2023 3rd International Conference on Emerging Smart Technologies and Applications (eSmarTA) | 979-8-3503-0533-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/ESMARTA59349.2023.10293582

Covert Channel Detection and Generation Techniques: A Survey

Nesmah A. AL-Khulaidi
(Member ,IEEE)
Department of Computer Networks
Yemen Academy for Graduate Studies
Sana'a, Yemen
nesmaalkhulaidi88@ieee.org

Ammar T. Zahary
(Senior Member, IEEE)
Department of Computer Science, Faculty of Computing and IT
University of Science and Technology
Sana'a, Yemen
a.zahary@ust.edu.ye

Muneer A.S Hazaa
(Member, IEEE)
Department of Computer Science, Faculty of Computer and Information System
Thamar University
Thamar, Yemen
muneer_hazaa@yahoo.com

Adel A. Nasser
Department of Information Systems and Computer Science, Faculty of Sciences
Sa'adah University
Sa'adah, Yemen
adel@saada-uni.edu.ye

***Abstract*— The use of covert communications has become more widespread recently as a solution to the information security issue. Information security can be partially solved by the discovery and creation of covert routes. Covert channel use is still in its early phases, even though information security concerns are growing as a result of quick technology advancements. As a result, several problems and concerns need to be resolved, and the future plan is foggy. This paper seeks to give a thorough comparison of earlier and more recent attempts in this field. It offers a survey of the literature on the drawbacks and gaps in conventional detection techniques, emphasizing the most recent techniques for discovering and creating these covert channels while carefully considering machine learning and deep learning-based detection techniques. Additionally, it broadens the topic to cover the crucial function that these channels play in technology.**

Timing channels, storage channels, and hybrid channels are just a few of the ways covert channels may be utilized to transfer data. They can be used to get around security measures like intrusion detection systems and firewalls. Additionally, they may be used to steal confidential data from a system, including passwords, credit card numbers, and intellectual property. System security is seriously threatened by covert channels, and more study on covert channel production and detection is required to stay up with the changing threat environment.

Keywords—: covert communication, covert channel detection techniques, covert channel generation techniques.

I. INTRODUCTION

Covert channels are a serious threat to network security. They are channels that allow data to be transmitted in a way that is not explicitly allowed by the system [1],[2]. This can be done by exploiting subtle changes in system behavior or by using unconventional methods of communication. Covert channels were first described by B.W. Lampson in 1973[1]. Lampson defined covert channels as "channels not designed for information exchange." This means that covert channels are ways of transmitting data that are not explicitly allowed by the system. For example, a covert channel could be used to transmit data by changing the timing of system events or by modifying the frequency of network traffic Girling established the architecture of covert channels in LAN protocols in 1987[2].

These channels are difficult to detect because they are designed to be hidden [9],[10],[15]. They often use subtle changes in system behavior that are difficult to detect with traditional security tools. Additionally, covert channels can be used to transmit data very slowly, making them difficult to detect even with sophisticated tools.

The relevance of covert channels is growing as a result of technological advancements and the threat posed by hackers [3] As systems become more complex, it becomes easier for hackers to hide covert channels. Additionally, hackers are constantly developing new techniques for using covert channels to exfiltrate sensitive information [4],[5]. As a result of these challenges, there is a growing need for new methods for detecting and preventing covert channels. Researchers are working on a variety of approaches [6], including statistical anomaly detection, traffic analysis, and protocol analysis. However, there is no single silver bullet for detecting covert channels. It is important to use a combination of techniques to provide comprehensive protection [7].

The purpose of this study is to introduce both traditional and contemporary covert channel generation and detection approaches. This is an important contribution to the field of information security, as it will help researchers to develop more effective methods for detecting and preventing covert channels and will open the field for new research directions.

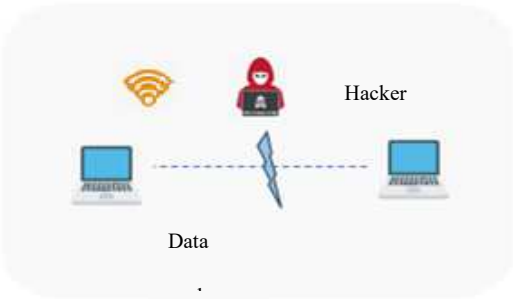

Fig. 1. Stealing information via covert channel

979-8-3503-0533-3/23/$31.00 ©2023 IEEE

This section provides a brief historical overview of covert communication and the effects of covert channels on security, which is thought to spur scholars to go further and learn about various methods of generation and detection. Section II provides multiple covert channel generation approaches due to their rule of conveying data covertly. Section III presents the many methods for detecting these channels, including the traditional and current techniques, and shows how hackers might play a negative role when dealing with covert channels. Section IV then discusses detection and generation methods and broadens the study to examine how covert channels may impact developing technology. While section V introduces a comparative analysis of the literature. VI discusses the limitations and trends, VII addresses contribution and future directions, then the paper is concluded in section VIII.

II. Generation

It is important to note that covert communication has two uses: it may be utilized to communicate private information or it can be used by hackers to steal the information and compromise security measures [9]. As a result, the study is split into two categories: first, studies to detect these hidden channels, which will be addressed later; and second, studies to find ways to improve them. Key technologies for building covert network channels are divided into two categories in [8]: communication content level (based on information steganography) and transmission network level (based on proxy and anonymous communication technology). [10] concentrated on the creation of hidden channels in Pcap files.

Owing to their superior strength, hidden channels are extremely important in network communication concerning timing. Based on the shared on-chip interconnect channels, [11] demonstrated how to construct a timed hidden channel for GPUs. In [12], HTTP-based covert channels were built, while in [13], a covert channel was built by modifying the packet order to produce the required pattern. Given how important the packet dropout covert channel is to safely transmit information, this affects packet length-based CTC.

III. Detection

The rapid advancement of technology and the threat posed by hackers as a result of information leaks caused by these covert channels prompted researchers to search for more sophisticated methods of covert channel identification. Traditional and contemporary detection methods are contrasted and briefly discussed in this section.

Figure 2 explains the discussion of covert channels in this paper.

IV. Overview of Covert Channel Detection Techniques

The methods a covert channel employs for sending illicit data make it difficult to detect. However, as will be detailed below, researchers have improved detection methods over time.

A. Classical Approaches

In [26], a detection scheme was introduced to detect covert channels with high noise levels using clustering and detection algorithms, while in [25], a detection technique was proposed by analyzing the behavior of TCP flows using a Markov model. There was also an attempt [24] to detect covert channels in wireless local area networks (WLAN) because the devices transmit data usable by the covert channels.

To find the differences between covert and overt traffic, a probability-based model [23] was developed, which proved to be more successful than the approaches currently in use. Replay confusion is a detection method described in this work [22] that employed straightforward hardware to find cache-based hidden channels.

B. Modern Approaches

Wireless covert channel detection is a serious issue since it takes into account a temporal covert channel that hides the information in the intervals between the packets. According to [17], [18], a correlation-based detection strategy is utilized to find such channels.

Hackers can conceal information in the packet delays of covert channels, making it more difficult to detect. [21] provided a method for identifying such channels based on multidimensional characteristics. These time intervals may also be translated into time symbols [15], and the transition time can then be counted to identify hidden channels. Various forms of hidden network timing channels can be found using different detection methods [19] based on a secret threshold.

On the other hand, a covert channel built into TCP/IP poses a danger to information security because attackers can readily steal data by creating one [20]. Because IPv6 is known for being able to endure IPv4's limitations, hackers frequently use it to set up covert channels, making it difficult for researchers to identify them; therefore, a code augmentation feature to find the hidden channel in the IPv6 flow label found in [14],[16].

Table I demonstrates how various covert channel detection techniques are divided into classical and current categories.

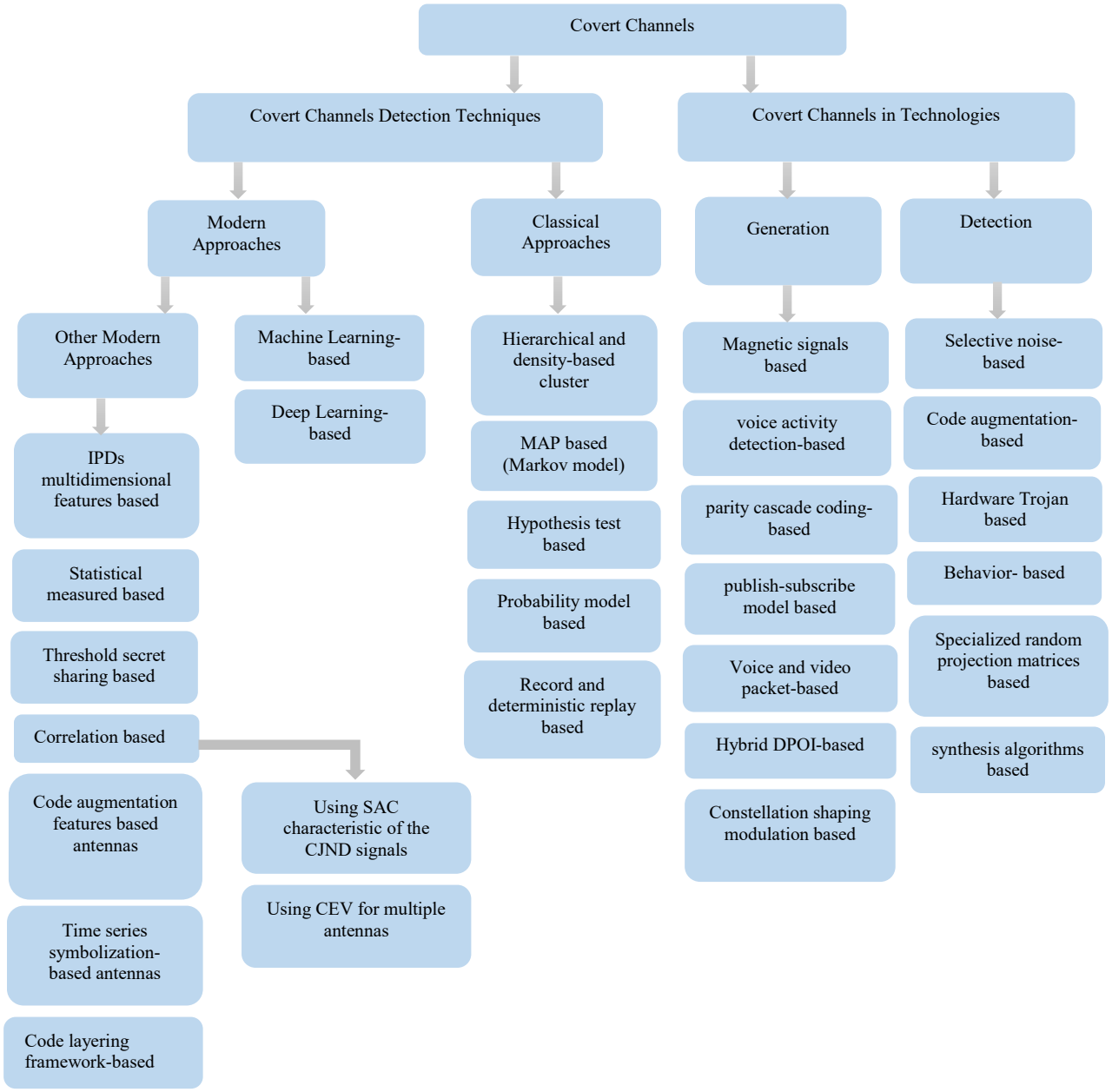

Fig. 2. Different generation and detection techniques

TABLE I. Modern and Classical Detection Techniques

Ref.	Approach	CTC	CSC	Classic	Modern	Year
[14]	Code layering framework-based.	√	√		√	2022
[15]	Time series symbolization based.	√			√	2021
[16]	Code augmentation features based.		√		√	2021
[17]	Correlation based (using the constellation error vectors (CEV) for multiple antennas).	√			√	2021
[18]	Correlation based (using SAC characteristic of a Joint Normal Distribution (CJND) signals).	√			√	2020
[19]	Threshold secret sharing based.	√			√	2020
[20]	Statistical measured based.		√		√	2020
[21]	Inter Packet Delays (IPDs) multidimensional features.	√			√	2019
[22]	Record and deterministic replay based.	√		√		2016
[23]	Probability model based.	√		√		2015
[24]	Hypothesis test based.	√		√		2015
[25]	MAP based (Markov model).		√	√		2013
[26]	Hierarchical and density-based cluster.	√		√		2012

C. Machine and Deep Learning

- *Role of Machine and Deep Learning in covert communication*

Owing to the advancement of computer systems over the past five years, the concepts of ML and DL have undergone significant evolution [27]– [33], employing highly accurate and precise algorithms and statistical models [34]– [40] to evaluate and deduce conclusions from patterns in data. Based on this idea, several researchers have been interested in utilizing DL and ML [57]to find hidden channels.

ML methodology was suggested in [39] to generate classification rules and make it possible to parameterize the descriptive analytics of traffic (DAT) detectors. A detection approach based on a support vector machine (SVM) is examined in [40], and the findings demonstrated a certain pace of advancement at that time.

In the early stages, a system based on SVM is suggested in [41] for the effective detection of clandestine communications, while the study [42] presented the first detection methods for protocol switching covert channels (PSCCs), which showed that the number of packets between network protocol switches and the time between switches can be monitored to detect PSCCs with 98–99% accuracy for bit rates of 4 bits/s or higher.

- *Modern Approaches in Machine and Deep Learning*

The ability to discriminate between field programmable gate arrays configured with Trojan-free logic and logic introduced by Trojans was proven in [27] to be more accurate than principal component analysis. A collection of scalable Trojans that we created and assessed using a quantum diamond microscope (QDM) was used to evaluate this framework. A multi-classifier strategy was employed in [28] with two scenarios: in the first scenario, the training size was 70% of the dataset, and in the second scenario, it was 90%

According to various methodologies in the literature [29], image-based characteristics may be extracted to detect covert traffic because covert channels produce traffic that can be transformed into colored pictures. These characteristics were used to train a classifier on a sizable dataset of covert and overt communications. The experimental findings demonstrate that detection based on the stacking model can successfully identify DNS covert channels, whereas [30] provided a stacking model that was examined in a campus network to identify and categorize the wireless covert channel with the modulation of the constellation point (WCC-MC) scheme.

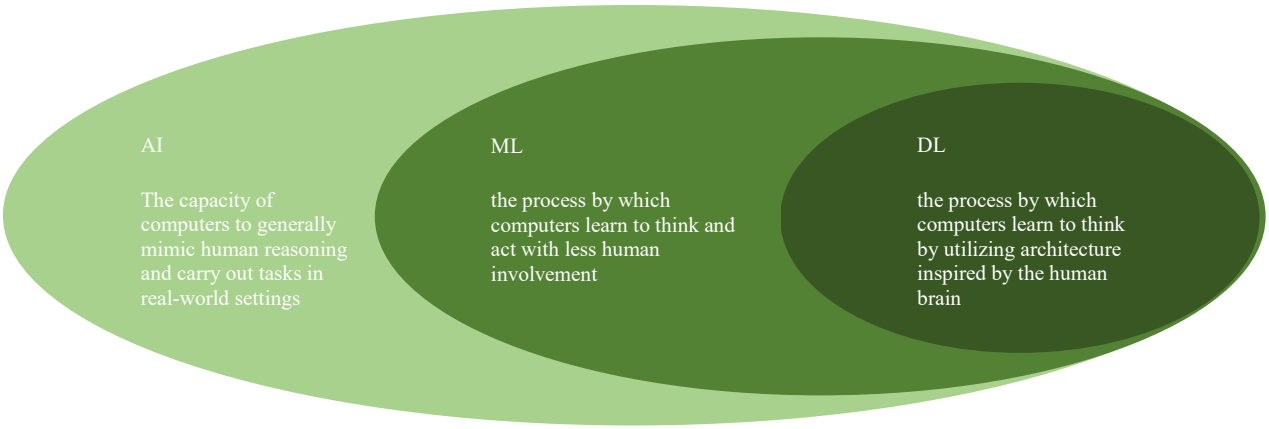

Fig. 3. AI, ML and DL

DL method based on amplitude-phase characteristics was presented in [31]. When identifying DNS covert channels utilizing the fully qualified domain name (FQDN), several studies have developed LSTM models that do not rely on feature engineering [32]. The test dataset had an accuracy of 99.38%. On the other hand, the k-Nearest Neighbour (k-NN) algorithm was used in [33] to suggest a CTC detection approach.

The authors in [34] suggested an all-purpose, protocol-independent method for detecting hidden network storage channels using supervised machine learning. The IP, TCP, and DNS protocols' covert channels were put to the test using the data set.

Each researcher utilized a unique dataset using different programs to test various classifiers. Different approaches have been devised to build datasets appropriate for use in machine learning and deep learning algorithms. Consequently, [35] constructed a dataset using eleven common covert channel tools, after which the covert channels were further categorized into patterns and given labels. Three distinct ML algorithms were trained using half of the obtained datasets. The performance of the algorithms was evaluated using the other half.

In [36], the authors suggested an ML-based domain generation algorithm (DGA) and DNS covert channel detection system that uses enhanced term frequency-inverse document frequency (TF-IDF), specificity score, and other methods to identify nefarious domain names. Some covert channels use the length of network packets to transmit hidden information by creating covert traffic that closely resembles regular traffic, making it difficult to identify these types of covert channels. ML detection strategy for this type that has attained a high level of detection accuracy that surpasses 98% was suggested in [37].

Using a novel DL model with a single classifier, [38] suggested an algorithmic strategy for identifying more complicated covert channels with long short-term memory (LSTM), this model is trained by importing normal network data into the algorithm model, which does not contain any hazardous information. After training, the model was imported into the network, which contained hazardous information.

Table II provides a brief explanation of various strategies.

TABLE II. A quick review on these techniques

Ref.	CTC	CSC	Types of classifiers	The best classifier	Percentage of accuracy	Year
[27]		√	CNN		87.2%	2022
[28]		√	Stack, NN, NB, LR, RF, SVM, DT, k-NN	Stack	98.9% data set 90% training 10% testing	2022
				Stack, NN and NB	98% Data set 70% training, 30% testing	
[29]	√		SVM, ANN, DT, NB	ANN	95.83%	2021
[30]		√	k-NN, Linear SVM, RF, Stacking	Stacking	99.01% AUC ROC	2021

[31]	√		CNN		98%	2021
[32]		√	LSTM		99.38%	2020
[33]	√		NB, SVM, LR, k-NN	k-NN	96%	2020
[34]		√	In network & transport layer: LR, SVM with linear and Gaussian kernels	SVM with Gaussian Kernel	99.78%	2019
			In application layer LR, K-NN, DT	DT	94.96%	
[35]		√	SVM, k-NN, DNN	k-NN	90%	2019
[36]		√	TF-IDF short text classification algorithm		99.92%	2019
[37]		√	NN, LR, NB, SVM, RF	NN	98%	2018
[38]		√	RNN		91.6%	2018

D. Covert Channels in Technology

Researchers pay more attention to the danger that covert channels bring. These channels affect new technologies such as VoIP, IoT, LTE, IoUT, and Smart grid [58],[59],[60].

[43] provided a unique technique for finding thermal covert channels (TCC) in response to growing interest in multi-core systems. To boost the bit error rate (BER) and maintain low power consumption, noise addition only occurs when there is a likelihood of accurate information transmission.

As a result of the switch from IPv4 to IPv6, [14], [16], attackers have been forced to create sophisticated stealing techniques that target this technology, consequently, [44] suggested an inspection framework for computing statistical indicators to uncover covert channels that target the IPv6 header. This demonstrated how attackers can exfiltrate information from air-gapped computers to adjacent smartphones through magnetic signals [45], establishing a new type of covert communication between air-gapped systems and nearby smartphones. The hidden channel worked well in confined spaces where wireless communication is prohibited.

In Voice over IP(VoIP) and the Internet of Things (IoT), there had been attempts to improve [46], [51],[48] the development of covert channels to obtain a high degree of security in transferring data, as well as efforts to detect [52], [56] them, as we previously noted that covert communication is a double-edged sword [9]. By enlarging the constellation points around the standard points, a constellation-shaping modulation-based approach was used [53] to improve such channels.

The 4th generation (4G) of mobile telecommunications networks has been dominated by Long Term Evolution (LTE) and Voice over LTE (VoLTE); nonetheless, this increases the possibility of hidden channels; therefore, the authors in [47], [49],[51] created a covert channel that guarantees the precision and efficacy of covert communication.

Operating systems commonly have covert channels, which pose a serious security risk to information systems, especially in cloud computing contexts; therefore, [54] introduced a unique technique for spotting covert channel abuse that takes behavior into account while analyzing the channels' basic characteristics, while [55] suggested a system called C2Detector to detect covert channels. The authors in [56] suggested a unique method that can precisely discover and evaluate hostile covert channels from the perspective of actions. Table III displays various covert channel production and detection systems.

TABLE III. Covert Channels in Technology

Ref.	Technology	CC Role	Detection	Generation	Year
[43]	Multi-core system	Used a thermal signal pattern to reduce the threats to sensitive data and information in many-core and multi-core systems.	√		2022
[44]	IPv6	Used in-kernel code augmentation to reduce the development effort without sacrificing Linux's packet processing efficiency.	√		2021

[45]	Magnetic field	Smartphones are used in the attack model to show how a nearby smartphone's magnetic sensors could pick up magnetic signals.		√	2021
[46]	VoIP	Enhanced end-user privacy and enterprises cooperating for cyber defense purposes.		√	2020
[47]	VoLTE	Modulated the packets' active dropping sequence numbers using the encrypted covert message. parity cascade coding allows the CTC to work without disclosing information.		√	2020
[48]	IoT	The first proposed covert channels for the publish-subscribe idea. ICC.1 and ICC.2 are two covert indirect channels.		√	2019
[49]	VoLTE	Made use of blocks of voice packet intervals and modular operation to reduce the disparity in traffic allocation between covert and overt traffic.		√	2019
[50]	LTE	Gave a novel idea for covert channel construction and is reliable and effective in an LTE-A.		√	2018
[51]	VoIP	Created a covert channel by breaking down the length distribution of real packet traffic into smaller chunks and mapping those chunks to data symbols.		√	2018
[52]	IoT	Demonstrated that a careful analysis of power profile data can identify anomalies in the devices.	√		2018
[53]	Wireless Communication	Boosted the covert channel's dependability and undetectability.		√	2018

V. Comparetive Analysis of the Literature

Provides an insightful comparative analysis of literature surrounding covert channel detection and generation techniques. Through a meticulous examination of various scholarly works, the authors shed light on the evolving landscape of covert communication methods and the corresponding countermeasures developed to mitigate potential security risks.

The survey begins by delving into the fundamentals of covert channels, elucidating their significance in the context of information security. Subsequently, the article navigates through an extensive range of literature, scrutinizing different approaches employed for covert channel detection [14]-[26]. The authors adeptly compare and contrast these methodologies, highlighting their strengths, limitations, and applicability in diverse scenarios.

Throughout the analysis, the authors skillfully integrate a comparative perspective of the detection of covert channels using ML and DL, allowing the readers to gain a comprehensive understanding of the contrasting techniques and their relative effectiveness.[27]-[38] They critically evaluate the surveyed literature, identifying classifiers, gaps, challenges, and emerging trends that require further investigation.

Moreover, the article delves into the exploration of covert channel generation techniques,[45]-[51] where the authors meticulously dissect the strategies employed to create hidden communication channels. By drawing upon a multitude of research papers, the survey elucidates the various covert channel generation mechanisms, their underlying principles, and the potential risks they pose.

VI. Limitations and Trends

Through the author's review of the literature [14]– [62], it is found that the data becomes increasingly exposed and a hotter target for hackers as a result of the swift growth of computer systems and technology. Numerous technologies, including IPv6, VoLTE, LTE, IoUT, IoT, smart grids, smart homes, smart automotive and transportation, VoIP, cloud computing, fog computing, and blockchain may be harmed by the presence and improper use of covert channels.

The following is a list of difficulties:

- *Security:* This difficulty can be regarded as the most crucial element. Researchers strive to provide the best answer each time.
- *Hybrid covert channels:* o date, no research has focused on HCC; instead, it has either focused on identifying or improving one particular form of covert channel.
- *Dataset:* A dataset is essential in ML and DL for training and evaluation; however, obtaining access to this data is frequently difficult because it is in a lab. generated, it is not available on the internet.
- *Classifiers:* Each publication chose one or more classifiers to experiment with, and these classifiers frequently vary from trial to trial. This makes it challenging to determine which classifier is best at detection.

- *Technology innovation:* Make hardware and software more complicated to make it harder to discover covert channels.
- *Exchanging information via the Internet:* Exposes these data to attackers who profit from data trafficking through the Internet.

On the other hand, researchers that work to improve covert channel production and strengthen it to share information safely will encounter a considerable obstacle to making these channels undetected, dependable, efficient, and successful.

It is important to note that a new covert channel that has not yet been classified or discovered might be produced by the swift improvement of agility.

VII. Contribution and Future direction

This paper significantly advances the area of information security in a several ways. It offers a thorough discussion of the most recent methods for creating and detecting covert channels. This is a valuable resource since it discusses and compares various covert channel creation and detection methods. Understanding the advantages and disadvantages of each approach as well as the variables affecting technique selection is aided by this. The paper also highlights the difficulties that must be overcome in the detection and generation of covert channels in the future.

Future work should focus on improving covert channel detection methods that can find covert channels that are difficult to spot with existing methods as well as developing more advanced covert channel generation methods that can transmit data more effectively and securely. as well as improving the security controls that may be put in place to stop sensitive information from being exfiltrated through covert routes.

Additionally, we want to investigate how unsupervised and reinforcement learning may be used to find more covert channels as well as how the identification of hybrid covert channels might help with information security issues and improve computer system privacy.

VIII. conclusion

In this paper, we review traditional and modern approaches to create and identify these channels and then extend these approaches to technologies.

In the past five years, articles have concentrated on the detection of these channels using ML and DL because of their high accuracy and precision; however, the dataset must be enhanced to make it easier to be trained and tested. Other contemporary methods also help to increase the effectiveness of detection owing to their important role in discreetly sending information, while other studies have concentrated on developing these channels to enhance information exchange security.

References

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

[2] C. G. Girling, "Covert Channels in LAN's*," IEEE Trans. Software Engineering*, vol. SE-13, no. 2, Feb. 1987, pp. 292–96

[3] L. Hélouët and A. Roumy, "Covert channel detection using Information theory," *Electronic Proceedings in Theoretical Computer Science*, vol. 51, pp. 34–51, Feb. 2011

[4] S. Z. Goher, B. Javed, and N. A. Saqib, "Covert channel detection: A survey based analysis," *High Capacity Optical Networks and Emerging/Enabling Technologies*, Dec. 2012.

[5] B. Carrara and C. Adams, "A Survey and Taxonomy Aimed at the Detection and Measurement of Covert Channels," *Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security*, Jun. 2016, doi: 10.1145/2909827.2930800.

[6] F. Gao, L. Zhu, K. Gai, C. Zhang, and S. Liu, "Achieving a Covert Channel over an Open Blockchain Network," IEEE Network, vol. 34, no. 2, pp. 6–13, Mar. 2020, doi: 10.1109/mnet.001.1900225.

[7] Z. Chen et al., "Blockchain Meets Covert Communication: A Survey," *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2022, doi: 10.1109/comst.2022.3204281.

[8] J. Tian, G. Xiong, Z. Li, and G. Gou, "A Survey of Key Technologies for Constructing Network Covert Channel," *Security and Communication Networks*, vol. 2020, pp. 1–20, Aug. 2020, doi: 10.1155/2020/8892896.

[9] C. Han, W. Gao, N. Yang, and J. M. Jornet, "Molecular Absorption Effect: A Double-edged Sword of Terahertz Communications*," IEEE Wireless Communications*, pp. 1–8, 2022, doi: 10.1109/mwc.016.2100704.

[10] M. Zuppelli and L. Caviglione, "pcapStego: A Tool for Generating Traffic Traces for Experimenting with Network Covert Channels," The 16th International Conference on Availability, Reliability and Security, Aug. 2021, doi: 10.1145/3465481.3470067.

[11] J. Ahn et al., "Network-on-Chip Microarchitecture-based Covert Channel in GPUs," *MICRO-54: 54th Annual IEEE/ACM International Symposium on Microarchitecture*, Oct. 2021, doi: 10.1145/3466752.3480093.

[12] 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, pp. 1–7, May 2022, doi: 10.1155/2022/2257524.

[13] L. Yuanzhang, L. Junli, X. Xinting, Z. Xiaosong, Z. Li, and Z. Quanxin, "A robust packet-dropping covert channel for mobile intelligent terminals," *International Journal of Intelligent Systems*, vol. 37, no. 10, pp. 6928–6950, Mar. 2022, doi: 10.1002/int.22868.

[14] M. Zuppelli, M. Repetto, A. Schaffhauser, W. Mazurczyk, and L. Caviglione, "Code Layering for the Detection of Network Covert Channels in Agentless Systems," *IEEE Transactions on Network and Service Management*, pp. 1–1, 2022, doi: 10.1109/tnsm.2022.3176752.

[15] S. Wu, Y. Chen, H. Tian, and C. Sun, "Detection of Covert Timing Channel Based on Time Series Symbolization," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 2372–2382, 2021.

[16] L. Caviglione, M. Zuppelli, W. Mazurczyk, A. Schaffhauser, and M. Repetto, "Code Augmentation for Detecting Covert Channels Targeting the IPv6 Flow Label," 2021 IEEE 7th International Conference on Network Softwarization (NetSoft), Jun. 2021.

[17] S. Huang, W. Liu, G. Liu, Y. Dai, and H. Bai, "A correlation-based approach to detecting wireless physical covert channels," *Computer Communications*, vol. 176, pp. 31–39, Aug. 2021.

[18] "Exploiting Correlation Characteristics to Detect Covert digital communication," *KSII Transactions on Internet and Information Systems*, vol. 14, no. 8, Aug. 2020.

[19] J. Xie, Y. Chen, L. Wang, and Z. Wang, "A Network Covert Timing Channel Detection Method Based on Chaos Theory and Threshold Secret Sharing," 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Jun. 2020.

[20] H. Nafea, K. Kifayat, Q. Shi, K. N. Qureshi, and B. Askwith, "Efficient Non-Linear Covert Channel Detection in TCP Data Streams," *IEEE Access*, vol. 8, pp. 1680–1690, 2020.

[21] S. Lu, Z. Chen, G. Fu, and Q. Li, "A Novel Timing-based Network Covert Channel Detection Method," Journal of Physics: Conference Series, vol. 1325, no. 1, p. 012050, Oct. 2019.

[22] M. Yan, Y. Shalabi, and J. Torrellas, "ReplayConfusion: Detecting cache-based covert channel attacks using record and replay," *2016 49th*

Annual IEEE/ACM International Symposium on Microarchitecture (MICRO),Oct. 2016.
[23] P. Yang, H. Zhao, and Z. Bao, "A probability-model-based approach to detect covert timing channel," 2015 IEEE International Conference on Information and Automation, Aug. 2015.
[24] H. Zhao and M. Chen, "WLAN covert timing channel detection," 2015 Wireless Telecommunications Symposium (WTS), Apr. 2015.
[25] J. Zhai, G. Liu, and Y. Dai, "Detection of TCP covert channel based on Markov model," *Telecommunication Systems*, vol. 54, no. 3, pp. 333–343, Jul. 2013.
[26] Q. Yuwen, S. Huaju, S. Chao, W. Xi, and L. Linjie, "Network Covert Channel Detection with Cluster based on Hierarchy and Density," *Procedia Engineering*, vol. 29, pp. 4175–4180, 2012.
[27] M. Ashok, M. J. Turner, R. L. Walsworth, E. V. Levine, and A. P. Chandrakasan, "Hardware Trojan Detection Using Unsupervised Deep Learning on Quantum Diamond Microscope Magnetic Field Images," *ACM Journal on Emerging Technologies in Computing Systems*, Apr. 2022, doi: 10.1145/3531010.
[28]M. A. Elsadig and A. Gafar, "Covert Channel Detection: Machine Learning Approaches," *IEEE Access*, vol. 10, pp. 38391–38405, 2022.
[29]S. Al-Eidi, O. Darwish, Y. Chen, and G. Husari, "SnapCatch: Automatic Detection of Covert Timing Channels Using Image Processing and Machine Learning," *IEEE Access*, vol. 9, pp. 177–191, 2021.
[30] P. Yang et al., "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.
[31] S. Huang, W. Liu, G. Liu, Y. Dai, and H. Bai, "Detection of Constellation-Modulated Wireless Covert Channel Based on Adjusted CNN Model," *Security and Communication Networks*, vol. 2021, pp. 1–14, Jun. 2021.
[32]S. Chen, B. Lang, H. Liu, D. Li, and C. Gao, "DNS covert channel detection method using the LSTM model," *Computers & Security*, vol. 104, p. 102095, May 2021.
[33]J. Han, C. Huang, F. Shi, and J. Liu, "Covert timing channel detection method based on time interval and payload length analysis," *Computers & Security*, vol. 97, p. 101952, Oct. 2020.
[34]M. A. Ayub, S. Smith, and A. Siraj, "A Protocol Independent Approach in Network Covert Channel Detection," 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), Aug. 2019.
[35]M. Chourib, "Detecting Selected Network Covert Channels Using Machine Learning," 2019 International Conference on High Performance Computing & Simulation (HPCS), Jul. 2019.
[36] Z. Wang, H. Dong, Y. Chi, J. Zhang, T. Yang, and Q. Liu, "DGA and DNS Covert Channel Detection System based on Machine Learning," Proceedings of the 3rd International Conference on Computer Science and Application Engineering - CSAE 2019, 2019.
[37] M. A. Elsadig and Y. A. Fadlalla, "Packet Length Covert Channel: A Detection Scheme," 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), Apr. 2018.
[38] Y. Sun, L. Zhang, and C. Zhao, "A Study of Network Covert Channel Detection Based on Deep Learning," 2018 2nd IEEE Advanced Information Management,Communicates,Electronic and Automation Control Conference (IMCEC), May 2018.
[39] F. Iglesias, V. Bernhardt, R. Annessi, and T. Zseby, "Decision Tree Rule Induction for Detecting Covert Timing Channels in TCP/IP Traffic," *Machine Learning and Knowledge Extraction*, pp. 105–122, 2017.
[40] Q. Li, P. Zhang, Z. Chen, and G. Fu, "Covert timing channel detection method based on random forest algorithm," 2017 IEEE 17th International Conference on Communication Technology (ICCT), Oct. 2017.
[41] P. L. Shrestha, M. Hempel, F. Rezaei, and H. Sharif, "A Support Vector Machine-Based Framework for Detection of Covert Timing Channels," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 2, pp. 274–283, Mar. 2016.
[42] S. Wendzel and S. Zander, "Detecting protocol switching covert channels," 37th Annual IEEE Conference on Local Computer Networks, Oct. 2012.
[43] P. Rahimi, A. K. Singh, and X. Wang, "Selective Noise Based Power-Efficient and Effective Countermeasure against Thermal Covert Channel Attacks in Multi-Core Systems," *Journal of Low Power Electronics and Applications,* vol. 12, no. 2, p. 25, May 2022, doi: 10.3390/jlpea12020025.
[44] M. Repetto, L. Caviglione, and M. Zuppelli, "bccstego: A Framework for Investigating Network Covert Channels," The 16th International Conference on Availability, Reliability and Security, Aug. 2021, doi: 10.1145/3465481.3470028.
[45] M. Guri, "MAGNETO: Covert channel between air-gapped systems and nearby smartphones via CPU-generated magnetic fields," *Future Generation Computer Systems*, vol. 115, pp. 115–125, Feb. 2021, doi: 10.1016/j.future.2020.08.045.
[46] J. Saenger, W. Mazurczyk, J. Keller, and L. Caviglione, "VoIP network covert channels to enhance privacy and information sharing," *Future Generation Computer Systems*, vol. 111, pp. 96–106, Oct. 2020.
[47] Y. Li, X. Zhang, X. Xu, and Y. Tan, "A Robust Packet-Dropout Covert Channel over Wireless Networks," *IEEE Wireless Communications*, vol. 27, no. 3, pp. 60–65, Jun. 2020, doi: 10.1109/mwc.001.1900431.
[48] A. Velinov, A. Mileva, S. Wendzel, and W. Mazurczyk, "Covert Channels in the MQTT-Based Internet of Things," *IEEE Access*, vol. 7, pp. 161899–161915, 2019.
[49] X. Zhang, L. Zhu, X. Wang, C. Zhang, H. Zhu, and Y. Tan, "A packet-reordering covert channel over VoLTE voice and video traffics," *Journal of Network and Computer Applications*, vol. 126, pp. 29–38, Jan. 2019, doi: 10.1016/j.jnca.2018.11.001.
[50] G. Xu, W. Yang, and L. Huang, "Hybrid covert channel in LTE-A: Modeling and analysis," *Journal of Network and Computer Applications*, vol. 111, pp. 117–126, Jun. 2018.
[51] C. Liang, Y. 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, Sep. 2018.
[52] J. Shelley, H. Mohammed, L. Zink, S. R. Hasan, and O. Elkeelany, "Covert Communication Channel Detection in Low-Power Battery Operated IoT Devices: Leveraging Power Profiles," SoutheastCon 2018, Apr. 2018.
[53] P. Cao, W. Liu, G. Liu, X. Ji, J. Zhai, and Y. Dai, "A Wireless Covert Channel Based on Constellation Shaping Modulation," *Security and Communication Networks,* vol. 2018, pp. 1–15, 2018.
[54] L. Wang, W. Liu, N. Kumar, D. He, C. Tan, and D. Gao, "A novel covert channel detection method in cloud based on XSRM and improved event association algorithm," *Security and Communication Networks,* vol. 9, no. 16, pp. 3543–3557, Jul. 2016.
[55] J. Wu, L. Ding, Y. Wu, N. Min-Allah, S. U. Khan, and Y. Wang, "C2 Detector: a covert channel detection framework in cloud computing," *Security and Communication Networks*, vol. 7, no. 3, pp. 544–557, May 2013.
[56] G. Garateguy, G. R. Arce, and J. Pelaez, "Covert channel detection in VoIP streams," 2011 45th Annual Conference on Information Sciences and Systems, Mar. 2011.
[57] E. S. Ali et al., "Machine Learning Technologies for Secure Vehicular Communication in Internet of Vehicles: Recent Advances and Applications," Security and Communication Networks, vol. 2021, pp. 1–23, Mar. 2021, doi: 10.1155/2021/8868355.
[58] M. K. Hasan et al., "Fischer Linear Discrimination and Quadratic Discrimination Analysis–Based Data Mining Technique for Internet of Things Framework for Healthcare," Frontiers in Public Health, vol. 9, Oct. 2021, doi: 10.3389/fpubh.2021.737149.
[59] M. K. Hasan, S. H. Yousoff, M. M. Ahmed, A. H. A. Hashim, A. F. Ismail, and S. Islam, "Phase Offset Analysis of Asymmetric Communications Infrastructure in Smart Grid," Elektronika ir Elektrotechnika, vol. 25, no. 2, Apr. 2019, doi: 10.5755/j01.eie.25.2.23209.
[60] E. S. Ali, R. A. Saeed, I. K. Eltahir, and O. O. Khalifa, "A systematic review on energy efficiency in the internet of underwater things (IoUT): Recent approaches and research gaps," Journal of Network and Computer Applications, vol. 213, p. 103594, Apr. 2023, doi: 10.1016/j.jnca.2023.103594.
[61] R. F. Mansour, H. Alhumyani, S. A. Khalek, R. A. Saeed, and D. Gupta, "Design of cultural emperor penguin optimizer for energy-efficient resource scheduling in green cloud computing environment," Cluster Computing, vol. 26, no. 1, pp. 575–586, May 2022, doi: 10.1007/s10586-022-03608-0.
[62] F. Gao, L. Zhu, K. Gai, C. Zhang, and S. Liu, "Achieving a Covert Channel over an Open Blockchain Network," IEEE Network, vol. 34, no. 2, pp. 6–13, Mar. 2020, doi: 10.1109/mnet.001.1900225.