*International Journal of Engineering & Technology*, 7 (2.4) (2018) 62-65

**International Journal of Engineering & Technology**

*Website: www.sciencepubco.com/index.php/IJET*

***Research Paper***

# Covert Channels Detection with Supported Vector Machine and Hyperbolic Hopfield Neural Network

**G Yuvaraj[1], Siva Rama Lingham N[2], Rajkamal J[3]**

*[12] Assistant Professor Department of Computer Science and Engineering School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,Avadi, Chennai-62, TamilNadu, India*
*3Assistant Professor, S.A Engineering College, Avadi, Chennai-62, TamilNadu, India*
**Corresponding author E-mail:gyuvarajdce@gmail.com*

**Abstract**

A mechanism that is intended to expose information against a security violation in a network is the use of network covert channel and it is difficult to detect information about data loss like location of loss using network covert channel. To identify the covert channel were the data pattern missing over the sharing of resources in networks. Several mechanisms are used to identify a large variation of covert channels. However, those mechanisms have more limitation like speed of detection, detection accuracy etc. In this paper, a new machine learning approaches called "Support Vector Machine and Hyperbolic Hopfield Neural Network" to overcome the drawbacks of existing methods. This approach is supported to classifying the different covert channels with data packets which is shared in networks and its supports to identifying the location of data loss or data pattern mismatched. Finally, the proposed methods properly detected covert channels with high accuracy and less detection high speed shared a network resources in effective manner.

***Keywords:*** *Covert Channels; Support Vector Machine and Hyperbolic Hopfield Neural Network.*

## 1. Introduction

Undercover channels give techniques to transmit data utilizing existing framework assets that were not intended to convey information. This makes them undetectable to basic system security instruments like firewalls. In light of their capacity to avoid identification, they make a grave digital security risk. Delicate and classified data can be spilled from a system with higher security benefits to an outside system by essentially setting up an apparently innocuous correspondence connect between them. Two gatherings with aim to transmit secretive information can undoubtedly convey and trade data over an open system without being distinguished. Consequently, it is extremely hard to recognize incognito interchanges and this can be an exceptionally compelling and harming security approach in the event that it is utilized for unsafe intentions. There are two countermeasure ways to deal with clandestine correspondences. One approach is utilizing a system observing substance called a system warden that adjusts all activity going through it paying little heed to whether it is clandestine or not. This is called dynamic superintendent approach.

This alteration of the fundamental activity may potentially make it unimaginable for the collector to unravel the shrouded message. Be that as it may, doing as such will unreasonably rebuff innocuous movement also, regularly prompting misuse of registering assets. A dynamic change of activity may not be conceivable without disregarding the QoS arrangements in the system, especially in applications where the request of parcels and the planning prerequisites of them are firmly guided by the correspondence convention. In this way, an aloof superintendent methodology which can recognize nearness of undercover message in the rush hour gridlock is required. Such methodologies will explore the movement and set up alerts, and take remedial endless supply of clandestine messages in a specific stream. A SVM-based area structure that can capriciously recognize CTCs. CTCs channels used to class of secret channels that insert bits into action by managing the arranging information of the movement[6].

The structure uses truthful impressions made from the development under enquiry as the component manage vectors toward set up a classifier in light of Support Vector Machine. [11]. The covered bits are embedded inside the arranging information, developing an identifier in light of the true fingerprints got from the arranging data itself will interface well with the closeness of such covert bits.

A novel machine learning approach called Support Vector Machine and Hyperbolic Hopfield Neural Network is used to classify the covert and overt channels data packets. The proposed approach is categorized into two phases such as Support Vector Machine Training and Convert Channel prediction. Finally, we shown the proposed method is an effective approach to detect the covert channels from the shared network resources [2]. Here, a new machine learning neural network approach called Hyperbolic Hopfield is used to improve the covert channels prediction in the shared network resources.

## 2. Related Work:

### 2.1 Covert Timing Channel:

The secretive planning channels grouped into two kinds: active and passive. Regarding clandestine planning channels, active channels discuss to covert timing channels that create extra movement to transmit data, while passive channels notices to secret planning channels that control the planning of existing activity. When all is said in done, dynamic secretive planning channels are speeded, however inactive clandestine planning channels are more hard to identify. Then again, dynamic undercover planning channels regularly require a traded off machine, though latent incognito planning channels, if inventively situated, don't. Most of the secret planning diverts talked about in this segment are dynamic incognito planning channels, aside from where expressed something else.

### 2.2 Time-Replay Covert Timing Channel

Cabuk [12] later composed a further developed clandestine planning channel in light of a replay assault, which we allude to as RCTC. TRCTC utilizes an example of honest to goodness movement Sin as info and replays Sin to transmit data. Sin is apportioned into two equivalent canisters S0 and S1 by an incentive to cut off . TRCTC transmits a 1-bit by arbitrarily replaying an entomb parcel delay from canister S1 and transmits a 0-bit by haphazardly replaying a bury bundle delay from container S0. In this way, as Sin is comprised of real movement, the appropriation of TRCTC activity is around equivalent to the circulation of real movement.

### 2.3 IP Covert Timing Channel

Cabuk et al. [13] To built up the principal IP undercover planning channel, which we allude to as IPCTC, and researched various outline issues. In this situation, a machine is traded off and the guarded edge spoke to as an edge firewall or interruption location framework screens correspondence with the outside. In this way, a secret planning channel can be utilized to go through the protective border undetected. IPCTC utilizes a straightforward interim based encoding plan to transmit data. IPCTC transmits a 1-bit by sending a bundle amid an interim and transmits a 0-bit by not sending a parcel amid an interim. A noteworthy preferred standpoint to this plan is that when a parcel is lost, a bit is flipped however synchronization isn't influenced. The planning interim t and the quantity of 0-bits between two 1-bits decide the conveyance of IPCTC entomb parcel delays. It is intriguing to take note of that if the example of bits is uniform, the circulation of bury bundle delays is near a Geometric conveyance. To abstain from making an example of entomb parcel delays at products of a solitary t, the planning interim t is pivoted among various esteems

The covert channel main aim is to hide existence the transfer data but in cryptography network doesn’t hide existence of data but the receiver can receive only readable transformed data. There is no intention to hide the data communication in cryptography Covert channel in computer network protocols and steganography are closely related but often confused. Some network are involves information hiding in text, audio, visual content. Covert channels require some protocol as a carrier while network requires some form of content as a cover. The network covert channel are communication stream must be embedded inside authorized channels but that are not designed nor intended to exist. The existing protocol may be based from OSI low layer protocol (eg: TCP/IP and UDP) to OSL high layer protocol (eg: HTTP and SMTP) [1]. The common idea of network covert channels to relies the data that data are used transferred in redundant or unused fields of system conventions.

The network security can thinking about to started analysing the covert channels communication in two terms first terms storage covert channels and second terms timing covert channels. The storage covert channels, one of the processes to write the data directly or indirectly in particular storage location, another processes read the data in that location itself. The number of protocol tools are establish the storage covert channels. These protocols tools are unused fields to transfer the information. In a way steganography can be seen as a form of storage covert channel.

The planning clandestine channel includes adjusting the time attributes to shroud data. Particularly it should be possible by regulating between parcel delays. We give careful consideration to identify secret channels identified with TCP ISN and IP ID fields[9]. At the SVM preparing time they gathered normal TCP/IP parcels utilizing a tcp dump instrument and abnormal TCP/IP packets(including incognito fields) produced from clandestine tcp and after that tried it for IP Identification field of IP header and grouping number field of TCP header[3].

The takes a shot at organize timing channels can be followed back to the work brought up that worldly undercover channels .Some system timing channels require time synchronization amongst encoder and decoder. Our proposed a planning channel where one piece is passed on through transmitting information or not and Cabuket connected a comparable plan to IP bundles [4]. To transmit a '1', the trojan visits a dynamically decided gathering of reserve sets (G1) and replaces the greater part of the constituent store squares, and for a '0' it visits another progressively decided gathering of reserve sets (G0) and replaces the greater part of the constituent reserve pieces.

The covert agent surmises the transmitted bits as tails: It replaces the greater part of the store obstructs in G1 and G0, and times the gets to theG1 and G0 sets independently. In the event that the gets to G1 sets take longer than the G0 sets (that is, the greater part of the G1 sets brought about reserve misses and G0 sets were store hits), at that point the covert operative derives '1'. Something else, if the gets to G0 sets take longer than the G1 sets (that is, the majority of the G0 sets brought about cache misses and G1 sets were reserve hits), at that point the government agent construes a '0'.

But we are using in Hyperbolic Hopfield neural network approaches technique used in our proposed system. This system is used to training and testing dataset from extraction data in database and its transmit detection dataset to prediction results.

## 3. System Design

In Fig 3.1, Wireshark tool to collect the dataset and transfer the dataset to Network traffic filter. The traffic filter selects network data packets for sample extraction that is a fingerprint [10]. A specific type of network port can defined on a port basis or on a

stream basis with the help of investigating source. The packet data is extracted after the statistical feature is derived by the fingerprint extractor through the data provided by the traffic filter [7]. After extracting all packet data transfer to testing and training the data. It provided to the Support Vector Machine framework for training the classifier with hyperbolic hop field neuralnetwork.

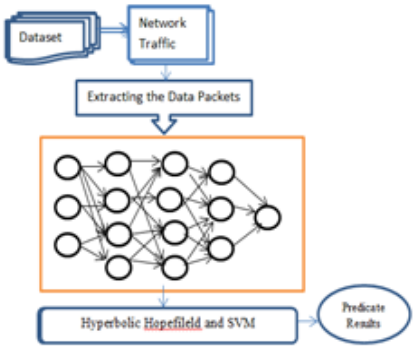


**Fig 3.1** Covert Timing Channels Detection Support Vector Machine & Hyperbolic Hopfield Neural Network

### 3.1 Neural Network:

Fig3.2 The neural network device is used to collect the many number of inputs and the receiver can collect one data output. The neural network has two different operational modes that are the mode of training and the mode of using. In Training mode, the neural network can be trained to fire (or not), for particular input stream or patterns. Second mode is the mode of using, after input pattern is detected at the input, its particular output becomes the current output. The network can allow signals supported vector machine to travel only from input to output. Feed-forward Neural network tend to be straight forward networks to transfer the data from inputs with outputs. They are extensively used in pattern recognition. In This type of organisation is also referred to as bottom-up or top-down.

The square graph portrayal of the location system. The identifier is basically organize screen that approaches all activity it is end to examine. It could either be executed to pass all system activity through it as appeared in figure, or it could just take advantage of the movement stream. It comprises of three essential units—an activity channel, a unique mark extractor and a SVM system. The activity channel chooses movement for unique mark extraction.

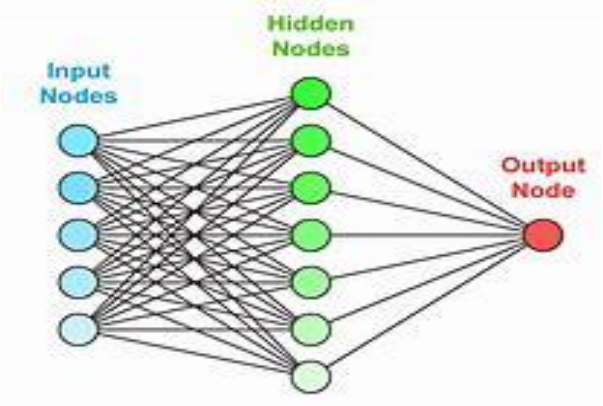


**Fig 3.2** To collecting the dataset from traffic filter after using the neural network to get predicting data results.

It can be portrayed on a port start to analyze a specific sort of action, or on a stream commence which helps in source following moreover. The remarkable finger impression extractor deduces the computation is being used to introduce secret bits in order to know which exceptional finger impression to trust. This is an indirect issue with no course of action. Also, we have showed up in that the use of these fingerprints falls flat when the degree of the embedded undercover message is nearly nothing. This approach that uses there granularity estimations as the component focuses have been proposed. In any case, this classifier can been attempted against only a solitary CTC.

**Table 1.** Case Study Scenarios of Network Traffic

| Scenarios Traffic Structure | |
|---|---|
| Scenario 1 | 20,000Normal-20,000Jitterbug-10,000Normal |
| Scenario 2 | 20,000Exponential-20,000 TimeReplay-10,000Exponential |
| Scenario 3 | 20,000Normal-20,000On-off-10,000Normal |
| Scenario 4 | 20,000Exponential-20,000 L-bits to N-packets10,000Exponential |

In the creators have effectively utilized the SVM classifier methods for grouping particular CSCs. The channels of creators talk about incognito channels that utilization header fields TCP/IP, for example, Sequence Number [8] and IP Identification, ICMP load circulation [5] and recognize them utilizing a SVM based example classifier.

The p-values obtained from applying WSR, WMM, and LR tests on ongoing mixed network traffic according to Table 1 scenarios utilizing detection buffers that store 2000 network traffic IPDs and are updated with 100 new IPDs. These parameters, values and settings are chosen according to our experimental observations to reach over 90% of confidence interval and have a sample IPDs that represent accurate distribution of network traffic. As we can clearly observe, the obtained overt traffic p-values for all of the case study scenarios are randomly distributed. However, the p-values for covert traffic fall into a given range, which is usually above 0.3 for all the case study scenarios. Therefore, we can reliably classify the IPDs that belong to the covert communication, if those reach above 0.3 for several consecutive p-value calculations, over updated detection buffers. Another key characteristic that we can explore from these low p-values that are gained coinciding with the covert communication start.

Therefore, the starting point of the covert communications can be detected by determining the transition from very low p-values that rapidly increase to a region of high p-values. The detection edges result from the very different IPD distributions, when the covert communication starts and the second detection buffer is partially filled with covert IPDs. This shows that the detection buffers are not from the same residents with high level of sureness.

According to the demonstrated results, our detection approach can reliably and accurately detect covert communication, validated against a range of well-known case study CTC algorithms. Also, we would like to mention that in addition to the case study scenarios that were discussed and presented in this study, we have tested our detection approach for other overt traffic distributions

and various settings of these CTC algorithms. Due to their similarity in the expressed accuracy and responsiveness in detecting covert channels, and also page limitations, these have been omitted from this paper[1].

## 4. Conclusion:

Presently accessible discovery strategies are intended to identify a certain kind of undercover stations, and the recognition rule can't be stretched out to consolidate more stations. Besides, they do not have the necessity of visually impaired recognition and versatility. A novel machine learning approach called Support Vector Machine and Hyperbolic Hopfield Neural Network is used to classify the covert and over channels data packets. The proposed approach is categorized into two phases such as Support Vector Machine Training and Convert Channel prediction. Finally, our proposed methods the shared network resources is to approach an effective manner to detect the covert channels.

## 5. References:


[1] Fahimeh Rezaei; Michael Hempel; Pradhumna Lal Shrestha; Sushanta Mohan Rakshit; Hamid Sharif “A novel Covert Timing Channel detection approach for online network traffic” IEEE Conference on Communications and Network Security (CNS) 2015.

[2] R. Archibald, D. Ghosal, "A comparative analysis of detection metrics for covert timing channels", Journal of Computers & Security Elsevier, vol. 45, pp. 284-292, 2014.

[3] R. A. Kemmerer, “A practical approach to identifying storage and timing channels,” in Proceedings of the 1982 IEEE Symposium on Security and Privacy, April 1982.

[4] S. Gianvecchio, H. Wang, "An entropy-based approach to detecting covert timing channels", Dependable and Secure Computing IEEE Transactions on, vol. 8, no. 6, pp. 785-797, 2001.

[5] Angelo Liguori; Francesco Benedetto; Gaetano Giunta; Nils Kopal; Arno Wacker” Analysis and monitoring of hidden TCP traffic based on an open-source covert timing channel” IEEE Conference on Communications and Network Security (CNS) 2015.

[6] Hong Zhao; Yun Q. Shi ” A phase-space reconstruction approach to detect covert channels in TCP/IP protocols ” 2010 IEEE International Workshop on Information Forensics and Security 2010.

[7] S. Cabuk, “Network covert channels: Design, analysis, detection, and elimination,” Ph.D. dissertation, Purdue University, West Lafayette, IN., USA, December 2006.

[8] F. Rczaei, M. Hempel, P. L. Shrestha, H. Sharif, "Evaluation and Analysis of Automated Covert Channel Modeling over Real Network Environment", IEEE Conference on Military Communication Conference (MILCOM), October 2014

[9] Richard M. Stillman “Detecting IP covert timing channels by correlating packet timing with memory content” IEEE SoutheastCon 2008 .

[10] Yusuf Ibrahim; Muhammed. B. Mu'Azu; Adewale. E. Adedokun; Yusuf. A. Sha'Aban “A performance analysis of logistic regression and support vector machine classifiers for spoof fingerprint detection” IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON) 2017

[11] Steven Gianvecchio; Haining Wang” An Entropy-Based Approach to Detecting Covert Timing Channels” IEEE Transactions on Dependable and Secure Computing Year: 2011, Volume: 8, Issue: 6

[12] S. Cabuk, “Network Covert Channels: Design, Analysis, Detection, and Elimination,” PhD dissertation, Purdue Univ., Dec. 2006.

[13] S. Cabuk, C. Brodley, and C. Shields, “IP Covert Timing Channels: Design and Detection,” Proc. ACM Conf. Computer and Comm. Security, Oct. 2004.