Network Protocol Covert Channels: Countermeasures Techniques

Muawia A. Elsadig
College of Computer Science and Technology, SUST.
Khartoum, Sudan.
muawiasadig@yahoo.com

Yahia A. Fadlalla
Lead Consultant/Researcher, InfoSec Consulting,
Hamilton, Ontario, Canada.
trusted_software@usa.net

***Abstract*—advanced developments in intrusion detection systems (IDS) and computer network technology encourage hackers to find new ways to leak confidential information without being detected. When the interpretation of a security model adopted by a system is violated by a communication between two users, or processes operating on their behalf, it is said that the two users are communicating indirectly or *covertly.* A network covert channel refers to any communication channel that can be exploited by a process to transfer information in a manner that violates a system's security policy. Loopholes in network protocols attract covert channel exploitation. This paper sheds light on network covert channel countermeasures and the most recent detection and prevention methods of such channels. The achievements and limitations of these countermeasures are discussed. The paper further introduces the concept of network covert channel triangle (DSM – Development, Switching, and Micro-protocol); three elements that have the most direct positive impact in a network covert channel environment. In addition, the paper reflects on the challenges such covert channels impose.**

Keywords—covert channel; security; channel detection; prevention; channel elimination; channel capacity; network protocols.

I. INTRODUCTION

A covert channel is a communication channel that allows the transfer of information between two processes on the network in a manner that breaks up the system's security policy [1, 2]. It allows people to communicate in an undetectable way to give-and-take hidden information.

A covert channel is categorized as a serious threat when exploited to pass malicious activities such as Trojans, viruses, etc. In this case the common firewalls or detection systems can't able to detect such malicious activates.

Commonly, a covert channel exists in two situations: stand-alone system and network–based system [3]. Initially, the research community focused on so-called local covert channels, in which two processes with different security levels can communicate with each other in order to leak information [4]. With the rapid development of computer networks, the focus has been shifted to a covert channel over the network in which covert information can be encoded into network protocols [5].

Covert channels in network protocols look similar to steganography techniques. Both use a carrier to send a covert message, but the nature of the carrier is different. In the case of steganography techniques, information is hidden in a carrier such as an image, video, text, sound, etc., which is known as "unstructured carrier". In network covert channel, a network protocol is used as a carrier; which is known as "structured carrier" [6, 7]. Some researchers refer to network covert channels as a type of data hiding techniques and they call it network steganography [8, 9]. To our best knowledge, the term network covert channel was coined before the term network steganography. Moreover, Zander et al. indicated that the first covert channels that based on network protocols were propsed in the time that the term "information hiding" has not yet been coined [7].

This work is mainly focused on covert channel as an effective tool to leak conditional information and threaten network security; however, from different perspective, some positive uses of covert channel are noticed as a network administrator may use it to secure the network management communications [10]. Qian et al. addressed that the technology of covert channels has become a novel method for some security approaches such as copyright protection, network authentication, cybercrime evidence, etc. [11]. In addition, some recent work seek to enhance vehicular ad hoc network security – which is considered a hot area of research that encompasses many challenges [12] – using covert channel techniques as presented in [13]. More positive uses for network covert channels can be seen in [14-21].

This section has introduced network protocol covert channels and given a general overview, definitions, and significant issues concerning them. The rest of the paper is structured as follows: the next section discusses the covert channel types. Section III sheds light on covert channel countermeasures methods that are commonly used to counter their threats. Subsequently, Section IV gives comprehensive discussions on recent related work that concerns countermeasures techniques along with their achievements and limitations. In addition, this section highlights some relevant and recent trends in network covert channels technologies. Section V concludes and introduces a noble concept: network covert channel triangle (DSM). Finally, future work is suggested in Section VI.

II. COVERT CHANNEL TYPES

This section demonstrates the two types of covert channel: covert storage channels and covert timing channels.

978-1-5386-2756-3/17/$31.00 ©2017 IEEE

A. *Covert Storage Channels*

Covert storage channels involve all methods that allow a process to write - directly or indirectly - in a shared storage location and allow another process to read - directly or indirectly - from that location [22]. These processes can be on a single computer or on multiple computers that communicate over a network (networked computers). In term of network, Network covert storage channels encompass the processes of encoding covert information into network protocol fields (sender) and retrieving back the covert information (receiver). It can be implemented through two techniques [23]: the first is based on modulating packet header fields (such as Type of Service (ToS) [24], Time to live (TTL) [25], Internet Protocol ID [26], etc.); the second is based on packet-length modification.

Obviously the bandwidth of the packet-length covert channels is significantly higher than the bandwidth of covert timing channels. Therefore, covert storage channels in networks have received more attention than timing covert channels. It represents a serious threat which can lead to significant security breaches.

Due to the variety of the network covert storage channels, Wendzel et al. sort them into two classes: (i) payload covert channels in which the covert message is hidden in the payload section of the protocol and the (ii) non-payload covert channel which alter the non-payload sections such as header fields [5]. And then Wendzel et al. sort the non-payload covert channels into seven patterns [5].

B. *Covert Timing Channels*

Covert timing channels "include all vehicles that would allow one process to signal information to another process by modulating its own use of system resources in such a way that the change in response time observed by the second process would provide information" [1]. In other words, In covert timing channels, a sender can signal information by manipulating packets, frames, or message timing; the intended receiver then observes and decodes the covert information [5, 7]. Similar to covert storage channel, covert timing channels can be found in a single computer setting or in a networked computer setting. More classification of Covert timing channels can be seen in [5], where Wendzel et al. classify them in four patterns.

III. Countermeasures

Due to the complex nature of computer network technologies, the detection and elimination of network covert channels is a real challenge. In most cases, It is difficult to attain a complete elimination of the potential covert channels [27, 28], therefore, numerous methods have been developed to mitigate the covert channel threats by reducing the covert channel bandwidth. However, these methods have impact at the system performance and usability due to their effect at the overt channel bandwidth. Therefore, an important attention should be paid to the overt channel bandwidth when trying to degrade the covert channel bandwidth.

To develop covert channel countermeasures, two processes have been proposed by Zander [7]. These processes are: (i) identifying the covert channel that being used and then (ii) applying a suitable countermeasure.

Numerous formal methods were developed to identify covert channels during the design phase or in already deployed systems. These methods can be classified into the flowing categories:

- Non-interference analysis,
- Information flow analysis,
- Covert Flow Tree (CFT) method,
- Shared Resource Matrix (SRM) method.

However, the aforementioned methods are only identified the covert channel in single host systems while there are a few work on formal techniques that dedicate to identify network-based covert channels [29].

The covert channel countermeasures are grouped into four broad categories: elimination, capacity reduction, auditing, and documenting. Interested readers can see more details in [7, 30, 31].

IV. Related Work

This section surveys and discusses recent and relevant work on covert channels countermeasures techniques along with their achievements and limitations. Moreover, it sheds lights on some covert channel recent trends. The section is organized into three subsections as follows: Section A gives comprehensive details on the recent network covert channel detection methods while section B covers network covert channel mitigation techniques. Section C is to showcase of some recent trends in covert channels.

A. *Network Covert Channel Detection*

Commonly, the signature-based approach is used as a detection approach for network covert channels. It distinguishes covert traffic from normal traffic. Schear used this approach to detect covert channel traffic [32]. However, this approach is unable to detect any covert channel which has not been found before [33].

Basing their work on Markov model, a detection algorithm for covert communication in TCP flows was developed by Zhai [34]. This detection approach attains good performance in detection of covert communication under many applications such as TELNET, SSH, SMTP, HTTP and FTP. The drawback of the aforementioned algorithm is inability to detect covert communication that uses tunneling technology.

It is commonly known that the TCP/IP protocols suite is the heart of the internet communication. However, this suite of protocols encompasses the most vulnerable protocols to be exploited by covert channel threats. As an example of these protocols, TCP protocol has a lot of fields that are vulnerable to be used for passing covert communications. The covert channel that uses the Initial Sequence Number (ISN) field of the TCP protocol is seemed the most difficult to detect

compared with the covert channels that uses other fields in the aforementioned protocol [35]. Based on the support vector machine (SVM) classification approach, Sohn et al. proposed a detection method to detect ISN covert communications [36]. However, their approach requires large amount of data for machine training purposes. It is time consuming and complicated. On the other hand, an alternative detection method for ISN covert communications based on characterizing the dynamic nature of ISNs was developed by Zhao and Shi. They used statistical classification model to identify the covert communications. Zhao and Shi claimed the well performance of this approach in detection of such type of covert channels with a few computational overheads. Furthermore, this approach can be used to monitor online traffic.

Tumoian and Anikeev proposed an ISN covert channels detection method using neural network approach [37]. The training phase is host- dependent due to the fact that the operating systems have variety of ISN values. The experimental result shows a little bit high rate of false negative which is reached up to 10%.

On the other hand, Murdoch and Lewis proposed two ISN covert channel approaches based on encoding data generated by OpenBSD and Linux operating systems [38]. They claimed that their approaches are hard to detect unless the warden knew the shared secret key. The reason for that is because the generated ISN data by the aforementioned approaches is typically closed to the normal data that generated by the genuine TCP\IP stack. So it is difficult to detect the variations that would assist in covert channel detection. In addition, the authors showed that their technique could be extended to work effectively with the other operating systems.

Covert channel techniques are rapidly developed to enhance their resistance against detection methods. Rohankar et al. pointed out the real challenge behind the developing of covert channel techniques that are based on using more than one field on a protocol for covert communications [39]. This way can strongly complicate the detection of such covert channels. Moreover, Dong et al. took different way, which is based on developing covert channel that relied on using more than one fields from different protocols to handle covert messages [40] . Dong et al. added that their covert channel is extremely hard to detect or eliminate.

A noteworthy contribution is done by Wendzel et al. trying to find out a common characteristics and behaviors of multiple covert channels instead of focusing in a single covert channel – as the traditional detection methods focused at. Wendzel et al. studied the covert channels of the period 1978 to 2013. They came up with that, about 70 % of the covert channel techniques for that given period are classified into four main classes [5]. This contribution will enhance covert channel detection methods capability and decrease the overheads that are caused by using a single detection method for each covert channel.

Due to the fact that many transmission protocols and applications are based on generating random lengths of network packets, the stenographers find their way by using these lengths to encode their secret message. In other words, a packet length is changed to transfer a secret message across the network - each packet length can encode a piece of information. Generally this type of covert technique is called packet length covert channel. Nair et al. raised up the wide spread of using this type of covert channel technique and its wide growth day by day [41].

Yao et al. proposed a packet length covert channel in which a covert message is encoded based on network packet lengths. A secret matrix of some unique lengths should be exchanged somehow between sender and receiver. The sender encodes a covert message based on the secret matrix and then the receiver retrieves the covert message using the same matrix [42]. However, this covert technique is easy to detect by detection methods that are based on comparing normal and abnormal traffic. Their covert traffic is not closely imitated the normal traffic. In contrast, Zhang et al. developed a packet length covert channel that able to generate a very close covert traffic to normal traffic which resists against the aforementioned detection methods. Zhang et al. verified their method resistance against detection [43].

In addition, another packet length covert channel that developed by Ji et al. is capable to resist against active detections [44] . This approach is based on using normal traffic as a reference to form covet traffic, so as to complicate the process of distinguishing between normal and abnormal traffic, however their technique is failed to fully imitate the normal traffic. Therefore, this weakens their technique to resist against detection. Accordingly, Ji et al. proposed another message length covert channel. They call it Normal-Traffic Network Covert Channel which indicates that their covert message is typically as normal traffic [45] . They claimed that their covert channel achieves high level of resistance against covert channel detection methods. In slightly different way, Hussain et al. proposed a network covert channel based on packet lengths and data payload [46]. It is capable to carry high bandwidth of covert data and temper resistance for network detector. This approach is used normal packet length features which are led to keep covert traffic looks similar to normal traffic.

Recently, Abdullaziz et al. proposed two packet length-based covert channels using UDP traffic [47]. As per the authors claim, the covert traffic that generated by the aforementioned approaches are very close to normal traffic. Therefore, the anomaly detection methods are failed to distinguish between normal and abnormal traffic. Moreover these approaches do not need a secret key to be shared between receiver and sender prior the transmission as many packet length-based covert channels need.

In context of packet length covert channel detection, Nair et al. developed steganalysis scheme to detect the presence of such type of covert channels based on classifying normal and malicious traffic which contains covert traffic [41]. They utilize two-dimensional feature space to get their scheme trained, which enrich its classification capabilities. Then the classifier scheme is used to separate normal and abnormal network traffic. A high accuracy of this steganalysis scheme is presented based on the authors' experimental results. In

addition, Nair et al. described their scheme as the first detection method for detecting such type of covert channels. As they indicated, no such detection scheme is presented before, therefore, no way to compare their scheme with the existing ones. However their detection scheme is only concerning packet length covert channel that based on user datagram protocol traffic. Recently, and bases on the assumption that, any change on network packet lengths to encode secret message can alter the statistical distribution of network traffic even if the amount of this change is too light, Sur et al. proposed a packet length covert channel detection scheme [48]. This scheme is also based on obtaining some features to train the scheme classifier and then the classifier is used to detect the presence of packet length covert channel. The authors demonstrated a considerable performance of their detection scheme and they claimed that their scheme could be extended to detect all types of packet length covert channels. However, their scheme is only evaluated under two types of packet length covert channels. Therefore, this claim needs to be proved as the fact that, packet lengths covert channels have different scenarios of construction.

Lu et al. explored many existing methods of packet length covert channels and highlighted some drawbacks concerning them. As an example of these drawbacks, the investigated covert channels are required for the covert message receiver to receive all packets in order [49]. Accordingly, Lu et al proposed a secure covert channel that based on secret sharing scheme. Their proposed method uses network packet length to send a secret message. The authors indicated that their covert channel can produce covert traffic that perfectly imitates normal traffic which in return leads to secure the covert channel against detention methods.

Fraczek et al. proposed many techniques for information leakage in Stream Control Transport Protocol (SCTP). The SCTP is expected to replace the Control Transport Protocol (TCP) and the User Datagram Protocol (UDP) [50].The proposed techniques are based on utilizing of the SCTP features (i.e. multi-streaming and multi-homing). This work presented significant contribution in describing numerous security attacks that may exploit the SCTP protocol and thus assist in developing detection techniques to discover such kind of attacks.

Machine learning approach is a promising area in handling different aspects of information technology and it is expected to play important role in detection of network covert channels [51]. Shen et al. proposed a covert channel detection scheme that is based on support vector machine (SVM) [52].They are basing their work on evaluating the correlation between the adjacent control fields of network packets and accordingly they can extract the effective features of the header fields. Then, based on the extracted features, the SVM is used to classify or to differentiate between covert and normal traffic and thus can detect the presence of covert channel. Successfully, this approach can detect up to ten different types of covert channels that are based on ten different TCP\IP header fields as the authors claimed. However, this approach needs to be extended to insure its capability to work with covert channels that exploit more different header fields and different protocol. As its technique is based on machine learning approach which can automatically learn and take action.

Goher et al. surveyed some covert channel detection methods and presented a comprehensive analysis of their techniques [53]. They indicate that covert channel detection approaches fall under two main types: signature based detection methods and anomaly detection methods. Accordingly they classified the surveyed methods. Based on their survey, Goher et al. pointed out that detection of hybrid covert channels is considerably difficult, as such covert channel is a combination of more than one covert channel (Timing and storage covert channel).

Rezaei et al. introduced a framework that can automatically model covert communication algorithms [54]. The framework was proposed to provide a reliable method to implement covert communication techniques. Based on the common characteristics and behaviors of covert channels, the aforementioned framework can define some common tasks and events and then convert them to executable codes. The author validated their model by implementing two selected covert channel algorithms. They insured that the extracted countermeasures and parameters from their model are the same with the theoretical expected results. Moreover this model was evaluated using real network platform [55]. Having such model can assist in analyzing and evaluating covert communication algorithms which afford better understanding of their functionality and thus help in discovering their vulnerabilities. Discovering covert algorithms vulnerabilities can gratefully help in developing detection methods to counter such threats. However, this framework is mostly dedicated for modeling covert time channels rather than covert storage channels.

In contrast to the previous framework, Fraczek and Szczypiorski proposed a framework that enables the creation of different network steganography methods utilizing network protocols as a carrier. The authors indicated that their framework can be used to build up perfectly undetectable steganography methods which refer to inability of any unlimited computational power to detect these methods [56]. May the authors developed this frame work to support security and for useful use. However, it is noteworthy to point out; the aforementioned framework is developing the creation of undetectable covert channel techniques which leads to complicate the way of developing covert channel countermeasures.

Seo et al. indicates that the number of high bandwidth overt channels is likely to growth due to the availability of faster communications and more complex processing systems [57]. On the other hand, the authors pointed out that no one solution can detect all types of potential covert channels while it is possible to train intrusion detection by all available techniques for the purpose of detection many types of covert channels. However this solution requires resources and causes more computational overheads which have high impact on the system performance. Instead, Seo et al. suggested developing a prevention system (i.e., traffic normalization) in order to mitigate potential covert channels. Connected to this suggestion, the next section of this paper surveys the recent

work in mitigation and elimination of network covert channels.

B. Network Covert Channel Mitigation and Elemination

With the emergence of computer networks in everyday activities that are benefited different aspects of human life, network covert channels have become a tremendous threat to confidentiality and integrity of information. In spite of many successful research that have been conducted in detection, elimination, mitigation and capacity reduction of such types of threat. However, the fully elimination is hard to be achieved or it affects the capacity of the overt channel communication and thus the system performance and usability. Therefore, limiting a covert channel capacity is an effective solution to mitigate covert channel threats. It is not a method for full elimination of covert channel but it can disturb the covert channel to achieve its fully task [58]. However, reducing covert channel capacity without affecting the system usability and performance is posing a real challenge. It is a matter of attaining a possible capacity reduction that effectively degrades covert channel threat with acceptable fewer effects on the system performance and usability. As an example, it is noteworthy that the full elimination of packet length covert channel can be achieved by set all packet lengths to maximum length or to decrease the possible lengths a packet could have. However, the both ways diminish the legitimate communication channel (the overt channel) [29].

A. Epishkina and K. Kogos pointed out that, packet length covert channels can be constructed even if data encryption is applied. Packet length covert channels are undetectable, complicated, and free of noise. In addition the authors claimed the nonexistence of techniques to limit the bandwidth of such type of covert channels [59]. Accordingly, A. Epishkina and K. Kogos analyzed the bandwidth of a packet size covert channel and proposed a countermeasure tool to limit its capacity. Their proposed method is based on introducing random traffic padding to reduce the channel capacity [23]. However, estimation of any investigated covert channel is required prior applying their technique. Some parameters of this technique are mainly based on covert chancel capacity estimation. Interested readers can see more about packet length covert channels in [60-62].

Some covert channels are built through a combination of storage and timing covert channel techniques. Such combined covert channels can gain high capacity and they would be difficult to detect. This due to the fact that storage channels techniques can provide high capacity while timing channel techniques complicate the channel detectability. The late-packet covert channel in [63, 64] are an examples of such type of covert channels. In which, the covert packets are sent with a certain delay. Therefore, the legitimate receiver discards these packets – because they are received out of the sequence of the data stream - while the covert receiver processes them and extracts the covert message. Trying to fight against such covert channels, Rezaei et al. proposed a detection method that tracks sequence numbers of the received packets [65]. They buffer these sequence numbers to detect late packets and then discard them. Rezaei et al. Claimed that their proposed method prevents such kind of covert channels effectively while maintains voice quality –as their experiment is applied on voice data. However, their method may have impact on system usability in case of video data stream. Therefore, the usability of aforementioned method needs to be verified in case of large data stream.

Internet protocol security (IPsec) is a protocol suite provides secure communication. It helps to secularly exchange confidential information over the internet. Unfortunately this protocol is vulnerable to covert communication. They are many proposed solutions of IPSec covert channels. However, these solutions have direct impact to the system usability [66]. This impact motivated Kundu to introduce a mitigation approach for IPSec covert channel threat. Kundu presented a detailed analysis of his approach security and usability. He showed that his approach provides better usability comparing with the existing approaches [66].

Dakhane and Deshmukh developed an active warden to block or eliminate TCP sequence number storage covert channel [3]. They indicated that, TCP sequence number is vehicle with a high covert channel capacity. They successfully reduced the covert channel bandwidth by normalizing ongoing and outgoing traffic as per their claim. However, the communication overheads that can be caused by applying this model was not presented or estimated to reflect the model usability.

Switching protocol based covert channel is initially presented in [67] which enable a covert channel to switch its presence from protocol to another. Initially this switching technique is a user command-based, while recently it has been developed so as a covert channel can switch itself automatically from protocol to another. Recent research shows the lack of countermeasures to counter such type of complicated covert channel scenarios. Really the switching technique is magnifying the risk behind such covert channels as they are so difficult to detect or to mitigate. Pushing on the way to develop countermeasure tools to fight against this threat, Wendzel and Keller developed an approach to limit the bandwidth of a covert channel that based on protocol switching technique (Protocol switching based covert channel). Basing their work on using an active warden to introduce constant delay that can decrease the covert channel capacity [68]. Later this warden has been enhanced to introduce both constant and random delays [69]. In addition, the authors enhance their countermeasure tool to insure that, the introduced delays have no effect on network normal traffic. However, their approach is not applicable for large network.

In network virtualization environment, any virtual node is subject to covert channel attacks. On the other words, two virtual nodes can communicate to each other covertly in a way that violates the system policy. Wang et al. pointed out that the mitigation of network virtualization covert channel threat is still a big challenge. Accordingly Wang et al. proposed a secure virtual network embedding scheme to lessen the covert channel risk [70]. They showed that their scheme is successfully mitigate the risk of virtual network covert channel attack. They compared their scheme with two existing models in [71, 72]. The result showed that their scheme

improves the security ratio by 40%. However, more enhancements in security ratio are required in this field to attain the maximum benefits of using the network virtualization technology.

C. Recent Trends

As covert channel techniques are rapidly developed, some research proposals have recently introduced significant improvement by including micro protocols within a covert message. The micro protocol facilitates some communication enhancements to ensure reliable communication, dynamic routing, and some other features that provide trustworthy communications for covert message. This type of covert channel is commonly known as covert channel–internal control protocols. The feature of using micro protocol with in a covert message can protect the covert channel from being detected and thus add more complications to network security concerns. Wendzel and Keller highlighted the lack of countermeasures that can counter such covert channels [73] In addition, Kaur et al. pointed out that, the existing methods to counter covert channels are insufficient to deal with covert channel–internal control protocols [74].

Kaur et al. presented a comprehensive details regarding attacks in micro protocols involve -not limited to- analysis, categorization, and classification of these attacks. Accordingly they proposed a novel attacking approach to counter two micro protocol-based tools, Ping Tunnel tool and smart covert channel tool. The feasibility of this approach was verified [75]. However this approach is applied where the structure of the micro protocol header is known or the micro protocol is predicted. In addition, Kaur et al. proposed an approach to enhance micro protocol structure to defense against attack. They proposed this approach to safeguard the micro protocols that implemented for good purposes. As the authors stated that their future work will focus on designing a blind countermeasure that work effectively where the micro protocol structure or presence are unknown [75].

With the evolution of the Intent of Things (IoT), the IoT devices have become more and more popular. As reported that by the year 2020, the prediction number of devices (things) that contented to the internet will be 50 to 100 billion devices [76]. Denney et al. indicates that considerable number of these devices could be wearable devices such as watches, glasses, sensors, etc. Moreover, estimation of 1 in 4 smartphone users will use wearable devices by the year 2019 [77]. This rises up the important to secure such communications. Really the coming future will magnify the challenges that the security provisional are facing. Denney et al. proposed a novel storage covert channel using Android based wearable devices. They evaluated their covert channel performance and ensure its feasibility and functionality.

On the other hand, with the fast development in cloud computing, many businesses are being utilizing its services. Bartels et al. indicates that by the year 2020, the public cloud market is expected to reach 191 billion USD [78]. It is well known that virtualization technology play important role in improving the utilization of cloud resources. However, the virtualization technology is highly vulnerable to covert communication attack which can be initiated between two virtual machines (VMs). This attack is commonly known as Cross VM covert channel [79]. Recently this kind of covert communication has attracted many researches due to its significant threats that can introduce. Tahir et al. presented cross-Virtual Network (cross-VN) covert channel to leak information between virtual networks that are logically separated. They thoroughly discussed and estimated their covert channel bandwidth. In addition, the authors proposed a mechanism to mitigate such type of covert channels by reducing the spent time on the network shared resources and make it difficult for attacker when trying to map out the network [80].

Qian et al. proposed the definition of covert behavior channel, in which, covert message can be delivered through a sequence of operations. Accordingly they developed a novel network covert channel based on the network sequence commands which can take some features from both storage and timing covert channels [81]. The evaluation of their results showed that, the new covert channel has successfully attained better robustness and higher bit rate comparing with covert timing channels and has achieved high level of resistant against detection methods better than covert storage channels.

Mileva and Panajotov indicated that, the recent directions are focusing in developing novel Internet services-based covert channels such as point to point (P2P) services (i.e. Skype), cloud commuting, social network (i.e. Facebook), new network protocols, IP telephony, etc. [82].

In spite of the spread of developing and designing of different types of covert channel that exploiting network protocols, still some protocols not yet been exploited to exchange covert message [83]. Especially, the recent developed protocols or the new ones.

V. Conclusion

It is clearly noticed that most covert channel detection methods rely on detecting the difference between normal and abnormal traffic in order to point out a covert behavior. However, recent research leads the way to introduce covert traffic that is typically close to normal traffic; this poses real challenge to detect such channels. As a matter of fact, it is illogical to build a covert traffic that is characterized as a normal traffic channel; always an amount of variation should be there. Detection methods seem to fail in case of slightly deviated but unnoticed traffic channel. Therefore, the challenge is to introduce detection techniques that sensitive to any level of variation. The authors suggest that, using of the machine learning approaches will fairly enhance the capabilities of covert channel detection techniques.

Encryption, as a traditional security measure, is promoting the design of different types of network covert channels. In addition, the fast development in network technologies is providing a rich environment for covert channels implementation. Therefore, security professionals are facing a real ongoing threat.

Due to diversity of covert channel types and techniques, it is noticed that each proposed solution is focused on a single

type of network covert channel instead of taking into consideration the common behaviors to develop a common framework to counter this threat. There are some new trends to classify the covert channels in order to come up with a solution to handle multiple types of covert channels – as it is clearly surveyed in this paper. However, this welcome direction still needs more efforts and contributions as covert techniques are rapidly on the rise.

This paper infers that most of the research in covert channel concentrates on the covert channels theory more than on practice; a lack of work in showing real practical scenarios is clearly noticed. The depth knowledge of practical implementations of covert channels can shed light on preventing or slowing down their developing and ongoing threats. The authors support the way in having real classes on covert channels implementation as presented in [66]. Such work helps to fill the gap between practice and theory.

The evolution of the Internet of Things (IoT), cloud computing, and data centers represents rich environment for implementing different types of network covert channels and heightens the motivation of developing new covert channel techniques; consequently, this may lead to serious security breaches. Accordingly, future network security challenges would be more sophisticated and complicated. Moreover, the virtualization technology, which is considered to be the backbone of utilizing cloud computing resources, would be highly vulnerable to covert channel attacks.

Instead of developing covert channels for positive use, it is preferably for those who work in this direction to direct their contributions into discovering the exploited vulnerabilities that lead to craft covert channels. This would be particularly beneficial for the purpose of overcoming weaknesses and vulnerabilities during a system design or other phases of defense against the presence of a potential covert channel.

The trend of developing a combined covert channel: engaging timing and storage covert channel techniques to form a hybrid covert channel is playing a significant role in complicating the detection of such channels. A combined covert channel can inherit the undetectable feature of timing channels and the high bandwidth feature of storage channels. Therefore, this trend would magnify the risk and might lead to a serious security breach.

A number of research papers indicate the possibility of full elimination of covert channels that utilize TCP/IP header fields through resetting the default values. But, such normalization technique would not work with fields that take random values, e.g., Initial Sequence Number field (ISN) and the Identifier field (ID). Therefore, detection of such covert channels still a challenge.

Finally, we survey some factors that may enrich, motivate, and encourage the development and design of network-based covert channels; which in turn heightens the threats and dangers which these channel pose:

- The rapid development in computer network technology.
- The evolution of Internet of Things (IoT) which is mainly based on networking platform.
- The fast spread of cloud computing, datacenters, virtualization techniques, etc.
- Switching techniques, which enable a covert channel to switch its presence from one protocol to another.
- Using different fields in a given protocol to carry covert messages.
- Internal control protocols technique, in which a micro protocol can be included within a covert message. Micro protocols facilitate reliable communication, dynamic routing, and some other features that provide trustworthy communications for covert message.

Accordingly, and based on this survey, it is noteworthy to introduce a network covert channel triangle which involve three elements that have the most direct impact in developing network covert channel technology. The triangle reflects the important of network covert channel and the security challenge that can pose. The three elements of this triangle are:

1. The rapid Development of network technology.
2. Switching Techniques.
3. Micro-protocols.

We refer to these three elements by the abbreviation DSM, where:

D: refers to the rapid Development of computer network technology that includes communications techniques, the internet of things, cloud computing, data centers, and all other aspects of technology that paly different roles in developing computer network environment. Selecting the word "development," is due to its flexibility to involve any sort of development now or later. The survey shows the huge impact of rapid development of network technology in developing network covert channels.

S: refers to the Switching techniques that include any such mechanism: switching a covert message from one file to another within a given protocol, from one protocol to another, or from a network to another – all forms of switching of a covert message. Choosing the word "switching" is due to its flexibility to involve any sort of future development in switching techniques. The switching techniques have huge impact in securing a covert channel from being detected and increasing the overhead of any suggested solutions.

M: refers to Micro-protocol. A micro-protocol can be embedded within a covert message to provide and support reliable communications. Selecting the word "micro-protocol" is due to its flexibility to include any communication features that a legitimate protocol can provide to secure communications. A micro-protocol has a huge impact in securing covert message. Moreover, the micro-protocols can inherent any development of network protocols. This leads to enrich a covert channel capability and undetectability. Clearly, a micro-protocol has a huge impact in providing reliable and secure communication for network covert channels.

DSM is sought to depict the danger of network covert channels and consequently the particular challenge faced by security experts.

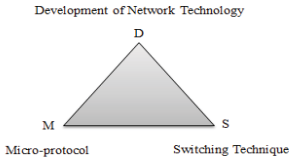

Figure (1): Network Covert Channel Triangle (DSM).

VI. Future Work

Future research in network covert channels is encouraged to focus on developing a common security model. The model is suggested to be based on the significant common behaviors of these types of channels. The suggested security model is to benefit from advances in machine learning algorithms research, which recently showed accurate results in different scientific aspects, especially in fields like the information security.

References

[1] D. C. Latham, "Department of defense trusted computer system evaluation criteria," Department of Defense, 1986.

[2] B. Carrara and C. Adams, "A Survey and Taxonomy Aimed at the Detection and Measurement of Covert Channels," in Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security, 2016, pp. 115-126: ACM.

[3] D. M. Dakhane and P. R. Deshmukh, "Active warden for TCP sequence number base covert channel," in Pervasive Computing (ICPC), 2015 International Conference on, 2015, pp. 1-5.

[4] Y. A. H. Fadlalla, Approaches to resolving covert storage channels in multilevel secure systems. The University of New Brunswick (Canada), 1997.

[5] S. Wendzel, S. Zander, B. Fechner, and C. Herdin, "Pattern-based survey and categorization of network covert channel techniques," ACM Computing Surveys (CSUR), vol. 47, no. 3, p. 50, 2015.

[6] S. Craver, "On public-key steganography in the presence of an active warden," in Information Hiding, 1998, pp. 355-368: Springer.

[7] S. Zander, G. Armitage, and P. Branch, "A survey of covert channels and countermeasures in computer network protocols," Communications Surveys & Tutorials, IEEE, vol. 9, no. 3, pp. 44-57, 2007.

[8] J. Lubacz, W. Mazurczyk, and K. Szczypiorski, "Principles and overview of network steganography," IEEE Communications Magazine, vol. 52, no. 5, pp. 225-229, 2014.

[9] M. Wojciech, W. Steffen, Z. Sebastian, H. Amir, and S. Krzysztof, "Network Steganography," in Information Hiding in Communication Networks:Fundamentals, Mechanisms, Applications, and Countermeasures: Wiley-IEEE Press, 2016, p. 296.

[10] D. V. Forte, C. Maruti, M. R. Vetturi, and M. Zambelli, "SecSyslog: An approach to secure logging based on covert channels," in Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop on, 2005, pp. 248-263: IEEE.

[11] Y. Qian, H. Song, F. Wang, and Z. Wang, "Network Covert Channel Encoding by Packet Length: Design and Detection," Journal of Computational Information Systems, vol. 7, no. 5, pp. 1463-1471, 2011.

[12] M. A. Elsadig and Y. A. Fadlalla, "VANETs Security Issues and Challenges: A Survey," Indian Journal of Science and Technology, vol. 9, no. 28, 2016.

[13] A. Singh and K. Manchanda, "Establishment of bit selective mode storage covert channel in VANETS," in 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2015, pp. 1-4.

[14] D. Dhobale, V. Ghorpade, B. Patil, and S. B. Patil, "Steganography by hiding data in TCP/IP headers," in Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, 2010, vol. 4, pp. V4-61-V4-65: IEEE.

[15] L. Spitzner, "Know Your Enemy: Sebek2 A kernel based data capture tool," ed, 2003.

[16] R. DeGraaf, J. Aycock, and M. Jacobson Jr, "Improved port knocking with strong authentication," in Computer Security Applications Conference, 21st Annual, 2005, pp. 10 pp.-462: IEEE.

[17] W. Mazurczyk and Z. Kotulski, "New security and control protocol for VoIP based on steganography and digital watermarking," arXiv preprint cs/0602042, 2006.

[18] H. Qu, Q. Cheng, and E. Yaprak, "Using Covert Channel to Resist DoS attacks in WLAN," in ICWN, 2005, pp. 38-44.

[19] M. H. Almeshekah, M. J. Atallah, and E. H. Spafford, "Layering authentication channels to provide covert communication," in Proceedings of the 14th Annual Information Security Symposium, 2013, p. 9: CERIAS-Purdue University.

[20] Y. Sun, X. Guan, and T. Liu, "A new method for authentication based on covert channel," in IFIP International Conference on Network and Parallel Computing, 2011, pp. 160-165: Springer.

[21] T. S. Fatayer and K. A. A. Timraz, "MLSCPC: Multi-level security using covert channel to achieve privacy through cloud computing," in 2015 World Symposium on Computer Networks and Information Security (WSCNIS), 2015, pp. 1-6.

[22] S. Hammouda, L. Maalej, and Z. Trabelsi, "Towards Optimized TCP/IP Covert Channels Detection, IDS and Firewall Integration," in 2008 New Technologies, Mobility and Security, 2008, pp. 1-5.

[23] A. Epishkina and K. Kogos, "A random traffic padding to limit packet size covert channels," in Computer Science and Information Systems (FedCSIS), 2015 Federated Conference on, 2015, pp. 1107-1111: IEEE.

[24] T. G. Handel and M. T. Sandford II, "Hiding data in the OSI network model," in Information Hiding, 1996, pp. 23-38: Springer.

[25] S. Zander, G. Armitage, and P. Branch, "Covert channels in the IP time to live field," in Proceedings of Australian Telecommunication Networks and Applications Conference (ATNAC), 2006.

[26] K. Ahsan and D. Kundur, "Practical data hiding in TCP/IP," in Proc. Workshop on Multimedia Security at ACM Multimedia, 2002, vol. 2.

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

[28] C. H. Rowland, "Covert channels in the TCP/IP protocol suite," First Monday, vol. 2, no. 5, 1997.

[29] D. J. Dye, "Bandwidth and detection of packet length covert channels," Monterey, California. Naval Postgraduate School, 2011.

[30] L. Barroso and M. Santos, "A Review on Covert Techniques."

[31] M. A. Elsadig and Y. A. Fadlalla, "Survey on Covert Storage Channel in Computer Network Protocols: Detection and Mitigation Techniques," in Proc. of the Intl. Conference on Advances in Information Processing and Communication Technology - IPCT 2016, 2016..

[32] N. Schear, C. Kintana, Q. Zhang, and A. Vahdat, "Glavlit: Preventing exfiltration at wire speed," IRVINE IS BURNING, p. 133, 2006.

[33] Q. Yuwen, S. Huaju, S. Chao, W. Xi, and L. Linjie, "Network covert channel detection with cluster based on hierarchy and density," Procedia Engineering, vol. 29, pp. 4175-4180, 2012.

[34] J. Zhai, G. Liu, and Y. Dai, "Detection of TCP covert channel based on Markov model," Telecommunication Systems, vol. 54, no. 3, pp. 333-343, 2013.

[35] H. Zhao and Y. Q. Shi, "A phase-space reconstruction approach to detect covert channels in TCP/IP protocols," in Information Forensics and Security (WIFS), 2010 IEEE International Workshop on, 2010, pp. 1-6: IEEE.

[36] T. Sohn, J. Seo, and J. Moon, "A study on the covert channel detection of TCP/IP header using support vector machine," in ICICS, 2003, pp. 313-324: Springer.

[37] E. Tumoian and M. Anikeev, "Network based detection of passive covert channels in TCP/IP," in Local Computer Networks, 2005. 30th Anniversary. The IEEE Conference on, 2005, pp. 802-809: IEEE.

[38] S. J. Murdoch and S. Lewis, "Embedding covert channels into TCP/IP," in Information hiding, 2005, pp. 247-261: Springer.

[39] N. D. Rohankar, A. Deorankar, and D. P. Chatur, "A Review of Literature on Design and Detection of Network Covert Channel," International Journal of Engineering Science and Innovative Technology (IJESIT) Volume, vol. 1, 2012.

[40] P. Dong, H. Qian, Z. Lu, and S. Lan, "A Network Covert Channel Based on Packet Classification," IJ Network Security, vol. 14, no. 2, pp. 109-116, 2012.

[41] A. S. Nair, A. Sur, and S. Nandi, "Detection of Packet Length Based Network Steganography," in 2010 International Conference on Multimedia Information Networking and Security, 2010, pp. 574-578.
[42] Q.-z. YAO and P. ZHANG, "Coverting channel based on packet length," Computer engineering, vol. 34, no. 3, pp. 183-185, 2008.
[43] L. Zhang, G. Liu, and Y. Dai, "Network packet length covert channel based on empirical distribution function," Journal of Networks, vol. 9, no. 6, pp. 1440-1446, 2014.
[44] L. Ji, W. Jiang, B. Dai, and X. Niu, "A novel covert channel based on length of messages," in 2009 International Symposium on Information Engineering and Electronic Commerce, 2009, pp. 551-554: IEEE.
[45] L. Ji, H. Liang, Y. Song, and X. Niu, "A normal-traffic network covert channel," in Computational Intelligence and Security, 2009. CIS'09. International Conference on, 2009, vol. 1, pp. 499-503: IEEE.
[46] M. Hussain and M. Hussain, "A high bandwidth covert channel in network protocol," in Information and Communication Technologies (ICICT), 2011 International Conference on, 2011, pp. 1-6: IEEE.
[47] O. I. Abdullaziz, V. T. Goh, H. C. Ling, and K. Wong, "Network packet payload parity based steganography," in 2013 IEEE Conference on Sustainable Utilization and Development in Engineering and Technology (CSUDET), 2013, pp. 56-59.
[48] A. Sur, A. S. Nair, A. Kumar, A. Jain, and S. Nandi, "Steganalysis of network packet length based data hiding," Circuits, Systems, and Signal Processing, vol. 32, no. 3, pp. 1239-1256, 2013.
[49] X. Lu, Y. Wang, L. Huang, W. Yang, and Y. Shen, "A Secure and Robust Covert Channel Based on Secret Sharing Scheme," in Asia-Pacific Web Conference, 2016, pp. 276-288: Springer.
[50] W. Frączek, W. Mazurczyk, and K. Szczypiorski, "Hiding information in a Stream Control Transmission Protocol," Computer Communications, vol. 35, no. 2, pp. 159-169, 2012.
[51] M. Wojciech, W. Steffen, Z. Sebastian, H. Amir, and S. Krzysztof, "Network Steganography Countermeasures," in Information Hiding in Communication Networks:Fundamentals, Mechanisms, Applications, and Countermeasures: Wiley-IEEE Press, 2016, p. 296.
[52] Y. Shen, L. Huang, X. Lu, and W. Yang, "A novel comprehensive steganalysis of transmission control protocol/Internet protocol covert channels based on protocol behaviors and support vector machine," Security and Communication Networks, vol. 8, no. 7, pp. 1279-1290, 2015.
[53] S. Z. Goher, B. Javed, and N. A. Saqib, "Covert channel detection: A survey based analysis," in High Capacity Optical Networks and Emerging/Enabling Technologies, 2012, pp. 057-065.
[54] F. Rezaei, M. Hempel, and H. Sharif, "A novel automated framework for modeling and evaluating covert channel algorithms," Security and Communication Networks, vol. 8, no. 4, pp. 649-660, 2015.
[55] F. Rezaei, M. Hempel, P. L. Shrestha, and H. Sharif, "Evaluation and Verification of Automated Covert Channel Modeling Using a Real Network Platform," in 2014 IEEE Military Communications Conference, 2014, pp. 12-17.
[56] W. Fraczek and K. Szczypiorski, "Steg Blocks: Ensuring Perfect Undetectability of Network Steganography," in 2015 10th International Conference on Availability, Reliability and Security, 2015, pp. 436-441.
[57] J. O. Seo, S. Manoharan, and A. Mahanti, "A Discussion and Review of Network Steganography," in 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), 2016, pp. 384-391.
[58] M. McFail, "Covert storage channels: A brief overview," in PACISE Conference, Bloomsburg, PA, 2005.
[59] A. Epishkina and K. Kogos, "Covert Channels Parameters Evaluation Using the Information Theory Statements," in IT Convergence and Security (ICITCS), 2015 5th International Conference on, 2015, pp. 1-5.
[60] A. Epishkina and K. Kogos, "Packet Length Covert Channel Capacity Estimation," in 2016 6th International Conference on IT Convergence and Security (ICITCS), 2016, pp. 1-4.
[61] A. Epishkina and K. Kogos, "A Traffic Padding to Limit Packet Size Covert Channels," in Future Internet of Things and Cloud (FiCloud), 2015 3rd International Conference on, 2015, pp. 519-525.
[62] M. A. Elsadig and Y. A. Fadlalla, "Survey on Covert Storage Channel in Computer Network Protocols: Detection and Mitigation Techniques," International Journal of Advances in Computer Networks and Its Security, vol. 6, no. 3, pp. 11-17, 2016.
[63] W. Mazurczyk and J. Lubacz, "LACK—a VoIP steganographic method," Telecommunication Systems, vol. 45, no. 2-3, pp. 153-163, 2010.
[64] W. Mazurczyk, "Lost audio packets steganography: the first practical evaluation," Security and Communication Networks, vol. 5, no. 12, pp. 1394-1403, 2012.
[65] F. Rezaei, M. Hempel, D. Peng, and H. Sharif, "Disrupting and Preventing Late-Packet Covert Communication Using Sequence Number Tracking," in MILCOM 2013 - 2013 IEEE Military Communications Conference, 2013, pp. 599-604.
[66] A. Kundu, "Mitigation of Storage Covert Channels in IPSec for QoS Aware Applications," Procedia Computer Science, vol. 54, pp. 102-107, 2015.
[67] P. Magazine, "7 (51) September 01, 1997, article 06 of 17 [LOKI2 (the implementation)]," ed.
[68] S. Wendzel and J. Keller, "Design and implementation of an active warden addressing protocol switching covert channels," in Proc. 7th International Conference on Internet Monitoring and Protection (ICIMP 2012), Stuttgart, 2012.
[69] S. Wendzel and J. Keller, "Preventing protocol switching covert channels," International Journal on Advances in Security, vol. 5, 2012.
[70] W. Zhiming, W. Jiangxing, G. Zehua, C. Guozhen, and H. Hongchao, "Secure virtual network embedding to mitigate the risk of covert channel attacks," in 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2016, pp. 144-145.
[71] S. Liu, Z. Cai, H. Xu, and M. Xu, "Towards security-aware virtual network embedding," Computer Networks, vol. 91, pp. 151-163, 2015.
[72] L. Gong, Y. Wen, Z. Zhu, and T. Lee, "Toward profit-seeking virtual network embedding algorithm via global resource capacity," in IEEE INFOCOM 2014-IEEE Conference on Computer Communications, 2014, pp. 1-9: IEEE.
[73] S. Wendzel and J. Keller, "Hidden and under control," annals of telecommunications-annales des télécommunications, vol. 69, no. 7-8, pp. 417-430, 2014.
[74] J. Kaur, S. Wendzel, and M. Meier, "Countermeasures for Covert Channel-Internal Control Protocols," in Availability, Reliability and Security (ARES), 2015 10th International Conference on, 2015, pp. 422-428.
[75] J. Kaur, S. Wendzel, O. Eissa, J. Tonejc, and M. Meier, "Covert channel□internal control protocols: attacks and defense," Security and Communication Networks, 2016.
[76] P. F. Drucker, "Internet of Things," 2015.
[77] K. Denney, A. S. Uluagac, K. Akkaya, and S. Bhansali, "A novel storage covert channel on wearable devices using status bar notifications," in 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2016, pp. 845-848.
[78] A. Bartels, J. Rymer, J. Staten, K. Khalid, and J. Clark, "The Public Cloud Market Is Now In Hypergrowth: Sizing the Public Cloud Market, 2014 To 2020," Forrester, April, vol. 24, p. 2014, 2014.
[79] W. Qi, J. Wang, H. Hovhannisyan, K. Lu, and J. Zhu, "A Generic Mitigation Framework against Cross-VM Covert Channels," in 2016 25th International Conference on Computer Communication and Networks (ICCCN), 2016, pp. 1-10.
[80] R. Tahir et al., "Sneak-Peek: High speed covert channels in data center networks," in IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications, 2016, pp. 1-9.
[81] Y. Qian, T. Sun, J. Li, C. Fan, and H. Song, "Design and analysis of the covert channel implemented by behaviors of network users," Security and Communication Networks, vol. 9, no. 14, pp. 2359-2370, 2016.
[82] A. Mileva and B. Panajotov, "Covert channels in TCP/IP protocol stack-extended version," Open Computer Science, vol. 4, no. 2, pp. 45-66, 2014.
[83] R. Rios, J. A. Onieva, and J. Lopez, "Covert communications through network configuration messages," Computers & Security, vol. 39, pp. 34-46, 2013.