Detection and Defense Mechanisms for Covert Timing communications

Vrushali Uday Uttarwar, Dhananjay M.Dakhane

Ramrao Adik Institute of Technology, D.Y. Patil Deemed to be University, India
Email: uttarwarvrushali@gmail.com

Abstract: This study presents a literature overview on methods for discovering and removing covert channels. Data transmission methods known as covert channels take advantage of system resources already in place but weren't intended for this purpose, such as firewalls, to transport data undetected. By setting up a seemingly secure channel of communication between two parties, sensitive information could be leaked from the more secure party to the less secure party. Using a shared network, two parties can easily communicate and exchange information to send confidential data without being detected. As a result, discovering covert communications is difficult. Network protocols place restrictions on Covert Storage Channels (CSC), preventing it from deviating from a set of guidelines. On the other hand, CTCs have stochastic behavior, which makes detection more challenging. Analysis of the state of art systems is done in this paper & it is found that the most likely option is an active warden which is a specialized network security system that is designed to filter out a range of irregularities seen in network data.

Keywords: Covert channel detection, Timing channel, Network security, Active warden, Detection methods.

1. Introduction

Covert channels, according to Lampson, are ones that aren't even meant to be used for information transit [1]. A device called a covert channel can be used to get around security precautions by letting information leak to an unauthorized party. To evade detection by network security measures such as firewalls, data transmission methods known as "covert channels" exploit system resources not anticipated for information transfer. By setting up a seemingly secure channel of communication between two parties, sensitive information could be leaked from the more secure party to the less secure party. Utilizing a shared network, two entities seeking to transmit confidential information can seamlessly converse and exchange data undetected. As a result, discovering concealed communications is difficult.

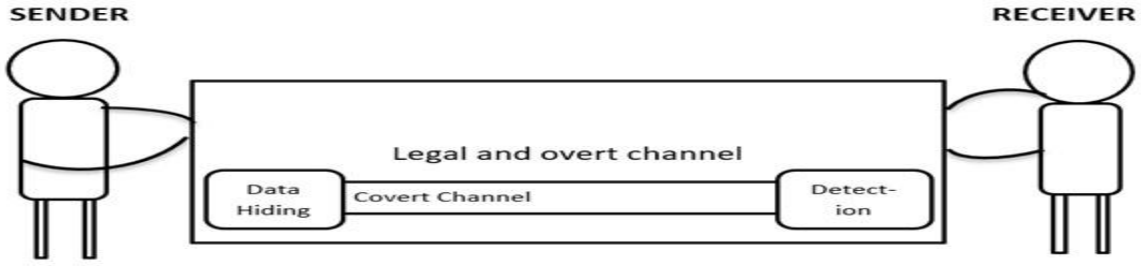

Figure 1.1: Covert Communication

Timing channels and storage channels are the two main categories of covert channels-based on how the information is hidden. One process writes to a storage place directly or indirectly, and another process reads directly or indirectly from the storage site. This is known as a storage channel [2]. In a timing channel, the sender adjusts its energy usage in order to provide a signal that can be received and decoded

by a receiver. Variable packet transmission rates, inter-packet times [3], and packet sorting [4] can be utilized for secret timing channel data encoding.

To encrypt storage channels in networks (TTL, TOS, ID, Checksum, etc.), senders can employ packet lengths or packet header information, while receivers can decode covert information using the same network objects. Network protocols place restrictions on Covert Storage Channels, preventing them from breaking the regulations. As a result, finding them is simpler in comparison. On the other hand, CTCs have stochastic behavior, which makes detection more challenging. The following measures can be done if a channel poses a risk to the protected system: removal, limitation, and detection. The design phase must identify and delete numerous covert channels as is practical. By standardizing and encrypting traffic (including protocol headers, packet sizes, and inter-packet delays), networks can be rendered invisible. The capacity of a channel should be reduced through restricting techniques if it cannot be eliminated. Numerous variables influence the performance of a network-timed hidden channel:

1. State of the network
2. Efficiency of the transmission and reception devices
3. The algorithmic complexity
4. The language's adaptability to different environments

An active warden is the most likely alternative. A specific network security system called an "active warden" is intended to filter out a variety of anomalies seen in network data. A particular type of network security system known as a "active warden" is designed to screen out various irregularities seen in network data. Active wardens can alter the data they possess. In order to reduce CTC (covert timing channel), active wardens might be used.

2. LITERATURE SURVEY

The literature survey is divided into various categories based on covert channel detection and elimination methods.

i. Storage and Timing covert channels:

Building automation systems (BAS) covert/side storage channels are described as being eliminated by the building-aware active warden, according to the author in [7]. To eliminate harmful (covert) components from communications, active wardens are a common tactic pertaining to steganography and covert channels in networks. New products, such as the network-aware active warden, have been created recently. The active warden concept suggested here is a network-aware variation considering building automation. A building's security can be improved with the help of active wardens who are aware of the building and can either comply with automated directives from users or ignore them altogether. It built a building-aware active warden and gave a single programming interface for applications by enhancing a building automation interoperability platform that supported hardware from two manufacturers. Later, Cabuk developed the time-replay channel, a more advanced covert timing channel approach, in [8]. According to a mutually agreed upon threshold, the sender and receiver divided the inter-packet delay sequence into two parts (S0,S1). To transmit a bit 0, the sender randomly repeats two inter-packet delays from the first segment S0, and to transmit a bit 1, the sender randomly replays a bit from the first segment S1.

This work [14] investigates various forms of covert network storage channels, demonstrates how to build a network traffic dataset that includes covert channels, and uses supervised machine learning to provide a general, technique that does not rely on any particular protocol to detect hidden storage channels in a network. By using the recommended generic detection model, fewer techniques may be required to block covert channel communication in network traffic. Testing datasets are available for additional investigation upon request and include storage covert channels in the following protocols: Internet Protocol (IP), Transmission Control Protocol (TCP), and Domain Name System (DNS).

Authors in [17] normalize incoming & outgoing network data before using an active warden to eliminate all practical storage-based hidden routes. Particularly designed for TCP sequence numbers, this field serves as the highest capacity conveyance for a storage-based hidden channel. According to experiments, the active warden paradigm maintains overt communication while reducing covert communication by up to 99 percent. In order to create a stealth communication infrastructure, the author [18] publishes a novel attacker model that seeks to transform FL systems into covert channels. The fundamental idea is that a malevolent sender can taint the global model by delivering purposefully produced samples during federated training. Even while the effects of model poisoning are negligible to

other participants and have no impact on the performance of the model as a whole, a malicious receiver may be able to detect them and use them to communicate a single bit.

In order to identify different types of covert timing channels, the author presents a new entropy-based method [25]. Based on the fact that the entropy of the first process is uniquely affected by the construction of a covert timing channel, researchers have devised a critical signal for identifying these channels. Proceeding from this discovery, the study investigates the role of entropy and conditional entropy in uncovering hidden temporal channels. As a result, test findings demonstrate that our entropy-based technique is capable of reliably detecting and detecting existing covert timing channels. One way to set up a secret timing channel is to sort packets. Because there are n! possible ways to arrange n packets, the maximum number of bits that may be sent is log2n!. The first packet order must be determined using per-packet sequence numbers in this method. The payload is left untouched because the technique just modifies the sequence numbers. SVM classifier algorithms were used by the authors of [26] to successfully categorize Covert Storage Channels. By utilizing an SVM-based pattern classifier, the authors show how to locate covert channels that make use of TCP/IP header information such IP Identification and Sequence Number. They cannot, however, simply be lengthened to make room for Covert Timing Channels.

In [27], we are given a system for dynamically controlling the flow of information that minimizes and eliminates termination and timing channels that are at odds with one another and allows termination and timing to be determined by hidden values. The division of potentially sensitive activity into several threads appears to be how concurrency is used. Our method compels any thread that notices these properties to modify its information-flow labels in line with the change, avoiding leaks to lower-labeled contexts, even though thread closure and timing may reveal hidden values. This method is put into use in a Haskell library, and its value of it is shown by creating a web server that limits untrusted web programs through information-flow control.

There is no interference, but it is easy to distinguish between overt and covert transmission, when the threshold is equal to or more than the twofold average interarrival period for overt traffic [28]. In addition to highlighting the challenges of creating suitable detection algorithms in such situations, this shows how difficult it is to anticipate covert timing channels with a packet delay threshold that is equal to or lower than the average of overt traffic interarrival delays.

Using the active warden concept, the authors of [30] dealt with the covert storage channel, which is concerned with aspects of covert channel behavior, by encoding covert messages in the TCP Sequence number field. An active warden normalizes incoming and outgoing network traffic to remove any potential covert pathways based on storage. It was created specifically for TCP sequence number since it has the most space available for a storage-based covert channel. Their approach destroys covert communication while having no effect on open communication.

This innovative encoding method creates imitations of acceptable traffic actions by starting with mimic functions. It also creates and employs a mimicking architecture that allows for the automatic construction of this brand-new sort of covert timing channel. Finally, to confirm the effectiveness of our imitating method, it uses state-of-the-art detection tests. The results of the experiment indicate that the planned covert timing channel may efficiently evade detection tests and still achieve a significant channel capacity [34]. The author invents and develops a secret TCP/IP timing channel [35]. This could be used to figure out how fast a hidden channel leaks data. It also demonstrates how the traffic patterns of the covert timing channel may be computationally made to blend in with ordinary traffic, avoiding discovery. It demonstrates significant performance improvements above the state-of-the-art in terms of both data rate & covertness, illustrative of the effectiveness of our method.

ii. Creation of covert channel:

Researchers in [60] offer a method for building a covert channel over a LAN by utilising the IP version 4 Timestamp option's Overflow field. The timestamp option is used in this technique to provide storage-based network steganography as well as to debug and measure over networks. By using permissible values in the Overflow field, we can make covert communication more difficult to identify.

In [62], the authors present a method for setting up a covert channel via a local area network using the Overflow field of the Internet Protocol, version 4, Timestamp alternate. This method implements storage-based network steganography by using the timestamp option for network measurement and debugging. Since authors used legitimate Overflow values, it can be challenging to spot any potential for clandestine communication.

In [61] author proposes a threshold secret sharing and chaos theory-based NCTC detection approach. Using chaos theory, we can reconstruct a space with high dimensions for stages from a low-dimensional series of times, allowing us to recover the channels' distinctive and stable characteristics. Then, using the secret restoration procedure from threshold secret sharing, a channel identifier is created in order to achieve the mapping of channel attributes to channel identifiers. According to experimental findings, the approach can dependably identify a variety of NCTCs and can greatly improve adaptation and resilience.

iii. Elimination and Limitation of covert channels:

This study's focus [13] is on finding and eliminating these types of data-hiding techniques in photographic images. It especially refers to the active warden issue, which is a method for suppressing any covert communications that may be taking place within host media. The conventional state-of-the-art approaches view the concealed information as a noise-like component despite extensive research in the literature, and as a defence they include de-noising algorithms, loss reduction, or noise addition. Lesser Components Distortion (LCD), a novel method that will be presented in this work, prevents clandestine communication while minimizing distortion on the host medium. Comprehensive testing has demonstrated that it is significantly more effective than typical attacks against steganography techniques in general, despite the fact that it is based on knowledge gained from important studies in the spread spectrum steganography field.

iv. Using machine learning techniques, covert timing channel detection:

This approach [9] trains a model based on machine learning with a collection of data on the time-frequency and payload size as features, then utilizes 10-fold cross-validation to enhance model performance. With an Area Under Curve (AUC) of 0.9737 and an accuracy for detection of 0.96, the experimental results show that the model performs well in the detection task. In this study, we investigate the challenge of creating secret keys over a public one-way state-dependent discrete memoryless channel. The channel state can be read by the warden, an enemy, at [10]. It develops an adaptive protocol that, if used in the situations that we expressly outline, not only enables the transmitter and authorized recipient to exchange the secret key but also conceals its use from the active warden. It partially covers the hidden secret key capability when used with passive adversaries that have no impact on the channel state. When the capacity of the covert channel and the capacity of the hidden secret key are equal, "free" secrecy is created.

In order to find hidden timing channels, the authors of [16] suggested exploiting the time delay between packets. A covert time channel detecting strategy is proposed using the k-Nearest Neighbour (kNN) algorithm. Using a range of characteristics related to the time interval and payload length as features, this method trains a machine learning model before performing 10-fold cross-validation to enhance model performance. The KNN algorithm was used to create a covert timing channel detecting method that performs better. However, over time, attackers have started to consider methods to evade the statistical evaluation of the covert timing channel and the attributes created by authors for the covert timing channel.

In [19] it provides a revolutionary generic hierarchical-based methodology for the identification of covert time channels. At progressively higher hierarchical stages of the detection process, a variety of statistical metrics are used to examine the inter-arrival times flows. The root of average mean error (RAME) is one of the statistical indicators that are taken into account, along with the mean, median, standard deviation, entropy, and others. Real statistics metrics timing channel occurrences are compiled into a covert and overt channel dataset. The produced dataset can be configured to be both flat, with statistical metrics calculated for every data movement, or hierarchical, with statistical metrics calculated for every stream of data at five levels of structure. Five distinct datasets were created using this technique, and a deep neural network-based system was trained and tested using them. The hierarchical strategy outperformed the flat one by 4–10% (in terms of accuracy), and it had a quick model training time (in terms of seconds), according to the findings of the accuracy and model training time performance tests. In terms of accuracy, which might range from 2.3 percent to 12 percent based on the kernel employed, and model time for training (a few seconds vs several hundreds of seconds), the deep neural network classifier fared better than the Support Vector Machine (SVM) classifier. The importance of the metrics used at each stage of the detection technique is also examined in this study.

The authors of [20] created a generic hierarchical based model to identify covert timing channels based on an expanded set of statistical metrics. The detection process requires looking at a variety of statistical markers at progressively higher levels of the flows of inter-arrival time. The following statistical

parameters are among those taken into account: mean, median, standard deviation, entropy, and Root of Average Mean Error (RAME). According to the performance findings, the hierarchical approach outperforms the at-one method in terms of accuracy and model training time. An overview of hidden channels in TCP/IP networks was given by the author in [21]. A quick explanation of the TCP and IP protocols is given before a discussion of the many kinds of covert channels and how to configure them in TCP/IP networks follows. The various methods for identifying and removing covert channels are then discussed. Researchers have developed an indirect covert channel that makes use of the relationship between a host's CPU temperature and the number of packets it processes per time unit, as well as how the temperature affects the host's system clock skew [22]. To receive and deliver packets to the covert sender and recipient, an intermediate is required. The hidden sender has two choices: communicating with the middleman by transmitting packets or remaining silent. A sequence of timestamps in the packets the intermediary sends are examined by the covert receiver to ascertain the clock skew of the intermediate.

To send encrypted messages, covert channels leverage side channels within an already-existing network infrastructure. They've been incorporated into portions of network resources that weren't designed with communication in mind in the first place. As a result [31], standard security tools like firewalls are unable to recognize them. Because they have the ability to elude detection, covert channels pose a severe security risk. So it's crucial to find them and stop them. However, there isn't a widely used method for finding a variety of hidden channels. The author provides a Support Vector Machines (SVM)-based solution for the accurate identification of covert communications [31]. The machine learning architecture classifies the traffic as overt or covert using fingerprints generated from the data under inspection. Our classifier was trained and evaluated using signatures from four well-known and distinct covert timing channel techniques. It has been shown that, even when the size of the covert message is reduced, the machine learning architecture is still capable of blindly recognizing hidden channels.

In [51] authors examined machine learning-based TCC detection situations and the viability of applying learning machine algorithms for identifying TCCs in the presence of various covert channel parameters, including flow capacity and encoding scheme.

3. Methodologies for detecting covert timing channels:

To identify such activities using IPD distributions of network traffic, the authors of this study [5] propose a novel approach called CTC Real-Time Detection (CTCRTD). The authors present and employ three distinct non-parametric statistical methodologies to provide distinct statistical test scores for overt and covert traffic IPDs. The novel detection technique is based on two key benefits: To begin with, the innovative detection technique may discover a number of CTC algorithms that have comparable effects on the IPD distributions of network traffic. Second, with the least amount of delay between the start of covert activity and the moment of discovery, the detection technique locates covert communication using real-time network data. According to the results, the innovative detection technique can detect covert communication activity and distinguish between overt and covert network traffic in 90% of situations [3]. The creation of a basic synchronized covert timing channel that employed an on-off switching mechanism to insert hidden binary bits into legitimate communication within a predefined time frame. The transmitter represents the first bit in the covert data by broadcasting a packet once every specified amount of time. To show that a bit is zero, it doesn't send any packets. After that, the receiver periodically scanned the traffic stream for newly arriving packets and decoded each bit as a 0 or 1. The notion behind this approach is really intriguing and it uses a simple encoding process. However, this method demands that the transmitter and recipient be completely in sync.

By advancing our knowledge of CTC detection techniques, our research advances their state-of-the-art [6]. The efficiency of three common methods for identifying CTCs—Jitterbug, model-based CTC (MB-CTC), and time-replay CTC (TR-CTC)—will first be carefully examined. A realistic corporate environment with substantial traffic traces is used for the performance analysis. The application, computational complexity, and classification rates of the detection algorithms are assessed for each of the three groups of CTCs. In addition to examining current strategies, the author suggests a novel shape test based on Welch's t-test and evaluates how well it performs in comparison to other detection techniques. It demonstrates that Welch's t-test's classification rate is at least comparable to other existing methods of detection while requiring less computational power. The Welch's t-test performs better at

detecting Jitterbug than the CCE test, but the CCE test performs better at detecting the TR-CTC than the Welch's t-test.

The Kolmogorov-Smirnov (K-S) shape test was recommended by the authors of [11] as a way to identify hidden temporal channels. The K-S test was utilised to determine the dissimilarity between the empirical distributions of illegal and authorised traffic. When there is a significant gap between the two distributions, it suggests that there are covert timing channels operating in legal traffic. The authors of [12] suggested certain traffic normalization strategies to restrict covert timing channels. The inter-packet delays must be completely normalized in order to get rid of covert timing channels. However, because it severely reduces the communication channel's capacity, this technique should only be used if the loss of a minor quantity of data is intolerable. In the opposite case, partial inter-packet times normalising techniques can be used to limit the capacity of a hidden channel.

In paper [15] goal is to examine trends and issues related to the creation of barriers against the most prevalent network covert routes. To accomplish this, it conducted an analysis of the pertinent literature with an emphasis on approaches that may effectively be utilized to pinpoint risks or broad injection mechanisms found in the wild. The focus has been on highlighting directions that should be looked at when creating mitigation strategies or organizing research to counter the rising tide of malware with information-hiding capabilities. The research reveals that many works are highly specialized and that it could be advantageous to take a high-level and universal strategy to addressing the security issues brought on by network hidden channels. Moreover, strategies to mitigate ambiguity exploitation should be incorporated into protocol and service design at the earliest stages.

The concept of "Minimum Requisite Fidelity" (MRF), which is a degree of signal fidelity that is detrimental to covert communications but acceptable to end users, is put forth. To obstruct subliminal information on unstructured carriers lacking objective semantics, wardens may employ strategies such as introducing cacophony. On the other side, similar tactics can impede covert exchanges between structured carriers using precise semantics. As a result, it uses a specification-based method to determine MRF [23]. In addition to creating software to take advantage of these channels and implementing an active warden to prohibit them, it employs MRF to reason about the possibility of inserting covert or subliminal information in network protocols. For unstructured carriers, human perception is a barrier to MRF, but for structured carriers, we have great confidence that a warden can rule out any latent or covert channels because of the well-known semantics. The establishment of covert channels using packet length is the subject of research [24], which explores new developments, tactics, and defences. The study also offers a technique for deleting lengthy packet-length hidden channels. The suggested method has already been tried out and used in real-world situations.

A novel image-based method for fully automatic CTC localization and identification is presented in [29]. Since hidden channels provide traffic that can be turned into vibrant graphics, that is how it operates. The method aims to automatically identify and locate the malicious component, defined as a group of packets, within the traffic based on this observation.

This method [29] identifies the hidden nodes within traffic flows to mitigate the QoS loss that occurs when complete traffic flows are blocked upon discovering hidden channels. It has the ability to turn traffic ownerships into vibrant images and then extract attributes from those images to detect traffic invisibly. It creates a classifier with these qualities based on a sizable data collection of covert and overt communication. With detection accuracy for cautious CTCs of 95.83% and covert traffic accuracy for 8-bit hidden messages of 97.83%, this system outperforms conventional statistical-based solutions.

Micro protocols are frequently tucked away in the hidden bits of a covert channel's payload and offer capabilities like dynamic routing, session management, and dependable data transmission for network covert channels. These characteristics make it possible for malware, in particular botnets, to communicate in a flexible & discrete way. Although there are a number of ways to combat network hidden channels, these techniques fall short when it comes to thwarting micro protocols. In [32] author makes the first attempt to categorize and develop workable defenses against micro protocols that may someday impair sophisticated covert channel communication. The author devised safeguards for the micro protocol-based apps Smart Covert Channel Tool and Ping Tunnel. The policies appear to be more successful in blocking micro protocols compared to existing ones that do not specifically target micro protocol activity, according to the data.

A taxonomy that enables a thorough description and interpretation of warden traits was proposed by the authors in [33]. They found flaws in the present regular (active but static) warden tactics, such as their inability to successfully thwart an adaptive situation involving clandestine communication parties. They

built a dynamic warden that can make it harder for adaptive covert communication parties to learn how to normalize themselves and severely restrict their capabilities. Additionally, they proved that adaptive covert communication parties can be blocked with far fewer active normalization rules.
Using the packet delay distribution, the authors of [36] distinguished hidden timing channels as either deterministic or non-deterministic and offered a method for determining the maximum transmission capacity in these channels. To conceal covert communication, methods similar to those described in [37] for encrypting binary symbols are given, with a predefined short delay in time signaling bit 0 and a predetermined duration delay signaling bit 1.
A unique image-based approach to completely automatic CTC recognition and localisation was introduced by the author in [49]. The tactic is based on the realization that traffic generated through hidden channels can be converted into coloured visuals. This insight served as the basis for the suggested solution, which aims to identify and pinpoint the malicious component (i.e., a set of packets) within a traffic flow. The suggested solution reduces the reduction in service quality brought on by stopping the full traffic flow in which covert channels are found by finding the covert portions within it. The authors first transform internet flows into coloured images in order to identify covert traffic, and then they extract features from the coloured images. We use a sizable dataset of covert and overt communication to train a classifier. This method performs remarkably well, outperforming common statistical-based solutions with detection accuracy for cautious CTCs of 95.83 percent and covert traffic accuracy for 8-bit covert messages of 97.83 percent.
A normalization protection mechanism against concealed channels is built and tested by the author in [50]. After looking at full and partial standardization, determining the capacity of the remaining covert channel in the occurrence of counteraction, and comparing the parameters, the best counteraction tool parameters are determined.
In [52], the author proposes a novel approach to CTCs detection that uses time series symbolization. Each discrete value in the sampled IATs is handled as a status after being first turned into a symbolic time series. After then, the status transition probability matrix (STPM) is generated by adding all the instances at which one state changes into another. Finally, it determines a similarity score to distinguish between the sampled IATs' overt and covert labels. Results from experiments on detection accuracy demonstrate that our approach beats traditional methods in a perfect network environment, with an average accuracy of about 96 percent.
In [53], authors looked into ways to calculate covert channel capacity while accounting for stochastic delay generation and network traffic conditions. The research focuses on scenarios in which a network has normal and exponential distributions in the time intervals between packet sending and receiving. Authors examined ways to assess covert channel capacity while accounting for network traffic situations in [54]. In this analysis, we focus on scenarios in which network packet sending and receiving times follow normal and exponential distributions, respectively. Data security, capacity, timing channel, delays, normal distribution, and exponential distribution.
It is also possible to send authentication information over covert channels. Several methods have been devised for presenting open firewall ports to authorized external users as closed while nevertheless allowing them access. Sending the authentication data across covert channels is one method, known as port knocking [55]. Using covert channels and steganography, Mazurczyk et al. suggested connecting control information, such as authentication data, to the actual data flows [56].
In [57], the author used the Linux kernel's new code augmentation feature, the enhanced Berkeley Packet Filter (eBPF), to show how this may be done automatically to track and record the actions of software processes. To show the adaptability of the strategy, researchers looked at two real-world use cases that employed two different attack tactics, namely two processes cooperating via file system manipulation and covert message-passing efforts embedded within IPv6 traffic flows. In [58] it provides a revolutionary generic hierarchical-based methodology for the identification of covert timing channels. In the detection process, the cross-temporal flows are analyzed using a set of quantitative measurements at progressively higher hierarchical levels. Several statistical measures are analyzed, including means, medians, standard deviations, entropy, and root-mean-squared errors (RAME). Real statistics metrics timing channel occurrences are compiled into a covert and overt channel dataset. Some traffic normalization techniques are recommended by the author [59] in order to reduce covert timing channels. Utilizing the counteraction strategies was suggested, and their impact on the capacity of the communication channel was evaluated.

Attacks that use information concealment to gain access to ICS typically result in significant damage. In order to accomplish total protocol compliance while also investigating embedding capacity, authors [63] demonstrated how 18 well-known patterns for data hiding in networks may be used with protocols found in ICS networks. Additionally, they used the Modbus/TCP example to show how information might be subtly embedded and retrieved. If the warden has any reason to suspect the presence of a hidden communication, we also provide a first inkling of warden-compliance (conspicuousness). They present an open-source software-based evaluation platform that facilitates assessment for a practical analysis. Based on a survey carried out, the following analysis is drawn considering different parameters:

Table I: Comparative analysis of covert channel detecting methods

Detection Technique	Method/ Algorithm of Detection	Covert Channel Type
[39]	Active Warden	Storage covert channel (TCP sequence)
[40]	ISN generation model, neural network	TCP/IP
[41]	Markov model, Kullback-Leiblei(KL)	TCP
[25]	Entropy-Based	Timing covert channel
[5]	Spearman Rho Test, Mann–Whitney-Wilcoxon (MWW) Rank Sum Test	Timing covert channel
[11]	Kolomogorov-Smirnov (K-S) shape test	Timing covert channel

Table II: Analysis of existing covert channel detection machine learning methods

Author	Machine Learning Approaches, Advantages, Limitations	Covert Channel Type
[65]	In this research, we analyzed DNS covert traffic and retrieved variables that help distinguish between covert and overt DNS traffic. For detection, a stacking-based machine learning classification ensemble model is employed. There is a merger of three classifiers: SVM, KNN, and Random Forest. The suggested model has a 99% detection accuracy rate. Although stacking techniques can improve classification accuracy, they may increase network performance overhead when compared to individual methods. This means that, especially in large networks, evaluating the model's efficiency is crucial.	DNS Covert Channel
[66]	This thesis anticipates covert storage traffic that inserts covert messages into the identification (ID) field of the internet protocol (IP) header using a detection method based on a logistic regression classifier. Using real-world network traffic samples to build their dataset, they were able to produce covert traffic by encoding bits in the ID. Each network packet carries two bytes of covert traffic. Results demonstrated astonishingly high accuracy rates for even the smallest hidden message, out of four tested sizes (4, 16, 64, 256 bytes). Nevertheless, their method of detection is limited to a basic hidden channel.	Covert channel storage (IP header ID)
[67]	An LSTM (long short-term memory) model was implemented for the detection of DNS covert channels. The datasets utilized in this study were generated through the application of various DNS covert channel tools, which include Iodine, Dnscat2, Dns2tcp, DNShell v1.7, Ozymandns, Cobaltstrike, DNSExfiltrator, and DET. The tools were utilized to simulate DNS-hidden traffic, while Wireshark was used to capture the data. The proposed model contains a single hidden layer. The achieved accuracy rate is 99.38%. The performance of this method exceeded that of the CNN model. It has been asserted that various techniques for identifying DNS tunneling, including this method, are effective in detecting tunneling traffic associated with viruses. However, these techniques rely on characteristics that can be easily obscured by advanced DNS tunneling methods[68].	DNS covert channel
[69]	The authors proposed [69] a technique to speed up the identification of covert timing channels by leveraging the hierarchal entropy algorithm. The parallelization of the detection of covert time channels was accomplished using the MapReduce technique. They fabricated a large dataset of elapsed times between arrivals and seeded it with hidden timing messages encoded in a variety of ways. After that, they looked for the message's position within the dataset. The MapReduce-based hierarchical entropy method outperformed	Storage covert channel

	its sequential counterpart in its ability to uncover secret timed messages.	
[70]	The hyper technique for feature selection utilizes C4.5 decision trees and the information gain method. This research presents an NB classifier-based detection strategy for hidden storage channels in the IPv6 protocol. The study found that IPv6 is vulnerable to covert channel attacks and proposed using the machine learning method stated earlier to detect these attacks. Compared to the other classification models used in this investigation, the suggested detection method exhibited better accuracy and lower false positive error rates. Even though they took unqualified properties into account, their suggested model could only detect covert channels using ICMPv6 packets.	Storage covert channel in IPv6
[71]	In this work, covert traffic was predicted using a random forest (RF) classifier. The ensemble classifier RF uses the bagging approach as its foundation. Ensemble classifier techniques usually achieve high accuracy compared to single classification models, especially in complicated network environments. Particularly in complex network contexts, ensemble classifier algorithms typically achieve high accuracy relative to single classification models. The RF classifier outperformed the SVM classifier in the author's comparison of their performances. The authors further asserted that their proposed classifier could identify unidentified CTCs when they tested it using three untrained CTCs, based on their actual experimental data. The results verified their assertions of strong performance. However, their model has a significant false positive (FP) rate, resulting in a high fraction of ordinary traffic being misclassified as covert traffic.	Four types of CTCs

Table III. Performance Analysis based on classifiers

Classifiers	Performance key indicators Training size: 70% Testing size: 30%		
	Recall	Precision	Accuracy
Stack	98%	98%	98%
Neural Network (NN)	97.9%	97.9%	97.9%
Naive Bayes (NB)	97.8%	97.8%	97.8%
Logistic Regression (LR)	97.8%	97.9%	97.8%
Random Forest(RF)	94.2%	94.2%	94.2%
SVM	96.8%	96.9%	96.8%
Decision Tree (DT)	88.3%	88.4%	88.3%
KNN	67.3%	80.2%	67.3%

Table IV. Performance Analysis based on classifiers

Classifiers	Performance key indicators Training size: 90% Testing size: 10%		
	Recall	Precision	Accuracy
Stack	98.9%	98.9%	98.9%
Neural Network (NN)	98.9%	98.9%	98.9%
Naive Bayes (NB)	98.8%	98.8%	98.8%
Logistic Regression (LR)	98.6%	98.6%	98.6%
Random Forest(RF)	96.4%	96.4%	96.4%
SVM	96.9%	97.1%	96.9%
Decision Tree (DT)	87.5%	87.6%	87.5%
KNN	68.6%	80.7%	68.6%

Fig 1.2: Classifier Accuracy

4. RESEARCH FINDING

The demand for security policies that guarantee the confidentiality, integrity, and accessibility of information has increased due to the quick development of computer networks. Due to this, hackers are now looking for ways to circumvent security measures and steal data utilizing network covert channel techniques. The primary premise of covert channel detection techniques is the identification of any behavior that deviates from the norm.

Signatures are used by today's generation of network systems for anomaly detection to classify data as either normal or abnormal according to a specified pattern. Despite advancements in statistical and machine learning methods, these tools are not yet capable of detecting every known and unknown kind of attack.

The establishment of covert channels imitates legal traffic and sidesteps all of these measures. Recognizing and understanding the mutual understanding between a sender and a receiver can be difficult. It cannot be straightforward, and it might be complicated as a result of a number of variables. Additionally, the sender may examine the network traffic to determine the basis for possible communications. Only when there is a high volume of traffic is the sender permitted to send information; avoid sending at odd times.

Contemporary detection techniques and methodologies offer solutions tailored to specific objectives rather than tackling the issue comprehensively. Moreover, the study clearly indicates that solely entropy-based approaches and their adaptations have been analyzed. There is a significant necessity to investigate computational and physiologically based approaches to address the issue comprehensively and reduce covert communications.

5. CONCLUSION

The technologies that are currently being used for identifying covert communications are thoroughly reviewed in this research. Using network resources already in place, such as packet headers and timing information, covert channels enable data transport. These are the tools that weren't developed with the goal of being utilized in communication. As a result, they are undetectable by traditional techniques. For instance, firewalls are an essential security precaution. If used maliciously, it creates a security concern. Therefore, it is crucial to have a generalized technique that can identify concealed communication in network data. This experiment also assesses the capability of machine learning algorithms for detecting covert channel attacks. This paper provides a high-level introduction to the topic of covert channel assaults and highlights its prevalence in today's prevalent technologies, such as the Internet of Things (IoT), the IPv6 protocol, and Voice over LTE (VoLTE) systems. This demonstrates the vulnerabilities of such systems and methods to covert channel assaults, as well as the opportunities they provide for constructing a wide range of such attacks, each of which presents its own unique challenges. With an emphasis on both their benefits and drawbacks, this survey work has made a contribution by evaluating the efficiency of machine learning algorithms in combating covert channel attacks.

References

[1] Lampson, B. W. A note on the confinement problem / B. W. Lampson // Communications of the ACM. | 1973. | P. 613-615.

[2] Ahsan, K. Practical data hiding in TCP/IP / K. Ahsan, D. Kundur // Proc. ACM Wksp. Multimedia Security. - 2002. - 8 p.

[3] Cabuk, S.; Brodley, C.E.; Shields, C. "IP covert timing channels: Design & detection", In Proceedings of the 11th ACM Conference on Computer & Communications Security, Washington, DC, USA, 25-29 October 2004; pp. 178-187.

[4] Ahsan, K. Practical data hiding in TCP/IP / K. Ahsan, D. Kundur // Proc. ACM Wksp. Multimedia Security. -2002.

[5] F. Rezaei, M. Hempel & H. Sharif, "Towards a Reliable Detection of Covert Timing Channels over Real-Time Network Traffic," in IEEE Transactions on Dependable & Secure Computing, vol. 14, no. 3, pp. 249-264, 1 May-June 2017, doi: 10.1109/TDSC.2017.2656078.

[6] Archibald R, Ghosal D, A Comparative Analysis of Detection Metrics for Covert Timing Channels, Computers & Security (2014), doi: 10.1016/j.cose.2014.03.007.

[7] S. Wendzel, "Covert & side channels in buildings & the prototype of a building-aware active warden," 2012 IEEE International Conference on Communications (ICC), 2012, pp. 6753-6758, doi: 10.1109/ICC.2012.6364876.

[8] Gianvecchio, S.; Wang, H.; Wijesekera, D.; Jajodia, S. Model-based covert timing channels: Automated modeling & evasion. In International Workshop on Recent Advances in Intrusion Detection; Springer: Berlin, Germany, 2008; pp. 211-230.

[9] Jiaxuan Han, Cheng Huang, Fan Shi, Jiayong Liu, Covert timing channel detection method based on time interval & payload length analysis, Computers & Security (2020), doi: https://doi.org/10.1016/j.cose.2020.101952

[10] M. Tahmasbi & M. R. Bloch, "Covert Secret Key Generation With an Active Warden," in IEEE Transactions on Information Forensics & Security, vol. 15, pp. 1026-1039, 2020, doi: 10.1109/TIFS.2019.2932906.

[11] Liu, Y.; Ghosal, D.; Armknecht, F.; Sadeghi, A.R.; Schulz, S.; Katzenbeisser, S. Robust & undetectable steganographic timing channels for id traffic. In International Workshop on Information Hiding; Springer: Berlin, Germany, 2010; pp. 193-207.

[12] Artem Sokolova, Konstantin Kogosa Inter-packet delays normalization to limit IP covert timing channels, Procedia Computer Science 169 (2020) 400-406

[13] Bisio, Igor, Fabio Lavagetto, Giulio Luzzati, & Andrea Sciarrone. "A Novel Active Warden Technique for Image Steganography." In 2016 IEEE Global Communications Conference (GLOBECOM), pp. 1-6 IEEE, 2016.

[14] M. A. Ayub, S. Smith & A. Siraj, "A Protocol Independent Approach in Network Covert Channel Detection," 2019 IEEE International Conference on Computational Science & Engineering (CSE) & IEEE International Conference on Embedded & Ubiquitous Computing (EUC), 2019, pp. 165-170, doi: 10.1109/CSE/EUC.2019.00040.

[15] Caviglione, L. Trends & Challenges in Network Covert Channels Countermeasures. Appl. Sci. 2021, 11, 1641. https://doi.org/10.3390/app11041641

[16] Jiaxuan Han, Cheng Huang, Fan Shi & Jiayong Liu, "Covert timing channel detection method based on time interval & payload length analysis".

[17] D. M. Dakhane & P. R. Deshmukh, "Active warden for TCP sequence number base covert channel," 2015 International Conference on Pervasive Computing (ICPC), 2015, pp. 1-5, doi: 10.1109/PERVASIVE.2015.7087183

[18] Costa, Gabriele, Fabio Pinelli, Simone Soderi, & Gabriele Tolomei. "Covert Channel Attack to Federated Learning Systems." arXiv: 2104.10561 (2021).

[19] Darwish, Omar, Ala Al-Fuqaha, Ghassen Ben Brahim, Ilyes Jenhani, & Athanasios Vasilakos. "Using hierarchical statistical analysis & deep neural networks to detect covert timing channels." Applied Soft Computing 82 (2019): 105546.

[20] Omar Darwish, Ala Al-Fuqaha, Ghassen Ben Brahim, Ilyes Jenhani, Athanasios Vasilakos, "Using hierarchical statistical analysis & deep neural networks to detect covert timing channels".

[21] Dakhane, D. M., Swapna Patil, & Mahendra Patil. "Detection & elimination of covert communication in transport & internet layer-A Survey." IJCA Proceedings on International Conference on Recent Trends in Information Technology & Computer Science (ICRTITCS-2011). 2012.

[22] Shorouq Al-Eidi, Omar Darwish, Yuanzhu Chen, & Ghaith Husari, SnapCatch: Automatic Detection of Covert, Timing Channels Using Image Processing & Machine Learning, Digital Object Identifier 10.1109/ACCESS.2020.3046234

[23] Fisk, G., Fisk, M., Papadopoulos, C., & Neil, J. (2002, October). Eliminating steganography in Internet traffic with active wardens. In International workshop on information hiding (pp. 18-35). Springer, Berlin, Heidelberg.
[24] M. A. Elsadig & Y. A. Fadlalla, "A balanced approach to eliminate packet length-based covert channels," 2017 4th IEEE International Conference on Engineering Technologies & Applied Sciences (ICETAS), 2017, pp. 1-7, doi: 10.1109/ICETAS.2017.8277839.
[25] S. Gianvecchio & H. Wang, "An Entropy-Based Approach to Detecting Covert Timing Channels," in IEEE Transactions on Dependable & Secure Computing, vol. 8, no. 6, pp. 785-797, Nov.-Dec. 2011, doi: 10.1109/TDSC.2010.46.
[26] Ahsan, K. Practical data hiding in TCP/IP / K. Ahsan, D. Kundur // Proc. ACM Wksp. Multimedia Security. | 2002. | 8 p. T. Sohn, J. T. Seo, & J. Moon, a study on the covert channel detection of TCP/IP header using support vector machine," in Proc. 5th Int. Conf. Inf. Commun. Secur., 2003, pp 313-324.
[27] Stefan, D., Russo, A., Buiras, P., Levy, A., Mitchell, J.C. & Mazieres, D., 2012. Addressing covert termination & timing channels in concurrent information flow systems. ACM SIGPLAN Notices, 47(9), pp.201-214.
[28] H. Qu, Q. Cheng, and E. Yaprak, ``Using covert channel to resist DoS attacks in WLAN," in Proc. ICWN, 2005, pp. 38-44.
[29] S. Al-Eidi, O. Darwish, Y. Chen & G. Husari, "SnapCatch: Automatic Detection of Covert Timing Channels Using Image Processing & Machine Learning," in IEEE Access, vol. 9, pp. 177-191, 2021, doi: 10.1109/ACCESS.2020.3046234.
[30] Dhananjay M. Dakhane; Prashant R. Deshmukh, Active warden for TCP Sequence Number base Covert Channel, DOI: 10.1109/PERVASIVE.2015.7087183
[31] P. L. Shrestha, M. Hempel, F. Rezaei & H. Sharif, "A Support Vector Machine-Based Framework for Detection of Covert Timing Channels," in IEEE Transactions on Dependable & Secure Computing, vol. 13, no. 2, pp. 274-283, 1 March-April 2016, doi: 10.1109/TDSC.2015.2423680.
[32] J. Kaur, S. Wendzel & M. Meier, "Countermeasures for Covert Channel-Internal Control Protocols," 2015 10th International Conference on Availability, Reliability & Security, 2015, pp. 422-428, doi: 10.1109/ARES.2015.88.
[33] Wojciech Mazurczak, Stefen Wendzel , Mehdi Chourib , Jorg Keller, “Countering adaptive network covert communication with dynamic wardens”, https://doi.org/10.1016/j.future.2018.12.047
[34] Wang, J., Guan, L., Liu, L., & Zha, D. (2014, May). Implementing a Covert Timing Channel Based on Mimic Function. In International Conference on Information Security Practice & Experience (pp. 247-261). Springer, Cham.
[35] S. H. Sellke, C. Wang, S. Bagchi & N. Shroff, "TCP/IP Timing Channels: Theory to Implementation," IEEE INFOCOM 2009, 2009, pp. 2204-2212, doi: 10.1109/INFCOM.2009.5062145.
[36] Yao, L.; Zi, X.; Pan, L.; Li, J. A study of on/off timing channel based on packet delay distribution. Comput. Secur. 2009, 28, 785-794.
[37] Berk, V.; Giani, A.; Cybenko, G.; Hanover, N. Detection of covert channel encoding in network packet delays. In Rapport Technique TR536; de l University de Dartmouth: Hanover, NH, USA, 2005; Volume 19.
[38] WJ Buchanan, & D Llamas, "Covert Channel Analysis & Detection with Reverse Proxy Servers using Microsoft Windows", Proc. IEEE Computer Society Symposium on Research in Security & Privacy, pp. 56-64, 1994.
[39] Cabuk. S, Brodley. C, & Shields. C, "IP Covert Timing Channels: Design & Detection ", Proc. of the lith ACM conference on Computer & communications security, pp. 178-187, 2004.
[40] Tumoian. E, "Network Based Detection of Passive Covert Channels in TCP/IP ", In Proceedings of the IEEE Symposium on Security & Privacy, 2006.
[41] Zhai. J, Liu. G, & Dai. Y, "A Covert Channel Detection Algorithm Based On TCP Markov Model", International Conference on Multimedia Information Networking & Security, 2010.
[42] Ahsan. K, "Covert Channel Analysis & Data Hiding in TCP/IP", Proc. 18th Annual Computer Security Applications Conference (ACSAC), pp. 109-118, 2002.
[43] Bidou. R Raynal. F, "Covert Channels", ACM Conference on Computer & Communications Security, pp. 178-187, 2004.
[44] Daemon9, & Alhambra, "Project loki: Icmp tunneling”, Phrack Magazine, VoL7, 1996.
[45] Lan. L, Linglin. X, & Wenhong. W, "Covert channel detection based on scale-free networks theory", 2nd International Symposium on Computational Intelligence and Design, 2009
[46] Chauhan. S, "Project Report: Analysis & Detection of Network Covert Channels", Proc. 18th Annual Computer Security Applications Conference (ACSAC), pp. 109-118, 2002.
[47] Berk. V, Giani. A, & Cybenko. G, "Detection of Covert Channel Encoding in Network Packet Delays" Department of Computer Science - Dartmouth College Technical Report TR536, 2005.
[48] Jadhav. M, & Kattimani. S, "Effective detection mechanism for TCP based hybrid covert channels in secure communication", proceedings of icetect, 2011.

[49] Al-Eidi, Shorouq & Darwish, Omar & Chen, Yuanzhu & Husari, Ghaith. (2020). SnapCatch: Automatic Detection of Covert Timing Channels Using Image Processing & Machine Learning. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.3046234.
[50] D. Frolova, K. Kogos & A. Epishkina, "Traffic Normalization for Covert Channel Protecting," 2021 IEEE Conference of Russian Young Researchers in Electrical & Electronic Engineering (ElConRus), 2021, pp. 2330-2333, doi: 10.1109/ElConRus51938.2021.9396163.
[51] Epishkina, M. Finoshin, K. Kogos & A. Yazykova, "Timing Covert Channels Detection Cases via Machine Learning," 2019 European Intelligence & Security Informatics Conference (EISIC), 2019, pp. 139-139, doi: 10.1109/EISIC49498.2019.9108873.
[52] S. Wu, Y. Chen, H. Tian & C. Sun, "Detection of Covert Timing Channel Based on Time Series Symbolization," in IEEE Open Journal of the Communications Society, vol. 2, pp. 2372-2382, 2021, doi: 10.1109/OJCOMS.2021.3118697.
[53] Belozubova, K. Kogos & A. Epishkina, "On/Off Covert Channel Capacity Limitation by Adding Extra Delays," 2021 IEEE Conference of Russian Young Researchers in Electrical & Electronic Engineering (ElConRus), 2021, pp. 2318-2322, doi: 10.1109/ElConRus51938.2021.9396545.
[54] Anna Belozubova, Konstantin Kogos, "How to limit capacity of timing covert channel by adding extra delays", Procedia Computer Science, Volume 190, 2021, Pages 64-70, ISSN 1877-0509,https://doi.org/10.1016/j.procs.2021.06.008.
[55] R. deGraaf, J. Aycock, and M. Jacobson Jr., ―Improved Port Knocking with Strong Authentication, Proc. 21st Annual Computer Security Applications Conf., Dec. 2005.
[56] W. Mazurczyk and Z. Kotulski, ―New Security and Control Protocol for VoIP Based on Steganography and Digital Watermarking, tech. rep., Institute of Fundamental Technological Research, Polish Academy of Sciences, June 2005.
[57] Luca Caviglione, Wojciech Mazurczyk, Matteo Repetto, Andreas Schaffhauser, Marco Zuppelli, Kernel-level tracing for detecting stegomalware & covert channels in Linux environments, Computer Networks, Volume 191, 2021, 108010, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2021.108010.
[58] Omar Darwish, Ala Al-Fuqaha, Ghassen Ben Brahim, Ilyes Jenhani, Athanasios Vasilakos, Using hierarchical statistical analysis & deep neural networks to detect covert timing channels, Applied Soft Computing, Volume 82, 2019, 105546, ISSN 1568-4946, https://doi.org/10.1016/j.asoc.2019.105546.
[59] Artem Sokolov, Konstantin Kogos, Inter-packet delays normalization to limit IP covert timing channels, Procedia Computer Science, Volume 169, 2020, Pages 400-406, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2020.02.236.
[60] Punam Bedi, Arti Dua, Network Steganography using the Overflow Field of Timestamp Option in an IPv4 Packet, Procedia Computer Science, Volume 171, 2020, Pages 1810-1818, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2020.04.194.
[61] 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), 2020, pp. 2380-2384, doi: 10.1109/ITNEC48623.2020.9085024.
[62] Punam Bedi, Arti Dua, "Network Steganography using the Overflow Field of Timestamp Option in an IPv4 Packet"Procedia Computer Science, Volume 171, 2020, Pages 1810-1818, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2020.04.194.
[63] Kevin Lamshöft, Jana Dittmann, "Assessment of Hidden Channel Attacks: Targeting Modbus/TCP", IFAC-Papers Online, Volume 53, Issue 2, 2020, Pages 11100-11107, ISSN 2405-8963.
[64] A. Salih, X. Ma, and E. Peytchev, "Detection and classification of covert channels in IPv6 using enhanced machine learning," in Proc. Int. Conf. Comput. Technol. Inf. Syst. (ICCTIS), Dubai, UAE, 2015, pp. 1-7.
[65] P. Yang, Y. Li, and Y. Zang, "Detecting DNS covert channels using stacking model," China Commun., vol. 17, no. 10, pp. 183-194, Oct. 2020.
[66] T. A. V. Sattolo, "Real-time detection of storage covert channels," Ph.D. dissertation, Dept. Syst. Comput. Eng., Carleton Univ., Ottawa, ON, Canada, 2021.
[67] S. Chen, B. Lang, H. Liu, D. Li, and C. Gao, "DNS covert channel detection method using the LSTM model," Comput. Secur., vol. 104, May 2021, Art. no. 102095.
[68] 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, pp. 1203-1217, Jun. 2021.
[69] O. Darwish, A. Al-Fuqaha, G. Ben Brahim, M. Javed, Using MapReduce and hierarchical entropy analysis to speed-up the detection of covert timing channels, in: 13th IEEE International Wireless Communications and Mobile Computing Conference, IWCMC 2017, 2017, pp. 1102–1107.
[70] A. Salih, X. Ma, and E. Peytchev, "Detection and classification of covert channels in IPv6 using enhanced machine learning," in Proc. Int. Conf. Comput. Technol. Inf. Syst. (ICCTIS), Dubai, UAE, 2015, pp. 1-7.
[71] Q. Li, P. Zhang, Z. Chen, and G. Fu, "Covert timing channel detection method based on random forest algorithm," in Proc. IEEE 17th Int. Conf. Commun. Technol. (ICCT), Oct. 2017, pp. 165-171.