UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

Design Enhanced, Undetectable & Robust Analog Fountain Timing Channels for VoIP and SSH Traffic

Mandeep Kaur[1], **Harsimranjeet Singh**[2]

ECE Dept, GIMET, Global Institute of Management & Emerging Technologies[1,2]

Abstract: In wireless and wired communication, several problems are faced such as noise, security of data, distortion etc. Reliable and secure communication is demanded in modern era. Today is the world of communication, there are so many applications such as IMO, VoIP, Skype required reliable and secure communication. For secure communication various methods and techniques are used. In earlier days, only encryption was used for the purpose of security. Another term also available such as steganography and cryptography and these terms are used in computer security. At present, covert channels are used for the secure transmission of data. Covert channels are of two types such as covert timing channels and covert storage channels. Covert timing channels are those which use timing properties of some communication channel and these are designed for passing unauthorized information and they passed the information at the speed at which things happen. But these covert timing channels controls time between transmissions of packets in overt communication. Different parameters are available to measure the performance of covert timing channels such as undetectability, robustness, delay, traffic received, traffic sent and collision count. Covert timing channels play a critical role in telecommunication, defence, banking etc. But main problem occurs in these channels is noise. So this paper aims to enhance the performance of covert timing channels by comparing different networks. Covert timing channels used for the purpose of security in different applications such as VoIP, SSH. The main properties of covert timing channels are undetectability and robustness. Covert timing channels are used to avoid unauthorized access from criminals, hackers & terrorists etc. But there are some disadvantages of covert timing channels, e.g. terrorists use covert channels to coordinate their actions. This paper also discusses about applications of covert timing channels.

Keywords: Covert Timing Channels, Security, Delay.

1. INTRODUCTION

Today in the world of communication e.g. VoIP, Skype, IMO etc. and many more but these applications required reliable secure & undetectable transmission of data, and to secure data from unauthorized access. In network covert timing channel mechanism behind transfer of secret information is carried by modification of timing properties of network traffic. So many apps such as IMO, SKYPE and Whatsapp are few of them which provides us platform to communicate. But the main point is that communication should be secure, and this security should be provided with the help of various techniques such as covert channels, encryption, steganography and information hiding etc.VoIP, Skype etc. and many more but these applications required reliable, secure & undetectable transmission of data. In network covert timing channel transfer of secret information is carried by modification of timing properties of network traffic, while transmission of data taken place.

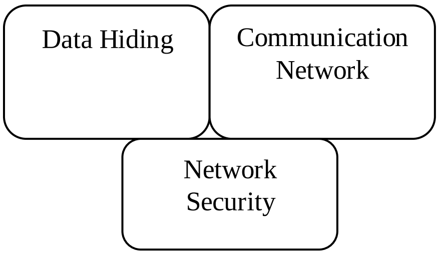

Fig. 1 Covert Channel Analysis and Data Hiding

Two main types of covert channels: storage channels that alter the medium's bits(e.g. jpeg, audio files or packet headers) & timing channels that embed a covert message timing characteristics of overt carrier(e.g. disk head timing, time between phone calls, or inter-packet delays). Here, sender and receiver shared codebook. Robustness and undetectablity are two main properties of timing covert channels were introduced with a new design methodology. The covert receiver

DOI10.17148/IARJSET.2017.4757

performs iterative demodulation/decoding of covert message for high level of robustness. Communication channel that can be exploited by a process to transfer information in a manner that violates a system's security policy. Covert timing channel manipulates the timing or ordering of events to transfer information. Information leaked by controlling the time between transmissions channels in network timing channels. Here two contributions were done, first is to quantify the threat posed by covert network timing channels, other is to use timing channels to communicate at a low data rate without being detected.

2. MECHANISM OF COVERT CHANNELS

The mechanism behind covert communication is that information is transmitted in a way that is difficult to detect. Packet networks communicate through packet contents and their headers.

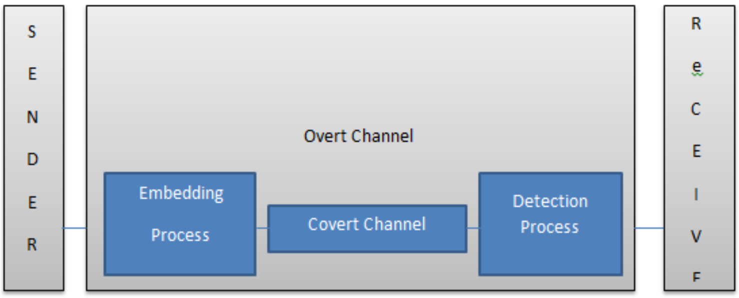

Fig. 2 Covert Communication by sender and receiver

The following are the characteristics of covert channels:

- Undetectability
- Robustness
- Covert Rate

Undetectability means channel should not be detectable to some monitoring system. This means that covert channel must be measureable by the intended recipient only. Existence of a file or time used for a computation, have been the medium through which a covert channel communicates. But covert channels are not easy to find because these media are so numerous and frequently used. A covert channel is so called because it is hidden from the access control mechanisms of ultra-high-assurance secure operating system, since it does not use the legitimate data transfer mechanism of the computer systems, and therefore cannot be detected or controlled by hardware based security mechanisms. Covert channels are hard to install in real systems. A covert time is undetectable according to some statistical test, if the test cannot distinguish between legitimate and covert traffic.

Robustness is a property of covert channel which is use to handle delay or error during transmission. The goal in designing a robust covert channel is to deal with the inherent network noise (e.g., network jitter), and prevent active adversaries from disrupting the covert channel by introducing additional noise into the channel (i.e., jamming). In fact, it is shown that adding random delays into inter-packet delays of the overt traffic can effectively diminish the throughput of timing covert channels in communication networks. In advance systems the covert message is directly embedded into the Inter-Packet Delays (i.e., IPD) of the overt traffic.

The another property of covert channel is covert rate. The covert rate is defined as exchange rate of covert information between covert sender and receiver. The covert rate should be as high as possible. Thus, these three characteristics robustness, undetectability and covert rate are used to measure the performance of covert channels.

3. PARAMETERS ENHANCED THE PERFORMANCE OF ANALOG FOUNTAIN TIMING CHANNELS

- Delay
- Packet Loss
- Traffic Received
- Traffic Sent
- Collision Count
- Load (bits per sec)

Implementation of Analog Fountain Timing channels is done in this work to enhance timing channel scheme for all kind of VoIP and SSH traffic by using efficient packet processing techniques and BP algorithm is used for high noise levels by removing convergence problem for higher noise power. By using this process performance of analog fountain timing channels can be enhanced. Timing channels allow multi user access to single channel. Wireless transmission links suffers from severe channel impairments, including noise, fading, path loss and interference. Thus, how to effectively increase the throughput of a wireless transmission in such time-varying channel has been one of the key researches focuses in wireless communications. Ideally, to achieve high throughput, the communication protocol needs to adapt well to variations in noise, fading, interference and so on, while performing well in all channel conditions. Having a general solution for all VoIP and SSH traffic will help in establishing solution for common channels for communication. The research will be focused on development of generic solution that can be used with all types of VoIP and SSH traffic.

4. SIMULATOR

In this paper, network simulator, Optimized Network Engineering Tools (OPNET)modeler 17.5 has been used as a simulation environment. OPNET is a simulator built on top of discrete event system (DES) and it simulates the system behaviour by modelling each event in the system and processes it through user defined processes. OPNET is very powerful software to simulate heterogeneous network with various protocols. then Results will be collected with these three different simulations of different networks then we will analysis which one is better with different performance metrics such as delay, traffic sink, traffic source, collision count, load, traffic received etc., performance has been measured on the basis of these parameters. In this proposed work network model is created. First of all model of a practical network is converted into a virtual network by using OPNET 17.5. Three networks are created, each of 20 nodes and among them node no. 17, 19 and 20 are used as covert channels. The performances of analog fountain timing channels are determined by different factors such as delay, packet loss, traffic sink etc. To create network, first nodes are selected from Object Palette we choose 19 ethernet wsksn, 1 ethernet-32 hub and these all are connected through 100 Base T. After that Profile is configured from Profile configuration. The next step is to configure reports and select ATM, Ethernet, FTP, LTE, TCP and UMTS. Then define statistics reports, e.g. Global statistics, Node statistics and Link statistics. Then the next step is to run simulation of these three networks and after the simulation is run different parameters are evaluated such as status, host name, simulation duration, simulation time elapsed, time elapsed, time remaining, num events, total memory, average events, current events, num log entry, output suffix, inter-arrival time. Finally then Results will be collected with these three different simulations of different networks then we will analysis which one is better with different performance metrics such as delay, traffic sink, traffic source, collision count, load, traffic received etc., performance has been measured on the basis of these parameters. Here, comparison is done among three Discrete Event Simulations. The network topology composed of the following network devices and configuration utilities:

- Ethernet wkstn
- Ethernet-32 hub
- 100 Base T

The network topology design is based on the layout of campus Network. We considered Ethernet Nodes, Ethernet Hub and 100 Base T in accordance with scenario correspondingly are taken. As far as real time applications are concerned in our thesis work, the Reports are set to support ATM, Ethernet, FTP, LTE, TCP and UMTS.

Discrete Event Simulation 1
Then individual DES statistics was chosen that would be viewed in the results from the DES menu. Finally, time duration to run the simulation was set.

Discrete Event Simulation 2
The DES 2 shows the results of second network and results are better than DES 1.

Discrete Event Simulation 3
The DES 3 shows the results of third network and results are better than DES 1 and DES 2.

5. RESULTS AND ANALYSIS

5.1 Global Statistics Results

In OPNET results are basically collected from two types of statistics, first one is Global statistics and another one is Object statistics. The main difference in between these two is that in Object statistics results collected from individual nodes and in Global statistics results collected from entire network.
Delay (bits/sec) of Network 1, 2, 3
Delay of network 1,2,3 are shown below which is improved in network 3.

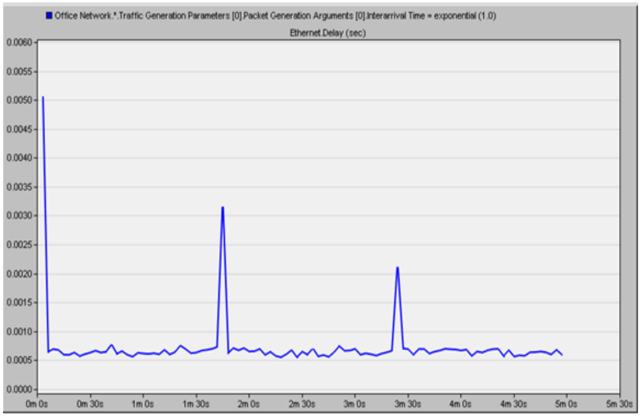

Fig. 3 Delay (sec) of DES 1

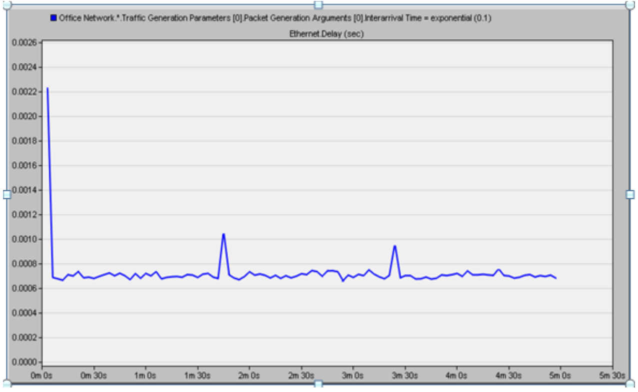

Fig. 4 Delay (sec) of DES 2

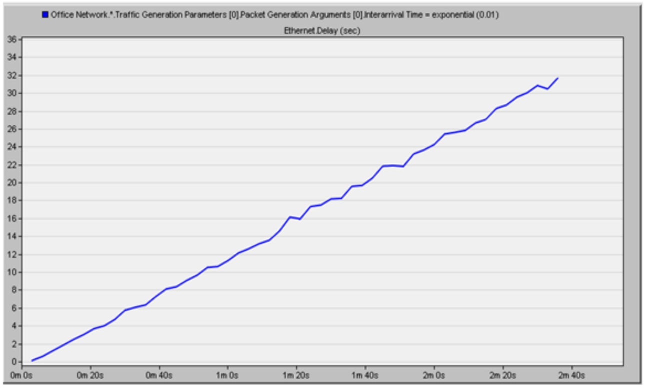

Fig. 5 Delay (sec) of DES 3

Traffic Received (bits/sec)
Traffic Received of network 1,2,3 is shown below which is improved in network 3.

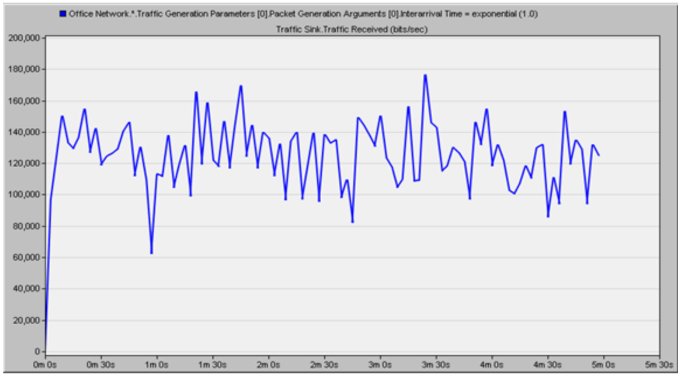

Fig. 6 Traffic Received (bits/sec) of DES 1

DOI10.17148/IARJSET.2017.4757

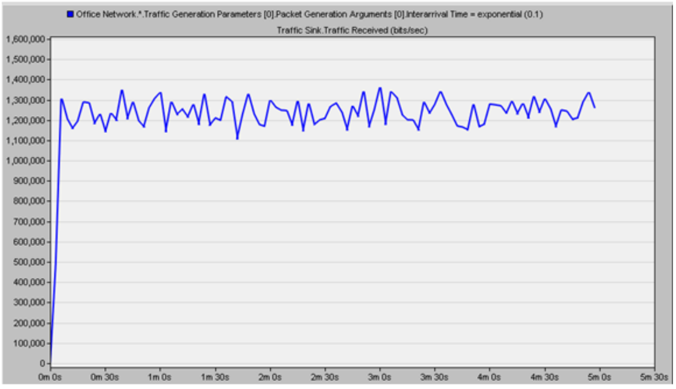

Fig. 7 Traffic Received (bits/sec) of DES 2

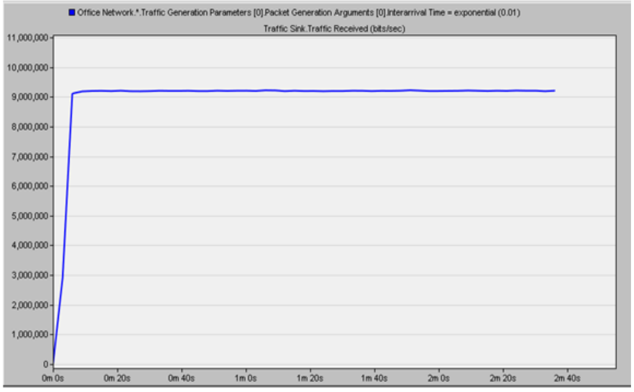

Fig. 8 Traffic Received (bits/sec) of DES 3

Traffic Sent (bits/sec)
Traffic Sent of network 1,2,3 is shown below which is Improved in network 3.

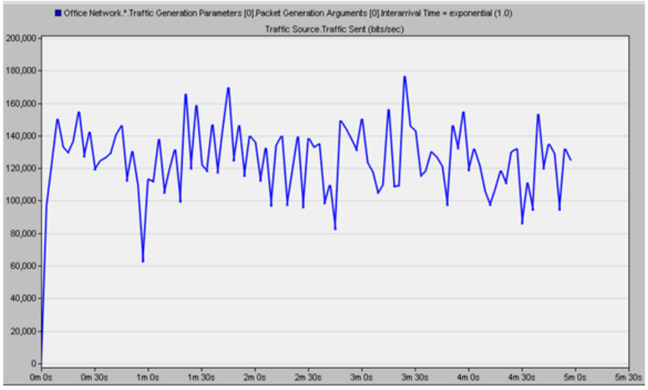

Fig. 9 Traffic Sent (bits/sec) of DES 1

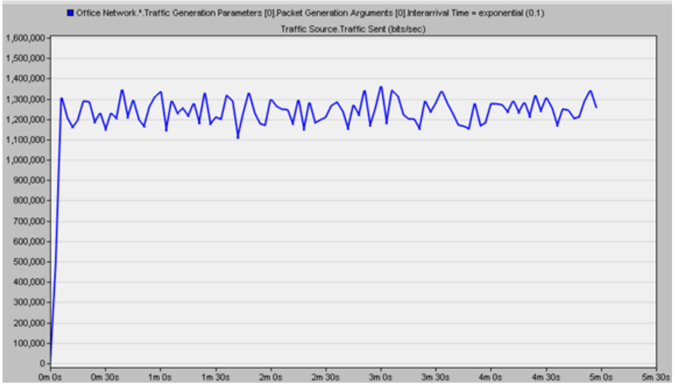

Fig. 10 Traffic Sent (bits/sec) of DES 2

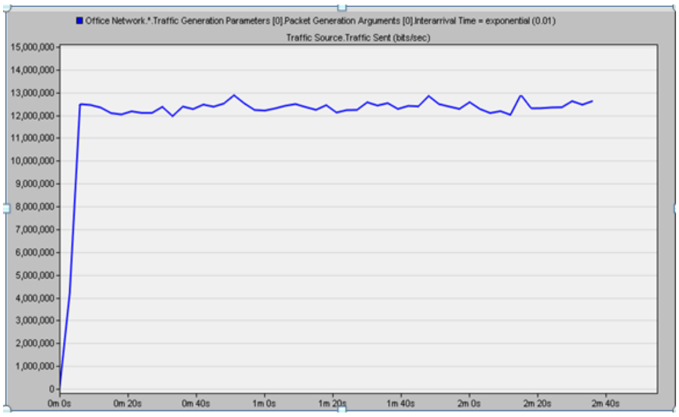

Fig. 11 Traffic Sent (bits/sec) of DES 3

Collision Count

Collision Count of network 1,2,3 is shown below which is Improved in network 3 and number of packets also increased.

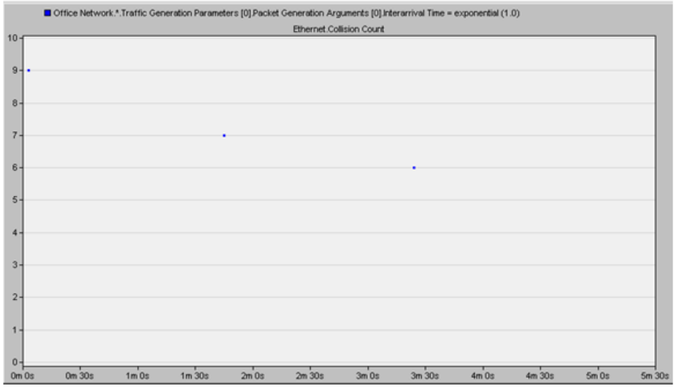

Fig. 12 Collision Count of DES 1

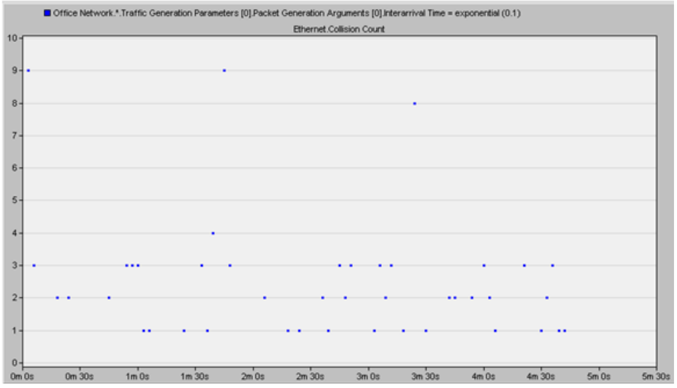

Fig. 13 Collision Count of DES 2

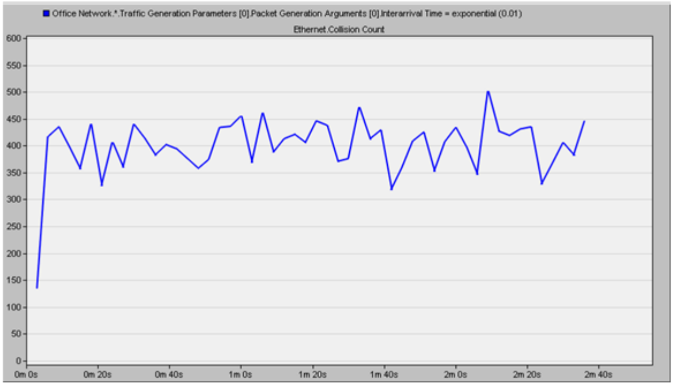

Fig. 14 Collision Count of DES 3

Copyright to IARJSET

DOI10.17148/IARJSET.2017.4757

6. CONCLUSION AND FUTURE WORK

In this paper, we have presented a comparative analysis of three networks of covert timing channels. Performance has been measured on the basis of some parameters that aimed to figure out the effects of analog timing channels. In our paper work, the simulation result has shown that third network provides us best results with Respective performance metrics – Delay, Traffic Sink, Traffic Source, Collision Count, Load, Traffic received etc. All the Network Performance has depended on its parameters. Different parameters have different attributes according to their environmental scenarios. From Simulator aspects we concluded that which is major factor that can affect the performance of Network that is Network size. The comparative analysis has been done between three networks for real time applications. Performance has been measured on the basis of some parameters that aimed to figure out the effects of covert channels. In this thesis, For this Research paper different Networks size are implemented with three networks each of 20 Nodes and Results are obtained from these Networks with Respective Performance Metrics Delay, Traffic Sink, Traffic Source, Collision Count, Load, Traffic received etc. In future, a research work can be done on the new analog fountain timing channels also and others Performance metrics also can be taken to enhance the performance of timing channels.

REFERENCES

[1] V. Paxson and S. Floyd, “Wide area traffic: The failure of Poisson modeling,” IEEE/ACM Trans. Netw., vol. 3, no. 3, pp. 226–244, Jun. 1995.

[2] J. Cao, W. S. Cleveland, D. Lin, and D. X. Sun, “On the non stationarity of Internet traffic,” in Proc. SIGMETRICS, vol. 156, no. 3, pp. 102–112, 2001.

[3] C. Cachin “An information-theoretic model for steganography,” Inf. Compute., vol. 192, no. 1, pp. 41–56, Jul. 2004.

[4] A. Shokrollahi, “Raptor codes,” IEEE Trans. Inf. Theory, vol. 52, no. 6, pp. 2551–2567, Jun. 2006.

[5] X. Luo, E. W. W. Chan, and R. K. C. Chang, “TCP covert timing channels: Design and detection” in Proc. IEEE Int. Conf. Dependable Syst. Netw., vol. 45, no. 4, pp. 420-429, Jun. 2008.

[6] S Gianvecchio, H. Wang, D. Wijesekera, and S. Jajodia, “Model-based covert timing channels: Automated modeling and evasion,” in Proc. Symp. Recent Adv. Intrusion Detect., vol. 34, no.3, pp. 211-230, 2008.

[7] N. Kiyavash and T. Coleman. “Covert timing channels codes for communication over interactive traffic,” in Proc. IEEE Int. Conf. Acoust., Speech Signal Process, vol. 5, no. 6, pp. 1485-1488 Apr. 2009.

[8] S.H. Sellke, C.-C. Wang. S. Bagchi, and N. Shroff, “TCP/IP timing channels: Theory to implementation,” in Proc. IEEE Conf. Comp. Communication (InfoCom), vol. 2, no. 7, pp. 2204-2212 Apr. 2009.

[9] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “Digital image steganography: Survey and analysis of current methods,” Signal Process., vol. 90, no. 3, pp. 727–752, Mar. 2010.