RESEARCH ARTICLE

Monitoring the Network and System Performance for Efficient Data Storage

Birunda Devi.M[1], Vairachilai.S[2]

PG Student[1], Assistant Professor[2]

Department of Computer Science and Engineering,
NPR College of Engineering and Technology,
TamilNadu, India

E-mail: birunda.devi@gmail.com[1], vairachilai2676@gmail.com[2]

Abstract- Network monitoring is becoming a critical component of small and large network areas network traffic data monitoring system that constantly monitors a computer network in order to maintain the system stability and availability. Monitoring the real-time network data streams is crucial for managing and operating data networks. This network traffic monitoring and analysis of fix network problems but also prevent from network failure for good network planning. This network traffic monitoring based on data acquisition method of local traffic flow by packet. And also the recording the packets can be taken on the real time. The users of the network and their data can be monitored and that data can be stored efficiently by the tool bzip2. The bzip2 is a data compression tool for the lossless data compression.

Index terms: network monitoring, traffic data, monitored data compression

I. INTRODUCTION

The network traffic data monitoring and measurement have become more and more important in the current and modern complicated network. In earlier the administrators of the networks have only monitor a few network devices or less than some hundred computers. But today's network administrators have to manage the high speed wired speed wired network and wireless networks. These types of network need more sophisticated network traffic data monitoring and analysis in order to maintain the network system stability and availability and also fix the network problems and ensure the network security strength and also make a good decision for network planning.

The network monitoring is that can be used for logging and analysis of the network traffic flow accurately, utilization and performance analysis of the network. The good network monitoring tools provide the efficient analysis and graphical representation of the status of the network. The network traffic flow information in this category is link utilization, interface bandwidth, and some other information if the device provides. Though the information is just the interface bandwidth, this is very important information for the administrators can monitor the availability of the link, the link usage, and the network usage behavior. This network traffic

characterization is aiming at finding spatial and temporal invariance of TCP/UDP based applications and also network data usages of the users can be monitored and stored efficiently.

Network traffic data analysis is a graphical network monitoring this type of monitoring provides the information about the user's usages on the internet applications. This monitored system can efficiently monitor the application, network, transport layer usage and the simulation of these layers. And this system can also monitor by the administrator and store the user usage of their data and that data can be efficiently stored by tool using the bzip2.

The network traffic can be monitored based on the packets/second, byte/second, or length of frames that can be considered as stochastic time series. This traffic trace can applied a method to the data characterize them in terms of packet inter arrival times and packet lengths. The characterizing the network traffic traces as a form of two time series one is the arrival times of the packets and the other is the packet length in bytes.

II. RELATED WORK

Dainotti et al proposed an approach based on the traffic into conversations and on packet level characterization of traffic inside conversations and that model based on two variables packet size and inter packet time. In the past study packet level approaches have based only on Telnet, FTP, and NNTP but they not analyses the characteristics of applications like HTTP, SMTP, or Peer – Peer traffic. In this packet level characterization can be TCP based applications on HTTP and SMTP. In this they investigate deeply of HTTP traffic modelling and characterization. This HTTP modelling gave two opportunities are well characterized of protocol and compared, contrasted understand of packet level characterization.

Vucetic proposed the information system stores the log files in multiple places for multiple purposes like user monitoring applications, system services, network servers, database management and utilities. The users log files are complex systems and also grow to huge size for the long period of time. These log file storage need convenience and economy. And in this they express the log files as a plain text file. The different five transform for improving better compression. This paper use compression gzip, bzip2 techniques for efficient compression and decompression and their ratios.

Aceto et al proposed the modern network monitoring involves transforms and storing huge amount of data. In this the compression technique reduces the space and time needed for these operations. The telecom operators can be using these in information for a number of tasks. The proposed techniques provide efficient space utilization and perform operations directly on the compressed data. These flows based traffic traces consist of record field timestamp, source IP, destination URL and load. The record represents as a single HTTP conversation. The bzip2 used the lossless data compression.

Ros et al monitoring the real time network data is critical to managing and operating data networks. The traffic data can be a different size and accuracy depending on the measurement task. In this paper express monitoring conditions of the extreme traffic in multiple and continuous traffic queries. This shedding focused only the resource of the CPU cycles. This load shedding proposed the effectively handle the uncontrolled packet losses. It provides the efficient monitoring without packet loss in overload situations.

Cho et al paper proposed the trend of network traffic and find anomaly increasing importance for both network researchers and operators. It expresses collects a set of free tools for building a traffic data repository. This traffic traces collected by tcpdump tool. Traffic traces are in raw format of all header information.

III.PROPOSED SYSTEM

Network packet traces are widely used for source of the internet measurement data for providing a detailed record of the internet traffic traversing on a link. The network traffic data analysis is a process of capturing network traffic and inspecting it closely to determine the network and also known by other names as network analysis, protocol analysis, packet sniffing and packet analysis . The network monitoring is to analyse and visualize the network traffic data both at packet and flow connection levels. The network traffic analysis based on the IP based network. The IP network traffic can provide a review of various statistical distributions utilization. And it provides the information about the layers of the TCP/IP model. These captured packets can be used for analyzing the protocols used by the users. That can be used for the analysis of the improvement of the sensitivity and scalability.

Winpcap is an industry standard open source tool for packet capture and filtering engine it including protocol analysers, network monitors, traffic generators and network testers, network intrusion detection systems, sniffers. It is used for network monitoring access in windows environments. This allows applications to

capture and transmit network packets bypassing the protocol stack. And also it has the kernel level packet filtering. This network monitoring can be for statistics engine and support for remote packet capture.

Jpcap is based on lipcap and is implemented in C and Java library for capturing and sending network packets. It used for develop application for capture packets from the network interface and that captured packet can be visualize/analyze that data. It hides the low level details of the packet captured by the network. And it also an open source library package for the capture network packets.

Preprocessing

Preprocessing is processing the input data and produces the output that can be used as input to another program. Preprocessing is found to predominantly rely on expert domain knowledge for identifying the most relevant parts of network traffic and for constructing the initial candidate set of traffic features. The preprocessor is responsible for preparing packages for analysis In this it performs basic operations such as filtering that the raw traffic input to produce decrease the amount of data which needs to be analysed. Preprocessing module to transform the value of the features of each packet from characters to numeric value provide such functions to allow the user to convert the continuous data into discrete format.

Classification

Classification scheme requires the parameterization of the objects to be classified. The fundamental object of this classified approach is a TCP/IP traffic flow, which is represented as a flow of one or more packets between a given pair of hosts. These traffic monitoring based on the consisting of the IP address. In this classification they can use to classify the preprocessed packets and analysed their protocols like the IPv4, IPv6,ARP,RARP,HTTP,SMTP,POP,FTPUDP, TCP, ICMP and etc., can be classified. And this classification can be based on the TCP/IP layers. Based on this the layer application, network, transport layers usages can be identified and also their usages also classified. And also the every packet detail can be classified and individual data about the packets can be represented by the understandable way.

Visualization

In this visualization can be used for graphical represent the usage of the layers in network traffic. In this represent they can be used pie and line chart for the usage of the network traffic data and their current usages. And also they can express the individual layers usages can be represented as the numbered format of packet size and no of packets.

Monitoring data compression

The monitoring of the network data can be developed at the administrator level. This monitor can be taken as the user's system name in some existing system can be monitored based on the IP address. This system is continuous monitoring can be monitored the behaviours of the users at the time of their usage. This monitored data's can be stored an efficient way for the future analysis of the user's usage. These monitored data can need to store in the efficient way by using the tool bzip2. The bzip2 is a tool for the lossless data compression. This bzip2 use the burrows wheeler algorithm and Huffman coding. This program does not compress multiple files like archives.

IV.PERFORMANCE EVALUVATION

In this type of data capturing network packets can be based on the user usage by using the winpcap, jpcap. And the capture packet can be used for analysed the network data. This capturing can be efficient in LAN compare to WAN. The number of packets capturing in WAN is slow compare to the LAN area networks. The bzip2 is the stores the data efficiently it can store data in data blocks. It can reduce the storage of the monitored data by using the data compression.

V. CONCLUSION

The paper proposed efficient network monitoring and analysis. This work used identify the components are involve in the packet capture, measurement of the packet and identify the usage by simulation. This type of network monitoring can be used on the telecommunication, internet advertisement, and small business areas.

REFERENCES

[1] S. Agrawal, C. N. Kanthi, K. V. M. Naidu, J. Ramamirtham, R. Rastogi, S. Satkin, and A. Srinivasan, "Monitoring infrastructure for converged networks and services," Bell Labs Technical J., vol. 12, no. 2, pp. 63–77, 2007.

[2] Y. Liu, D. Towsley, T. Ye, and J. Bolot, "An information-theoretic approach to network monitoring and measurement," in 2005 IMC.

[3] Dainotti, A. Pescap`e, and G. Ventre, "A packet-level characterization of network traffic," in Proc. 2006 CAMAD, pp. 38–45.

[4] M. Munk, J. Kapusta, and P. Svec, "Data preprocessing evaluation for web log mining: reconstruction of activities of a web visitor," Procedia Computer Science, vol. 1, no. 1, pp. 2273–2280, 2010.

[5] K. Cho, K. Mitsuya, and A. Kato, "Traffic data repository at the WIDE project," in Proc. 2000 USENIX Annual.

[6] M. Peuhkuri, "A method to compress and anonymize packet traces," in Proc. 2001 ACM Internet Measurement Workshop, pp. 257–261.

[7] B. Claise, G. Sadasivan, V. Valluri, and M. Djernaes, "Cisco systems netflow services export version 9," RFC 3954, Oct. 2004, Tech. Rep.

[8] Pescap´e, "Entropy-based reduction of traffic data," IEEE Commun. Lett., vol. 11, no. 2, pp. 191–193, Feb. 2007.

[9] B. Pfaff, "Performance analysis of BSTs in system software," in ACM SIGMETRICS Performance Evaluation Review, vol. 32, no. 1, pp. 410–411, 2004.

[10] M. AdelsonVelskii and E. Landis, "An Algorithm for the Organization of Information". Defense Technical Information Center, 1963.

[11] G. Aceto, A. Botta, A. Pescap´e, and C. Westphal, "An efficient storage technique for network monitoring data," in 2011 IEEE International Workshop on Measurements & Networking.