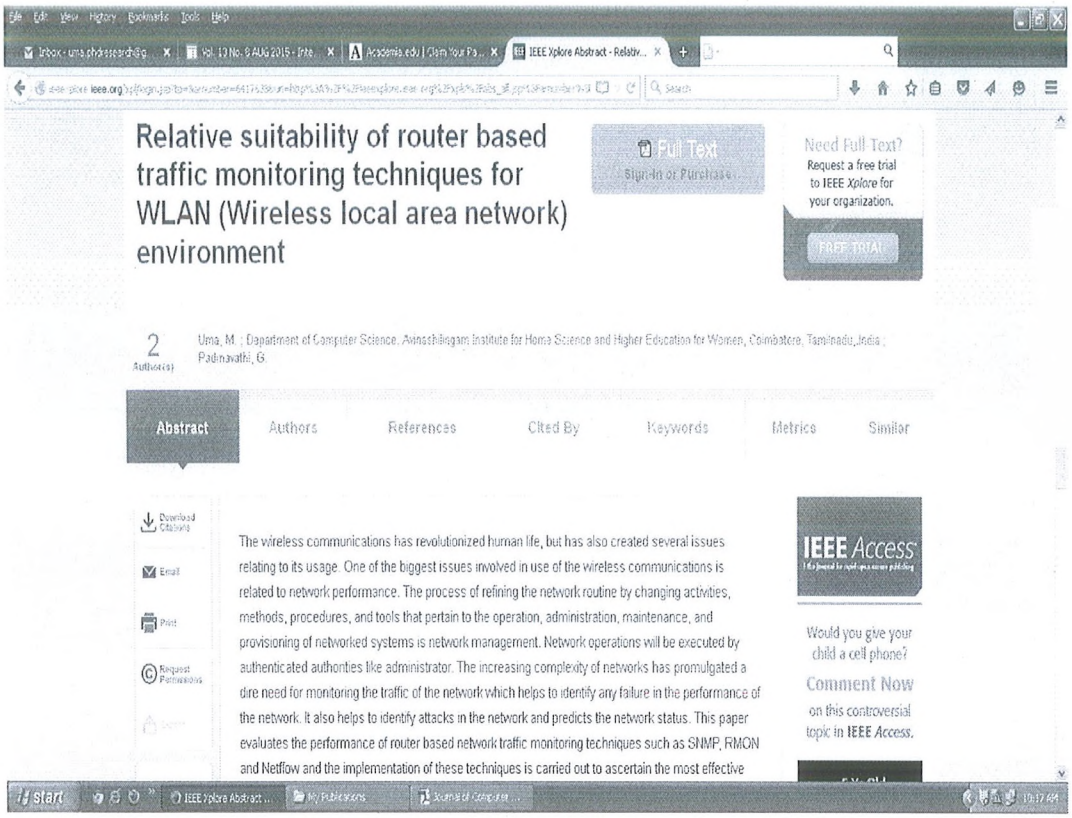

Relative suitability of router based traffic monitoring techniques for WLAN (Wireless local area network) environment
Full Text
Need Full Text?
Request a free trial to IEEE Xplore for your organization.
FREE TRIAL
2 Authors(s)
Uma, M. ; Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamilnadu, India
Padmavathi, G.
Abstract
Authors
References
Cited By
Keywords
Metrics
Similar
The wireless communications has revolutionized human life, but has also created several issues relating to its usage. One of the biggest issues involved in use of the wireless communications is related to network performance. The process of refining the network routine by changing activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems is network management. Network operations will be executed by authenticated authorities like administrator. The increasing complexity of networks has promulgated a dire need for monitoring the traffic of the network which helps to identify any failure in the performance of the network. It also helps to identify attacks in the network and predicts the network status. This paper evaluates the performance of router based network traffic monitoring techniques such as SNMP, RMON and Netflow and the implementation of these techniques is carried out to ascertain the most effective
IEEE Access
Would you give your child a cell phone?
Comment Now
on this controversial topic in IEEE Access.
start

Relative Suitability of router based traffic monitoring techniques for WLAN (Wireless Local Area Network) environment

M.Uma
Ph.D Research Scholar
uma.phdresearch@gmail.com

Dr.G.Padmavathi
Professor and Head
ganapathi.padmavathi@gmail.com

Department of Computer Science
Avinashilingam Institute for Home Science and Higher Education for Women
Coimbatore, Tamilnadu, India

Abstract - The wireless communications has revolutionized human life, but has also created several issues relating to its usage. One of the biggest issues involved in use of the wireless communications is related to network performance. The process of refining the network routine by changing activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems is network management. Network operations will be executed by authenticated authorities like administrator. The increasing complexity of networks has promulgated a dire need for monitoring the traffic of the network which helps to identify any failure in the performance of the network. It also helps to identify attacks in the network and predicts the network status. This paper evaluates the performance of router based network traffic monitoring techniques such as SNMP, RMON and Netflow and the implementation of these techniques is carried out to ascertain the most effective monitoring technique among the three. The NS-2 simulator is used for implementation. SNMP performs better than the other two methods for WLAN.

Keywords: Router based monitoring, SNMP, RMON, Netflow

I. INTRODUCTION

The transfer of information between two or more points that are not physically connected by distances which can be short, such as a few meters for television remote control, or as far as thousands or even millions of kilometers for deep-space radio communications is termed as wireless communication [3].Network monitoring describes the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator (via email, SMS or other alarms) in case of outages. It is a subset of the functions involved in network management. The capability of gathering, examine the network traffic is termed as traffic monitoring. The current position and outline of the network traffic will be known by the administrator by monitoring the network traffic and if there is any abnormal activity in the traffic will also be found. Traffic monitoring is a method by which detection of network failure occurs through the use of monitoring agents to detect, isolate, and correct malfunctions in the network and possibly recover the failure by warning the administrators to fix the problems within a minute [2]. The stable network monitoring constantly for a threat from either inside or outside network is mandatory. Another role of traffic to is regularly check the network performance to identify whether the network devices are overloaded by collecting information about network usage which can be used to make a network plan for short-term and long-term future improvement. The need for more sophisticated network traffic monitoring and analysis tools is to maintain the network system stability and retain the ability to fix network problems on time or to avoid network failure, to ensure the network security strength, and to make good decisions for network planning[4]. It is a difficult and demanding task on the part of a Network Administrator who constantly strives to maintain smooth operations of their network. A network compromised for even a small period of time would cause a decline in the productivity of the company and in the case of public service departments the ability to provide essential services would be compromised [5]. Hence are attempts has been made to study the router based monitoring techniques and comparison of those techniques for their suitability to WLAN.

The structure of the paper is organized as follows: Section 2 discusses the traffic monitoring techniques and its classification; In Section 3 Experimentation and Evaluation of implementations are discussed. Conclusion is given in Section 4.

II. TRAFFIC MONITORING TECHNIQUES

Network monitoring gives the ability to monitor the activities of the applications and the devices to ensure

expected and normal operations. On the other hand it helps to detect problems and take the necessary actions to correct them. It can guide us to discover the security holes opened through one's network intentionally by attackers or unintentionally such as disabled or unused suspicious services that may be enabled by mistake. There are generally three basic goals for network monitoring Performance monitoring, Fault monitoring and Account monitoring [6]. As the complexity of network increases so does the problem in usage, maintenance and chance for compromise of the network. Traffic monitoring is essential for prevention of attacks and the problem has to evolve on a daily basis to meet the challenges of modern wireless networks. Traffic monitoring techniques can be broadly classified into two techniques – Router based and non-router based [3]. Router based monitoring techniques are systems where monitoring functionalities that are built-into the routers themselves and do not require additional installation of hardware or software[4].In this study three important router based techniques are compared to determine the most efficient router based technique for usage in complex and demanding environments. Network traffic monitoring technique classification diagram is given if figure 1.

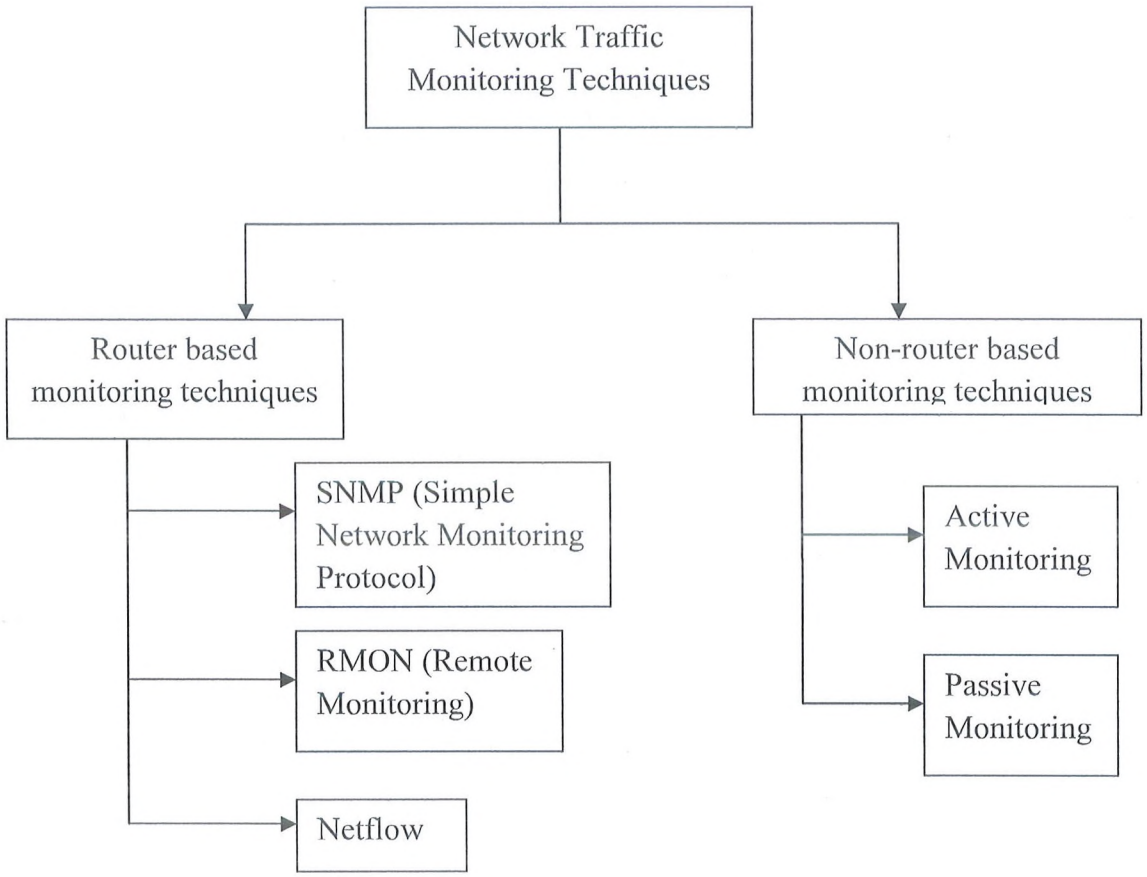


Figure.1 Network Traffic Monitoring Techniques

Router Based Monitoring Techniques

Router based monitoring technique is a process of fixing the input data strongly in to the router and which allow to profound a modest agreement. Three significant router based protocols are

1) SNMP (Simple Network Monitoring Protocol)

In order to share the information of particular network SNMP is considered as a standard. The SNMP is recognized in 1980 for being developed to deal with TCP/IP. To control the resources of transport layer protocol SNMP has been developed [1]. SGMP (Simple Gateway Management Protocol) is the ancestor of SNMP purposely developed to observe the status of the network and to handle the resources of the network. SNMP consists of three components like Structure of Management Information (SMI), the Management Information Base (MIB), and the SNMP agents [4]. The merits of SNMP are managing skill, competence and reputation [10] [11] [14].

2) RMON (Remote Monitoring)

RMON which is an extension of the SNMP Management Information Database (MIB) enables various network monitors and console systems to exchange network-monitoring data. RMON is able to set alarms that will monitor the network based on certain criteria unlike SNMP which must

send out a request for information [6]. RMON allows Administrators to manage local networks as well as remote sites from one central location. It monitors at the Network Layer and below. RMON has 2 versions RMON and RMON 2. RMON [RMON] uses 9 different monitoring groups to obtain information about the network. They include Statistics, History, Alarm, Host, HostTopNand Packet capture [4].

3) Netflow

Cisco introduced a new feature in routers that gives the ability to collect IP network traffic as it enters an interface. A network administrator can determine things such as the source and destination of the traffic, class of service, and the cause of congestion by analyzing the data that is provided by Netflow. The three components of Netflow include flow caching, Flow Collector, and Data Analyzer. The IP data flows that enter an interface is collected by flow caching and prepares the data for exportation. The first packet of a flow through the standard switching path is processed to create the cache. Packets with similar flow characteristics are used to create a flow record which is kept in the cache for all active flows. The flow record tracks the packet sand bytes per flow. The cache information is then periodically exported to the Flow Collector. Data collection, filtering, and storage is done by the flow collector which contains a history of flow information. The presentation of data is done by data analyzer.

B. Non-Router Based monitoring techniques.

Non-Router based techniques do not have inbuilt monitoring capabilities and require additional hardware and software to be installed and provide greater flexibility. They are classified as either active or passive.

1) Active

Active monitoring measurements between at least two endpoints in the Network is collected by transmitting probes into the network to collect data Metrics such as Availability, Routes, Packet Delay, Packet Reordering, Packet Loss, Packet Inter-arrival Jitter, Bandwidth Measurements (Capacity, Achievable Throughputs).Commonly used tools such as ping, which measures delay and loss of packets, and trace route which helps to determine topology of the network, are examples of basic active measurement tools. Network topology can also be measured by active techniques.

2) Passive

Passive monitoring does not inject traffic into the network or modify the traffic that is already on the network like an active monitoring technique. Passive monitoring collects information about only one point in the network that is being measured rather than between two endpoints as active monitoring measures. Information such as Traffic and protocol mixes are dealt by passive methods Moreover, accurate bit or packet rates Packet timing and inter-arrival timing are the focus of such systems. Passive monitoring can be achieved with the assistance of any packet sniffing program.

III. EXPERIMENTATION AND EVALUATION

The wireless local area network has been setup with the surface area 1500mm x 1500mm. The three performance metrics end to end delay, packet loss and throughput have been evaluated for three router based network traffic monitoring techniques such as SNMP, RMON and Netflow. AODV is used as a routing protocol because of its unique feature stability, it is an on demand routing protocol which requires minimum number of broadcasts. The simulation parameters are summarized in Table.1

TABLE.1 SIMULATION PARAMETER

Parameter	Value
Simulator	NS-2
Channel Type	Wireless Channel
Number of Nodes	100
Node Placement Strategy	Random
Propagation Model	Two way Ground
Traffic Model	CBR
Terrain area	1500m x 1500m
Transmission Range	150 m - 250m
MAC Protocol	802.11
Routing Protocol	AODV
Observation Parameter	End to End Delay, Packet loss, Throughput

A. PERFORMANCE METRICS

1) 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.

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

2) Packet loss:

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

Packet loss = No.of Packets Received – No.of Packets Sent

3) Throughput:

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

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

B.RESULTS

The results after implementation are given below. Figure 1 to Figure 6 shows the graphical representation of the results. Table 1 gives the result based on data transfer rate and Table 2 gives the result based on time which is shown at the end.

Comparative Results based on Data Transfer Rate

Figure.1 End to End

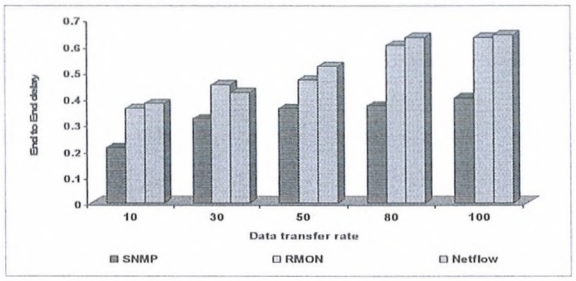
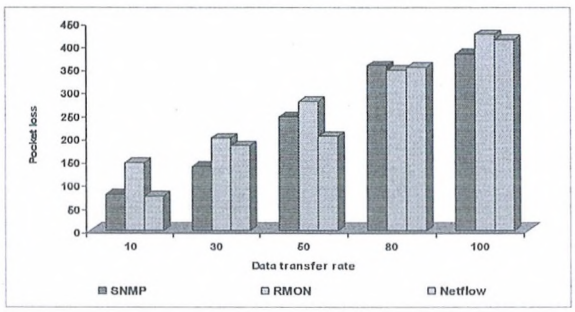
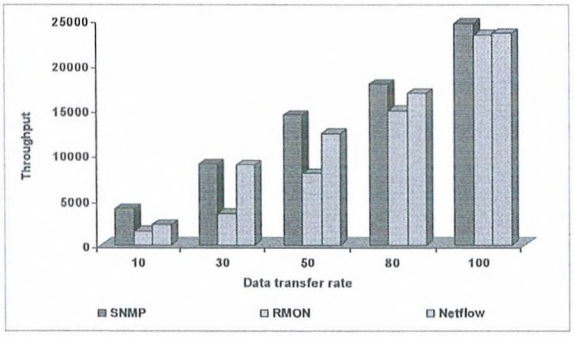


Figure.2 Packet Loss



gure 3 Throughput



Comparative Results based on Time (Seconds)

Figure.4 End to End Delay

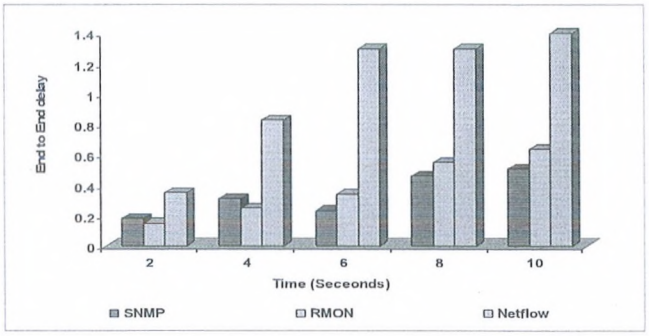


Figure.5 Pocket Loss

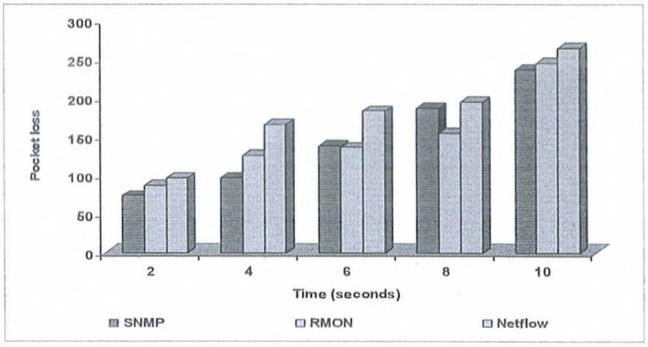
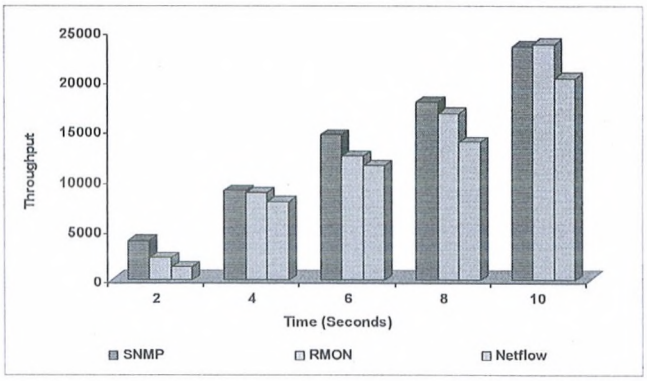


Figure.6 Throughput



C. NUMERICAL COMPARISON

The performance metrics are classified into three types Additive, Multiplicative and Concave metrics. Additive metrics are used for delay; multiplicative metric is used for packet loss [8]. The formula to calculate performance metrics End to End delay, Packet loss and Throughput are calculated is given below:

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

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

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

Performance Metrics	SNMP	RMON	Netflow
End to End delay	90.0002	90.0007	90.0004
Packet loss	1152	10635	10022
Throughput	1678	1337.5	611

D. DISCUSSION

Router based monitoring techniques SNMP, RMON and Netflow are implemented using NS-2 simulator in 1500mm X 1500mm surface area based on data transfer rate and time using the three performance metrics end to end delay, packet loss and throughput which are the most important parameters to evaluate the network performance. By seeing the result it is obvious to conclude that SNMP performs better than RMON and Netflow. Hence it is also proved numerically by using the mathematical formula.

IV. CONCLUSION

The study has been done to compare three router based performance techniques such as SNMP, RMON and Netflow in order to identify the best method for traffic monitoring in WLAN. The analysis of the data by comparison of metrics such as Packet loss, Throughput and End to End Delay conclusively proves the use of SNMP that shows a great deal of consistency and accuracy in traffic monitoring and suggests that SNMP is best for monitoring networks among the three router based techniques.

REFERENCES

[1]. Ming-Han, Wan and Mong-Fong Horng, "An Intelligent Monitoring System for Local Area Network Traffic", Eighth International Conference on Intelligent Systems Design and Applications"

[2]. Olatunde Abiona, "Bandwidth Monitoring & Measurement (tools and services)", Obafemi Awolowo University, Ile-Ife, NIGERIA

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

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

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

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

[7]. Frederic Beck, "NetFlow, RMON and Cisco-NAM deployment" Theme COM — Systems Communicants, Projet MADYNES, August 2007.

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

[9]. Oleg Berzin, "Bandwidth, Delay, Throughput and Some Math", www.ccieflyer.com)

[10]. Martin. Bj Orklund, Klas Eriksson, "Simple Network Management Protocol"

[11]. Simple Network Management Protocol, Asante Networks,Inc

[12]. wikipedia.org

[13]. netflow.cesnet.cz

[14]. "SNMP Monitoring: One Critical Component to Network Management" networkinstruments.com

[15]. cse.wustl.edu/~jain/cse567-06/ftp/net_traffic_monitors3/index.html#Section1.0

[16]. cse.wustl.edu/~jain/cis788-97/ftp/net_monitoring/index.htm#Fundamentals-of-Network-Monitoring

TABLE.2 RESULTS BASED ON DATA TRANSFER RATE (BYTES)

Performance Metrics	Traffic Monitoring Techniques														
	SNMP					RMON					Netflow				
	10	30	50	80	100	10	30	50	80	100	10	30	50	80	100
End to End delay	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	77	138	244	355	381	145	198	278	346	423	73	182	202	352	411
Throughput	3986	8924	14348	17819	24559	1458	3458	7895	14874	23263	2236	8797	12355	16766	23457

TABLE.3 RESULTS BASED ON TIME (SECONDS)

Performance Metrics	Traffic Monitoring Techniques														
	SNMP					RMON					Netflow				
	2	4	6	8	10	2	4	6	8	10	2	4	6	8	10
End to End delay	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	74	97	138	187	237	87	126	136	155	245	97	166	183	195	264
Throughput	3932	8965	14523	17819	23413	2253	8743	12368	16672	23678	1264	7843	11420	13783	20253