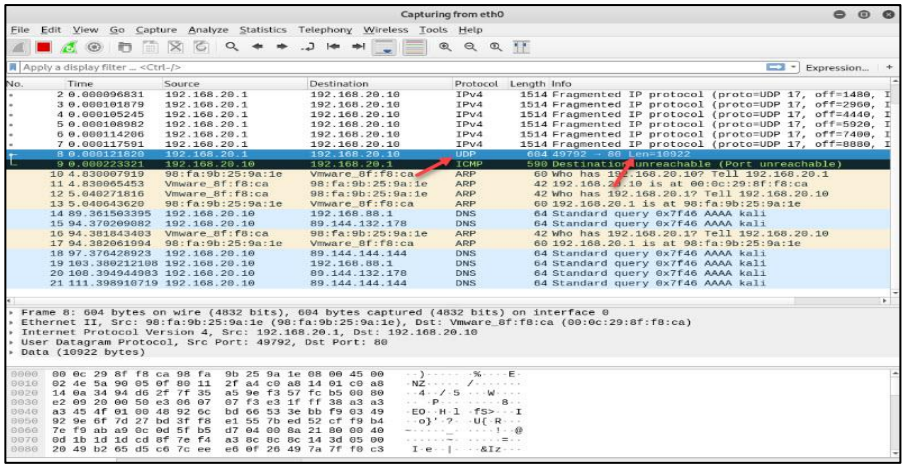

Figure 5: Data packet length comparison

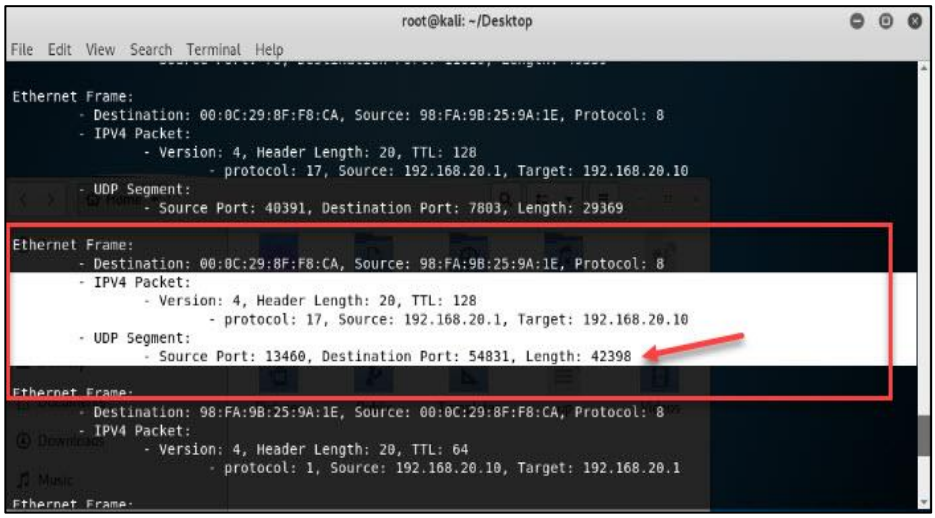

Figure 6: Data packet length comparison

We compared the results of our proposed program with the results of Wireshark network software. According to the obtained results, the covert channel can change the value of the packet length field. However, network analysis cannot detect changes in the field.

The proposed method in this study can correctly determine the value of the packet length field and alert the presence of the covert channel by checking the checksum field and calculating it accurately.

IV. Conclusion

This research has addressed the problem of discovering covert channels in the transmission layer using the advantages of packet length change detection and checksum in the UDP protocol. The superiority of the proposed method regarding the detection accuracy of covert channels was proved by operational implementation. In this research, an improved method for discovering covert channels by detecting steganography based on packet length change in UDP protocol from the transport layer is proposed. By considering the traffic between the sender and the receiver in the UDP protocol and paying attention to the traffic balance at the network level, a path is selected. Then along the way, suspicious traffic detection techniques and packet length changes are used to detect the covert channel in this protocol. The two secondary achievements of this study are: finding the covert packet length with minimum energy consumption and reducing the energy consumption in the entire network traffic in a certain period.

Our goal in the next study is to discover the exact steganographic place based on the received data. Subsequently, based on one of the methods of dealing with covert channels such as removal, the filter process is implemented. A steganographic classifier is trained using a 2D feature space to distinguish between normal traffic and extreme traffic. The proposed detector can detect the presence of steganography with high accuracy.

The following subjects are recommended for future research to develop the discovery of covert channels.

- Combining the proposed method with other checksum calculation algorithms such as the MD5 algorithm
- Apply other useful parameters to reduce network latency

Applying changes and various criteria in choosing the data transmission path and improving the discovery of covert channels concerning suspicious traffic

REFERENCES

[1] Chourib, Mehdi, detection selected network covert channels using machine learning, Hal, 2020,8

[2] Ovadya, adra, cross-router covert channels, faculty of engineering sciences, 2019,12

[3] selvi, Jose, covert channel over social networks, SANS, 2012, 28

[4] Daniel Geisler, Wojciech Mazurczyk, J¨org Keller, Towards Utilization of Covert Channels as a Green Networking Technique, 2018

[5] Hermine Hovhannisyan, Kejie Lu, Jianping Wang, A Novel High-Speed IP-Timing Covert Channel: Design and Evaluation, 2015

[6] Si-Hyeon Lee, Ligong Wang, Ashish Khisti, Member, Gregory W. Wornell, Covert Communication With Channel-State Information at the Transmitter, 2018

[7] Zerafshan Gober, z, Covert Channel Detection: A Survey Based Analysis, SEECS, 2012, 9

[8] Ahmadzadeh, S.A, Behavioral Mimicry covert communication, Electrical and computer Engineering, 2013

[9] Fahimeh Rezaei, Michael Hempel, Sushanta Mohan Rakshit, Hamid Sharif, Automated Covert Channel Modeling over a Real Network Platform, International Wireless Communications and Mobile Computing Conference (IWCMC), 2014

[10] Tianwen Huang, Lejun Zhang, Xiaoyan Hu, Xiaoying Lei, A data validation method based on IP covert channel packet ordering, 14th International Conference on Computational Intelligence and Security (CIS), 2018

[11] Antoine Lemay, Scott Knight, A timing-based covert channel for SCADA networks, International Conference on Cyber Conflict (CyCon U.S.), 2017

[12] Erik Brown, Bo Yuan, Daryl Johnson, Peter Lutz, Covert Channels in the HTTP Network Protocol: Channel Characterization and Detecting Man-in-the-Middle Attacks, jinfowar volume-9-issue-3 ,2010

[13] Igor Ruban, Nataliia Lukova-Chuiko, The mothod of hidden Terminal Transmission of network attack signatures, 2018

[14] Yu-an Tan, Xiaosong Zhang, Kashif Sharif, Chen Liang, Quanxin Zhang, and Yuanzhang Li, Covert Timing Channels for IoT over Mobile Networks, IEEE Wireless Communications • December , 2018

[15] Zhen Ling, Xinwen Fut Weijia Jia, Wei Yu§ and Dong Xuan, A Novel Packet Size Based Covert Channel Attack against Anonymizer, the Mini-Conference at IEEE INFOCOM, 2011

[16] Lei Zhao, Youtao Zhang, Jun Yang, Mitigating Shift-Based Covert-Channel Attacks in Racetrack Last Level Caches, 2017

[17] Adel El-Atawy, Qi Duan, Ehab Al-Shaer, A Novel Class of Robust Covert Channels Using Out-of-Order Packets, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING , 2015

[18] Muawia A. Elsadig, Yahia A. Fadlalla, Network Protocol Covert Channels: Countermeasures Techniques, 9th IEEE-GCC Conference and Exhibition (GCCCE), 2017

[19] Hermine Hovhannisyan, Kejie Lu, Jianping Wang, A Novel High-Speed IP-Timing Covert Channel: Design and Evaluation, IEEE International Conference on Communications (ICC), 2015

[20] TamerS.A. Fatayer, Generated Un-detectability Covert Channel Algorithm for Dynamic Secure Communication Using Encryption and Authentication, 2017 Palestinian International Conference on Information and Communication Technology

[21] Joanna Rutkowska, The Implementation of Passive Covert Channels in the Linux Kernel, December 2004

[22] A. Elsadig, Muawia, Packet Length Covert Channel: A Detection Scheme, 2018,