RESEARCH ARTICLE OPEN ACCESS

Improving Intrusion Detection Method for Covert Channel in TCP/IP Network

T K Vivek[1], M Kalimuthu[2]
Post Graduate Student[1], Associate Professor[2]
Department of IT, SNS college of Technology, coimbatore-641035,
Tamil Nadu-India.

ABSTRACT
Network security mainly involves authorization of access to data in a network, which is controlled by the network administrator. Networks can be private as well as public access. An anomaly-based intrusion detection system will monitor the network traffic and log audit purposes then for later high-level analysis. Communication between two hosts using a network mainly involves encryption and decryption to maintain privacy. Covert channels are one of the malicious conversations in a legitimate secured network communication that violates the security policies. Covert channels are used for the secret transfer of information but they are differing from encryption. Encryption only protects communication from being decoded by unauthorized parties, whereas covert channels aim to hide the very existence of the communication. They allow individuals to communicate truly undetectable and exchange hidden information. The huge amount of data and vast number of different protocols in the internet seems ideal as a high-bandwidth vehicle for covert communication. Phase space reconstruction method creates a processing space for detecting covert channels in TCP ISNs. Based on this model, a classification algorithm is developed to identify the existence of information hidden in ISNs. In proposed method a new detection method with more efficiency is implemented by using ACO Algorithm.

Keywords- Channel, Network Steganalysis, Genetic Algorithm, Phase space reconstruction, TCP/IP Network, ACO

I. INTRODUCTION

Network Security plays a vital role in today's world. Covert Channel is a challenging attack in network security. Classification algorithm is one of the best methods for detecting covert channel. Genetic Algorithm (GA) is an ideal technique for finding solutions for optimization problems.

Computer network is unpredictable due to information warfare and is prone to various attacks. Such attacks on network compromises on the most important attribute the privacy. Most of such attacks are devised using special communication channel called "Covert Channel". The word "Covert" stands for hidden or non-transparent.

Covert channel was first introduced by Lampson in 1973 (Lampson, 1973) to denote an illegal communication mechanism in a single host, by which a process at a high security level leaks information to a process at a low security level that has no permission to access the information. In computer network, for secure communication numbers of security policies are used. For example -firewall, Network Intrusion Detection System (NIDS), packet anomaly detection system, etc [1].

A covert channel is created by using some of the space available either within the padding or within other parts of the transport of network packets. Covert channels data can be added to a data stream without affecting the main content of data being transmitted. This allows the covert receiver to abstract data from a system without creating any type of data trail. A single packet might only contain one or two bits of the covert data stream, and making detection very difficult. Creating a covert channel takes some ingenious programming, and access to the file system at the source end of the communication is essential. This means that a covert channel can only be investigate through viral infection or through a programming effort that has administrative or other authorized access to the system.

Genetic Algorithm (GA) is a model used to identify the behavior of the evolutionary processes in nature [6]. It is known to be a best ideal technique for finding solutions for optimization problems. Ant colony optimization is one of the known genetic algorithm based optimization

techniques. The data packets are basically selected through random manner.

II. PROBLEM STATEMENT

Existing system has following problems while detecting covert channel in computer networks.

- The method they had developed is complicated for detection of covert channel.
- Traffic congestion will be occurred due to this method.
- Especially online malicious detection method will take more time consumption in the existing method because first-come first serve concept is behind this method.
- Few parameters are only taken in this existing system for detection of covert channel.

III. PROPOSED METHOD

The proposed system consists of five processes. Such as

- Covert Channel Analysis
- Dimensionality reduction in Feature Selection
- Attacker Prediction
- Proposed Classifier Method
- PRM Model
- ACO

A. Covert Channel Analysis and Attacker Prediction

TCP/IP covert channels alter header fields to carry information for transmit without impacting the normal communications. Modification of some header fields and using header fields which require random number. Unused header fields have high possibilities for altering during transmission. The randomness of ISNs makes attackers hard to predict these numbers.

At first data packets are captured and stored in database. Then feature dataset are created and used for training process. Featured dataset is obtained from above method.

B. Dimensionality Reduction in Feature Selection

Then the feature selection is classified by means of dimensionality reduction in feature selection for multidimensional data's. I.e. discarding irrelevant features for more simplification and increasing performance of the process. Some of the existing works on feature selection are such as wrapper, filter, hybrid and Meta heuristic. Where Ant Colony Optimization are based on Meta heuristic, which is best suitable for this optimization process.

In Wrapper method, predefined learning method are assumed, and features are selected which justify the performance of particular learning model. In Filter model, statistical analysis of feature set is needed, without using any learning model. Whereas hybrid model, uses the combined model of wrapper and filter model. Meta heuristics also known as global search approach, to find the high quality solution by beans of genetic algorithms.

C. Phase Space Reconstruction Method

According to phase space reconstruction method a dynamic system can be described by a phase space diagram [8]. It is truly based on chaos theory, i.e. any changes in any part the system will change the entire behavior of that system.

The dimensions phase vector is

$P = (u, v, s, t)$

Then equations will be

$u = ISN(k) - ISN(k-1)$

$v = ISN(k-1) - ISN(k-2)$

$s = ISN(k-2) - ISN(k-3)$

$t = ISN(k-3) - ISN(k-4)$ **Eqn. (1)**

Where p is an dimensional vector, which consist of parameter such as u, v, s, t. The equation explains about the first order, second order etc to find the distance between the two data's i.e. classifying the data's by means of comparisons.

D. Proposed Classifier Algorithm

The ISN field of each incoming packet will be reconstructed for encoded data. Modifications in ISNs are detected by proposed classifier algorithm. Accuracy rate for identifying normal and steganography ISNs are greatly increased by means of this algorithm [8].

E. Ant Colony Optimization (ACO)

Parallelization of Ant Colony Optimization (ACO) is introduced to optimize the covert channel detection by means of decreasing work load such as Computational time, speed [6]. This method changes the detection method from FIFO to random detection. Also it provides Covert channel differentiation from legitimate channels and presents a new detection measures that provide detection rates using ACO Algorithm.

F. Block Diagram of Proposed System

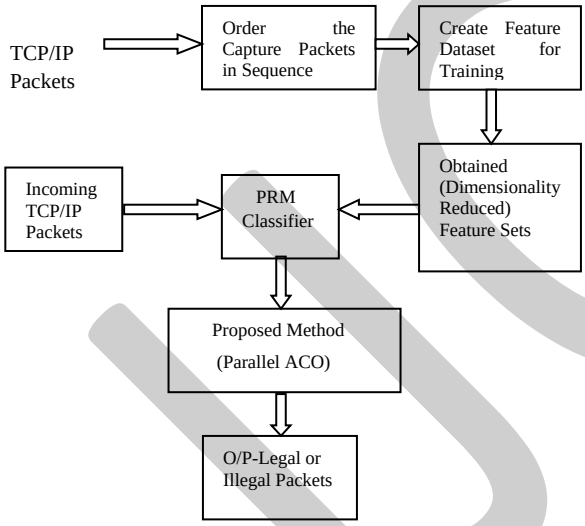

Fig 3.1 Block Diagram for covert channel detection

Here the block diagram clearly explains every about capturing data's, test and trained and how they are applied to the classifier algorithm for detection of covert channel.

In Existing system Proposed classifier algorithm is used for detecting covert channel in TCP/IP networks. Then Phase Reconstruction method (PRM) method is maintained for detection covert channel. Detection is based on test and training method and selection are on FIFO services.

III. ALGORITHMS

A. Proposed Classifier Algorithm

Step 1: While receiving ISN(k), calculate
p (u, v, s, t) as in eqn. 1
Step 2: For j = 1 to M compute $d_{k,j}$ distance
between p (u, v, s, t) and all vectors in R
Step 3: Obtain vector d = $[d_{k,1}, d_{k,2},\ldots d_{k,m}]$
Step 4: Get the second order statistics σ^2_k =
var(d)
Step 5: For ISN (k-1), ISN (k-2), repeat the
steps from1 to 4 to get σ^2_{k-1}, σ^2_{k-2}
Step 6: If var > T
Step 7: True++; legal ISN number
Step 8: Else false++; illegal ISN number

B. Ant colony Optimization Algorithm

Step 1: {Initialization}
Initialize $\tau_{i\psi}$ and $\eta_{i\psi}$, $\forall$ ($i\psi$).
Step 2: *{Construction}
For each ant k (currently in state ι) do Repeat choose in probability the state to move into. append the chosen move to the k-th ant. until ant k has completed its solution.
end for
Step 3: {Trail update}
For each ant move ($i\psi$) do compute $\Delta\tau_{i\psi}$ update the trail matrix.
End for.
Step 4: {Terminating condition}
If not (end test)
Go to step 2

Algorithm 1 explains the classification of the covert channel data's by means of comparing to the previous trained data. Then classify according to them. Here the incoming data are treated as FIFO process. Whereas algorithm 2 optimize the above process by means of implementing new approach for searching the data for comparison in the way of random search method.

IV. RESULTS

Two algorithms are implemented namely PRM Classifier algorithm and Ant colony optimization algorithm. Optimization technique, Ant Colony Optimization (ACO) method is introduced to optimize the covert channel detection by means of decreasing work load such as Computational time, speed and also it provide Covert channel differentiation from legitimate channels and present an new detection measures that provide best detection rates using Parallelization of ACO Algorithm.

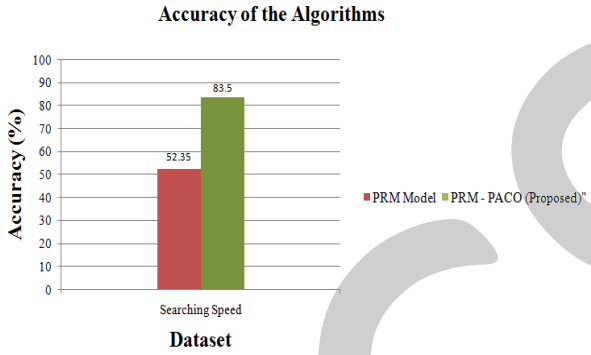

Fig 5.1 Comparison Graph

This graph shows comparison of both the methods.

V. CONCLUSION AND FUTURE ENHANCEMENT

The huge amount of data transmitted over Internet by using TCP/IP protocols makes it ideal as a carrier in steganography. Attacks based on covert channels become a potential threat to the Internet. Covert channels based on the reserved fields, unused combinations of flag field of TCP/IP header, or modification of some header fields can be easily detected or removed. Detecting covert channels in TCP ISN field is known as one of the most difficult covert channels to be detected. Proposed method uses the Parallel ACO to detect covert channels in the ISN field with more efficient manner.

In Future to develop a system which provides a solution to achieve high-performance traffic classification without time-consuming training samples labelling. Moreover, a big challenge for current network management is to handle a large number of emerging applications, where it is almost impossible to collect sufficient training samples in a limited time.

REFERENCES

[1]. S. Zander, G. Armitage, and P. Branch, "A survey of covert channels and countermeasures in computer network protocols," IEEE Commun. Surveys Tuts. vol. 9, no. 3, pp. 44 – 57, 3rd quarter, Mar 2007.

[2]. Xiapu Luo, Peng Zhou, Edmond W. W. Chan, Rocky K. C. Chang and Wenke Lee, "A Combinatorial approach to Network Covert Communications with Applications in Web leaks," dsn, IEEE/IFTP International Conference on Dependable Sys and Net, pp. 475-485, 2011.

[3]. D. V. Forte, C.Maruti, M. R. Vetturi, and M. Zambelli, "SecSyslog: An Approach to secure logging based on covert channels," in Proc. First Int. Wksp. Systematic Approaches to Digital Forensic Engineering, pp. 248–263, Nov 2005.

[4]. Ping Dong, Huanyan Qian, Zhongjun Lu, and Shaohua Lan, "A Network Covert Channel Based on Packet Classification" International Journal of Network Security, Vol.14, No.2, PP. 109-116, Mar 2012.

[5]. Zhenghong Wang, Jing Deng, and Ruby B. Lee. "Mutual Anonymous Communications: A New Covert Channel Based on Splitting Tree MAC" IEEE INFOCOM, 2008.

[6]. Taeshik Shon and Jongsub Moon, "A hybrid machine learning approach to network anomaly detection", Information Sciences 177 (2007) 3799–3821.

[7]. X. Luo, E. Chan, and R. Chang, "TCP covert timing channels: Design and detection," in Proc. IFIP/IEEE DSN, 2008.

[8]. Hong Zhao, and Yun-Qing Shi, "Detecting Covert Channels in Computer Networks Based on Chaos Theory", Dec 2013.

[9]. David N.,Muchene, Klevis Luli, and Craig A. Shue, "Reporting Insider Threats via Covert Channels" IEEE Security and Privacy Workshops, 2013.

[10]. C. Brodley and C. Shields, "IP covert channel detection," ACM Trans. Inf. Syst. Security, vol. 12, no. 4, Article 22, 2009.

[11]. S. Gianvecchio and H. Wang, "Detecting covert timing channels: An entropy-based approach," in Proc. ACM CCS, 2008.