ISSN 2250-0987
*Ripal shah* et al, UNIASCIT, Vol 2 (1), 2012, 147-148

# A Survey of Traffic Analysis

**Ripal Shah**[1], **Sandip Chauhan**[2]

[1]*Dept of computer science and engineering,*
*Gujarat technological university, Ahmedabad, Gujarat, India.*
[2]*Kalol institute of technology,*
*Kalol, Gandhinagar, Gujarat, India.*

**Abstract:** In recent years not only use of internet is increased very rapidly but attackers on internet increased. The use of internet nothing but a transferring of data from one place to another place now when many users at a time transferring data from one place to another that create traffic. It is very desirable to perform data analysis on traffic aggregated over thousands of node; which will provide network operator with a holistic view of network operation. Recently attackers are attacking on internet traffic. This is noble idea way to attack on internet. Now in this survey paper, we proposed a way that analyzed or detect traffic. Combinations of hardware and software tool what can detect decode and manipulate traffic on the network.

**Keywords:** Information security, network security, computer security, confidentiality, integrity, availability, active attack, passive attack, traffic analysis, network traffic monitoring, network traffic measurement

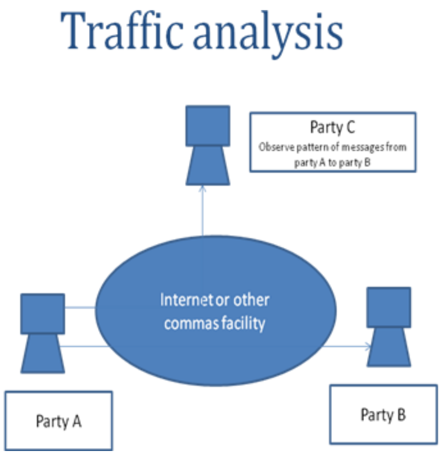
## INTRODUCTION

Meaning of Information Security is protecting the information. Information system from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. The computer security and network security are in Information security. The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. The Network Security consists of provisions and policies by network administrator. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Network security covers a variety of computer networks, both public and private[1].

Information security fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information. Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. In information security, integrity means that data cannot be modified undetectably. For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Authenticity and non-repudiation are goals of protecting information such as that in computing, e-Business and information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are and non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer[1].

In network security involve active attack and passive attack. Firstly introduced Active attack such that some modification of data stream or creation of false stream. Sender or receiver is aware that a third party has read message or observed traffic pattern easily identified attacks. This type of attack requires the attacker to be able to transmit data to one or both of the parties, or block the data stream in one or both directions. It is also possible that the attacker is located between the communicating parties. And second introduced Passive attacks such as the process of intercepting and examining of messages in order to deduce information from pattern in communication. Performed even when messages is encrypted but can not decrypted. It is concerned to computer security. Bit patterns can be made not to leak information. Passive attack "attempts to learn or make use of information from the system but does not affect system resources"[1].

Above all contents are the basic information of area of information security. In information security, the attack of traffic analysis is introduced here.


Traffic analysis
Party C
Observe pattern of messages from party A to party B
Internet or other commas facility
Party A
Party B

**TRAFFIC ANALYSIS:**

**Traffic analysis** is the process of intercepting and examining messages in order to **deduce information from patterns** in communication. Traffic analysis is also a concern in computer security.[2] An attacker can gain important information by monitoring the frequency and timing of network packets. In traffic analysis attacks, it is performed encrypted but not decrypted messages. Traffic analysis can be performed in the context of military intelligence or counter-intelligence, and is a concern in computer security[3]. Bit-patterns can be made not to leak any information."The art of using communication meta-data to infer information about network nodes identities or characteristics, their relations or actions in the network". It can be used: Radio commas, Trace IP traffic, HTTP log analysis, Spam filtering, Compromise the security properties of hardened systems[4].

Very little has done to look at information leaked and minimizing this leak from communication traffic data. Traffic data comprised the time and duration of a communication, the detailed shape of the communication streams.

Sniffer attack also read, monitor and capture network data exchanges and read network packets. If packets are not encrypted, a sniffer provides a full view of data inside packet. Even encapsulated packets can be broken open and read unless they are encrypted and attacker does not have access to key[5].

We need to monitor and measure bandwidth because to know if the Internet Service Provider is providing us if the required bandwidth, to be able to optimize the available bandwidth and 59% of institution do not monitor for manage bandwidth. we understand the traffic monitoring and traffic measurement as following.

**Traffic Measurement and Monitoring**:

**Network traffic measurement** is the process of measuring the amount and type of traffic on a particular network[4].

**Network monitoring** monitors a computer network for slow or failing systems and that notifies the network administrator via email, pager or other alarms[4].

**Network monitoring techniques:**

There are two techniques active monitoring and passive monitoring. **Active monitoring** reduce system overhead by using small number of probe packets that have smaller sizes compare to real data packet so that performance measures may not be accurate. **Passive monitoring** monitors a lot of data packets, it has system overhead problem so that its performance is more accurate and reliable than active monitoring[4].

**Conclusion:**

In this paper, we surveyed those basic types of attacks whatever how do work in system and how damaged information does. Such as traffic analysis attacks not only can be used to collect more information but can be used to bypass security mechanisms in place. The informations do not leak or not modified but just read or learning or monitoring and analysis activities.

**References:**

[1] Attack and Defense by RogerNeedham And Butler Lampson,chap:18 in 367-390

[2]Introducing Traffic Analysis Attacks, Defences and Public Policy Issues by George Danezis K.U. Leuven, SAT/COSIC, Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium.

[3]Traffic Analysis for Network Security
using Learning Theory and Streaming Algorithms by Shobha Venkataraman, CMU-CS-08-157, September 2008

[4Introduction to Traffic Analysis by George Danezis University of Cambridge,
Computer Laboratory.

[5]Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems by Jean-Franc¸ois Raymond Zero-Knowledge Systems, Inc. jfr@zeroknowledge.com
19th December 2000

[6]F-TAD: Traffic Anomaly Detection for Sub-Networks using Fisher Linear Discriminant by Hyunhee Park,dept. of Electical Engineering korea university seoul,korea; Meejoung Kim,Research Institute for Information and Communication Technology, Korea University seoul, korea and Chul-Hee Kang,
Dept. of Electrical Engineering, Korea University, Seoul, Korea