An Efficient Network Traffic Monitoring for Wireless Networks

M. Uma
Ph.D Research Scholar

G. Padmavathi, Ph.D
Professor and Head

Department of Computer Science
Avinashilingam Institute for Home Science and Higher Education for Women
Coimbatore – 641043

ABSTRACT
Wireless technology has enormous development in the recent years which enable to develop a new wireless system. The importance of transmission to modern wireless networks has lead to the development of several network traffic monitoring techniques. The term traffic monitoring describes the method by which all the data that is sent and received by a network is identified, faults and harmful events are detected and the good data packets are allowed to pass through the networks. Network traffic monitoring is a vital part of cyber security in modern times because of the increasing complexity of the networks and the threats posed by attacks on the network and it is an initial step to capture attacks. Router based monitoring techniques have evinced keen interest in the recent times because of their ease of use, applicability for research and effectiveness in monitoring of the wireless networks. The research work aims to propose an efficient system to monitor network traffic. The proposed system performs two times better than the existing systems.

Keywords: Traffic Monitoring Techniques, SNMP, RMON, Netflow

1. INTRODUCTION
Monitoring of network traffic with accuracy is a difficult process due to the enormous nature of the Internet. Prediction of irregularity of response to the server is extremely complicated. Network performance analysis can be achieved through traffic monitoring [1]. By monitoring the traffic, condition of that particular network can be recognized by the user. Additionally it provides the complete details about the data, resources which are connected with that network. Unauthenticated service or approaches to the server will be identified by regularly monitoring the traffic. The network convention and statistics about the traffic will be known easily which helps to troubleshoot the network. Security events will also be investigated and the entry of the user will be maintained for responsibility. The main objective of this work is to identify and to propose a best technique available to monitor the network.

The structure of this paper is arranged as follows: Section 2 discusses the various traffic monitoring techniques and its classification, In Section 3 simulations and implementation of those techniques are explained. In Section 4 results and comparison of the performance of different methods are discussed. Conclusion is given in Section 5.

2. STATE OF THE ART
There are various traffic monitoring techniques available based on many concepts and they are classified into four types such as Based on Queuing Theory, Based on Forecasting Algorithm, Based on Statistical Method and Monitoring and Analysis Techniques. The network Traffic Monitoring Techniques classification is given in Fig.1

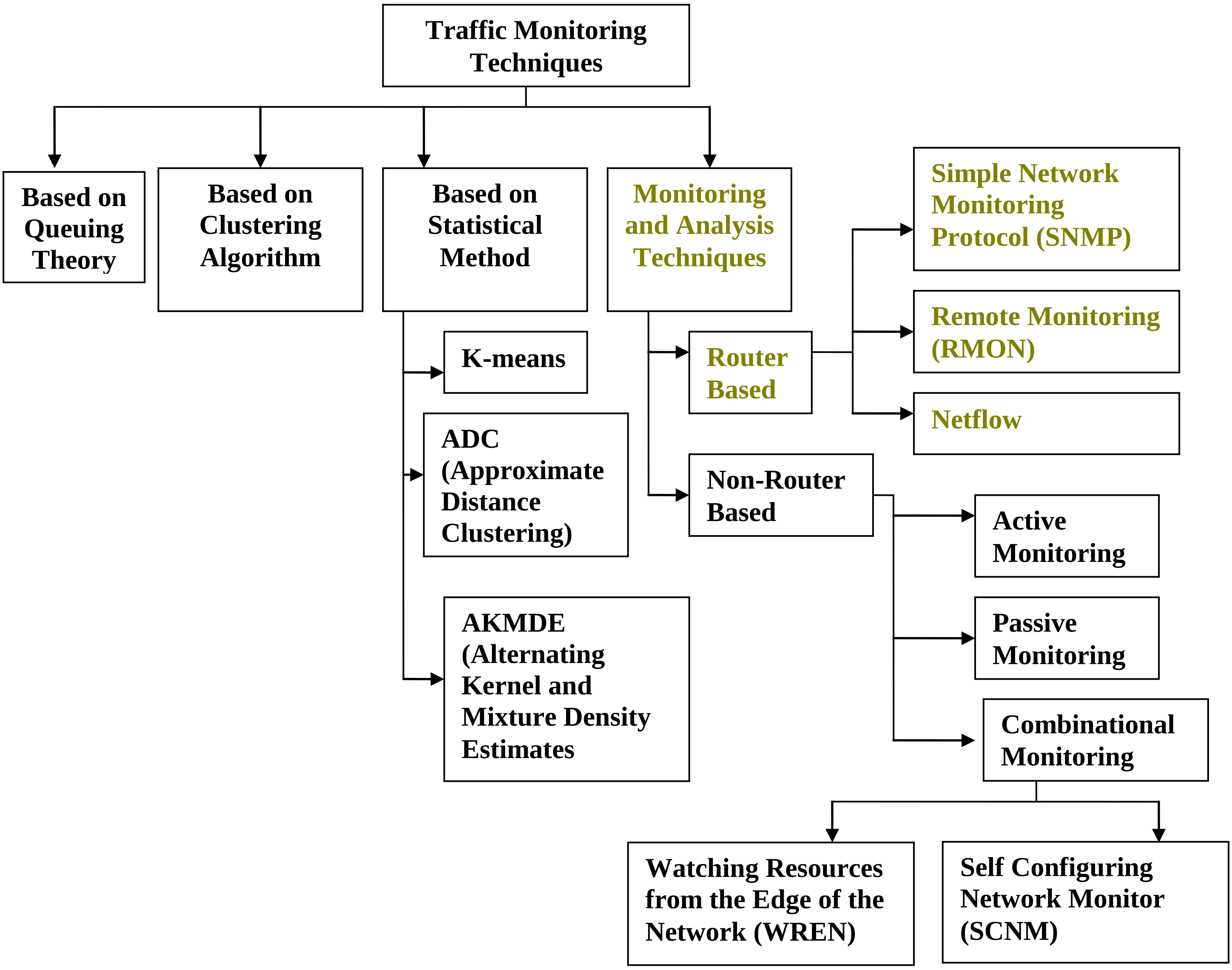

Fig.1 Classification of Network Traffic Monitoring Techniques

2.1. Based on Queuing Theory

One of the most generally used and significant approach to analyze the network performance which helps to get the entire information about the traffic. This method is a division of Operation Research in Mathematics and also it shows the way to make a mathematical model by analyzing the traffic statistics also. The queuing theory allows the network traffic forecasting and permits for the development of stable congestion rate formula [2].

Pros

- Optimize
- Convenient and
- Simple

Cons

- Quantifying
- Analytical solution

2.2. Based on Clustering Algorithm

Clustering algorithm is also used to identify the traffic of transport layer in particular network. Two unsupervised clustering algorithms K-means and DBSCAN are used for the first time to classify the network traffic [3]. Both these algorithms are compared with the existing algorithm AutoClass and it is observed finally concluded that the AutoClass gives the superlative performance in obtaining overall accuracy. DBSCAN has enormous potential in providing connected small subset of the clusters.

2.2.1. K-means Clustering

K-means algorithm is considered to be the most simple and quickest among the available partition-based clustering algorithm. It helps to divide the data set of an object into fixed number of disjoint subsets. The square error is calculated using the necessary formulae. The centres are randomly chosen within the subspace. According to the centres the dataset is partitioned and repartitioned into nearest clusters. The same process will be continued till the final partitioning is done. The pros and Cons [12] of k-means are as follows:

Pros

- The model building time is faster and it is more appropriate

Cons

- Networks are dynamic in nature.

2.2.2. DBSCAN Clustering

DBSCAN means Density Based Spatial Clustering of Applications with Noise. Density attainable and association are the basic concept behind the DBSCAN Clustering. The two input parameters of DBSCAN algorithm are epsilon (eps) and minimum number of points (minPts). The neighborhood of eps and the distance about the object is termed as epsilon. Firstly all the object of the data set are considered to be unassigned and then DBSCAN sets one object as a core and finds out the connected objects based on eps and minPts and finally all those objects are termed as new cluster. The algorithm stops when all the objects are assigned. The pros and cons [3] of DBSCAN are as follows:

Pros

- Potential is enormous

Cons

- Accuracy is low

2.2.3. AutoClass

Automatic selection of the cluster numbers and soft clustering are the basic things done by this algorithm. In order to govern the distinct probability distributions of every cluster Expectation Maximization (EM) algorithm is used to achieve this. Two steps are involved in EM algorithm such as an expectation step and maximization step. The first step helps to predict the parameters of pseudo-random numbers and to re-estimate those parameters and the mean and variance are used so that it is converge to a local maximum. The pros and cons of AutoClass [3] are as follows:

Pros

- Produces the best overall accuracy

Cons

- Time Consuming

2.3. Based on Statistical Method

To make a generalization of network traffic two clustering methods are applied to data of the network. In this technique the machines are clustered into activity groups which help to compare with the recent activity profiles so that it is easy to capture the abnormal status of the network data. The count on the specific port will be monitored for hourly or weekly basis for 993 machines if the counts are strangely high then it is an indication that, it may be a problem. Three algorithms such as k-means, ADC (Approximate Distance Clustering) and AKMDE (Alternating Kernel and Mixture Density Estimates) are used and it is concluded that k-means and ADC are better than use, rather than AKDME [4].

2.3.1. K-means

In any situations, the algorithm works in a simple manner and its implementation is effortless. For TCP and UDP the counters will be kept separately for every count and to generate probability vector size the normalization is prepared with on the whole sum of traffic. It helps to guess the structure of the data. The dimensionality of the data is reduced with the help of projection and model is build with in the projection space. The pros and cons are as follows [4]

2.3.2. ADC (Approximation Distance Clustering)

To select the subset of the data and it is termed as witness set. The distances of each element of the witness set is calculated and the smallest distance keeps hold and it is utilized as a point to earn projected. It is essential to estimate the density of the data when it is projected once for constructing a normal mixture model. Some mathematical formula is used to develop a mixture model. This helps to measure concurrently the number of components and the parameters of component.

Pros

- All type of attacks can be identified
- The quality of this method is better than other methods.

Cons

- The data is high dimensional in nature.

2.3.3. AKMDE (Alternating Kernel and Mixture Density Estimates)

The basic concept of AKMDE is that, a term is added if the parametric model is not adequate where one uses a nonparametric estimator of the density. After that the estimators are compared with one another. To construct the best nonparametric value one uses the mixture and assuming that mixture as a correct and the same process will be continued until mixture matches the estimator sufficiently.

2.4. Monitoring and Analysis Techniques

Recently the importance of Intranets is increasing rapidly in companies, the network administrator must have a clear idea about the traffic and its types so that it will be easy to handle if any problem arises. In this paper summary of the monitoring techniques are classified into two types such as Router Based and Non-Router Based. The most widely used tools of router based monitoring techniques SNMP (Simple Network Monitoring Protocols), RMON (Remote Monitoring) and Netflow are discussed in detail and some information is provided about two new monitoring methods of non-router based techniques which uses Passive Monitoring, Active Monitoring and the combination of both passive and active monitoring WREN (Watching Resources from the Edge of the Network) and SCNM (Self Configuring Network Monitor).

3. MONITORING AND ANALYSIS TECHNIQUES

In recent years the technology has grown extensively, though it has many advantages it can also be used in an erroneous way so it is difficult to maintain information confidentially. In the networking field there are problems like attacks which may be an intentional or unintentional attack. Attacks spoil the nature of the work so it is very much essential to monitor the traffic of the network because it helps to separate the genuine request from the malicious one. It is the most challenging task and essential component for a network administrator. The network administrator will look for operation of their systems without any issues. The monitoring and analysis techniques [5] such as Router Based Monitoring Techniques and Non-Router based Monitoring Techniques. Figure 2 represents the monitoring and analysis techniques.

3.1. Router Based Monitoring Techniques

The main idea behind the router based monitoring techniques is embedding the input data to the router in a straight line and it proposes modest compliance. There are two classifications come under this technique. They are Router Based Monitoring and Non-Router Based Monitoring. The router based monitoring consisting of three methods such as SNMP (Simple Network Monitoring Protocols), RMON (Remote Monitoring) and Netflow.

3.2. Non-Router Based Monitoring Techniques

Non-Router based monitoring techniques are having restricted capability but the elasticity are more rather than router based monitoring techniques. This is also classified in to three methods such as Active Monitoring, Passive Monitoring and Combinational Monitoring.

3.2.1. Active Monitoring

Active monitoring shows the way to gather the dimensions between two endpoints in a particular network. Availability, Routes, Packet delay, Loss probability, Jitter, Bandwidth are the parameters used by active monitoring. Interfering into the network to examine its performance is the problem that exists in active monitoring due that the normal traffic information seems to be questioning the validity of the network information.

3.2.2. Passive Monitoring

Packet sniffing is the support for passive monitoring; it can analyze the measurement through offline whereas it cannot be collected. It has the advantage than active monitoring that the overhead data are not added into the network. It also has problem that the post processing will require more time.

3.3.3. Combinational Monitoring

Active monitoring and passive monitoring both have demerits of their own; to overcome that issue the combination of both active and passive monitoring is developed. The combinational monitoring collects the best aspects of both active and passive monitoring. It consists of two techniques such as Watching Resources from the Edge of the Network (WREN) and Self-Configuring Network Monitor (SCNM).

4. ROUTER BASED MONITORING TECHNIQUES

The router based monitoring techniques are SNMP (Simple Network Monitoring Protocols), Remote Monitoring (RMON) and Netflow are discussed below.

4.1. Simple Network Monitoring Protocol (SNMP)

SNMP is an application layer protocol which is a division of TCP/IP suite which helps to handle the resources involved in that particular network [6]. It is the benchmark to exchange the information of that particular network. The statistics of the traffic will be gathered through the passive sensors. The flow generates from the router to the host. SNMP consists of three components such as Managed Devices, Agents and Network Management Devices. Managed devices include pieces of equipment like Router, Switch, Hub, Printer, etc. The agent is software which resides on managed devices collects the data from the managed devices and transmits the data over the network that uses SNMP. Controlling and Monitoring of managed devices is the responsibility of Network Management Devices. The communications between the Agent and Network Management Devices is made through messages such as GetRequest, SetRequest, GetNextRequest, GetResponse and Trap. It is otherwise known as device based management.

4.2. Remote Monitoring (RMON)

The network administrator can examine the network with no issues using Remote Monitoring (RMON). It is an extension of SNMP. It sets alarm to monitor networks. RMON has two components such as the probe and the client. It also helps the administrator to analyze the fault, plan and regulate the performance [12] of the information gathered in that network. Client/ Server is the working characteristic of RMON. It is otherwise called as flow based management. It does not concentrate on any of the devices connected with that particular network rather it focuses on the pattern of the network traffic [11].RMON consisting of two goals such as offline operation, proactive monitoring, problem detection and reporting, value added data and multiple managers [12]. In remote monitoring, there are nine monitoring groups which are used to gather information. They are Statistics, History, Alarm, Host, HostTopN, Filters, Packet capture, Events and Token ring.

4.3. Netflow

Netflow is a feature introduced in Cisco router. In order to collect the IP traffic information, Cisco system developed a network protocol called Netflow. It is termed as the standard of industries for monitoring the traffic [13]. It is a tool to evaluate the process of the network [14]. It also deals with traffic monitoring, clarify with the elegant flow, accumulate and estimate the statistics, [13] maintain details about source and destination IP addresses and protocols. Apart from that, if any unusual movement is found in the network, the Netflow analyzer will accord with those activities.

The three existing system SNMP, RMON and Netflow are implemented, compared and found that SNMP performs better than other two techniques and still it needs some improvements. The proposed system concentrates on providing the same.

5. PROPOSED SYSTEM

Proposed network traffic monitoring system is described in this section, the proposed system aims to provide efficient and time saving monitoring system which helps to achieve reduced packet losses, lesser end to end delay and higher throughput. In the network there will not be any route to the destination node from the source node. The source node will broadcast route request about the data packets to all the nodes whenever it is in a position to send the packets. The source node that does not have a route to the destination when it has data packets to be sent to the destination, it initiates a RouteRequest packet, the RouteRequest is sent to all the nodes of that network. Each node, upon receiving a RouteRequest packet, rebroadcasts the packet to its neighbors if it has not forwarded it already to avoid the retransmission of data the proposed system aims to send the NACK which helps the nodes to learn about the neighboring routes traversed by data packets which provides reliability to the existing technique SNMP and helps to save time whereas the proposed system provides better results comparatively.

Proposed System Algorithm

S → Source Node
D→ Destination Node

repeat
S sends a RREQ to all nodes
checks sequence number
for all neighbor nodes do
if TTL (Time To Live) exceeded
then
STOP
then
assign DTS message to recover failure data
then
send NACK to control message format bits
end if
RRER reaches S

S starts a new RREQ

6. EXPERIMENTAL SETUP AND RESULTS

NS-2 simulator is used for experimentation. Random waypoint model is used for mobility in a terrain area of 200m x 200m up to 1500m x 1500m. The simulation parameters are summarized in Table1.

Table 1: Simulation Parameters

Parameter	**Value**
Simulator	NS-2
Channel Type	Wireless
Number of nodes	100
Traffic Model	CBR
Maximum mobility	60 m/s
Terrain area	200m x 200m upto 1500m x 500m
Transmission Range	250m
Routing Protocol	AODV
MAC protocol	802.11
Observation Parameter	End to end delay, Packet loss, Throughput

The simulation is done to analyze the performance of the network's various parameters. The metrics used to evaluate the performance are:

End to End Delay:

The end-to-end delay where delay is the time between when a message (CBR data packet) is sent and when it is received.

$$End\ to\ End\ Delay = \frac{\sum (time_{recieved} - time_{sent})_{Packet}\ ID}{number\ of\ count\ packets}$$

Packet loss:
The Packet lost is calculated as the number of packet received will be deducted with the number of packet sent.

$$Packetloss = no.of\ \ packets\ received - no.of\ \ packets\ sent$$

Throughput:
Throughput is the number of bytes (bit) received in a time since the first packet is sent and the last packet is received

$$Throughput = \frac{\sum bytes_{received}}{time_{end} - time_{received}}$$

Table.2 and Table.3 shows the results of the proposed system which is compared with the existing techniques for the above said parameters. Figure 1 – Figure 6 shows the comparative results of the proposed system with the existing system.

Comparative Results based on Data Transfer Rate

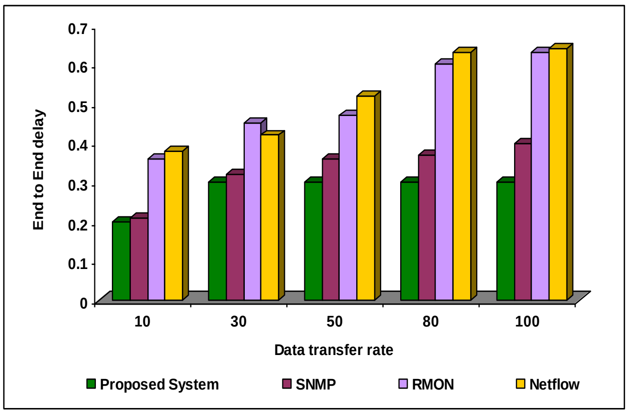

Figure.1 End to End Delay

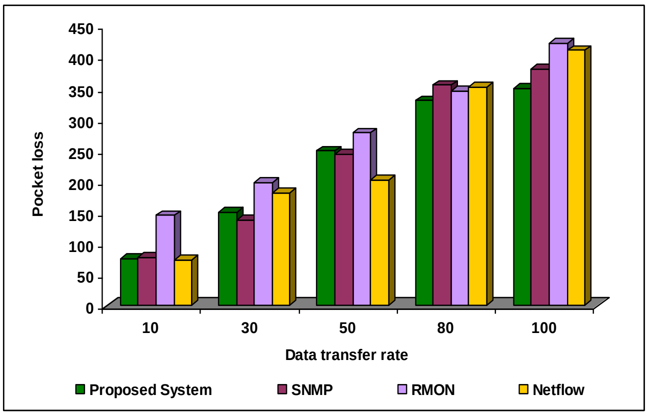

Figure.2 Packet Loss

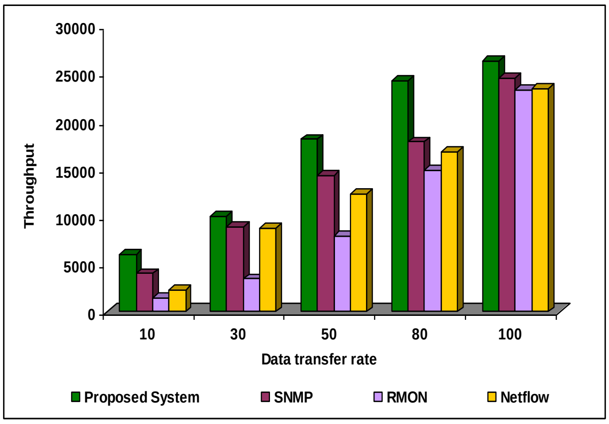

Figure.3 Throughput

Comparative Results based on Time (Seconds)

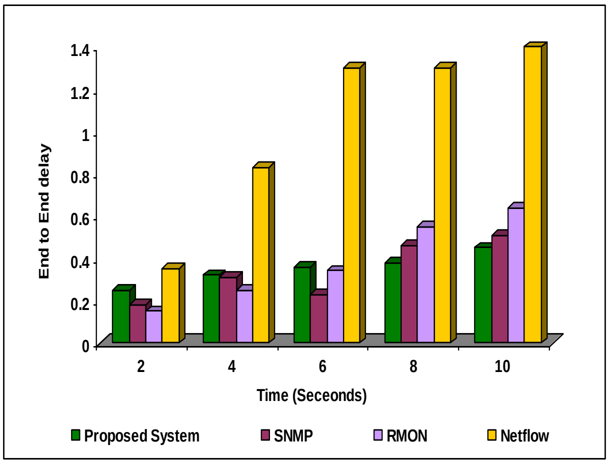

Figure.4 End to End delay

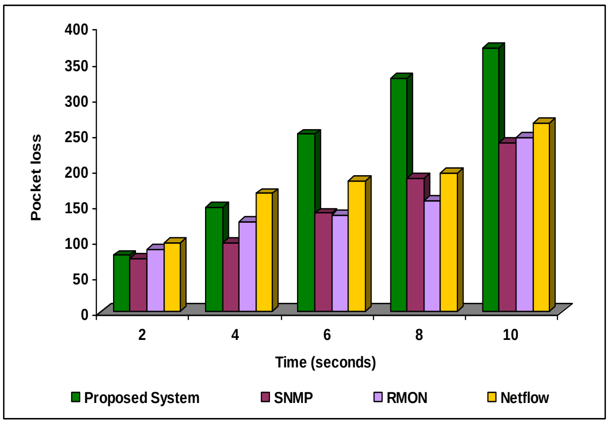

Figure.5 Packet loss

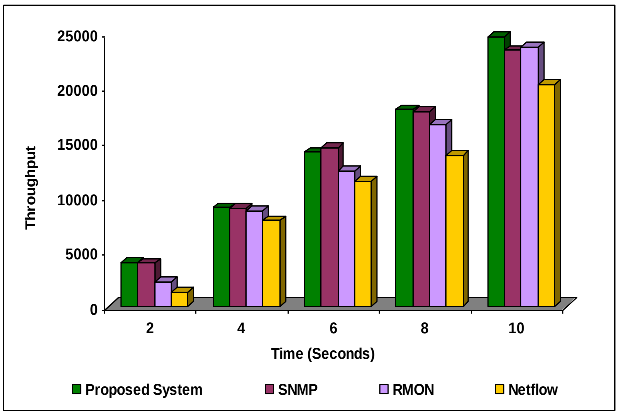

Figure.6 Throughput

7. NUMERICAL COMPARISON

The performance metrics are additive, multiplicative and concave. Additive is used for delay and multiplicative for packet loss[12[. The formula used is given below:

$$Additive: d(p) = d(n1,n2) + d(n2,n3) + ... + d(n_{m-1}, n_m)$$

$$Multiplica\,tive: d(p) = d(n1,n2) x d(n2,n3) \times .... \times d(n_{m-1}, n_m)$$

$$Throughput: T_n = \frac{K(P+H)}{D_2}$$

Performance Metrics	Proposed System	SNMP	RMON	Netflow
End to End delay	89	90.0002	90.0007	90.0004
Packet loss	9477	10120	10635	10022
Throughput	1902	1678	1337.5	611

8. CONCLUSION

The aim of this research work is to propose most efficient traffic monitoring techniques. Router based monitoring technique is found to be suitable for the research work and chosen for implementation. Three methods in router based traffic monitoring techniques such as SNMP, RMON and Netflow are implemented and results are compared with the proposed system. The proposed system provides two times better results than the existing system.

REFERENCES

[1] Alisha Cecil, "A Summary of Network Traffic Monitoring and Analysis Techniques" http://www.cse.wustl.edu/~jain/cse567-6/ftp/net_monitoring/index.html

[2] David Marchett, "A Statistical Method for Profiling Network Traffic", Proceedings of the Workshop on Intrusion Detection and Network Monitoring Santa Clara, California, USA, April 9–12, 1999.

[3] Ian A. Finlay, "A Brief Tour of the Simple Network Management Protocol", CERT® Coordination Center http://www.cert.org, July 1st 2011.

[4] Jeffrey Erman, Martin Arlitt and Anirban Mahanti, “Traffic Classification Using Clustering Algorithms” *SIGCOMM’06 Workshops* September 11-15, 2006, Pisa, Italy.

[5] Liu Yingqiu, Li Wei, Li Yunchun, “Network Traffic Classification Using K-means Clustering” IEEE Second International Multisymposium on Computer and Computational Sciences, 2007 pp.no. 360 – 365.

[6] Martin Bj ̈orklund, Klas Eriksson, “Simple Network Management Protocol”

[7] Olatunde Abiona, “Bandwidth Monitoring & Measurement (tools and services)”, Obafemi Awolowo University, Ile-Ife, NIGERIA

[8] Oleg Berzin, “Bandwidth, Delay, Throughput and

[9] Philipp Becker, “QoS Routing Protocols for Mobile Ad-hoc Networks – A Survey” August 2007.

[10] S. Waldbusser., et.,al, “Introduction to the Remote Monitoring (RMON), Family of MIB Modules”, Network Working Group.

.

[11] Simple Network Management Protocol (SNMP), Internetworking Technology Overview, June 1999.

[12] SIMPLE NETWORK MANAGEMENT PROTOCOL, Asante Networks, Inc.

[13] Some Math”, **www.**ccieflyer.com*)*

[14] Wang Jian-Ping and Huang Yong, “The Monitoring of the network traffic based on Queuing theory”, The 7th International Symposium on Operations Research and Its Applications (ISORA’08) October 31 –November 3, 2008.

Web References

[1] www.cisco.com

[2] www.wikipedia.org

[3] www.netflow.cesnet.cz

[4] “SNMP Monitoring: One Critical Component to Network Management” www.networkinstruments.com

Table 2. Comparative Results based on Data Transfer Rate (Bytes)

Performance Metrics	Network Surface Area	Traffic Monitoring Techniques																			
		Proposed System					SNMP					RMON					Netflow				
		10	30	50	80	100	10	30	50	80	100	10	30	50	80	100	10	30	50	80	100
End to End Delay	200x200	**0.07**	**0.18**	**0.32**	**0.35**	**0.37**	0.19	0.21	0.23	0.26	0.30	0.40	0.38	0.37	0.36	0.32	0.51	0.50	0.49	0.46	0.43
	400x400	**0.19**	**0.21**	**0.38**	**0.41**	**0.48**	0.21	0.37	0.42	0.45	0.49	0.37	0.42	0.57	0.36	0.33	0.39	0.42	0.52	0.53	0.53
	600x600	**0.15**	**0.42**	**0.44**	**0.45**	**0.50**	0.19	0.41	0.43	0.45	0.49	0.38	0.46	0.49	0.59	0.65	0.41	0.48	0.51	0.68	0.69
	800x800	**0.19**	**0.31**	**0.39**	**0.45**	**0.58**	0.18	0.31	0.30	0.29	0.26	0.33	0.46	0.49	0.58	0.63	0.40	0.47	0.56	0.66	0.68
	1000x1000	**0.06**	**0.18**	**0.30**	**0.35**	**0.37**	0.18	0.30	0.24	0.45	0.50	0.35	0.65	0.83	0.75	0.84	0.15	0.25	0.24	0.55	0.66
	1200x1200	**0.19**	**0.30**	**0.34**	**0.35**	**0.38**	0.22	0.37	0.38	0.38	0.44	0.39	0.42	0.48	0.59	0.63	0.39	0.43	0.52	0.61	0.64
	1400x1400	**0.19**	**0.34**	**0.35**	**0.39**	**0.40**	0.22	0.33	0.36	0.39	0.41	0.37	0.41	0.46	0.56	0.62	0.38	0.42	0.49	0.63	0.63
	1500x1500	**0.20**	**0.3**	**0.3**	**0.3**	**0.3**	0.21	0.32	0.36	0.37	0.40	0.36	0.45	0.47	0.60	0.63	0.38	0.42	0.52	0.63	0.64
Packet Loss	200x200	**73**	**182**	**322**	**356**	**370**	74	185	324	318	315	143	294	377	385	399	73	162	282	383	401
	400x400	**78**	**122**	**281**	**341**	**362**	74	125	284	335	345	139	214	297	385	402	77	192	242	393	431
	600x600	**76**	**188**	**286**	**365**	**380**	79	185	284	365	385	163	198	297	385	451	84	192	242	383	419
	800x800	**53**	**146**	**220**	**348**	**370**	75	135	226	345	375	153	198	276	348	431	78	185	212	358	421
	1000x1000	**65**	**116**	**313**	**340**	**372**	80	125	220	345	380	149	199	275	350	400	80	180	200	350	400
	1200x1200	**73**	**148**	**251**	**341**	**328**	75	154	354	365	385	153	196	278	355	431	77	188	232	382	440
	1400x1400	**75**	**125**	**230**	**345**	**366**	76	126	225	336	378	145	195	278	346	425	75	186	212	358	413
	1500x1500	**76**	**150**	**249**	**330**	**350**	77	138	244	355	381	145	198	278	346	423	73	182	202	352	411
Throughput	200x200	**4000**	**9000**	**14700**	**19000**	**24000**	3975	8988	14543	17909	23969	1482	3488	7909	14990	23282	2233	8797	12323	16773	23482
	400x400	**9200**	**12100**	**14100**	**21000**	**24400**	3679	8938	14363	17869	23589	1472	3479	7918	14786	23273	2284	8817	12382	16791	23429
	600x600	**4000**	**11000**	**14200**	**22000**	**24800**	3998	8938	14353	17849	23589	1469	3448	7998	14679	22425	2283	8789	12372	16783	23463
	800x800	**4000**	**9000**	**14200**	**18000**	**24400**	3987	8958	14463	17889	23669	1452	3468	7888	14858	21273	2253	8798	12332	16763	23435
	1000x1000	**4100**	**9000**	**14100**	**18900**	**24300**	4003	8927	14594	18799	23001	1486	3412	8031	15252	23623	2276	8965	13298	17424	23491
	1200x1200	**6300**	**12000**	**16100**	**22900**	**26900**	3947	8958	14363	17879	23669	1432	3438	7898	14879	23233	2243	8796	12332	16783	23473
	1400x1400	**4300**	**12000**	**18000**	**22000**	**29800**	3995	8995	14453	17951	24600	1435	3448	7897	14889	23139	2253	8878	12332	16776	23453
	1500x1500	**6000**	**10000**	**18100**	**24300**	**26400**	3986	8924	14348	17819	24559	1458	3458	7895	14874	23263	2236	8797	12355	16766	23457

Table 3. Comparative Results based on Time (Seconds)

Performance Metrics	**Network Surface Area**	**Traffic Monitoring Techniques**																			
		Proposed System					**SNMP**					**RMON**					**Netflow**				
		2	**4**	**6**	**8**	**10**	**2**	**4**	**6**	**8**	**10**	**2**	**4**	**6**	**8**	**10**	**2**	**4**	**6**	**8**	**10**
End to End Delay	200x200	**0.06**	**0.09**	**0.12**	**0.16**	**0.20**	0.18	0.28	0.33	0.35	0.40	0.51	0.49	0.47	0.45	0.43	0.63	0.58	0.56	0.53	0.52
	400x400	**0.19**	**0.40**	**0.65**	**0.98**	**1.43**	0.22	0.31	0.24	0.44	0.43	0.15	0.26	0.41	0.52	0.68	0.75	0.92	1.44	1.53	1.63
	600x600	**0.18**	**0.77**	**0.81**	**0.88**	**1.0**	0.19	0.36	0.21	0.47	0.50	0.18	0.25	0.37	0.59	0.65	0.85	1.0	1.41	1.43	1.49
	800x800	**0.28**	**0.39**	**0.48**	**0.57**	**0.7**	0.17	0.33	0.23	0.46	0.49	0.21	0.28	0.34	0.54	0.64	0.37	0.84	1.26	1.38	1.45
	1000x1000	**0.05**	**0.09**	**0.12**	**0.16**	**0.20**	0.21	0.30	0.22	0.36	0.51	0.16	0.25	0.33	0.54	0.63	0.35	0.82	1.26	1.34	1.43
	1200x1200	**0.28**	**0.65**	**0.76**	**0.98**	**1.0**	0.12	0.32	0.23	0.48	0.50	0.15	0.25	0.33	0.54	0.64	0.39	0.84	1.3	1.4	1.45
	1400x1400	**0.15**	**0.35**	**0.67**	**0.86**	**1.09**	0.20	0.31	0.24	0.45	0.52	0.15	0.25	0.33	0.54	0.64	0.35	0.84	1.25	1.4	1.5
	1500x1500	**0.25**	**0.32**	**0.36**	**0.38**	**0.45**	0.18	0.31	0.23	0.46	0.51	0.15	0.25	0.34	0.55	0.64	0.35	0.83	1.3	1.3	1.4
Packet Loss	200x200	**70**	**96**	**182**	**194**	**202**	74	97	185	197	207	87	152	142	134	123	94	182	194	189	233
	400x400	**68**	**100**	**140**	**164**	**199**	76	92	139	185	197	85	132	139	152	258	94	165	186	192	283
	600x600	**89**	**109**	**129**	**159**	**209**	94	107	178	227	257	95	132	162	184	253	98	182	232	254	273
	800x800	**77**	**100**	**139**	**180**	**210**	75	95	148	189	247	88	132	142	164	253	96	167	186	195	268
	1000x1000	**70**	**100**	**118**	**162**	**203**	78	99	160	199	259	84	121	136	158	242	99	164	182	200	260
	1200x1200	**78**	**100**	**149**	**190**	**240**	76	98	148	189	238	86	124	135	156	245	95	164	186	195	266
	1400x1400	**78**	**79**	**139**	**190**	**240**	74	97	138	187	237	85	122	132	154	243	95	166	185	197	267
	1500x1500	**79**	**146**	**249**	**327**	**370**	74	97	138	187	237	87	126	136	155	245	97	166	183	195	264
Throughput	200x200	**4000**	**9000**	**14200**	**18700**	**24900**	3987	8907	14043	17809	24569	2233	8797	12322	16773	23243	1283	7907	11372	13793	20293
	400x400	**4000**	**8000**	**14000**	**18400**	**25000**	3769	8916	14412	17723	23464	2334	8972	12142	16875	24265	1218	7914	11266	13913	21184
	600x600	**4000**	**9000**	**14300**	**18000**	**24300**	3994	8628	14363	17839	23579	2253	8798	12342	16783	23253	1243	7898	11352	13783	20263
	800x800	**4000**	**9000**	**14200**	**18300**	**24400**	3997	8824	14744	17229	23679	2543	8895	12361	16632	22513	1265	7963	11418	13783	20142
	1000x1000	**4100**	**9000**	**14100**	**18000**	**24000**	4002	9110	14524	18534	24335	2675	9234	12243	17806	23554	1413	8631	11922	14634	20321
	1200x1200	**4000**	**9100**	**14200**	**18000**	**24300**	3988	8948	14428	17118	24157	2236	8752	12332	16548	23253	1253	7898	11256	13726	20242
	1400x1400	**4100**	**9000**	**14233**	**18300**	**24400**	3845	8977	14347	18215	23579	2243	8798	12172	16752	23253	1253	7872	11374	13774	20248
	1500x1500	**4000**	**9000**	**14100**	**18000**	**24700**	3932	8965	14523	17819	23413	2253	8743	12368	16672	23678	1264	7843	11420	13783	20253