Journal of Theoretical and Applied Information Technology
15th December 2022. Vol.100. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

PACKET LENGTH COVERT CHANNEL DETECTION: AN ENSEMBLE MACHINE LEARNING APPROACH

Muawia. A. Elsadig[1], Ahmed Gafar[2]

[1]Assistant Professor of information security, DSR, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam, Saudi Arabia

E-mail: muawiasadig@yahoo.com

[2]Deanship of Scientific Research, Imam Abdulrahman Bin Faisal University (IAU), P.O. Box 1982, Dammam, KSA

ABSTRACT

The use of covert channel techniques has increased the capacity to carry out dangerous and undetectable attacks. Traditional security procedures cannot identify them because they utilize methods not meant to transmit information. A covert channel type that is difficult to identify, reduce the impact of, or eradicate is a packet-length covert channel. This covert channel makes use of differences in network packet lengths to send secret messages. Recent studies have emphasized the advantages of using machine learning techniques to identify covert channel attacks. As a result, this work offered an effective ensemble classification model to find these kinds of assaults. Three machine learning techniques make up the ensemble model, which serves as our model's primary classifiers. These classifiers consist of Support Vector Machine (SVM), Random Forest (RF), and Naive Bayes (NB) (SVM). The output of the proposed ensemble classifier was produced by combining the primary classifiers' outputs using the logistic regression (LR) classifier which is served as a meta classifier. Our proposed ensemble model performed well, according to the results. It surpasses all single classification algorithms by achieving a considerable accuracy rate to detect such type of covert channel attacks.

Keywords: *Covert Channels, Packet Length Covert Channels, Network Attacks, Machine Learning, Ensemble Classification, Deep Learning, Stacking Technique.*

1. INTRODUCTION

A covert channel is a channel that secretly conveys confidential data in a manner that breaches system security policy [1, 2]. This illegal flow of data was initially presented by Lampson in 1973 [3]. It uses channels that are not dedicated to convey information at all [4]. In 1987, this concept was expanded to exploit computer networks [5]. In networks, covert channels are methods used to hide information in the normal network traffic so as to remain undetected [6]. Computer networks have become a rich environment to construct different types of covert channels [7, 8]. Additionally, even the most recent technologies in this area do not adequately consider the vulnerabilities, that can be exploited to construct covert channels, throughout the designing phases of these technologies [2]. Readers interested in learning more about covert channels that exploit the new generation protocol, IPV6 are directed to [9-12].

In [13], the authors introduced a number of elements that are crucial to the growth of network covert channel attacks. These include (i) the advanced development of network technologies, which provide a rich environment for the introduction of various covert channel techniques, (ii) switching techniques that enable a covert message to change its storage location from one field to another in a given protocol or to another field in a different protocol, which makes it more difficult to detect such attacks, and (iii) internal control protocol techniques that make use of micro protocol approaches to secure reliable communication and dynamic route for covert traffic.

One of the common methods for concealing secret messages is to employ covert channels that use the length of data packets as the carrier. In which a secret data is sent to the intended recipient by taking advantage of the difference in data packet lengths. There are numerous methods in the literature for using network packet lengths to create various forms of this attack. Unfortunately, even if encryption techniques are used, this kind of attack could still occur.

Packet length covert can be applied to different protocols such as IPv6 datagrams. No one detection method can discover all packet length covert channel techniques, therefore, developing some high-level indicators can serve as a foundation for designing universal detectors, for instance by utilizing widely used machine learning classification approaches or frameworks that capable to discover statistical anomalies [14].

VoIP traffic, which contains continuous transmission of a significant amount of data, is an enriching environment that attracts the developing of different types of packet-length covert channels. Particularly mobile VoIP, which is increasingly used for sending big volumes of data, is a viable target for creating covert channels with high throughput.

Eventually, it becomes evident that new methods for creating covert channel attacks are constantly being developed. Additionally, covert communication can be used for a variety of malicious activities, posing significant dangers to our data and confidentiality. Therefore, additional effort is needed to develop suitable defenses against such attacks.

This study developed an ensemble classification model for packet-length covert channel detection. It is a machine learning model based on the stacking technique, which combines the outputs of some classifiers to produce superior outcomes that lead to more accurate results.

In this model, three classifiers serve as the base classifiers, while the LR classifier serves as the meta-classifier to aggregate the output of the base classifiers.

This Section gave readers a quick introduction to covert channels and an explanation of its basic notion with a focus on packet-length-based covert channels. The most common types of covert channels were identified in the following Section. Then, relevant work is provided in Section 3 where the most recent developments in packet length covert channel techniques and their countermeasures were covered. Section 4 provides a description of the suggested ensemble model. It gives a detailed explanation of the procedures used to build and validate the suggested model. The results are discussed in Section 5, and the study is wrapped up in Section 6.

2. COVERT CHANNEL TYPES

The two main categories of covert channels are storage covert channels (SCC) and timing covert channels (TCT) [15, 16]. In SCC, the covert message is written in a storage location [17], e.g., header and payload fields, while in TCT, the timing aspects of the network traffic are used to modulate a covert message [18, 19]. To put it another way, SCCs deliver covert messages using objects, but TCTs abstract the statistical characteristics of the time-domain into symbols to send a message [20].

A third category of covert channels known as a hybrid covert channel, which poses a significant challenge, can be created by integrating both timing and storage techniques. It offers the advantages of both TCT and SCC.

3. RELATED WORK

Covert channels are undetectable by conventional intrusion detection techniques. This motivated attackers to exploit them to convey secret data. Constructing network covert channels to leak information has become a common practice today and presents significant security challenges. Packet length covert channel is a type of network covert channels that take advantage of packet length variations to pass secret messages. It may be more challenging because some of these channels produce covert traffic that closely resembles normal traffic. As a result, detection techniques that look for differences between normal and covert traffic may miss these channels.

3.1 Packet-length covert channels overview

Padlipsky and Girling were the first to put up the idea of Packet length covert channels, which take advantage of the changes in network packet lengths to transmit secret messages in 1978 and 1987, respectively [21]. On the basis of this, various techniques have been developed.

In the covert channel techniques presented in [22, 23], the sending and receiving sides should exchange certain rules before beginning their transmission phase. In these channels, it is straightforward to determine whether such channels exist because the detection techniques can easily pick up differences between covert and overt traffic. Therefore, these methods are susceptible to being discovered.

Yao et al. [24]. presented a covert channel that takes advantage of network packet length variations. Before beginning their communication

session, the sender and receiver that want to initiate covert communication should share a matrix of unique packet lengths. However, this covert channel is subject to be discovered [25], [5].

Ji et al. in [25] presented a packet length covert channel approach. The authors of this covert channel claimed that detection techniques are unable to detect their proposed channel because it can carry normal network traffic. But the authors of [26] suggested a detection approach that can recognize their proposed covert channel.

Ji et al. [27] developed a packet length covert channel with claim that their approach offers strong defences against detection techniques. Nevertheless, this kind of covert channel is susceptible to being discovered due to the static nature of its reference list [28].

A covert channel that offers a high capacity for covert messages was proposed by Hussain et al. [29] The data payload and packet lengths are exploited to initiate this covert channel. However, due to the utilization of the data payload, the construction of this form of covert channel is complicated [30] and it may be susceptible to detection.[31].

Based on network packet lengths, the authors of [32] proposed a covert channel. Each network packet allows transmission of one bit of a covert message. Despite having a small bandwidth, this covert channel is very hard to identify and doesn't require the exchange of a shared key to initiate a covert communication session [33].

Two new methods that are anticipated to be more resistant to detection techniques were introduced by Sabeti et al. [33]. Both methods have been developed in which each pair of lengths is utilized to insert one bit of a covert message. When the first length is less than the second, this indicates a "0" bit, while the reverse case suggests a "1" bit. It may be required to swap packets to form the intended covert message. One of these methods allows for the free selection of paired packets, whereas the other groups packets into buckets so that paired packets selection is limited to a single bucket. According to the authors, the method that divides packets into buckets is more secure than the other method; however, it has a limited capacity. The main drawback is that the two proposed methods do not work when network packet lengths are constant. Additionally, the first approach is susceptible to detection since packet swapping might result in anomalies that enable the channel to be discovered.[34].

A packet-length covert channel over mobile VoIP was proposed by Liang et al. [35]. According to the authors, the throughput, reliability and undetectability of their scheme were assessed, and the experiments showed the potential of their suggested scheme. However, the Authors acknowledged some restrictions, such as the fact that the covert communication would be broken if an adversary be able to decrypt the packet content and retrieve the packets in their original order.

3.2. Detection and elimination

The authors in [36] offered two approaches to resolve packet length covert channels based on traffic normalization techniques. Their approach relies on using padding and splitting techniques to make all packet lengths equal in size. However, this approach causes considerable overhead, which will have an impact on network performance. This overhead associated with the process of measuring each packet's size and then using padding or splitting techniques. As a result, the proposed solution requires more improvements to assure its effectiveness in terms of network performance.

In general, packet length covert channel can be avoided by having all packets have the same length (the maximum length), however this technique reduces network capacity [37] and is therefore not thought to be a sufficient solution. In contrast, a popular topic in network security is the use of machine learning techniques to thwart different security attacks including covert channel attacks. In this context, the rest of this sub section is dedicated to review some machine learning approaches that used ensemble techniques to detect covert channel attacks.

Any machine learning classifier has advantages and drawbacks; therefore, ensemble approaches can produce superior results by combining several classifiers in a way that maximizes their achievements and minimizes their drawbacks [38]. Stacking is an ensemble method in which a metaclassifier is trained to combine individual classifiers [38] to improve the prediction accuracy [39]. It is a technique to generate strong model with less biased compared to its base classifiers.

To detect a DNS covert channel, the authors of [40] proposed a detection approach based on stacking techniques. In comparison to other methods, their model performed exceptionally well, as the authors stated.

A detection model based on stacking technique, an aggregation technique that combines weak learners to create a more potent classifier, was proposed by Yang et al. [41] K nearest neighbors (KNN), SVM, and RF serve as the model's base classifiers, while a neural network classifier serves as the model's meta classifier. Their model is intended to discover DNS covert channels. It performs well compared to some existing models.

The authors in [42] proposed an ensemble classification approach based on the stacking technique. In the proposed approach, KNN, LR, SVM, and NB are served as the base classifiers, whereas RF is served as a meta-classifier. The proposed approach performed better compared to other approaches and taking reasonable processing time. The authors highlighted that, under performance and cost restrictions, stacking ensemble classifiers can be used as a cost-effective alternative to deep learning approaches.

Based on the analysis of pertinent work about these attacks that discussed above, the authors are motivated to suggest a detection model based on stacking approach to identify covert channels that exploit packet length variation to convey secret messages.

4. THE PROPOSED METHOD

This study provides an ensemble classification method for a covert channel assault that exploits network packet lengths to establish an unauthorized flow of secret information in violation of security regulations. In order to convey a "0" bit of the secret message, the technique of this attack adjusts the length of a packet to an odd value, and to an even value to convey a "1" bit of the secret message, or vice versa. This indicates that an attacker alters the length of network packets in accordance with the covert message they wish to exchange. The intended recipient keeps track of the data lengths received in order to decode the modulated message.

4.1. Dataset

According to the description of our target covert channel given above, a dataset has been constructed. Software called Wireshark was used to record Skype network traffic. Two parts of the captured traffic were separated. One part was left intact to symbolize typical traffic (normal traffic) whereas the other part was altered using the Python language's Scapy tool to create malicious traffic (covert traffic). Consequently, a dataset with 200 cases was created. There are 100 instances of normal traffic and 100 instances of covert traffic.

4.2. The Ensemble Classifier Model

In order to increase prediction accuracy, the suggested ensample technique employs a stacking mechanism to aggregate the results of a number of classifiers. It is well known that compared to single classification models, ensemble classifiers have a greater accuracy rate. Our ensemble approach's base classifiers were carefully chosen based on their track record of accurately reflecting performance. These classifiers include Support Vector Machine (SVM), Naive Bayes (NB), and Random Forest (RF). The outputs of the base classifiers are aggregated using the Logistic Regression (LR) classifier which serves as a meta classifier of our proposed ensemble model.

4.3. Experiments & Evaluation

Using our developed dataset, which contains 200 instances of covert and overt traffic, the base classifiers of our suggested ensemble technique were fully trained and tested. The ensemble technique was created by combining the output of the aforementioned classifiers using the RF classifier. A cross-validation technique was used to evaluate the effectiveness of the suggested model. It is a sampling technique that applies various portions of the provided dataset to the training and testing of a machine learning model across various iterations. It is a technique for resampling used to assess machine learning models [43]. Readers who are interested in learning more about cross-validation techniques are directed to [44].

In our experiment, 80% of the dataset was used for training and the remaining 20% for testing. the 5-fold cross-validation method was applied in which the dataset is split into five sections (folds). The model is then five times trained and tested. Each time the model is tested, a different fold is employed, and the remaining dataset is used to train the model. The training and testing data are altered repeatedly, resulting in a more thorough validation.

By producing the error matrix (confusion matrix), which shows the proportion of instances that are successfully classified versus the instances that are misclassified, the performance of our suggested ensemble technique compared to individual classifiers was investigated.

Other evaluation metrics were also calculated, including classification accuracy,

sensitivity, precision, and specificity, which were determined using the relevant equations (1), (2), (3), and (4).

Accuracy = (TP +TN)/(FN+FP+TP+TN). (1)
Sensitivity = TP / (TP+FN). (2)
Precision = TP / (FP +TP). (3)
Specificity = TN / (TN +FP). (4)

Where:

TP: true positive, refers to the covert cases are correctly classified.

TN: true negative, refers to the legitimate cases are correctly classified.

FP: false positive, refers to the legitimate cases are incorrectly classified.

FN: false negative, refers to the covert cases are incorrectly classified.

Table 1: Classifiers performance

Classifier	Classifier's performance measures			
	Specificity	Sensitivity	Precision	Accuracy
RF	94.1%	96%	92.3%	94%
SVM	96.6%	99%	94.3%	96.5%
Naïve Bayes	98%	99%	97.1%	98%
The proposed ensemble Classifier (stack)	98.5%	99%	98%	98.5%

5. RESULTS AND DISCUSSIONS

The reported results, as shown in table 1, showed that our ensemble model, which was proposed by this work, had achieved high level of accuracy compared to other single classifiers that made up the model. It outperformed them all by identifying packet length-based covert channels with a detection accuracy rating of 98.5%. Furthermore, the ensemble classifier demonstrated strong performance in terms of specificity, accuracy, and recall, which are metrics frequently used to assess the effectiveness of binary classifiers. High values for these metrics were obtained. These findings support our hypothesis that our ensemble classifier can increase classification accuracy. To visualize our findings as a graph, Figure 1 compared the classification accuracy of all classifiers, including the suggested ensemble classifier. In terms of classification errors, table 2 showed the classification errors that computed by applying the confusion matrix. The suggested classifier clearly beats all other classifiers, reaching exceptional performance with the fewest classification errors, followed by NB and SVM, although RF lagged behind by producing more errors than the others. Further evaluation was done by obtaining the Receiver Operator Characteristic (ROC) Curves. Figures 2, 3, 4, and 5 depict the ROC curves for the proposed classifier, NB, SVM and RF respectively, while Figure 6 displays the ROC curves for all classifiers. The proposed classifier demonstrated superior performance than all other classifiers, as seen by the ROC curves, edging out all of them.

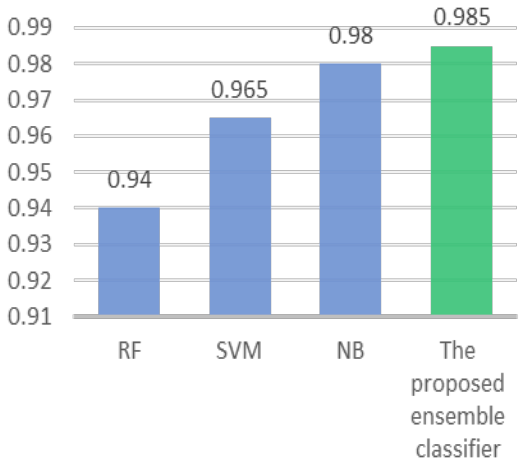

Figure 1: Accuracy of the Classifiers

Table 2: Classification errors

Classifier	Classification errors

	False Positive FP	False Negative FN
RF	0.08	0.04
SVM	0.06	0.01
Naïve Bayes	0.03	0.01
The proposed ensemble Classified (stack)	0.02	0.01

Eventually, our proposed model has improved the detection accuracy of packet length covert channel, as shown by the experiments that were conducted and the evaluation tools used. In comparison to other classifiers, it attained the high accuracy with the fewest classification mistakes. To our knowledge, the proposed classifier has outperformed every detection strategy now in use to thwart this kind of assault.

It's important to note that while NB and SVM classifiers are able to obtain decent classification accuracy, our proposed model still surpasses them.

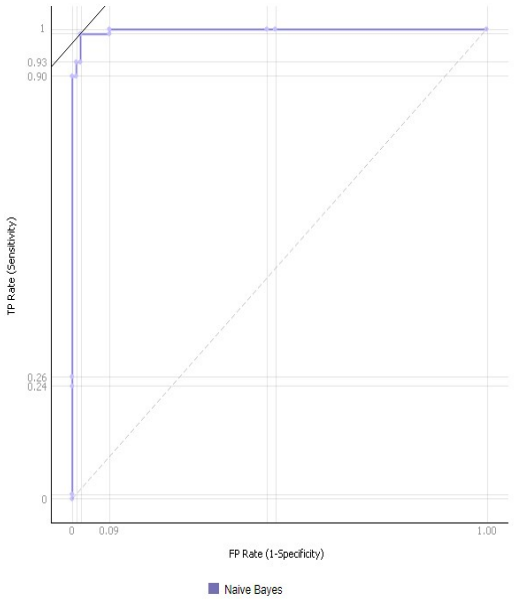

Figure 3: ROC curve for the NB classifier

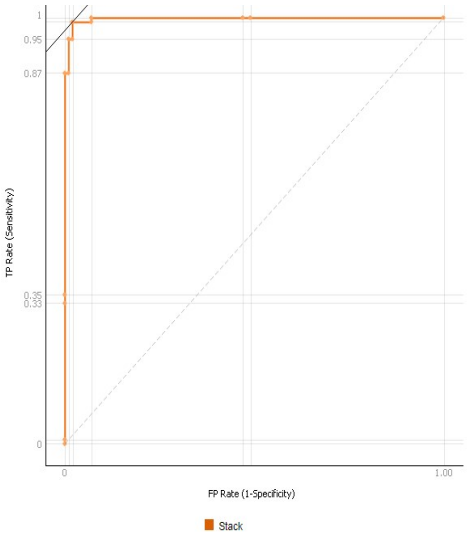

Figure 2: ROC curve for the proposed classifier (stack).

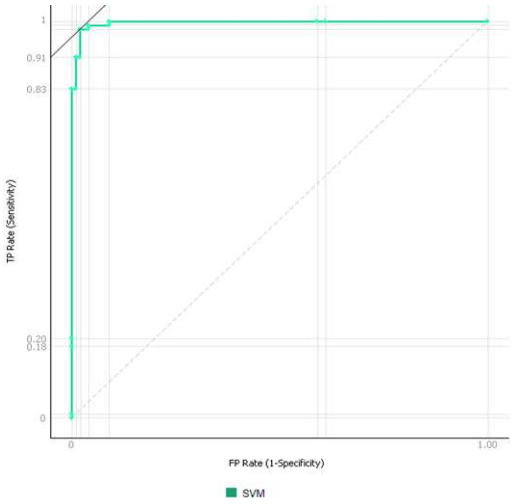

Figure 4: ROC curve for the SVM classifier

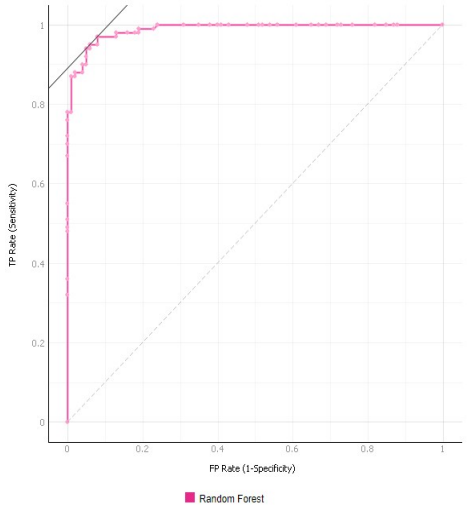

Figure 5: ROC curve for the RF classifier

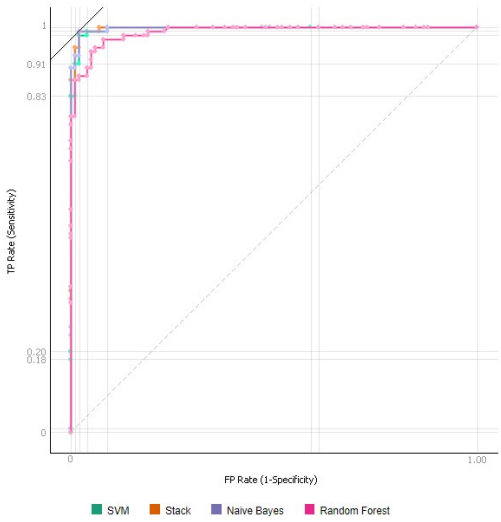

Figure 6: ROC curve for all classifiers

6. CONCLUSION

In several domains, including information security, machine learning technology has demonstrated its value. Numerous machine learning techniques have been used with impressive results to find malicious activity.

An ensemble classification model was developed in this study to identify covert channels that use data packet lengths to pass covert messages. This type of covert channels sends secret messages by taking advantage of differences in network packet lengths. It is a dangerous and undetected assault that can produce malicious traffic (covert traffic), which frequently resembles legitimate traffic (overt traffic), making it impossible for detection methods to detect the changes.

The proposed ensemble mode is composed of three machine learning methods: Support Vector Machine (SVM), Random Forest (RF), and Naive Bayes (NB) which are considered the base classifiers. Whereas, the logistic regression (LR) classifier is used to merge the results of these classifiers. It acts as a meta classifier of our proposed model.

When compared to single classification models, the proposed ensemble detection model performed superbly, its detection accuracy was 98.5%.

As far as we know, the proposed ensemble model has surpassed all currently available detection approaches that were provided to contour this sort of covert channels in terms of classification accuracy rate.

ACKNOWLEDGMENT

The authors are grateful that this research was supported by the IAU Deanship of Scientific Research under grant number 2019342-DSR.

REFRENCES:

[1] F. Iglesias, F. Meghdouri, R. Annessi, and T. Zseby, "CCgen: Injecting Covert Channels into Network Traffic," *Security and Communication Networks,* vol. 2022, 2022.

[2] M. A. Elsadig and A. Gafar, "Covert Channel Detection: Machine Learning Approaches," *IEEE Access,* vol. 10, pp. 38391-38405, 2022.

[3] B. W. Lampson, "A note on the confinement problem," *Communications of the ACM,* vol. 16, no. 10, pp. 613-615, 1973.

[4] C. Heinz, M. Zuppelli, and L. Caviglione, "Covert Channels in Transport Layer Security: Performance and Security Assessment."

[5] M. A. Elsadig, "Resolving Network Packet Length Covert Channels," Ph.D. dissertation, Computer Science and Technology, Sudan University of Science & Technology, Sudan, 2018.

[6] J. Hielscher, K. Lamshöft, C. Krätzer, and J. Dittmann, "A Systematic Analysis of Covert Channels in the Network Time Protocol," 2021, pp. 1-11.
[7] M. A. Elsadig and Y. A. Fadlalla, "Network Protocol Covert Channels: Countermeasures Techniques," 2017: IEEE, pp. 1-9.
[8] M. A. Elsadig and Y. A. Fadlalla, "Survey on Covert Storage Channel in Computer Network Protocols: Detection and Mitigation Techniques," *International Journal of Advances in Computer Networks and Its Security,* vol. 6, no. 3, pp. 11-17, 2016.
[9] L. Caviglione, A. Schaffhauser, M. Zuppelli, and W. Mazurczyk, "IPv6CC: IPv6 covert channels for testing networks against stegomalware and data exfiltration," *SoftwareX,* vol. 17, p. 100975, 2022.
[10] B. Blumbergs, M. Pihelgas, M. Kont, O. Maennel, and R. Vaarandi, "Creating and detecting IPv6 transition mechanism-based information exfiltration covert channels," 2016: Springer, pp. 85-100.
[11] A. Salih, X. Ma, and E. Peytchev, "Implementation of Hybrid Artificial Intelligence Technique to Detect Covert Channels Attack in New Generation Internet Protocol IPv6," in *Leadership, Innovation and Entrepreneurship as Driving Forces of the Global Economy*, Cham, R. Benlamri and M. Sparer, Eds., 2017// 2017: Springer International Publishing, pp. 173-190.
[12] P. Bedi and A. Dua, "Network Steganography Using Extension Headers in IPv6," 2020: Springer, pp. 98-110.
[13] A. Epishkina and K. Kogos, "A Traffic Padding to Limit Packet Size Covert Channels," in *Future Internet of Things and Cloud (FiCloud), 2015 3rd International Conference on*, 24-26 Aug. 2015 2015, pp. 519-525, doi: 10.1109/FiCloud.2015.20.
[14] L. Caviglione, "Trends and Challenges in Network Covert Channels Countermeasures," *Applied Sciences,* vol. 11, no. 4, p. 1641, 2021.
[15] M. A. Elsadig and Y. A. Fadlalla, "An Efficient Approach to Resolve Covert Channels," *IJ Network Security,* vol. 20, no. 5, pp. 898-906, 2018.
[16] M. Nasseralfoghara and H. R. Hamidi, "Covert timing channels: analyzing WEB traffic," *Journal of Computer Virology and Hacking Techniques,* pp. 1-10, 2021.
[17] M. A. Elsadig and Y. A. Fadlalla, "A balanced approach to eliminate packet length-based covert channels," in *2017 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS)*, Nov. 29 2017-Dec. 1 2017 2017, pp. 1-7, doi: 10.1109/ICETAS.2017.8277839.
[18] A. K. Koundinya and G. H. Satyanarayana, "A typical analysis of hybrid covert channel using constructive entropy analytics," *International Journal of Electrical & Computer Engineering (2088-8708),* vol. 12, no. 4, 2022.
[19] L. Jin, Z. Liu, F. Huang, Z. Lin, and M. Li, "Covert Channel Construction Method Based on HTTP Composite Protocols," *Journal of Electrical and Computer Engineering,* vol. 2022, 2022.
[20] Z. Tang, J. Wang, H. Li, J. Zhang, and J. Wang, "Cognitive Covert Traffic Synthesis Method Based on Generative Adversarial Network," *Wireless Communications and Mobile Computing,* vol. 2021, 2021.
[21] A. Epishkina and K. Kogos, "Covert Channels Parameters Evaluation Using the Information Theory Statements," in *IT Convergence and Security (ICITCS), 2015 5th International Conference on*, 24-27 Aug. 2015 2015, pp. 1-5, doi: 10.1109/ICITCS.2015.7292966.
[22] C. G. Girling, "Covert Channels in LAN's," *IEEE Transactions on software engineering,* vol. 13, no. 2, p. 292, 1987.
[23] M. A. Padlipsky, D. W. Snow, and P. A. Karger, "Limitations of end-to-end encryption in secure computer networks: Technical report ESD-TR-78-158," *Massachusetts: The MITRE Corporation,* 1978.
[24] Q.-z. YAO and P. ZHANG, "Coverting channel based on packet length," *Computer engineering,* vol. 34, no. 3, pp. 183-185, 2008.
[25] L. Ji, W. Jiang, B. Dai, and X. Niu, "A novel covert channel based on length of messages," in *2009 International Symposium on Information Engineering and Electronic Commerce*, 2009: IEEE, pp. 551-554.
[26] A. S. Nair, A. Sur, and S. Nandi, "Detection of Packet Length Based Network Steganography," in *2010 International Conference on Multimedia Information Networking and Security*, 4-6 Nov. 2010 2010, pp. 574-578, doi: 10.1109/MINES.2010.126.

[27] L. Ji, H. Liang, Y. Song, and X. Niu, "A normal-traffic network covert channel," in *Computational Intelligence and Security, 2009. CIS'09. International Conference on*, 2009, vol. 1: IEEE, pp. 499-503.
[28] K. U. Sharma and A. U. Sharma, "High Bandwidth Covert Channel using TCP-IP Packet Header." In : International Conference on Electronics and Communication Systems (ICECS), Feb 2016.
[29] M. Hussain and M. Hussain, "A high bandwidth covert channel in network protocol," in *Information and Communication Technologies (ICICT), 2011 International Conference on*, 2011: IEEE, pp. 1-6.
[30] M. A. Elsadig and Y. A. Fadlalla, "Packet Length Covert Channels Crashed." J Comput Sci Comput Math, 2018, 8.4: 55-62, doi: 10.20967/jcscm.2018.04.001.
[31] M. A. Elsadig and Y. A. Fadlalla, "Packet Length Covert Channel: A Detection Scheme," 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), 2018, pp. 1-7, doi: 10.1109/CAIS.2018.8442026.
[32] O. I. Abdullaziz, V. T. Goh, H. C. Ling, and K. Wong, "Network packet payload parity based steganography," in *2013 IEEE Conference on Sustainable Utilization and Development in Engineering and Technology (CSUDET)*, May 30 2013-June 1 2013 2013, pp. 56-59, doi: 10.1109/csudet.2013.6670985.
[33] V. Sabeti and M. Shoaei, "New High Secure Network Steganography Method Based on Packet Length," *The ISC International Journal of Information Security,* vol. 12, no. 1, pp. 24-44, 2020.
[34] Okello, M. O, "Optimal Covert Communication Techniques," International Journal of Informatics and Applied Mathematics , 5 (1) , 1-26, 2022. doi: 10.53508/ijiam.1073205.
[35] C. Liang, Y.-a. Tan, X. Zhang, X. Wang, J. Zheng, and Q. Zhang, "Building packet length covert channel over mobile VoIP traffics," *Journal of Network and Computer Applications,* vol. 118, pp. 144-153, 2018.
[36] D. Frolova, K. Kogos, and A. Epishkina, "Traffic Normalization for Covert Channel Protecting," 2021: IEEE, pp. 2330-2333.
[37] A. Epishkina, K. Kogos, and D. Frolova, "A Technique to Limit Hybrid Covert Channel Capacity via Random Increasing of Packets' Lengths," *Procedia Computer Science,* vol. 190, pp. 231-240, 2021.
[38] M. A. Bertoni, G. H. d. Rosa, and J. R. F. Brega, "Optimum-path forest stacking-based ensemble for intrusion detection," *Evolutionary Intelligence,* pp. 1-18, 2021.
[39] M. A. Elsadig, "Ensemble Classifier for Breast Cancer Detection," *Journal of Theoretical and Applied Information Technology,* vol. 100, no. 10, 2022.
[40] P. Yang, X. Wan, G. Shi, H. Qu, J. Li, and L. Yang, "Naruto: DNS covert channels detection based on stacking model," 2020, pp. 109-115.
[41] P. Yang, X. Wan, G. Shi, H. Qu, J. Li, and L. Yang, "Identification of DNS Covert Channel Based on Stacking Method.", International Journal of Computer and Communication Engineering, vol. 10, no. 2, pp. 37-51, 2021, doi: 10.17706/ijcce.2021.10.2.37-51.
[42] H. Li, Y. Jin, J. Zhong, and R. Zhao, "A Fruit Tree Disease Diagnosis Model Based on Stacking Ensemble Learning," *Complexity,* vol. 2021, 2021.
[43] R. Wazirali, "An improved intrusion detection system based on KNN Hyperparameter tuning and cross-validation," *Arabian Journal for Science and Engineering,* vol. 45, no. 12, pp. 10859-10873, 2020.
[44] M. W. Browne, "Cross-validation methods," Journal of mathematical psychology, vol. 44, no. 1, pp. 108-132, 2000, doi: 10.1006/jmps.1999.1279.