ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 2, Issue 2, February 2013

Network Traffic Monitoring, Analysis and Anomaly Detection

[1] Himanshu Kumar, [2] Sunil Kumar Shrinarayan Singh, [3]Ajay Kumar, [4]Remya Joseph, [5]Sudhanshu Kumar, [6]Praveen Kumar

[1,2,3,4] M.tech IT(Networking), [6] M.tech Software Technology, School of Information Technology and Engineering, VIT University, Vellore -632014, Tamil Nadu.

[5]Business Analyst at Deloitte, Hyderabad

Abstract- **The basic concept behind the Internet is expressed by the scalability argument: mechanism or service should be introduced into the Internet if it does not scale well. A key corollary to the scalability argument is the end-to-end argument: to maintain scalability, algorithmic complexity should be pushed to the edges of the network whenever possible. Although the best example of the Internet concept is TCP congestion controls [1], which is implemented primarily through algorithms operating at end systems. Unfortunately, TCP congestion control also illustrates some of the short comings the end-to-end argument. As a result of its strict adherence to end-to-end congestion control, the current Internet suffers from main maladies: congestion collapse from undelivered packets.**

NTM[14][16] entails the exchange of feedback between routers at the borders of a network in order to detect and restrict unresponsive traffic flows before they enter the network, thereby preventing congestion within the network. The Internet's excellent scalability and robustness result in part from the end-to-end nature of Internet congestion control. End-to-end congestion control algorithms alone, however, are unable to prevent the congestion collapse and unfairness created by applications that are unresponsive to network Congestion. To address these maladies, we propose and investigate a novel congestion-avoidance mechanism called Network Traffic Monitoring (NTM).

Index Terms— **TCP, UDP, backward feedback, forward feedback, round trip time, time to live.**

I. INTRODUCTION

Network Traffic Monitoring is a core-stateless congestion avoidance mechanism. The basic principle of NTM is to compare, at the borders of the network, the rates at which each flow's packets are entering and leaving the network. If packets are entering the network faster than they are leaving it, then the network is very likely to be buffering or, worse yet, discarding the flow's packets. In other words, the network is receiving more packets than it can handle. NTM [14] prevents this scenario by "monitoring" the network's borders, ensuring that packets do not enter the network at a rate greater than they are able to leave it. This has the beneficial effect of preventing congestion collapse (congestion collapse is a phenomenon in which the maximum of network bandwidth is used by the packets which ultimately do not reach the destination but are lost

due to congestion in between) from undelivered packets, because in this case unresponsive flow's undeliverable packets never enter the network in the first place.

Depending on which flow it is operating on, an edge router may be viewed as ingress or an egress router. An edge router operating on a flow passing into a network is called an ingress router, whereas an edge router operating on a flow passing out of a network is called an egress router. NTM prevents congestion collapse through a combination of per-flow rate monitoring at egress routers and per-flow rate control at ingress routers. Rate monitoring allows an egress router to determine how rapidly each flow's packets are leaving the network, whereas rate control allows an ingress router to police the rate at which each flow's packets enter the network. Linking these two functions together are the feedback packets exchanged between ingress and egress routers; ingress routers send egress routers forward feedback packets to inform them about the flows that are being rate controlled, and egress routers send ingress routers backward feedback packets to inform them about the rates at which each flow's packets are leaving the network.

The main feature of NTM is its core stateless approach, which allows routers on the borders (or edges) of a network to perform flow classification and maintain per-flow state but does not allow routers at the core of the network to do so. This serves the ultimate goal of networking i.e. bringing the complexity to the edge of network as far as possible.

II. Working Principle

Mainly two algorithms are used in this project for congestion control:

A. The leaky bucket algorithm:-

This algorithm [17] is a single-server queuing system with constant service time. The host is allowed to put one packet per clock tick onto the network. This can be enforced by the interface card or by the operating system. This mechanism turns an uneven flow of packets from the user processes inside the host into an even flow of packets onto the network, smoothing out bursts and greatly reducing the chances of congestion. The leaky bucket consists of a finite queue. When a packet arrives, if there is room on the queue it is appended to the queue otherwise it is discarded. At every clock tick, one packet is transmitted.

Token bucket represents the *Policing* function of Traffic Conditioning Block of different server. A token bucket flow is defined by (r, b), r denotes the rate at which tokens (credits) are accumulated and b is the depth of the token pool (in bytes).

New token are adding to the bucket at rate of r tokens/sec, the maximum token can be accumulated is b bytes. If the bucket is full, the incoming tokens will be thrown away. The Token Bucket (TB) profile contains three parameters: an average rate, a peak rate, and burst size.

B. Time sliding window (TSW):-

The Time Sliding Window [6][9] Three Conformance level meter TSWTCL meters a traffic stream and determines the conformance level of its packets. Packets are deemed to belong to one of the three levels, Red, Yellow or Green, depending on the committed and peak rate. The meter provides an estimate of the running average bandwidth. It takes into account burstiness and smoothes out its estimate to approximate the longer-term measured sending rate of the traffic stream. The estimated bandwidth approximates the running average bandwidth of the traffic stream over a specific window (time interval).It estimates the average bandwidth using a time-based estimator. When a packet arrives for a class, TSWTCL re-computes the average rate by using the rate in the last window (time interval) and the size of the arriving packet. The window is then slid to start at the current time (the packet arrival time). If the computed rate is less than the committed configuration parameter, the packet is deemed Green; else if the rate is less than the peak rate, it is yellow else Red. To avoid dropping multiple packets within a TCP window, TSWTCL probabilistically assigns one of the three conformance level to the packet.

The basic working principle of NTM is pictorially represented as below:

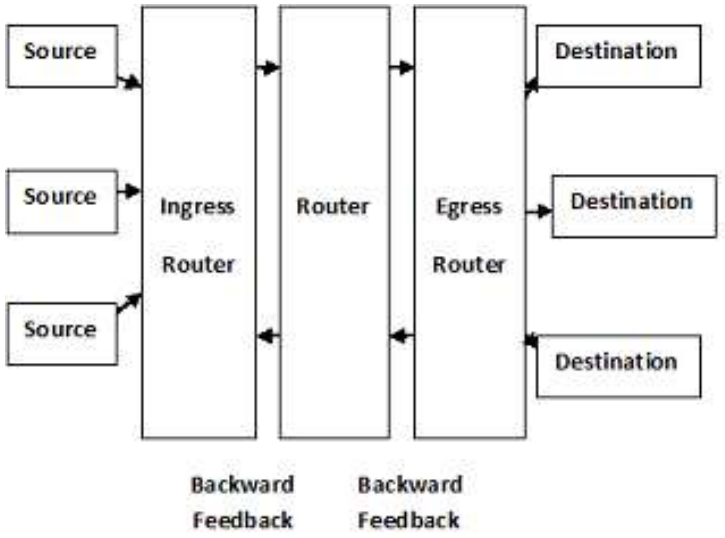


Fig 1.

III. Overall system design [18]

From the analysis it can be said that the following are the major modules of NTM.

*A.Source module:-*The task of this Module is to send the packet to the Ingress router.

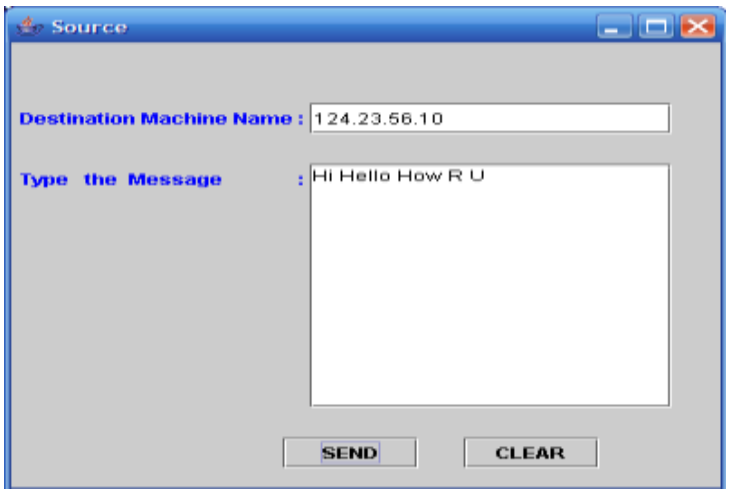
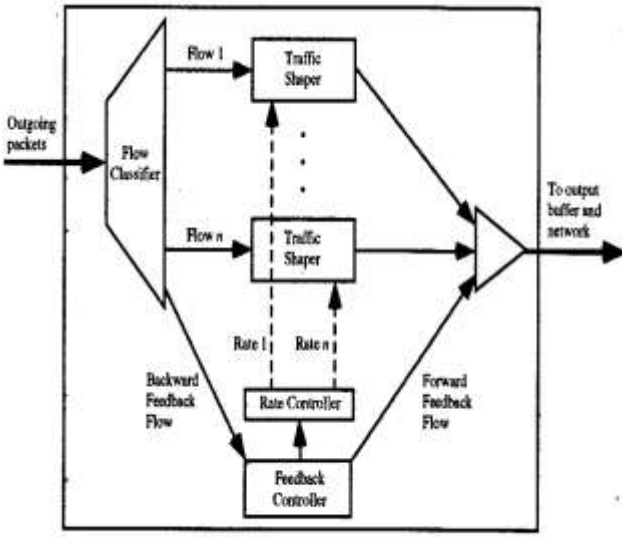


Fig 2.

B. Ingress router module [19]:-

An edge router operating on a flow passing into a network is called an ingress router. NTM prevents congestion collapse through a combination of per-flow rate monitoring at egress routers and per-flow rate control at ingress routers. Rate control allows an ingress router to police the rate at which each flow's packets enter the network. Ingress Router contains a flow classifier, per-flow traffic shapers (e.g., leaky buckets), a feedback controller, and a rate controller.



An output port of NTM ingress router

Fig 3.

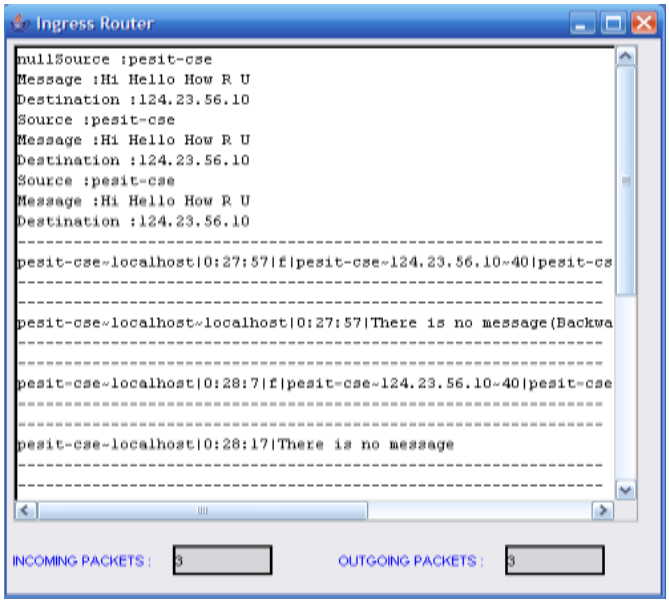


Fig 4.

C. Router module:-

The task of this Module is to accept the packet from the Ingress router and send it to the Egress router.

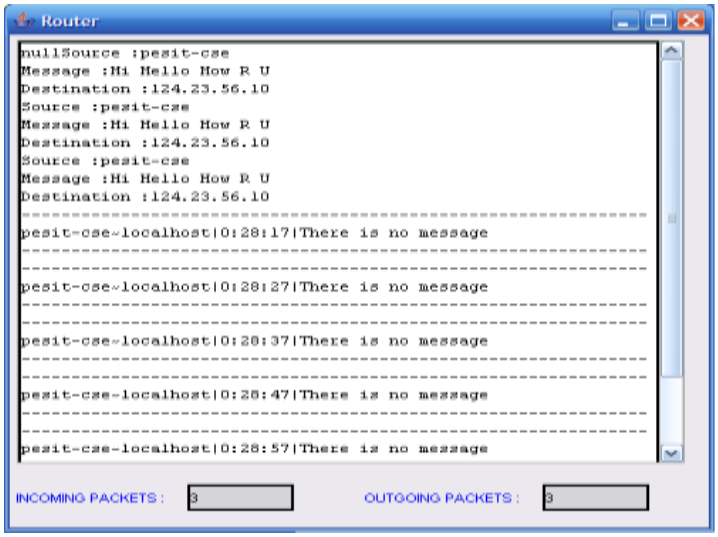
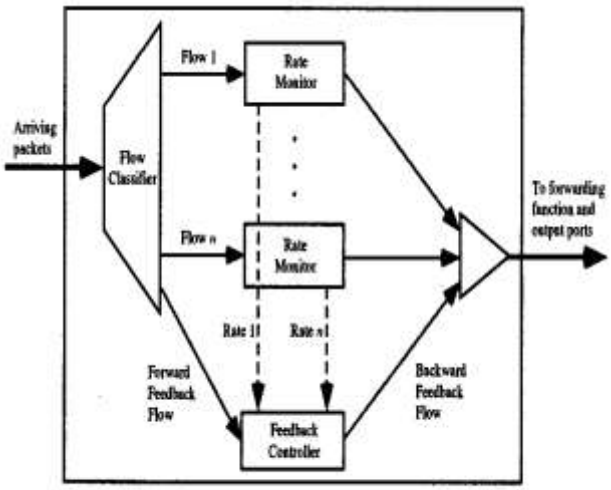


Fig 5.

D. Egress router module [19]:-

An edge router operating on a flow passing out of a network is called an egress router. NTM prevents congestion collapse through a combination of per-flow rate monitoring at egress routers and per-flow rate control at ingress routers. Rate monitoring allows an egress router to determine how rapidly each flow's packets are leaving the network. Rate monitored using a rate estimation algorithm such as the Time Sliding Window (TSW) algorithm. Egress Router contains a flow classifier, Rate monitor, a feedback controller.



An input port of NTM Egress router

Fig 6.

Fig 7.

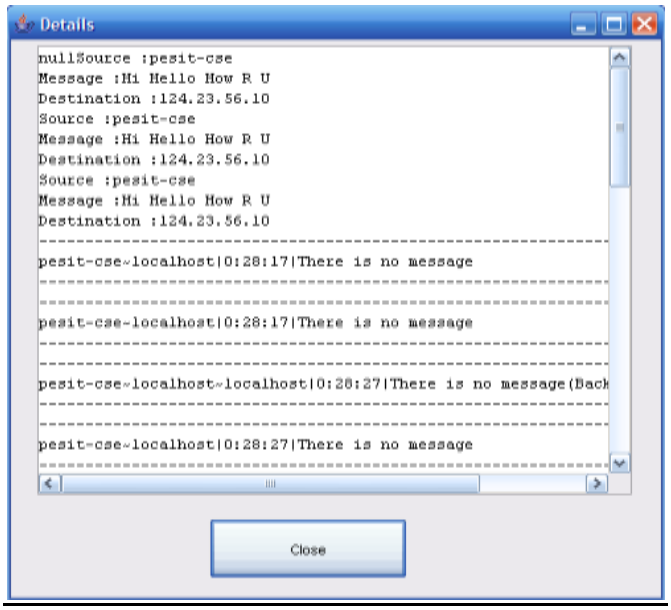


Fig 8.

E. Destination module:-

The task of this Module is to accept the packet from the Egress router and stored in a file in the Destination machine.

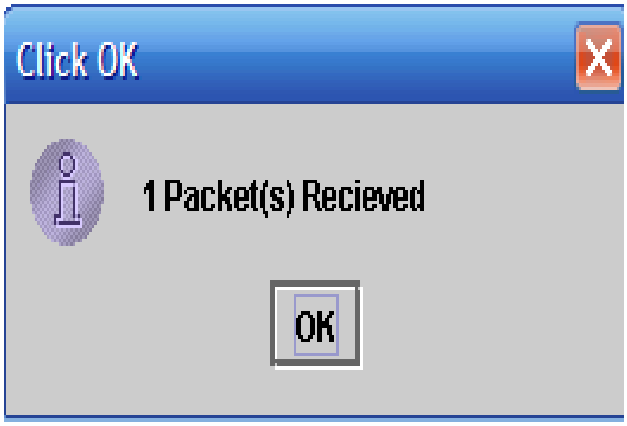


Fig 9.

IV. CONCLUSION

In this project, we have implemented a novel congestion avoidance mechanism for the Internet called Network Traffic Monitoring. Unlike existing Internet congestion control approaches, which rely solely on end-to-end control, NTM is able to prevent congestion collapse from undelivered packets. It does this by ensuring at the border of the network that each flow's packets do not enter the network faster than they are able to leave it. NTM requires no modifications to core routers nor to end systems. Only edge routers are enhanced so that they can perform the requisite per-flow monitoring, per-flow rate control and feedback exchange operations .Extensive experimental simulation results done at different levels show that NTM successfully prevents congestion collapse from undelivered packets.

REFERENCES

[1] S. Floyd and K. Fall, "Promoting the Use of End-to-End Congestion Control in the Internet," *IEEE/ACM Transactions on Networking*, August 1999, to appear.

[2] J. Padhye, V. Firoiu, D. Towsley, and J. Kurose, "Modeling TCP Throughput: A Simple Model and its Empirical Validation," in *Proc. of ACM SIGCOMM*, September 1998, pp. 303-314.

[3] B. Sutter, T.V. Lakshman, D. Stiliadis, and A. Choudhury, "Design Considerations for Supporting TCP with Per-Flow Queuing," in *Proc. of IEEE Infocom '98*, March 1998, pp. 299-305.

[4] B. Braden *et al.*, "Recommendations on Queue Management and Congestion Avoidance in the Internet,'' RFC 2309, IETF, April 1998.

[5] A. Demers, S. Kershaw, and S. Shankar, "Analysis and Simulation of a Fair Queuing Algorithm," in *Proc. of ACM SIGCOMM*, September 1989, pp. 1-12.

[6] A. Parekh and R. Gallager, "A Generalized Processor Sharing Approach to Flow Control - the Single Node Case," *IEEE/ACM Transactions on Networking*, vol. 1, no. 3, pp. 344-357, June 1993.

[7] I. Stoica, S. Shankar, and H. Zhang, "Core-Stateless Fair Queuing: Achieving Approximately Fair Bandwidth Allocations in High Speed Networks," in *Proc. of ACM SIGCOMM*, September 1998, pp. 118-130.

[8] D. Lin and R. Morris, "Dynamics of Random Early Detection," in *Proc. of ACM SIGCOMM*, September 1997, pp. 127-137.

[9] D. Bartsekas and R. Gallagher, "Data Networks, second edition," Prentice Hall, 1987.

[10] R. Jain, S. Kalyanaraman, R. Goyal, S. Fahmy, and R. Viswanathan, "ERICA Switch Algorithm: A Complete Description," NTM Forum Document 96-1172, Traffic Management WG, August 1996.

[11] D. Clark and W. Fang, "Explicit Allocation of Best-Effort Packet Delivery Service," *IEEE/ACM Transactions on Networking*, vol. 6, no. 4, pp. 362-373, August 1998.

[12] W. Stevens, "TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms,'' RFC 2001, IETF, January 1997.

[13] LBNL Network Research Group, "UCB/LBNL/VINT Network Simulator - ns (version 2)*,"* http://www-mash.cs.berkeley.edu/ns/, September 1997.

[14] B. Vanda lore, S. Fahmy, R. Jain, R. Goyal, and M. Goyal, "A Definition of Generalized Fairness and its Support in Switch Algorithms," NTM Forum Document 98-0151, Traffic Management WG, February 1998.

[15] W.K. Tsai and Y. Kim, "Re-Examining Maxmin Protocols: A Fundamental Study on Convergence, Complexity, Variations, and Performance," in *Proc. of IEEE Infocom*, April 1999, pp. 811-818.

[16] G.K, Drivakis Saxena ,Prof.J.P Gupta "Anomaly Detection in Network Traffic"2nd international conference on computer and Engineering Technology-vol-7, 978-1-4244-6349-7/10/$ 26.00 @ 2010 IEEE

[17] V.Mannem and R.sankar,"Improved leaky bucket policing algorithm for NTM network"IEEE GLOBECOM 1994.

[18] T.Sasipraba and S.K.srivastava,"Network Border patrol, a novel congestion avoidance mechanism for improving QOS in wireless network", Information Technology Journal, 5 (3):427-432, 2006 ISSN 1812-5638, 2006 Asian Network for Scientific Information.

[19] Celio A., Brett J.V., T.Suda, "Network Border Patrol: Preventing Congestion Collapse and promoting fairness in the Internet", in proc of IEEE infocom 2000, March 2000.

First Author: Himanshu Kumar

I have completed my B.E in computer science and Engineering Degree from Manipal University, Manipal, Karnataka, India in 2009. Currently I am pursuing M.Tech In information Technology (Networking) at VIT University, Vellore, Tamil Nadu, India. My Major Research areas are Network Security, Theory of computation, Logic Design, wireless adhoc network, Operating System, Data Structure and Algorithm, RDBMS. I have Completed Successfully Research Project Entitled rainbow table to crack password using md5 hashing algorithm..Currently I am doing my final project on web usage mining trends and navigational pattern.

Second Author:-Remya Joseph

I have completed my B.Tech in computer science and Engineering Degree from Mahatma Gandhi (MACE) University, kothamangalam, Kerala, India in 2010. Currently I Am Pursuing My M.Tech In information Technology (Networking) at VIT University, Vellore, Tamil Nadu, India. My Major Research areas are Network Security, High performance TCP/IP network, and wireless adhoc network, Operating System, Data Structure and Algorithm, RDBMS. I have Completed Successfully Research Project Entitled Efficient web usage mining in formal concept analysis. Currently I am doing my final project on automating IOT Cases in Robot Framework in Alcatel Lucent.

Third Author:-Sudhanshu Kumar

I have completed my B.E. in computer science and Engineering Degree from RVCE, VTU University, Bangalore in 2009.My major Research areas are computer Network, Software Engineering, and Cryptography and network security, DBMS, Data

Structure and Algorithm. Currently I am working as a Business analyst in Deloitte, Hyderabad.

Fourth Author:-Ajay Kumar

I have completed my B.E in computer science and Engineering Degree from LNCT, Indore, and Madhya Pradesh, India in 2011. Currently I am pursuing M.Tech In information Technology (Networking) at VIT University, Vellore, Tamil Nadu, India. My Major Research areas are Network Security, Theory of computation, Compiler Construction, wireless adhoc network, Operating System, Data Structure and Algorithm, RDBMS. I have Completed Successfully Research Project Entitled rainbow table to crack password using md5 hashing algorithm..Currently I am doing my final project on Development of the Universal Automation Tester Framework in VMware.

Fifth Author:-Praveen Kumar

I have completed my B.Tech in Electronics and Communication Engineering Degree from Integral University, Lucknow India in 2010. Currently I am pursuing M.Tech in Software Technology at VIT University, Vellore, Tamil Nadu, and India. My Major Research areas are Information Security, Cloud Computing, Software Engineering, Operating System, Data Structure and Algorithm, RDBMS. I have Completed Successfully Research Project Entitled Sql-Injection Tool for Finding The Vulnerability and Automatic Creation of Attacks on JSP..Currently I am doing my final project on Design and Development of Cloud Computing Based Framework for District Resource Planning

Sixth Author:-Sunil Kumar Shrinarayan Singh

I have completed my B.E in Information Technology from ADPIT, Sardar Patel University, India in 2010. Currently I am pursuing M.Tech In information Technology (Networking) at VIT University, Vellore, Tamil Nadu, India. My Major Research areas are Cryptography and Network Security, Computer Network, Theory of computation, wireless adhoc network, Operating System, Data Structure and Algorithm, RDBMS. I have Completed Successfully Research Project Entitled rainbow table to crack password using md5 hashing algorithm..Currently I am doing my final project on Integrated Solutions Management and Maintenance Using Loosely Coupled Architecture in IBM.

.