Title : Packet Sniffer

Description:

A packet sniffer — also known as a packet analyzer, protocol analyzer or network analyzer — is a piece of hardware or software used to monitor network traffic. Sniffers work by examining streams of data packets that flow between computers on a network as well as between networked computers and the larger Internet.

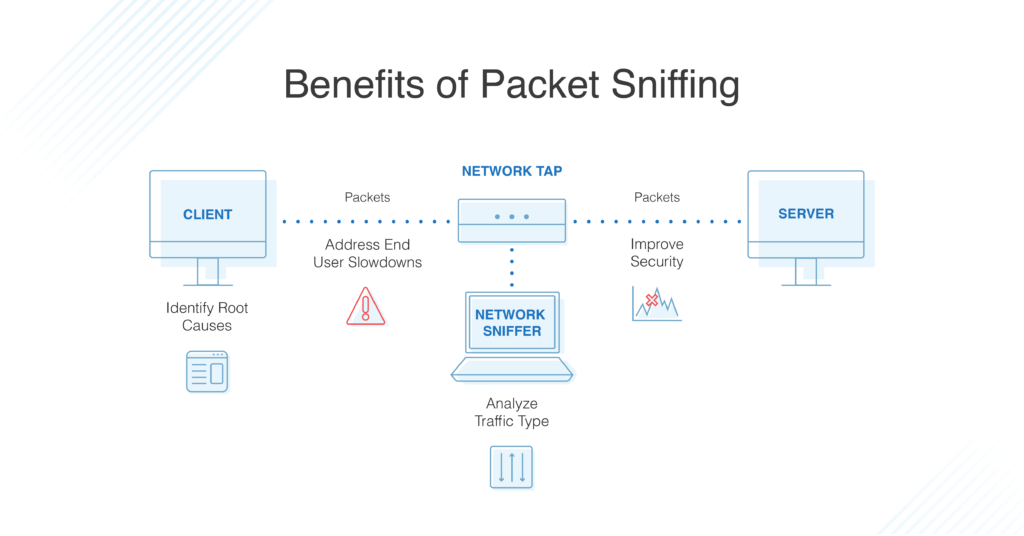
Packet sniffers can be used on both wired and wireless networks — their efficacy depends on how much they are able to "see" as a result of network security protocols. On a wired network, sniffers might have access to the packets of every connected machine or may be limited by the placement of network switches. On a wireless network, most sniffers can only scan one channel at a time, but the use of multiple wireless interfaces can expand this capability.

Area\Concept Involved:

It is recommended you have a foundational knowledge of TCP/IP, familiarity with the OSI model, a basic understanding of how computer networks work, and knowledge of the different types of network packets (e.x. HTTP, ARP, etc).

Sniffing Tools are:

1. Tcpdump : it is a powerful tool that allows us to sniff network and make some statistical Analysis out of those dumps.
2. Sniffit : Robust packet sniffer with good filtering.
3. Ethereal: A free network protocol analyzer for UNIX and Windows. It allows you to examine data from a live network or from a capture files on disk.
4. Hunt: The main goal of the HUNT Project is to develop tools for exploiting well-known weakness in the TCP/IP protocol suite.
5. Dsniff : It is a collection of tools for network auditing and penetration testing.
6. IP Spoofing: When the sniffing program is on a segment b\w two communicating end points, the intruder can impersonate one end in order to hijack the connection.



BENEFITS OF PACKET SNIFFING

1. [Detecting the Root Cause of a Network Issue](https://www.tek-tools.com/network/all-about-packet-sniffers#detecting-root-cause)
2. [Troubleshooting Network Issues](https://www.tek-tools.com/network/all-about-packet-sniffers#troubleshooting-network)
3. [Traffic Analysis](https://www.tek-tools.com/network/all-about-packet-sniffers#traffic-analysis)
4. [Bandwidth Management](https://www.tek-tools.com/network/all-about-packet-sniffers#bandwidth-management)
5. [Network Security and Compliance](https://www.tek-tools.com/network/all-about-packet-sniffers#network-security)

SOME PACKET SNIFFERS

1. [SolarWinds Network Performance Monitor](https://www.tek-tools.com/network/all-about-packet-sniffers#solarwinds-npm)
2. [ManageEngine NetFlow Analyzer](https://www.tek-tools.com/network/all-about-packet-sniffers#manageengine-na)
3. [PRTG Network Monitor](https://www.tek-tools.com/network/all-about-packet-sniffers#prtg)
4. [Wireshark](https://www.tek-tools.com/network/all-about-packet-sniffers#wireshark)
5. [Tcpdump](https://www.tek-tools.com/network/all-about-packet-sniffers#tcpdump)
6. [OmniPeek Network Protocol Analyzer](https://www.tek-tools.com/network/all-about-packet-sniffers#omnipeek)
7. [NetworkMiner](https://www.tek-tools.com/network/all-about-packet-sniffers#networkminer)
8. [Colasoft Caspa](https://www.tek-tools.com/network/all-about-packet-sniffers#colasoft)

We are making Packet Sniffer using Linux and C programming Language.

We can either code by using Sockets api provided by Kernel or by using some Packet Capture Library Like LIBPCAP.

Socket API : The socket API is a collection of socket calls that enable you to perform the following primary communication functions between application programs: Set up and establish connections to other users on the network. Send and receive data to and from other users.

Libpcap : Libpcap allows us to capture or send packets from a live network device or a file. These code examples will walk you through using Libpcap to find network devices, get information about devices, process packets in real time or offline, send packets, and even listen to wireless traffic.

SOME IMPORTANT LINKS :

CODE IN C :

Source 1: <https://www.binarytides.com/packet-sniffer-code-c-linux/>

Source 2 : <http://simplestcodings.blogspot.com/2010/10/create-your-own-packet-sniffer-in-c.html>

**INTRODUCTION:**

**Purpose:**

The main objective of this system shows how real time network connection behaviour can be modelled as chromosomes and how the parameters in genetic algorithms can be defined in this respect.

**SCOPE OF THE PROJECT:**

The main objective of this project shows how network connection information can be modelled as chromosomes. The objective of the system is to create a new set of rules during run time. So the intruder cannot be able to attack the system with viruses.

In recent years, Intrusion Detection System (IDS) has become one of the hottest research areas in Computer Security. It is an important detection technology and is used as a countermeasure to preserve data integrity and system availability during an intrusion.

An Intrusion Detection System is a system for detecting intrusions and reporting them accurately to the proper authority. Intrusion Detection Systems are usually specific to the operating system that they operate in and are an important tool in the overall implementation of an organisation's information security policy, which reflects an organisation's statement by defining the rules and practices to provide security.

A methodology of applying genetic algorithms into network intrusion detection technique is unique as it considers both temporal and spatial information of network connections during the encoding of the problem; therefore, it should be more helpful for identification of network anomalous behaviours.

**About the Project:**

This project aims at developing a Network Packet Sniffer. Network Packet Sniffer is a piece of software that monitors all network traffic. This is unlike standard network hosts that only receive traffic sent specifically to them. As data streams flow across the network, the sniffer captures each packet and eventually decodes and analyses its content. For network monitoring purposes it may also be desirable to monitor all data packets in a LAN and to mirror all packets passing through a shared bus.

This project will be comprised of three modules namely the User Interface module, Statistics module and Packet Analysis module. User Interface module provides all the Graphical Interface components necessary for the user to interact with the System. The Analysis Module will analyze the incoming packets into a computer, identify them and passes the information into the Statistics module. Finally the statistics module does the necessary calculation based on the information and produce information that can be understood by the user.

This system is thus very useful to the users and a network administrator in particular who is generally responsible for monitoring things on a network.

This system is a network analyzer (also known as protocol analyzer & packet sniffer), it performs real-time packet capturing, 24x7 network monitoring, advanced protocol analyzing, in-depth packet decoding, and automatic expert diagnosing. It allows you to get a clear view of the complex network, conduct packet level analysis, and troubleshoot network problems.

This system is useful for a network administrator who needs to identify, diagnose, and solve network problems, a company manager who wants to monitor user activities on the network and ensure that the corporation's communications assets are safe, or a consultant who has to quickly solve network problems for clients.

This provides an administrator with a full set of reports such as Summary view, Endpoints view, and Protocols view.

NETWORK PACKET SNIFFER is a desktop application which facilitates online monitoring of packets which are traveling over the network..

NETWORK PACKET SNIFFER I is a tool in which the packets source and destination addresses and other information is captured

The source and destination address protocols that are used by a connection are also monitored and detected

The graph or charts displayed on the valuation and need .

The monitored packets source and destination address is captured. This shows the traffic on a network.

**EXISTING SYSTEM :**

As a network administrator who needs to identify, diagnose, and solve network problems, a company manager who wants to monitor user activities on the network and ensure that the corporation's communications assets are safe, or a consultant who has to quickly solve network problems for clients. It is difficult to identify the problems if the network traffic is not tracked, as an administrator in general we depend on the analyzer provided by the operating system (if any) or the anti virus software that is installed to provide real-time network security. However, it is identified that these systems provide specific set of reports which may not be enough for an administrator to trace all the problems. To handle these types of issues we want to implement a specific network analyzer that can track all the incoming and outgoing calls.

The Conversations tab allows us to monitor network traffic by each conversation and the figure out which conversation has generated the largest network traffic.

**Drawbacks with the Existing System:**

· Administrators need to put lot of efforts to identify the traffic

· Time taking process.

· No possibility of automatic network control.

· Presence of administrator is compulsory.

**PROPOSED SYSTEM**

As a network analyzer (as a. packet sniffer), this system make it easy for us to monitor and analyze network traffic in its intuitive and information-rich tab views. With this system network traffic monitor feature, we can quickly identify network bottleneck and detect network abnormities. This article is to discuss how we can monitor network traffic with this network traffic monitor feature.

This system provides a Summary view that provides general information of the entire network or the selected node in the explorer. In Summary view we can get a quick view of the total traffic, real-time traffic, broadcast traffic, multicast traffic and so on. When we switch among the node from the explorer, corresponding traffic information will be provided.

The Endpoints view; we can monitor network traffic information of each node, both local and remote. With its easy sorting feature we can easily find out which host is generating or has generated the largest traffic.

The Protocols view will list all protocols applied in network transmission. In Protocols view we can monitor network traffic by each protocol. By analyzing network traffic by protocol, we can understand what applications are using the network bandwidth, for example "http" protocol stands for website browsing, "pop3" stands for email, etc.

**Advantages with the proposed system:**

· Network Admin can monitor the packets any where through out the world.

· Traffic can be controlled

· System performance will be increased

· Immediate generation of reports on demand.

· Graphical data is available to analyze the network.