Chapter

Network Covert Channels

Muawia Elsadig

Abstract

With the rapid advancement of communication and computer network technologies, covert channels are now more secure, quicker to set up, harder to detect, and easier to design than ever before. By breaking a system security policy, a covert channel can be utilized to leak confidential communications. Undoubtedly, one of the most difficult challenges is still detecting such harmful, unobservable, and covert dangers. Due to the fact that this danger takes advantage of techniques not intended for communication, it is invisible to conventional security solutions. This chapter offers a concise overview of covert channel concept, techniques, classifications, and countermeasures, emphasizing how new technologies are vulnerable to being exploited for initiation of different covert channels and how they offer a rich environment for developing effective but challenging covert channel attacks. It gives a comprehensive review of common covert channel countermeasures with more focus on machine learning detection techniques. Although some research studies have revealed beneficial uses of covert channel, which is natural given that many approaches have a double-edged sword impact, this chapter focuses on covert channels as a security threat that compromise our data and networks.

Keywords: covert channel, network covert channel, data hiding, information security, network security, cybersecurity, machine learning, security, covert storage channel, steganography, covert timing channel

1. Introduction

A communication channel between two parties (sender and recipient) that are not permitted to exchange information is known as a covert channel [1]. A significant area of study in information concealment is covert communication, which uses hidden routes to send information covertly. When people are communicating covertly, their relationship can be safeguarded and confidential information cannot be reached, detected, or recovered by unauthorized parties [2]. On the other hand, a covert channel provides an open avenue for hackers to spread destructive activity or leak private information without being discovered [3].

Attackers are increasingly using steganographic and information-hiding tactics to evade detection and stay undetected for extended periods of time. They have, for example, been used to exfiltrate secret information in Advanced Persistent Threats (APTs), conceal the presence of malware within seemingly innocent images, and conceal malicious code or extra functionalities with the goal of implementing covert

multistage loading architectures. Creating covert channels is one of the most common and successful techniques of information concealment to promote insecurity [4].

The expansion of computer networks and intrusion detection systems has given rise to creative methods by which hackers might pilfer or reveal sensitive data. A network hidden channel or covert channel may be used to do this, which is a useful bonus.

With a covert channel, people may share secret information while being invisible to one another. In addition to being used for the transmission of secret information, covert channels may also be used to transmit malware, Trojan horses, viruses, and other threats in a fashion that evades detection by standard firewalls or detection programs. When such harmful acts are paired with a covert channel, the combination is considered a major threat.

Cabaj et al. stated that fraudsters have employed a variety of information-hiding strategies with evil intent. Among other possible techniques, attackers are increasingly using network covert channels to mask their harmful activity, such as downloading more malware modules or exfiltrating sensitive and private data. It should be noted that this trend is anticipated to continue, and the digital forensics and security industries will face significant challenges as there is a rise in the use of advanced covert channel techniques for harmful purposes [5]. Cabaj et al. further stated that in order to facilitate hidden data exchange, attackers can use Distributed Network Covert Channels (DNCCs), which are defined as network covert channels that disperse secret data among numerous flows, protocols, and hosts or that employ a variety of data hiding methods within a single flow or within Protocol Data Units (PDUs). The security industry is paying more attention to DNCCs these days since they give the attacker the following advantages: (i) they allow sending of smaller parts of secret data *via* a variety of covert channels, which can increase the overall stealth and bandwidth of the concealed connection, and (ii) they enable getting beyond protective measures that are already in place, which make it harder to detect these types of covert channels.

Steganographic material was previously communicated using invisible ink or concealed tattoos. These days, steganography may be easily communicated with thanks to computer and network technology. The military, intelligence operations, and online social networks can all benefit from the usage of covert channels to ensure user privacy or coordinate protests and so on [6].

In certain situations, a covert channel can be used to conceal secret messages rather than posing a threat. For example, a network administrator may utilize a covert channel to safeguard network management communications from hacker assaults. In addition, for several security techniques, like copyright protection, network authentication, cybercrime evidence, and so forth, covert channel technology has emerged as a cutting-edge technique [7]. Although many research studies have revealed beneficial uses of covert channels [8–10], they pose real security challenge and risks.

This section provides an overview, definitions, and important concerns related to the idea of covert channels. Furthermore, it emphasizes that covert channels are not always dangerous; in fact, their technology may be used for security objectives, as copyright defense, network authentication, cybercrime evidence, and other security strategies have found new applications for covert channels. The remaining part of the chapter is presented as follows: Section 2 divides covert channels into two categories, one classifies covert channels into two classes, covert storage channels and covert timing channels, while the second classifies them in three classifications: host-based, network-based, and physical. Subsequently, Section 3 addresses network covert channel classification. The typical covert channel model is illustrated in Section 4.

Section 5 outlines some factors that are behind the advanced development of covert channels and have direct impact in their widespread, while Section 6 discusses the prevalent of covert channel techniques in modern technologies and how they may offer a rich environment for creating many scenarios of covert communication that can have both beneficial and detrimental effects. Section 7 illustrates the countermeasures that are commonly used to counter covert channel, while Section 8 gives through and comprehensive details on covert channel identification methods with a focus on their achievements and drawbacks. A discussion and recommendations are provided in Section 9, while the chapter is concluded in Section 10.

2. Type of covert channels

A communication channel used to leak confidential information in a manner that is against security policy of a system is known as a covert channel. It is a highly hazardous, undetectable, persistent, and evolving threat that eludes detection technologies and presents a real challenge [11]. The idea of a covert channel was initially presented by Lampson [12]. Basically, covert channels can be classified into two types: covert timing channels and covert storage channels [13]. A method that lets one process to write to a shared storage location and permits another process to read from that storage location is considered a covert storage channel [14]. Both the read and write processes might run on a single computer setting or on a networked system. The operations of encoding secret information into network protocol fields (sender) and receiving the information back (receiver) are referred to as network covert storage channels. Two methods may be used to achieve it: the first modifies packet header information (such Internet Protocol ID, Time to live (TTL), and Type of Service (ToS)); the second modifies the length of the packet. In covert timing channels, a sender conveys secret data through the manipulation of packets, frames, or message timing; the intended recipient can then observe and decode the covert data. Covert timing channels also can exist in a networked or single-machine environment [13].

This categorization makes two configurations for a covert channel possible: a networked system and a stand-alone system. The secret data is sent between entities in the stand-alone system, whereas the secret data is sent *via* the network in a system that is network-based [15]. The research community first concentrated on what are known as local covert channels, which allow two processes with varying security levels to communicate to each other and exchange data. A process with a high security level usually divulges information to a process with a low security level. The emphasis has switched to network covert channels, where covert data may be encoded into a network protocol, as a result of the emergence and quick growth of computer networks [16].

Miketic et al. [1] indicated that host-based, network-based, and physical are the three basic categories into which covert channels fall. The timing and storage characteristics of the host system are usually altered in host-based covert channels. Network-based covert channels allow devices connected to a network to communicate with each other by modifying a portion of the network traffic. Lastly, using physical sources or side-channel signals (such as power, temperature, electromagnetic radiation, or optical) to transmit and encode data is known as physical covert channel. To ensure a dependable communication channel, physical covert channels need a certain level of closeness between the transmitter and receiver components. **Figure 1** shows the aforementioned three types of covert channel, which include host-based, network-based, and physical covert channels.

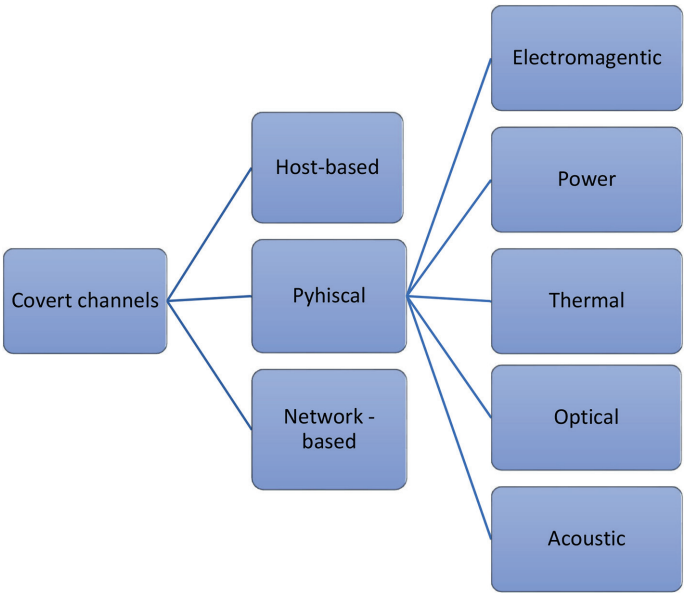

Figure 1.
Covert channel types [1].

3. Network covert channel classification

Network covert channels are information exchange channels that let two processes on the network to connect in a way that is beyond the system's security guidelines. In 1987, Grilling expanded the idea of a covert channel to include networked computer settings. In a local area network, Grilling created the first network covert channel. Hackers and steganographers have been inspired to create various network covert channel scenarios by the quick evolution of network protocols and methods. This has led to the development of several network-based covert channel approaches [17].

Network covert channels are often classified into two types: network covert timing channels and network covert storage channels [18, 19].

Encoding covert data into network protocol fields by a sender and receiving it back by a receiver are the two activities that make up a network covert storage channel. Through adjusting packets, frames, or message timing, a sender can transmit secret information and the intended recipient can then watch and decode the concealed data. These two activates of the sender and recipient make up a network covert timing channel. Network covert timing channels may be used maliciously to spread malware, plan attacks, and steal secrets, all of which pose major risks to cybersecurity [20].

Two methods are available to achieve network covert storage channels: the first modifies packet header information (such Internet Protocol ID, Time to live (TTL), and Type of Service (ToS)); the second modifies packet length. It is evident that network covert storage channels have a substantially larger bandwidth than the covert timing channels. As a result, network covert storage channels have drawn greater attention than their time channels. They pose a severe risk and have the potential to cause major security lapses.

Wendzel et al. [16] divide network covert storage channels into two categories: (i) techniques that change header fields or other non-payload elements and (ii) techniques

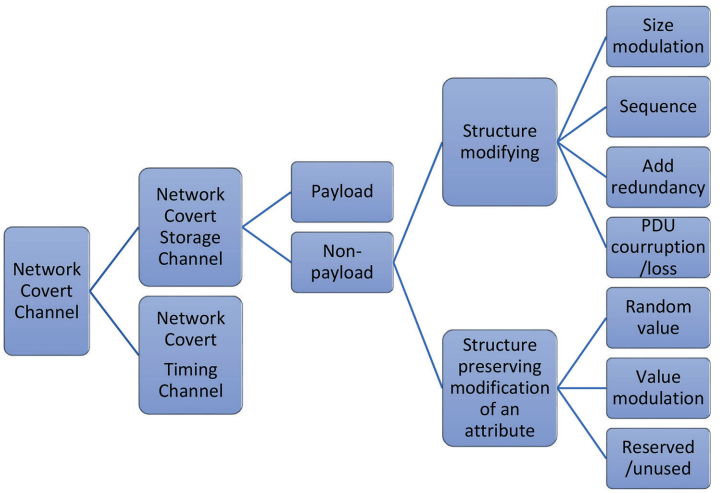

Figure 2.
Network covert channel classification.

that conceal covert messages into the payload section. Moreover, seven patterns are used to categorize the non-payload techniques. These seven categories include random value, add redundancy, sequence, size modulation, value modulation, and reserved/unused. In terms of network covert timing channels, Wendzel et al. classified them into four categorization patterns that include retransmission, PDU order, rate, and inter-arrival time. **Figure 2** shows the classification of network covert channels.

4. Typical covert channel model

Simmons [21] described the prisoner's dilemma that serves as an example of a typical or common covert channel scenario.

Two prisoners named Alice and Bob want to talk to each other so that they may plot their escape. However, Wendy, a third party, keeps an eye on the potential

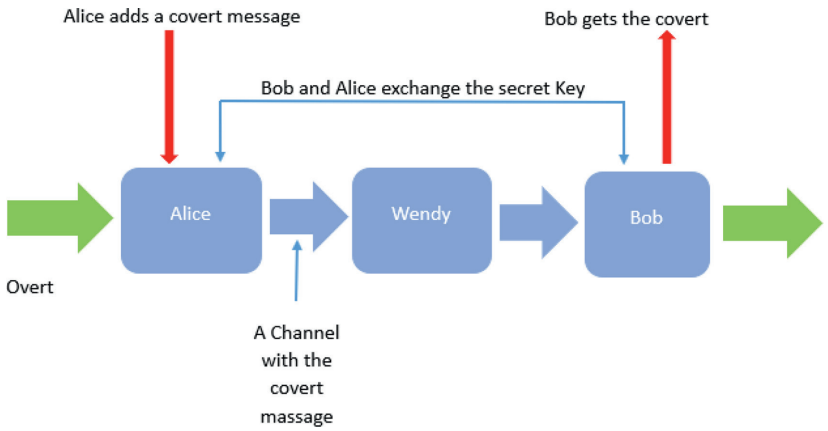

Figure 3.
Typical covert channel model.

communication channel between them. Alice and Bob will be placed in solitary confinement without the ability to share information if Wendy or the warden discovers any suspicious activity on this channel. In order to communicate covertly, Alice and Bob must attempt to conceal the information they transmit in a way that Wendy cannot discover. By supposing that Alice and Bob are communicating *via* two networked computers, this scenario may be adapted to network covert channels [22]. The covert channel model is depicted in **Figure 3**.

5. Factors behind the advanced development of covert channels

The following points are a summary of some significant elements that are crucial in the development of covert channel techniques [23]:

- The rapid advancement of cloud computing, virtualization technologies, communication protocols, data centers, and network technologies. This cutting-edge research offers a wealth of opportunities to create various covert channel strategies.

- Techniques known as switching that enable a covert channel to change how it appears inside a particular protocol or from one protocol to another. This technique helps in creating covert channels that are difficult to discover.

- Internal control protocol technology that offers a trustworthy and dependable channel of communication for a covert message. This method employs a micro protocol to provide dynamic routing and dependable communication to a covert message.

6. Covert channels and modern technology

This section discusses the prevalence of covert channels among modern technologies and how these modern technologies offer a rich environment for creating many scenarios of covert communication that can have both beneficial and detrimental effects.

Khulaidi et al. indicated that scholars are increasingly focused on the threat posed by covert channels. These channels have an impact on emerging technologies including smart grid, VoIP, IoT, LTE, and IoUT [24].

The development of covert channels has been facilitated by IoT applications and related new technologies. There are a lot of covert communication techniques that take use of IoT protocols.

Network interfaces on the majority of Internet of Things (IoT) devices make them publicly accessible. These devices are typical in that they lack proper security measures and have limited resources, including memory, computing power, and batteries. As a result, they can be taken advantage of by many kinds of assaults.

Tan et al. [25] provided evidence of how IoT settings are susceptible to covert timing channels. They examined five techniques to building covert time channels for the Internet of Things. These five channels are based on scheduling, packet loss, rate switching, packet reordering, retransmission, and packet switching. Each of these covert channels operates differently.

Message Queuing Telemetry Transport (MQTT) is a lightweight client–server message transport protocol that is particularly well-suited for machine-to-machine and Internet of Things (IoT) connectivity. It is appropriate for high-latency and low-bandwidth situations, push communications, enterprise backends to mobile communications, and devices with limited resources. MQTT version 5.0 was examined by Mileva et al. [26] to see if it could be exploited by covert channels. It was discovered that some features in this version might be used to set up several covert channels.

Numerous covert channels that exploit Constrained Application Protocol (CoAP) were presented in [27]. CoAP is a web transfer protocol that is utilized for constrained networks and devices. It is among the protocols that will be most frequently abused in the upcoming years.

This indicates the continued advancement of covert channels and their deployment capabilities despite the sophisticated development of network techniques, particularly the Internet of Things, which has evolved into a widely used communication platform.

Despite the fact that IoT security has been the subject of several studies, not much attention has been paid to assessing the potential effectiveness of the covert channels threat in IoT contexts [5].

Permissionless blockchain is a potential option for covert communication because it is an emerging network application with qualities like decentralization, immutability, anonymity, and security. Wide access, large capacity covert channels, information concealment and identity anonymity, and resilient communication channels are among the benefits of blockchain technology for covert communication. Zang et al. [2] investigated covert channels across several blockchain layers and identified six types of covert channels in contract layer, network layer, data layer, and motivation layer of blockchain. A great medium for covert communication is the blockchain network [28].

A framework for covert channels based on blockchain that attempts to get beyond censorship was proposed by [29]. The authors tested the functionality of a prototype system they had designed for their proposed covert channel. The prototype is durable, efficient, and unobservable, according to the results obtained as indicated by the authors.

By investigating twenty-two years of traffic, Żórawski et al. addressed the Internet's vulnerability to covert channels. Evidence suggests that the opportunities for setting up covert channels are many and have changed throughout time. One-fits-all solutions are not practical; thus, as part of ongoing cybersecurity monitoring, there should be a periodic quantification of the information that may be concealed in traffic [30].

7. Countermeasures

Merely safeguarding communication content is no longer enough to satisfy the present standards for information security. Traditional encryption approaches and physical layer security strategies try to stop eavesdropping on communication content. However, meeting the current standards for information security requires more than just safeguarding communication content. Certain sensitive information may still be leaked *via* metadata, such as network traffic patterns, even when the data is encrypted [31].

The ability to fully understand covert channel techniques is essential for developing countermeasures. Computer network communication technology is developing

so quickly; therefore, it is not logical to try to fully eliminate or prove the nonexistence of all potential covert channels. Alternatively, techniques to reduce or deteriorate the bandwidth of such covert channels have been developed [32]; however, in those cases, it is important to maintain a balance to keep the overt channel functional while attempting to reduce the covert channel capacity. Common techniques for capacity reduction or bandwidth reduction include adding noise, inserting dummy packets, limiting host-to-host connections, and establishing a fixed size for network packet length [33].

The common countermeasures for covert channels include:

i. Elimination: the process to eliminate a covert channel such as normalization of a protocol headers.

ii. Limitation: the process of limiting a covert channel bandwidth such as applying random traffic padding techniques.

iii. Audit: the process of auditing a covert channel that requires a reliable passive warden as a detection approach.

iv. Documenting a covert channel.

The majority of suggested detection strategies rely on the identification of abnormal behavior. Since the warden often understands the normal traffic patterns within a given network, it may quickly identify unusual activity resulting from covert communication. Nevertheless, these methods are unable to identify hidden traffic if there are significant changes in the normal traffic. Furthermore, it will be challenging to identify any covert traffic that resembles regular traffic.

Caviglione [4] pointed out that future research indicates that covert channels will continue to be a popular model for stegomalware empowerment and data exfiltration, new assaults will likely be more complicated, cross-layer, and capable of using the intricate interactions between hardware and software. Due to ambiguity about what to check and where to position wardens within the broader network architecture, this enlarges the gap between attackers and defenders. Caviglione pointed out the key patterns in the development of countermeasures together with the challenges that need to be overcome as follows:

- Generalization: using a variety of collecting methods and inspecting many heterogeneous carriers may be necessary for data collection, network covert channel identification, and sanitization.

- Abstraction: one intriguing method is to provide more abstract measurements that can be utilized to identify the steganographic assault regardless of the carrier that is being employed. However, this may require further security measures that degrade the performance.

- Cloud: cloud infrastructures will continue to be an important part of the Internet of the future. Recent studies have shown how cloud designs may be used to provide pathways for communication *via* the Internet. Consequently, it is imperative to safeguard cloud and virtualized systems against attacks that might conceal information such as covert network channels.

- Everything-as-a-service: the detection of covert channels needs a significant amount of processing and storage capacity. For small- to medium-sized actors, it might not be possible to operate sophisticated detection software or deploy wardens to secure large-scale networks while still providing acceptable performance. Consequently, it might be advisable to investigate Warden-as-a-Service strategies.

- Reversibility: in case of reversible network covert channels, the warden should gather communications from various network segments and do some sort of comparison. This presents a number of challenges, including legal and technical matters.

- Resistance by design: ambiguous designs or imperfect implementations are typically the cause of the capacity to store arbitrary data or alter protocols. When creating network protocols, one should take into account the patterns that serve as the foundation for the establishment of covert channels. Another interesting trend to investigate is the use of formal methods to provide a warden the capacity to do runtime checks or model unexpected risks.

In light of this, Caviglione suggests that future studies concentrate on creating more comprehensive frameworks and indications as well as strategies for simultaneously inspecting several carriers. Although there is some evidence of this tendency in the literature, it has to be strengthened in order to be useful. Educating developers and engineers about the dangers posed by network coverts channels is another worthwhile avenue to explore.

Modern malware uses information hiding to evade detection and employ a variety of deceptive and hostile techniques. Developing covert channels is turning into one of the most effective ways to obtain more harmful payloads or exfiltrate confidential data. Notwithstanding their influence on Internet security, a clear assessment of network traffic's vulnerability to covert channels is lacking. Furthermore, in order to develop countermeasures, it is essential to comprehend how the targeted protocol and its diffusion drive the hiding capacity [30].

It is preferable for individuals who emphasis on developing covert channels for legitimate use to focus their efforts on identifying the exploited vulnerabilities that lead to the creation of covert channels rather than creating covert channels for beneficial purposes. In order to overcome flaws and vulnerabilities in the system architecture or other stages of security against the possibility of a covert channel, this would be very helpful [13].

8. Covert channel detection

Techniques for using covert channels have improved the ability to carry out risky and unobserved assaults. Because they take use of methods not meant for information transmission, they are invisible to conventional security procedures [34]. There is a challenge to identify, reduce, or remove them. Several research papers demonstrate the practical application of machine learning (ML) classification techniques for the identification of covert channels. Because ML and deep learning (DL) have great accuracy and precision, studies over the last 5 years have focused on identifying covert channel using ML and DL; nevertheless, the dataset has to be improved to facilitate training and testing [24].

This section examines the benefits and drawbacks of detection techniques mostly based on ML classification models, in which recent work has been given more attention.

The Internet's core protocols are TCP/IP suite. It involves the greatest number of protocols that might be exploited by attackers *via* covert channels. Compared to other fields, a covert channel that exploits ISN field of TCP protocol appears most difficult to discover [35]. To identify ISN covert channels, Sohn et al. [36] introduced a detection technique using support vector machine (SVM) classifier. However, their approach is time-consuming and requires a significant number of both normal and malicious ISNs traffic to be trained in order to effective in identifying covert attacks [37].

The majority of detection approaches to detect network covert channel concentrate on a particular type of covert channel technique rather than focusing on the shared characteristics of several different types of covert channels. In this context, Wendzel et al. [16] categorized covert channel approaches into eleven categories in an effort to develop a mechanism to identify common behaviors of covert channels. Wendzel et al. noted that almost 70% of these methods fall into four major categories. This result aids to introduce a common framework or common frameworks to be used to develop a common detection model that is capable to identify a group of covert channels instead of a applying a single model for each covert channel. This significantly reduces the security system overhead.

A detection method that uses hierarchy and density clusters was proposed by Yuwen et al. [38]. They stated that their detection technique could identify various kinds of covert channels and could also effectively discriminate between covert and normal traffic even at channel noise rates of up to 20%.

The simplest method for removing covert channels based on packet length is usually to equalize packet lengths to their maximum length. This can unquestionably prevent packet length covert channel; nonetheless, this approach lowers network capacity and is therefore seen as insufficient. In another method, covert channels packet lengths can be restricted by limiting the range of lengths that a packet can have. This reduces the number of states that a covert message may exploit, hence limiting the capacity of the covert channel. If a packet is too small, zeroes can be appended to it as padding. This method, however, consumes the bandwidth of the overt channel. Consequently, it remains a problem to find an efficient way to reduce or limit the capacity of covert channels without compromising the capacity of overt communication. In a recent study, Elsadig et al. [39] have noted that a popular area in network security is the use of ML approaches to detect different security threats, such as covert channel assaults. As a result, they provided an ensemble approach to identify packet length covert channels. Basing their work in the fact that ensemble approaches—which combine multiple classification methods in a manner that increases their benefits and reduces their weaknesses—can yield better results. The proposed ensemble approach combines the output of several classifiers using a stacking technique. Among these classifiers are Naive Bayes (NB), Random Forest (RF), and Support Vector Machine (SVM), whereas the output of these classifiers is aggregated by Logistic Regression (LR) classifier that acts as a meta-classifier for the proposed ensemble approach. According to the published results, the proposed ensemble approach outperformed the other individual classifiers that made up the approach in terms of accuracy. It performed better than all of them, detecting covert channels based on packet length with a 98.5% detection accuracy rate. Additionally, the proposed ensemble classifier performed well in terms of recall, accuracy, and specificity.

ML techniques function only in situations where there is some variance between covert and regular communication. As a result, the ML system either loses its ability to detect covert assaults or experiences a decline in detection accuracy when an attacker tries to imitate regular traffic.

An ML algorithm must be regularly taught to maintain its performance in order for it to monitor network live traffic and be successful. If not, the algorithm's efficiency will eventually decline. Classification models must be updated and retrained on a regular basis to withstand the fast growth of both overt and covert traffic. Periodic retraining, however, increases expense and degrades network speed and service quality. Elsadig et al. [40] looked at how effective ML techniques were at identifying covert channel assaults. They gave a succinct overview of covert channel assaults, emphasizing how emerging technologies like IPv6 protocol, IoT, and VoLTE frequently employ covert channel approaches. This demonstrates how these technologies are susceptible to covert channel assaults and how they offer a rich environment conducive to the development of a wide range of challenging covert channel attacks. Elsadig et al. investigated the benefits and drawbacks of ML classification methods for thwarting covert channel assaults. Their study reported that ML algorithms can successfully meet the demands of the modern security industry while also significantly assisting in the detection of covert channel assaults; however, they reported out some issues regarding using ML classifiers to identify covet channel as follows:

- For experimentation, several authors have created their own datasets; but they are not making them publicly available. Additionally, there are several issues with current datasets, including unevenness and outdated content.

- One important question about the datasets generated is how researchers verify that the regular traffic, upon which their study is based, is, in fact, overt traffic. It is likely that there is a type of covert channel that has not been discovered yet; thus, researchers need to use several traffic samples from different networks and circumstances to corroborate their results in order to create dependable normal traffic. That means validation of a dataset is highly required, which leads to reliable findings.

Due to overlapping within the time range of normal and abnormal network traffic, it will be challenging to distinguish between the two types of traffic in covert timing channels. This overlap may occur if the packet delay threshold used to hide a covert message is equivalent to or lower than 25% of the mean of inter-arrival time of the normal network traffic. If the double mean of inter-arrival time of normal traffic is reached or exceeded by the threshold, then the overlap will not occur, and therefore, covert traffic may be easily distinguished [41]. This illustrates how difficult it is to forecast covert timing channels with a packet delay threshold of at least 25% of the mean inter-arrival time of overt traffic. This suggests that developing suitable detection techniques for these kinds of situations would likely be more challenging [40].

An approach to identify covert timing channels was put out by Al-Eidi et al. [42]. Their method is made specifically to identify covert communications using ML and image processing. The traffic's inter-arrival times were transformed into colored images. In order to identify covert channels, a variety of ML classifiers were then trained using attributes that were taken from the colored images. Furthermore, the authors suggested a method for identifying the covert data inside a traffic flow, enabling the dropping of only the portion of the flow containing the covert message

as opposed to the full flow. However, according to Ali [43], this method and the others described in [44, 45] primarily exploit the network flow's time information as a feature to identify covert timing channels that encrypt data using time. This indicates that an HTTP cookie covert channel that does not employ the time to encrypt information cannot be identified by these methods. Moreover, this approach is unreliable in cases where the behavior of a covert channel is marginally altered [46].

A stacking technique-based ensemble classification approach is introduced by [47]. Three classifiers were merged into this ensemble classifier: SVM, RF, and KNN. When compared to the techniques described in [48–51], the area under the curve (AUC) increased and reached 0.999, according to the authors. However, there is not enough indications to support the capacity of the proposed approach to identify even unknown covert or malicious traffic, despite its ability to identify two types of unknown traffic [40].

Han et al. [52] pointed out the drawbacks of a number of already available detection techniques that are intended to identify particular kinds of covert timing channels; as a result, they suggested a detection approach to address these problems. Their suggested model makes use of a KNN classifier that was trained using a number of statistical variables related to time intervals and payload lengths. Their scheme's AUC was 0.9737, and its accuracy rate was 0.96. To make sure their proposed scheme is capable to identify various CTCs, a variety of CTCs were put into practice. However, if attackers know the way to evade the statistical analysis of the covert channels, then the detection scheme may fail. Put otherwise, the detection technique breaks down when an attacker figures out how to get around the channel's statistical analysis. As a result, the extracted characteristics that are working well now could not work well in the future.

According to Wu et al. [53], there are three types of classic detection methods for CTCs: entropy-based, ML, and statistical-based methods. Ali summed up the drawbacks of the aforementioned techniques as follows:

- Less robustness: when there is none ideal network condition, for instance, jitter or packet loss, the detection accuracy of these approaches may deteriorate.

- Poor real-time performance: these techniques cannot identify CTCs quickly since they need more sampled inter-arrival times.

- Less universality: a couple of these techniques are limited to detecting a small number of distinct CTC types.

To get around these shortcomings. Wu et al. [53] proposed a time series symbolization-based detection technique for CTC identification. They convert inter-arrival times into symbolic representation using the k-Means clustering technique. Additionally, they proposed a method for calculating similarity that is based on the state transition probability model. The outcomes of their experiment demonstrated that, in optimal network conditions, the proposed detection approach may reach a 96% detection accuracy. While the proposed approach performs somewhat better than traditional approaches in the situation of existing network jitter, its performance also deteriorates noticeably with increasing network jitter.

Zillien and Wendzel [46] investigated two highly cited detection techniques: compressibility score [54] and ϵ -similarity [55]; both were proposed by Cabuk et al. Furthermore, two other new ML-based detection techniques, GAS [20] and SnapCatch [42], were examined. The authors pointed out that in the event that

a covert channel behavior is marginally altered, these approaches are unreliable. Specifically, Zillien and Wendzel showed that all these detection techniques can be evaded or the performance may be drastically decreased when faced with a straightforward covert channel, named ϵ - κ libur, although the covert channel continues to provide a high bitrate.

Using a dataset that included both malicious traffic (packet length based covert channel) and valid traffic, the authors in [40] tested and trained eight different classification models, stack, decision tree (DT), K-nearest neighbors (KNN), support vector machine (SVM), logistic regression (LR), random forest (RF), neural network (NN), and naïve bayes (NB), to examine the best model in identifying packet length covert channel. The authors categorized these classifiers into four groups, poor, moderate good, and very good, based on their findings. With very good accuracy rates over 97.5%, Stack, NB, NN, and LR outperformed the good group that includes RF and SVM. They both attained accuracy rates of 96.4% and 96.9%. The DT earned a reasonable (moderate) accuracy that reached 88.3%, while the KNN classifier lagged behind with a poor accuracy rating of 68.6%.

Sattolo [56] proposed a detection method using LR classifier to identify a covert channel that exploits ID field of the IP protocol. Their method obtained a remarkable accuracy rate to identify the aforementioned IP covert channel. However, this detection method is effective for a simple covert channel.

9. Discussion

Modern advancements in computer network and intrusion detection system (IDS) technologies enable hackers to come up with new strategies for surreptitiously leaking private data. It is argued that two users are speaking covertly or indirectly when a communication between them, or between processes acting on their behalf, violates the interpretation of a security model set by a system. A covert channel is any communication route that might be utilized by a process to transfer data in a manner that is prohibited by a system's security policy. Vulnerabilities in network protocols are a source of hidden channel abuse.

Covert channel technology has emerged as a cutting-edge technique that presents several security techniques such as cybercrime evidence, network authentication, copyright protection, and so forth. However, it would be preferable to focus on identifying the weaknesses that are subject to be exploited to create a covert attack rather than creating covert channels for beneficial purposes.

A deep comprehension of covert channel strategies and techniques is necessary to develop countermeasures for covert channels. Owing to the complexity and the advanced growth of the technology of networking and communication, seeking to completely eliminate any possible hidden channels or demonstrating their nonexistence is irrational.

It is critically necessary to put more effort to introduce alternate solutions, for instance, lowering a covert channel capacity, inspecting a covert channel, recording covert channel, and so on. Furthermore, when reducing channel bandwidth, the solution should maintain the capacity for normal traffic while reducing the bandwidth of the channel.

The effectiveness of ML algorithms to thwart covert channel assaults was explored in this chapter, with a particular emphasis on their advantages and disadvantages. The analysis concludes that ML algorithms can effectively address present security

needs in the real world and play a significant role in detecting covert channel attacks. However, when ML algorithms are used to mimic regular traffic, they either become less accurate in detecting covert channels or fail to identify them at all. Furthermore, there are several flaws in ML algorithms that let attackers launch complex assaults. Consequently, it is essential to evaluate ML technique vulnerabilities early in the development process in order to counter such attacks.

It is not feasible to have a different solution for each kind of covert channel as this might result in increasing overhead for network capacity and performance, which would lower quality of service (QoS). The majority of the detection techniques now in use are restricted to identifying particular kinds of covert channels and cannot be expanded to include more covert channels.

As a result, it is strongly advised to build multi-detection techniques that can identify many kinds of hidden channels. But as with multi-detection systems, creating such approaches calls for careful design to guarantee a high detection accuracy rate with low overheads.

Most recommended detection techniques are predicated on identifying abnormal behavior. Given its familiarity with the normal traffic patterns inside a network, the warden can detect unexpected behavior that may be the result of covert communication. However, if there are notable variations in the normal traffic, these techniques are unable to detect covert traffic. It will also be difficult to spot any covert traffic that looks like normal traffic.

Despite the fact that IoT security has been the subject of several studies, not much attention has been paid to assessing the potential effectiveness of the covert channels threat in IoT contexts. Generally, designers and developers should take into consideration in early phases the weaknesses that can be exploited by covert channel attacks.

10. Conclusion

A network covert channel provides an open avenue for hackers to spread destructive activity or leak private information without being discovered. An overview of covert channel concepts, techniques, classifications, and countermeasures is provided in this chapter, with a focus on how new technologies are often used to create covert channel assaults. This shows how they provide a rich setting for developing such attacks. This chapter provides an extensive overview of popular covert channel detection, emphasizing machine learning-based detection techniques for enhanced concentration. In addition, this chapter gives a through comprehensive investigation on the common countermeasure techniques that include elimination, limitation, detection, auditing, and documentation with a focus on their advantages and limitations. Even while several studies have shown that hidden channels can be advantageous and have emerged as a cutting-edge technique, this chapter emphases on covert channels as a threat that compromise our data and networks. There has been a thorough discussion on the risks associated with covert channels and the extent to which developers, designers, and security experts must work together to overcome any potential weaknesses than can be exploited to commit covert channel attacks.

Conflict of interest

No conflict of interest.

DOI: http://dx.doi.org/10.5772/intechopen.1005053

Author details

Muawia Elsadig
Imam Abdulrahman Bin Faisal University, Damma, KSA

*Address all correspondence to: muawiasadig66@gmail.com

IntechOpen

References

[1] Miketic I, Dhananjay K, Salman E. Covert channel communication as an emerging security threat in 2.5D/3D integrated systems. Sensors. 2023;**23**(4). DOI: 10.3390/s23042081

[2] Zhang T, Li B, Zhu Y, Han T, Wu Q. Covert channels in blockchain and blockchain based covert communication: Overview, state-of-the-art, and future directions. Computer Communications. 2023;**205**:136-146. DOI: 10.1016/j.comcom.2023.04.001

[3] Elsadig MA, Fadlalla YA. Packet length covert channels crashed. Journal of Computer Science & Computational Mathematics. 2018;**8**(4):59-66. DOI: 10.20967/jcscm.2018.04.001

[4] Caviglione L. Trends and challenges in network covert channels countermeasures. Applied Sciences. 2021;**11**(4). DOI: 10.3390/app11041641

[5] Cabaj K, Żórawski P, Nowakowski P, Purski M, Mazurczyk W. Efficient distributed network covert channels for Internet of things environments. Journal of Cybersecurity. 2020;**6**(1):tyaa018

[6] Makhdoom I, Abolhasan M, Lipman J. A comprehensive survey of covert communication techniques, limitations and future challenges. Computers & Security. 2022;**120**:102784. DOI: 10.1016/j.cose.2022.102784

[7] Elsadig MA, Fadlalla YA. Survey on covert storage channel in computer network protocols: Detection and mitigation techniques In: Proceedings of the International Conference on Advances in Information Processing and Communication Technology - IPCT 2016, Rome, Italy. 2016. pp. 79-85. DOI: 10.15224/ 978-1-63248-099-6-71

[8] Ying X, Bernieri G, Conti M, Poovendran R. TACAN: Transmitter authentication through covert channels in controller area networks. In: Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems, Montreal, QC, Canada. 2019. pp. 23-34. DOI: 10.1145/3302509.3313783

[9] Vanderhallen S, Van Bulck J, Piessens F, Mühlberg JT. Robust authentication for automotive control networks through covert channels. Computer Networks. 2021;**193**:108079

[10] Xie H, Zhao J. A lightweight identity authentication method by exploiting network covert channel. Peer-to-Peer Networking and Applications. 2015;**8**(6):1038-1047

[11] Elsadig MA, Fadlalla YA. An efficient approach to resolving packet length covert channels. In: 6th International Conference on Computer Engineering and Mathematical Sciences, Lankawi, Malaysia. 2017

[12] Lampson BW. A note on the confinement problem. Communications of the ACM. 1973;**16**(10):613-615

[13] Elsadig MA, Fadlalla YA. Network protocol covert channels: Countermeasures techniques. In: 2017 9th IEEE-GCC Conference and Exhibition (GCCCE); Manama, Bahrain; 8-11 May 2017. 2017. pp. 1-9. DOI: 10.1109/IEEEGCC.2017.8447997

[14] Hammouda S, Maalej L, Trabelsi Z. Towards optimized TCP/IP covert channels detection, IDS and firewall integration. In: 2008 New Technologies, Mobility and Security, Tangier, Morocco, 5-7 November 2008. 2008. pp. 1-5. DOI: 10.1109/NTMS.2008.ECP.101

[15] Dakhane DM, Deshmukh PR. Active warden for TCP sequence number base covert channel. In: 2015 International Conference on Pervasive Computing (ICPC), Pune, India, 8-10 January 2015. 2015. pp. 1-5. DOI: 10.1109/PERVASIVE.2015.7087183

[16] Wendzel S, Zander S, Fechner B, Herdin C. Pattern-based survey and categorization of network covert channel techniques. ACM Computing Surveys (CSUR). 2015;**47**(3):50

[17] Elsadig MA, Fadlalla YA. A balanced approach to eliminate packet length-based covert channels. In: 2017 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS), Salmabad, Bahrain, 29 November - 1 December 2017. 2017. pp. 1-7. DOI: 10.1109/ICETAS.2017.8277839

[18] Tian J, Xiong G, Li Z, Gou G. A survey of key technologies for constructing network covert channel. Security and Communication Networks. 2020;**2020**:1-20. DOI: 10.1155/2020/8892896

[19] Bedi P, Jindal V, Dua A. SPYIPv6: Locating covert data in one or a combination of IPv6 header field(s). IEEE Access. 2023;**11**:103486-103501. DOI: 10.1109/ACCESS.2023.3318172

[20] Li H, Song T, Yang Y. Generic and sensitive anomaly detection of network covert timing channels. IEEE Transactions on Dependable and Secure Computing. 2023;**20**(5):4085-4100. DOI: 10.1109/TDSC.2022.3207573

[21] Simmons GJ. The prisoners' problem and the subliminal channel. In: Advances in Cryptology. Vol. 1984. Boston, MA: Springer US; 22 Aug 1984. pp. 51-67

[22] Handel TG, Sandford MT. Hiding data in the OSI network model. In: Information Hiding. Berlin Heidelberg: Springer; 1996. pp. 23-38. DOI: 10.1007/3-540-61996-8_29

[23] Elsadig MA, Fadlalla YA. Packet length covert channel: A detection scheme. In: 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 4-6 April 2018. 2018. pp. 1-7. DOI: 10.1109/CAIS.2018.8442026

[24] Khulaidi NAA, Zahary AT, Hazaa MAS, Nasser AA. Covert channel detection and generation techniques: A survey. In: 2023 3rd International Conference on Emerging Smart Technologies and Applications (eSmarTA), Taiz, Yemen, 10-11 October 2023. 2023. pp. 01-09. DOI: 10.1109/eSmarTA59349.2023.10293582

[25] Tan Y-A, Zhang X, Sharif K, Liang C, Zhang Q, Li Y. Covert timing channels for IoT over mobile networks. IEEE Wireless Communications. 2018;**25**(6):38-44

[26] Mileva A, Velinov A, Hartmann L, Wendzel S, Mazurczyk W. Comprehensive analysis of MQTT 5.0 susceptibility to network covert channels. Computers & Security. 2021;**104**:102207

[27] Mileva A, Velinov A, Stojanov D. New covert channels in Internet of Things. In: the 12th International Conference on Emerging Security Information, Systems and Technologies - SECURWARE 2018, Venice, Italy, September 16-20, 2018. 2018. pp. 30-36

[28] Zhang P, Cheng Q, Zhang M, Luo X. A blockchain-based secure covert communication method via Shamir threshold and STC mapping. IEEE Transactions on Dependable and Secure Computing. 2024:1-12. DOI: 10.1109/

TDSC.2024.3353570. Available from: https://ieeexplore.ieee.org/abstract/document/10398427

[29] Chen Z, Zhu L, Jiang P, Zhang C, Gao F, Guo F. Exploring unobservable blockchain-based covert channel for censorship-resistant systems. IEEE Transactions on Information Forensics and Security. 2024;**19**:3380-3394. DOI: 10.1109/TIFS.2024.3361212

[30] Żórawski P, Caviglione L, Mazurczyk W. A long-term perspective of the internet susceptibility to covert channels. IEEE Communications Magazine. 2023;**61**(10):171-177. DOI: 10.1109/MCOM.011.2200744

[31] Qiao S, Zhu R, Ji X, Zhao J, Ding H. Optimization of covert communication in multi-sensor asymmetric Noise systems. Sensors. 2024;**24**(3). DOI: 10.3390/s24030796

[32] Zander S, Armitage G, Branch P. A survey of covert channels and countermeasures in computer network protocols. Communications Surveys & Tutorials, IEEE. 2007;**9**(3):44-57

[33] Elsadig MA, Fadlalla YA. Survey on covert storage channel in computer network protocols: Detection and mitigation techniques. International Journal of Advances in Computer Networks and Its Security. 2016;**6**(3):11-17

[34] Elsadig MA, Gafar A. An ensemble model to detect packet length covert channels. International Journal of Electrical & Computer Engineering. 2023;**13**(5):5296-5304. DOI: 10.11591/ijece.v13i5.pp5296-5304

[35] Zhao H, Shi Y. Q. A phase-space reconstruction approach to detect covert channels in TCP/IP protocols. In: 2010 IEEE International Workshop on Information Forensics and Security. Seattle, WA, USA, 12-15 December 2010. 2010. pp. 1-6. DOI: 10.1109/WIFS.2010.5711441

[36] Sohn T, Seo J, Moon J. A study on the covert channel detection of TCP/IP header using support vector machine. In: Information and Communications Security. Berlin, Heidelberg: Springer; 2003. pp. 313-324. DOI: 10.1007/978-3-540-39927-8_29

[37] Elsadig MA. Resolving network packet length covert channels. [Ph.D. dissertation] Computer Science and Technology. Sudan: Sudan University of Science & Technology; 2018

[38] Yuwen Q, Huaju S, Chao S, Xi W, Linjie L. Network covert channel detection with cluster based on hierarchy and density. Procedia Engineering. 2012;**29**:4175-4180

[39] Elsadig M, Gafar A. Packet length covert channel detection: An ensemble machine learning approach. Journal of Theoretical and Applied Information Technology. 2022;**100**(23):7035-7043

[40] Elsadig MA, Gafar A. Covert channel detection: Machine learning approaches. IEEE Access. 2022;**10**:38391-38405. DOI: 10.1109/ACCESS.2022.3164392

[41] Qu H, Cheng Q, Yaprak E. Using covert channel to resist DoS attacks in WLAN. In: Proceedings of the 2005 International Conference on Wireless Networks, ICWN 2005, Las Networks. Vegas, Nevada, USA, June 27-30, 2005. 2005. pp. 38-44

[42] Al-Eidi S, Darwish O, Chen Y, Husari G. SnapCatch: Automatic detection of covert timing channels using image processing and machine learning. IEEE Access. 2021;**9**:177-191. DOI: 10.1109/ACCESS.2020.3046234

[43] Yuan W, Chen X, Zhu Y, Zeng X, Yue Y. HTTP cookie covert channel detection based on session flow interaction features. Security and Communication Networks. 2023;**2023**:1348393. DOI: 10.1155/2023/1348393

[44] Al-Eidi S, Darwish O, Chen Y. Covert timing channel analysis either as cyber attacks or confidential applications. Sensors. 2020;**20**(8). DOI: 10.3390/s20082417

[45] Darwish O, Al-Fuqaha A, Ben Brahim G, Jenhani I, Vasilakos A. Using hierarchical statistical analysis and deep neural networks to detect covert timing channels. Applied Soft Computing. 2019;**82**:105546. DOI: 10.1016/j.asoc.2019.105546

[46] Zillien S, Wendzel S. Weaknesses of popular and recent covert channel detection methods and a remedy. IEEE Transactions on Dependable and Secure Computing. 2023;**20**(6):5156-5167. DOI: 10.1109/TDSC.2023.3241451

[47] Yang P, Wan X, Shi G, Qu H, Li J, Yang L. Identification of DNS covert channel based on stacking method. International Journal of Computer and Communication Engineering. 2021;**10**(2):1-15

[48] Nadler A, Aminov A, Shabtai A. Detection of malicious and low throughput data exfiltration over the DNS protocol. Computers & Security. 2019;**80**:36-53

[49] Shafieian S, Smith D, Zulkernine M. Detecting DNS tunneling using ensemble learning. Cham: Springer; 2017. pp. 112-127. DOI: 10.1007/978-3-319-64701-2_9

[50] Karasaridis A, Meier-Hellstern K, Hoein D. Detection of DNS anomalies using flow data analysis, global telecommunications conference, 2006. In: GLOBECOM'06. IEEE; 2006

[51] Farnham G, Atlasis A. Detecting DNS tunneling. SANS Institute InfoSec Reading Room. 2013;**9**:1-32

[52] Han J, Huang C, Shi F, Liu J. Covert timing channel detection method based on time interval and payload length analysis. Computers & Security. 2020;**97**:101952

[53] Wu S, Chen Y, Tian H, Sun C. Detection of covert timing channel based on time series symbolization. IEEE Open Journal of the Communications Society. 2021;**2**:2372-2382

[54] Cabuk S. Network covert channels: Design, analysis, detection, and elimination [Ph.D.]. United States -- Indiana, 3260014: Purdue University; 2006. [Online]. Available from: https://library.iau.edu.sa/dissertations-theses/network-covert-channels-design-analysis-detection/docview/305285689/se-2?accountid=136546; http://by7nn3rg6h.search.serialssolutions.com/?genre=article&sid=ProQ:&atitle=Network+covert+channels:+Design,+analysis,+detection,+and+elimination&title=Network+covert+channels:+Design,+analysis,+detection,+and+elimination&issn=&date=2006-01-01&volume=&issue=&spage=&author=Cabuk,+Serdar

[55] Cabuk S, Brodley CE, Shields C. IP covert timing channels: Design and detection. In: Proceedings of the 11th ACM Conference on Computer and Communications Security, Washington, DC, USA, October 25-29, 2004. 2004. pp. 178-187. DOI: 10.1145/1030083.1030108

[56] Sattolo TAV. Real-time detection of storage covert channels. [Ph.D. dissertation] Department of Systems and Computer Engineering. Ottawa, Canada: Carleton University; 2021