Journal of IoT in Social, Mobile, Analytics, and Cloud (ISSN: 2582-1369)
www.irojournals.com/iroismac/

A Comprehensive Survey on Exploring Covert Timing Channels in Network Security

S. Revathi[1], B. Praveen kumar[2], M. Ranjith[3], M. Sachithanantham[4]

[1]Assistant Professor, Department of Computer Science and Engineering, Erode Sengunthar Engineering College, Perundurai, Erode, Tamil Nadu, India.

[2,3,4]Student, Department of Computer Science and Engineering, Erode Sengunthar Engineering College, Perundurai, Erode, Tamil Nadu, India.

E-mail: [1]revathiesec25@gmail.com, [2]kuttypraveenkumar2@gmail.com, [3]ranjithcseng432@gmail.com, [4]sachithanantham1412@gmail.com

Abstract

Covert timing channels play pivotal roles in spying, hacking, and data theft, enabling secret communication and surreptitious data exchange. They also find utility in secure conversations, message concealment, security testing, and privacy protection, underscoring their versatile application across diverse domains. However, the accuracy of covert timing channels may be compromised by network traffic patterns and time delays, potentially affecting data integrity. This survey paper primarily provides an brief overview of identifying and mitigating these influencing factors of existing covert timing channels and presents a suggested system that integrates Reversible Covert Timing Channel (CTC) steganography and Elliptic Curve Cryptography (ECC) to ensure secure communication and data encryption. By leveraging this combination, the system aims to enhance the resilience of covert communication channels against adversarial interference while safeguarding the confidentiality and integrity of transmitted data.

Keywords: Reversible Covert Timing Channel steganography, Elliptic Curve Cryptography, Data Encryption, Privacy Protection, Message Concealment.

DOI: https://doi.org/10.36548/jismac.2024.1.003
Received: 03.01.2024, received in revised form: 08.02.2024, accepted: 26.02.2024, published: 07.03.2024

1. Introduction

In cybersecurity, covert timing channels are like secret tunnels used to send messages and data without being noticed. They're used for things like spying and keeping information private. These secret tunnels work by taking advantage of small differences in how long it takes for data to travel through a network, so they can transfer information without anyone knowing. They're really useful because they can be used in lots of different situations, like keeping conversations secure or testing how safe a system is. But sometimes, things like how busy a network is or how long data takes to travel can mess up these secret tunnels, which might make the information they carry less reliable.

In this study, we're going to explore these secret tunnels in cybersecurity. We'll look at how we can make the system more reliable by using Elliptic Curve Cryptography (ECC), in combination with the Reversible Covert Timing Channel (CTC) steganography, we're trying to make these secret tunnels stronger against people who might try to interfere with them. The goal is to make sure that when you're sending secret messages, they stay secret and safe from anyone who might try to snoop around.

The introduction of subtle and powerful challenges to the complex field of cybersecurity has come with the rise of covert timing channels. A sophisticated kind of covert communication, covert timing channels allow information to be sent between organizations without requiring direct interaction. These covert channels, which function covertly within processes that appear innocuous at first glance, have emerged as a focus area for cyber-attacks. This introduction explores the hidden nature of timing channels, highlighting the growing ubiquity of these channels and the imperative necessity for reliable detection systems. Understanding these hidden channels' subtleties is crucial because they represent a serious danger to the confidentiality of sensitive data. This investigation lays the groundwork for understanding the complexities of covert timing channels and emphasizes the need for creative solutions that can successfully locate and block these unseen conduits in the always changing field of cybersecurity.

A state-of-the-art development in cybersecurity, Snap Catch [13] was created expressly to tackle the growing issues associated with hidden communication channels. Covert channels have become a sophisticated danger at a time when safeguarding sensitive information is crucial. This is especially the case with those that take use of timing mechanisms. So Snap Catch, was developed to make sure the use of the advantages of both machine learning and

image processing in covert timing channels. This cutting-edge technology, which can automatically detect hidden timing channels contained in seemingly innocent photos, has the potential to completely change the detection landscape. Though the SnapCatch technique seems promising in automating and accurately detecting covert timing channels, there are potential disadvantages. like training complexities and real time detection etc.

So, to overcome the challenges in the existing the proposed method utilizes the capability of ECC and the Reversible Covert Timing Channel (CTC) steganography in order to address the major issues like efficiency, security and real time responsiveness.

Elliptic Curve Cryptography (ECC) is a robust cryptographic technology that uses the algebraic features of elliptic curves over finite fields to ensure secure communication and data protection. It provides a high degree of security with lower key lengths than other standard cryptographic systems, such as RSA, making it ideal for resource-constrained contexts like mobile and IoT devices. ECC is widely utilized in different applications, such as secure communication protocols, digital signatures, and key exchange methods, enabling efficient and strong security solutions in today's digital environment.

1.1 Objective

- To study the covert timing channel in network security
- To suggest a proposed work flow on elliptic curve cryptography and covert timing channel
- To discuss the advantages of the suggested method and future progress of the research

2. Related Study

In this study, Peng Yang et al. [1] proposed a computer programs that employ covert channels as information routes to get by security guards and steal data. Domain name system protocol implement one of the basic techniques for creating a covert channel. Attackers may only use DNS secret routes for malicious purposes. Consequently, it is critical to successfully identify DNS hidden routes for the security of computer systems and networks. In an attempt to tackle the problem of DNS hidden channel detection, the author has provided a method for identifying them based on stacking models. The results of the experiment show that the DNS covert channels may be effectively identified using detection methods based on the stacking model. The stacking paradigm on a campus network was investigated. It also has the ability to identify activities on unknown hidden channels. With an area under the curve (AUC) of 0.9901,

the strategy performs better than the current techniques. The domain name system (DNS), which associates IP addresses with domain names, serves as the foundation and fundamental source for the modern Internet. Most users are unaware of the DNS protocol's potential vulnerability to data exfiltration since it is so widely used and most firewalls do not monitor DNS packets. Because of this, fraudsters are taking advantage of DNS and the DNS protocol. Many DNS covert channels serve nefarious purposes, including the revelation of confidential data and the establishment of hidden pathways for botnet command transmission. Presently, numerous programs create concealed tunnels utilizing the DNS protocol. Security devices often allow DNS traffic to get through despite having strict access control rules in place, which is necessary for hostile communications based on the DNS protocol.

The authors in this system [2] has utilized IPv6 protocol in the place of IPv4 protocol due to the increasing demand for IP addresses globally as a result of growing Internet usage. As a result, IPv6 security has become an important area of research. One of the biggest threats to Internet security is the availability of Network Covert Channels (NCCs), which provide a great deal of support for carrying out covered communications, such as sending secret data or stealing private information from companies. In order to prevent such dangerous conduct, real-time networks urgently need the development and implementation of effective detection technologies. Deciphering the encrypted chats also requires locating hidden information. To detect and pinpoint storage-based covert channels (NCCs) in IPv6, we introduce a novel approach combining a Deep Neural Network and the One-vs-Rest (OvR) technique built upon a Support Vector Machine framework. their system operates across two layers: Layer 1 classifies IPv6 packets as either normal or covert, while Layer 2 identifies the location of hidden data within covert packets detected in Layer 1. To validate their method, dataset comprising legitimate and illicit IPv6 packets using the pcapStego tool and the CAIDA dataset was generated. Experiments were carried out to choose the optimal classifiers for the two levels of the proposed system. With an accuracy of 99.7% and an average prediction time of 0.0719 seconds per covert sample, the proposed system can find covert data in IPv6 packets and is suitable for real-time implementation. The classifiers used for Layer 1 and Layer 2 were DNN and OvR SVM, respectively. Because technology is advancing so quickly, the Internet has become a seamless part in daily lives. Due to global lockdowns prompted by Covid-19, most companies have expanded remote work options for employees, heightening their reliance on the Internet In addition, there has been an abnormally high increase in other cyberattacks, including intrusions, online fraud, scams, and security lapses.

The authors MUAWIA A et al. [3] in his findings stated that the advancements in computer networks and communication technologies have made it easier, faster, and more secure than ever to establish clandestine connections. A covert channel is a means of exposing private messages while evading security measures in a system. Still, one of the hardest parts is locating such deadly, invisible, and hidden threats. This threat is too subtle for traditional security protocols to detect since it uses methods not meant for communication. The definitions, types, and developments of covert channels have been briefly reviewed in this study, with a focus on machine learning (ML)-based detection techniques. It goes into great depth into the limitations and successes of the most widely utilized covert channels as well as the machine learning techniques used to stop them. A comparative experimental analysis of a few well-liked machine learning techniques that are often used in this field is also included in this research. The efficacy of these classifiers was evaluated and documented in light of this. The study's conclusion highlights the reality that nothing is really protected and that further investigation is required to locate hidden conduits, demonstrate how vulnerable our data remains. Using a covert channel is one way to strike up a discussion between two individuals while surreptitiously disclosing information. This message violates the organization's stated security policies. This unlawful communication was first defined by Lampson in 1973.

Ishikura et al. [4] have proposed this system. Businesses across the board are concerned about targeted attacks that attempt to steal data. Attackers have been utilizing their software to launch these attacks in recent years by circumventing DNS tunneling and misusing the domain name system (DNS). Despite various research efforts in this regard, the techniques now in use to detect DNS tunneling rely on qualities that advanced tunneling systems may quickly obfuscate by simulating trustworthy DNS clients. This kind of obfuscation would lead to data leaking. In order to address this problem, we focused on a difficult-to-hide "trace" that DNS tunneling leaves behind. When data is exfiltrated via DNS tunneling, the malware connects directly to the DNS cache server, and the DNS tunneling requests that are sent back ensure that no data is cached. A novel method for detecting DNS tunneling is presented in this study, utilizing cache property-aware features. It is demonstrated through their experiments that one of the proposed characteristics is highly effective in accurately identifying DNS tunneling traffic. The method additionally presents an LSTM-based filter and a rule-based filter with the aid of this proposed functionality. The rule-based filter detects DNS tunneling attacks more often than the LSTM filter, which does it more quickly, despite the fact that both filters have low misdetection rates.

According to ASAF NADLER et al. [5] a malware software designed for data exfiltration in this system has to take a devious path to achieve its goal in the face of security countermeasures. One of the covert channels that is now in use is the DNS protocol. Despite extensive research on detecting covert channels through DNS over the past decade, previous studies have primarily focused on a specific subset: DNS tunneling. While recognizing tunneling is crucial, it has been disregarded that a broader category of malware capable of low-throughput DNS exfiltration exists. This work aims to address this gap by presenting a method for detecting both DNS tunneling and low-throughput data exfiltration. To achieve this objective, we propose a system comprising a trained, interchangeable, and supervised anomaly detection model alongside a supervised feature selection approach. The process begins with the identification of domain-specific traffic anomalies through a one-class classifier. Following this, to mitigate false positives associated with detecting low-throughput data exfiltration, a rule-based filter is employed to scrutinize data exchanges over DNS channels utilized by authorized services. Evaluation of our methodology was conducted using a substantial dataset comprising over 75,000 legitimate transactions and more than 2,000 fraudulent attempts recorded in recursive DNS server logs. The assessment indicates that while pinpointing low-throughput exfiltration is challenging, our approach achieves a high recall rate of at least 99% for identifying DNS tunneling with a minimal false positive rate of less than 0.01%. This method reduces the attack's effectiveness by limiting malware that attempts to avoid detection to a maximum payload rate of 1 kb/h (five credit card numbers or ten user passwords per hour) while still adhering to DNS syntax requirements.

Lejun Zhang et al. [6] the construction of covert channels has been a focal point in information security research, with utilizing IP data packets as a crucial method. This study introduces a novel approach called "enlarging-the-capacity packet sorting covert channel." It explores the correlation between the number of ports, packet intervals, and different time intervals within the IP covert channel based on packet sorting. By analyzing transmission efficiency and performance, the proposed method optimizes the IP covert channel, specifically in packet sorting, leading to an enhanced total data transmission capacity in the covert channel. This highlights its effectiveness in expanding the capabilities of covert communication through IP packet manipulation.

Shuhong Wu et al. [7] Covert Timing Channels (CTCs) serve as a method for surreptitiously leaking information by manipulating interarrival time sequences (IATs) between packets. Traditional network security measures like firewalls and proxies face

challenges in effectively detecting CTCs, as these channels exclusively modify IATs. The malicious exploitation of CTCs by criminals poses a substantial threat to network security. Traditional CTC detection methods, such as the KS test and entropy test, have limitations in terms of generality and robustness, thus requiring a larger number of IATs to ensure accurate detection. Consequently, enhancing the performance of detection methods against CTCs has become a focal point of research in recent years. This pursuit aims to develop more effective and versatile approaches to counteract CTCs, considering their potential for misuse in compromising network security. Researchers are actively engaged in exploring methodologies that transcend the constraints of classic detection techniques, seeking advancements in universality and robustness to fortify networks against the evolving landscape of covert timing channel threats.

Xiaosong Zhang et al. [8] the article unveils a method to safeguard against life-threatening CAN bus attacks like suspension, injection, and masquerade, particularly those posing risks such as brake disablement. Introducing TACAN (Transmitter Authentication in CAN), it ensures secure authentication of Electronic Control Units (ECUs) on the conventional CAN bus. Significantly, TACAN utilizes covert channels, eliminating the necessity for CAN protocol adjustments or adding extra traffic. TACAN incorporates three covert channels: Inter-Arrival Time (IAT)-based, which utilizes CAN message IATs; Least Significant Bit (LSB)-based, hiding authentication within the LSBs of typical CAN data; and a hybrid channel, combining the advantages of the first two. Validation on the University of Washington Eco CAR (Chevrolet Camaro 2016) testbed underscores TACAN's effectiveness.

Yu-an Tan et al. [9] given the increasing prevalence of security threats, In an untrusted Internet of Things (IoT) context, covert time channels have become a major choice for conveying sensitive data. This article seeks to showcase the vulnerability of IoT to covert timing channels, particularly when operating over mobile networks. The focus begins with introducing the system model of a covert timing channel designed for IoT. Next, in the context of IoT operating in 4G/5G networks, an analysis is conducted to determine the applicability of typical hidden time channels based on inter-packet delays.

Dan Deng et al. [10] ensuring secure transmission and privacy is paramount in various application scenarios, necessitating the use of covert communication. Intelligent Reflective Surface (IRS) assisted relay networks often use two-way protocols to facilitate covert communication, effectively preventing wireless signal eavesdropping. In this unique scenario, the study quantifies the performance of secret communication by deriving a closed expression

for the probability of interruption and its asymptote. For the most exceedingly bad conceivable clandestine communication situation, a comprehensive investigation of the ideal normalized control limit for assurance and finder is performed utilizing complex Gaussian conveyance guess. The Table.1 below illustrates the merits and the demerits of the literature discussed in the related study.

Table 1. Comparative Table

Ref. No	Methodology	Merits	Demerits
[1]	DNS covert channel detection method, Stacking method	Real-World Evaluation, Relevance to cybersecurity	Potential Overfitting, Limited Evaluation, Scalability Concerns
[2]	Statistical Test Identification, Low-Latency Analysis	Comprehensive Approach, Real-Time Detection, Statistical Analysis	Limited Scope, Resource Intensive, Hardware Dependency
[3]	Machine Learning Detection Technique, ML classifiers	Lack of Detailed Methodology, Negative Conclusion	Focus on ML only, Specific types of covert channels, Low accuracy
[4]	Rule-based filter, LSTM-based filter	Unique Approach, Multiple Detection Filters	Complexity of LSTM-based Filter, Dependency on cache misses.
[5]	DNS Tunneling, Anomaly Detection	Comprehensive Detection, Automatic Daniel, Novelty	Dependency on DNS Logs, Potential Overhead, False positives
[6]	Proposes an extended packet sorting covert	Maximizes covert data transmission through	Possible security vulnerabilities

	channel, establishing a model to maximize covert information transmission	extended packet sorting covert channel.	Complex implementation Network performance impact
[7]	Time series symbolization. Similarity measurement Prediction of unknown traffic	Detects covert timing channels through time series symbolization, similarity measurement, and prediction of unknown traffic.	Detect the covert timing channel not provide the security of the data.
[8]	Encoding Modulation RTCP Feedback	Proposes VoLTE covert channel with adaptive feedback, emphasizing encoding, modulation	Commonly focused on mobile network
[9]	Investigate covert communication covert state-dependent channels, deriving covert capacity and secret key rate requirements	Security, Stealth, Covert	Complicate to calculate the detection error Probability
[10]	Develops closed-form expressions for outage probability, analyses optimal power threshold, and provides simulations for validation.	Offers insights into covert communications and security in IRS-assisted networks.	Limited focus on practical implementation and scalability for real-world scenarios.

3. Existing System

With the continued advancement o computer networks and communication technologies, covert connections are now more secure, quicker, easier to set up, and undetected than before. By going against a system security policy, a covert channel can be used to leak confidential communications. One of the hardest parts is still finding these harmful, unwatchable, and concealed hazards. Since it uses techniques not intended for communication, conventional security procedures are unable to identify this threat. A brief overview of covert channel definitions, kinds, and advances has been provided in this study, with an emphasis on machine learning (ML)-based detection methods. The most popular covert routes and machine learning strategies for thwarting them are covered in detail, along with their benefits and drawbacks The study concluded that there is still a risk to our information, nothing is considered safe, and more work has to be done on the identification of hidden channels. So, the study suggests a system that integrates Reversible Covert Timing Channel (CTC) steganography and Elliptic Curve Cryptography (ECC) to ensure secure communication and data encryption. By leveraging this combination, the system aims to enhance the resilience of covert communication channels against adversarial interference while safeguarding the confidentiality and integrity of transmitted data

4. Proposed System

The proposed system for reversible CTC steganography consists of many modules that enable safe message embedding and extraction from cover objects. The Message Embedding module uses covert timing channels (CTC) methods to elegantly insert hidden messages into cover objects while maintaining their integrity. Index Table Generation and CTC Index Table Generation modules assign message bits to their proper places inside cover objects, allowing for more precise embedding and extraction procedures. The Patch Composition Process splits cover objects into manageable portions to enable efficient message embedding, whereas Message-Oriented Texture Synthesis improves textures to efficiently conceal messages. The Stego Synthesis Texture module combines cover objects and embedded messages to create visually indistinguishable stego objects. Finally, the Extract Source Texture and Extract Message module reverses the embedding process, removing both the original cover object and the hidden message with no distortion, providing safe communication while preserving cover object integrity.

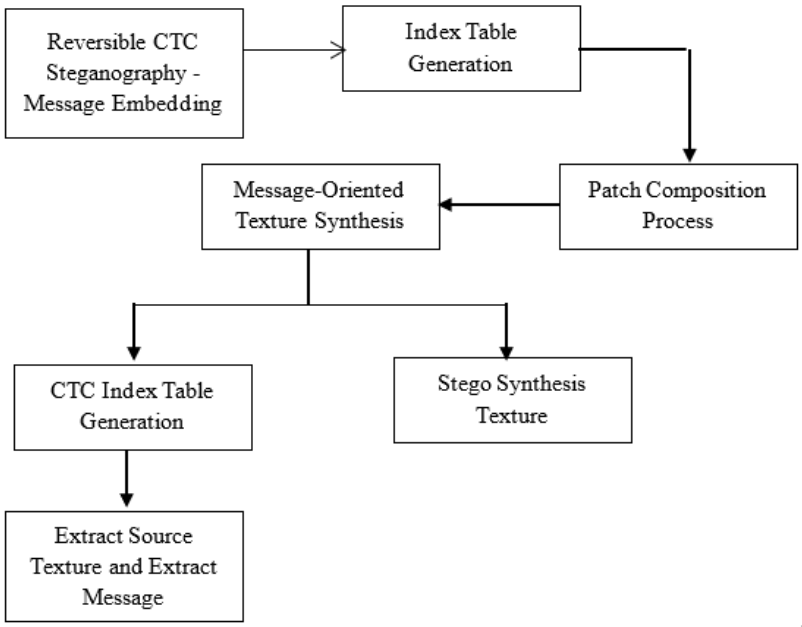

Figure 1. Flow Diagram

4.1 Integration of ECC with Steganography

In the suggested system, Elliptic Curve Cryptography (ECC) is combined with steganography to improve communication security and data encryption. ECC is typically used for encryption within the system. When a message has to be conveyed safely, it is encrypted using ECC, which produces lower key sizes than standard cryptographic methods while retaining strong security.

Following encryption, the encrypted message is implanted in a carrier media utilizing Reversible Covert Timing Channel (CTC) steganography methods. These strategies ensure that the message may be buried inside the carrier media, such as graphics or textures, while without materially affecting its look. By combining ECC encryption and steganography, the method assures that the message is not only securely encoded, but also hidden inside the carrier media.

In this combination, ECC provides the encryption layer, ensuring the message's secrecy, whilst steganography provides a technique of concealing the encrypted message inside the carrier media, therefore improving overall communication security. This combination technique guarantees that sensitive information is transferred safely and discreetly, making it difficult for unauthorized parties to intercept or decode the message.

4.2 Reversible CTC Steganography Message Embedding

This module embeds hidden messages into cover objects like pictures or textures using reversible covert timing channels (CTC) steganography techniques. It assures that the embedded messages may be removed without causing loss or distortion to the original cover item.

4.3 Index Table Generation

The Index Table Generation module generates tables or indices that help map message bits to their relevant positions inside the cover object. These indexes are critical for properly embedding and extracting messages throughout the steganography process.

4.4 Patch Composition Process

To allow for fast message embedding, the Patch Composition Process module divides the cover object into patches or segments. Each patch is separately handled to guarantee that the concealed message is seamlessly integrated while preserving the cover object's visual integrity.

4.5 Message-Oriented Texture Synthesis

This module creates textures designed for message embedding. Users may enter secret messages, and the system creates textures that are specifically designed to successfully disguise these secrets. The created textures provide resistance against detection while supporting the encoded message.

4.6 Stego Synthesis Texture

The Stego Synthesis Texture module combines the cover object and embedded message to create the stego object. This stego object is superficially identical to the original cover object, but it has a secret message within its structure.

4.7 CTC Index Table Generation

Similar to the Index Table Generation module, this component creates index tables for covert timing channels (CTC). These tables make it easier to encode and decode covert messages sent at different times, ensuring precise communication between sender and receiver.

4.8 Extract Source Texture and Extract Message

Similar to the Index Table Generation module, this component creates index tables for covert timing channels (CTC). These tables make it easier to encode and decode covert

The system aims to provide safe communication by securely encoding and hiding messages within cover objects, making it difficult for unauthorized parties to intercept or decode the messages. It seems to have a comprehensive approach to secure communication, combining both encryption and steganography techniques.

The Table.2 below shows the advantages of using ECC with Reversible Covert Timing Channel.

Table 2. Advantages of Elliptic Curve Cryptography with Reversible Covert Timing Channels

Advantages	Real-Time Analysis
Advantages of using Elliptic Curve Cryptography	Enhanced Security
	Resource Efficiency
	Flexibility and Adaptability
	Comprehensive Security Assurance
	Real-Time Threat Detection
	Mitigation of Side-channel Attacks

5. Future Work

The suggested method for reversible CTC steganography includes several modules designed to securely embed and extract hidden messages from cover objects. These modules utilize covert timing channels (CTC) and advanced techniques such as index table generation, patch composition, and texture synthesis to efficiently conceal messages while preserving cover object integrity. Future work focuses on the design and the development of this suggested model and further optimizing these modules for improved efficiency and security, exploring advanced CTC methods, refining message allocation within cover objects, enhancing texture synthesis, and further improving the reversal process for safe communication.

6. Conclusion

In conclusion, covert timing channels serve as crucial tools in various activities, from spy to privacy protection, due to their ability to facilitate secretive communication and data exchange. However, their reliability can be compromised by factors like network traffic patterns and time delays, which can impact data integrity. This study has focused on addressing these challenges through the application of Elliptic Curve Cryptography (ECC). By integrating Reversible Covert Timing Channel (CTC) steganography with ECC, the proposed system aims to enhance the security and resilience of covert communication channels. Through this combination, the study endeavors to safeguard the confidentiality and integrity of transmitted data, ultimately contributing to the protection of digital information in an increasingly interconnected world. The designing, development and the evaluation of the suggested method efficiency under various real-world scenarios would be carried out in the future work of the research.

References

[1] 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. 1–15, 2021.

[2] Sattolo, Thomas AV. "Real-time detection of storage covert channels." PhD diss., Carleton University, 2021.

[3] Elsadig, Muawia A., and Ahmed Gafar. "Covert channel detection: machine learning approaches." IEEE Access 10 (2022): 38391-38405.

[4] N. Ishikura, D. Kondo, V. Vassiliades, I. Iordanov, and H. Tode, "DNS tunneling detection by cache-property-aware features," IEEE Trans. Netw. Service Manage., vol. 18, no. 2, June 2021, pp. 1203–1217.

[5] Nadler, A. Aminov, and A. Shabtai, " Detection of Malicious and Low Throughput Data Exfiltration over the DNS Protocol," Computer Security, vol. 80, January 2019, pp. 36-53.

[6] Hu, X. Huang, T. Rasheed, W. Zhang, L. and Zhao, C. (2019) 'An Enlarging The-Capacity Packet Sorting Covert Channel', IEEE Access, Vol.7, pp.145634–145640.

[7] Wu, Shuhong, Yonghong Chen, Hui Tian, and Chonggao Sun. "Detection of covert timing channel based on time series symbolization." IEEE Open Journal of the Communications Society 2 (2021): 2372-2382.

[8] Guo, L. Xue, Y. Zhang, Q. and Zhang, X. (2019) 'A Two-Way VoLTE Covert Channel with Feedback Adaptive to Mobile Network Environment', IEEE Access, Vol.7, pp.122214–122223.

[9] Tan, Y.-A. Zhang, X. Sharif, K. Li, Y. Liang, C. Zhang, Q. (2018) 'Covert Timing Channels for IoT Over Mobile Networks', IEEE Wireless Communication., Vol.25, No.6, pp.38–44.

[10] Deng, Dan, Xingwang Li, Shuping Dang, M. Cenk Gursoy, and Arumugam Nallanathan. "Covert communications in intelligent reflecting surface-assisted two-way relaying networks." IEEE Transactions on Vehicular Technology 71, no. 11 (2022): 12380-12385.

[11] Tian, Jing, Gang Xiong, Zhen Li, and Gaopeng Gou. "A survey of key technologies for constructing network covert channel." Security and Communication Networks 2020 (2020): 1-20.

[12] Bao, Jiaxu. "Research on the security of elliptic curve cryptography." In 2022 7th International Conference on Social Sciences and Economic Development (ICSSED 2022), pp. 984-988. Atlantis Press, 2022.

[13] Al-Eidi, S. Chen, Y. Darwish, O. and Husari, G. (2021) 'SnapCatch: Automatic Detection of Covert Timing Channels using Image Processing and Machine Learning', IEEE Access, Vol.9, pp.177–191.