Global Journal of Computer Science and Technology
Volume 11 Issue 19 Version 1.0 November 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Verification of Lost Data Packets and Regularizing Packets Transmission

By N Vinutha, G Varalakshmi
Aurora's Technological and Research Institute

Abstract - Security in the network remains a major challenge which is highly susceptible to maliciousness. The routers especially are a major threat to the network. They can be malicious enough to disrupt the transmission of the data in the form of packets. In this paper, along with the detection of a malicious router, the transmission of packets is regularized to maximum extent possible. A Conditional Packet Buffering (CPB) algorithm is used to increase the through put of the router.

Keywords : *Distributed systems, Data packets, malicious router, and Packet regularization.*

GJCST Classification : *C.2.1*

Strictly as per the compliance and regulations of:

Verification of Lost Data Packets and Regularizing Packets Transmission

N Vinutha [α], G Varalakshmi [Ω]

Abstract - **Security in the network remains a major challenge which is highly susceptible to maliciousness. The routers especially are a major threat to the network. They can be malicious enough to disrupt the transmission of the data in the form of packets. In this paper, along with the detection of a malicious router, the transmission of packets is regularized to maximum extent possible. A Conditional Packet Buffering (CPB) algorithm is used to increase the through put of the router.**

Keywords : Distributed systems, Data packets, malicious router, and Packet regularization.

I. Introduction

A distributed system consists of multiple autonomous computers that communicate through a computer network. The computers interact with each other in order to achieve a common goal. The routers play a major role to achieve this goal.

The router is a primary component in the infrastructure of today's Internet. Routing messages in a network is an essential component of Internet communication, as each packet in the Internet must be passed quickly through each network (or autonomous system) that it must traverse to go from its source to its destination. Network routers occupy a unique role in modern distributed systems. They are responsible for cooperatively shuttling packets amongst themselves in order to provide the illusion of a network with universal point-to-point connectivity. Although, a great deal of attention has been paid to securing network communication.

To a first approximation, networks can be modelled as a series of point-to point links connecting pairs of routers to form a directed graph. Since few endpoints are directly connected, data must be forwarded hop-by-hop from router to router, toward its ultimate destination. Therefore, if a router is compromised, it stands to reason that an attacker may drop, delay, reorder, corrupt, modify, or divert any of the packets passing through. Thus network routing is vulnerable to disruptions caused by malfunctioning or malicious routers that draw traffic towards them but fail to correctly forward the traffic. In this paper, two queues are maintained to hold the packets – one which holds the regular packets sent by the previous router and the other to hold the packets that may have been maliciously dropped by the router or due to time out. This ensures that maximum packets are sent to the destination in a scenario where the router turns out to be malicious.

The protocol used in the network is Transmission control Protocol. The TCP provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer. TCP is the protocol that major Internet applications such as the email, remote administration, file transfer and World Wide Web rely on.

The reminder of this paper is organized as follows. In section II, I put my ideas within the context of prior and ongoing research related to malicious router detection. In section III, discuss the technique in regularization of the packets and shows the comparison of an existing solution and the proposed solution in which the increase in the throughput of the router is highlighted. In section IV the results achieved are put in the form of a graph. The conclusion is presented in section V.

II. Related Work

Based on my literature survey I have analyzed that attempt was only made to detect the packet loss. There is no attempt to regularize the packet loss. In this paper the packet loss is minimized by transmitting them in case they are dropped maliciously or due to time out.

In an earlier work [1], a compromised router detection protocol (X) is developed that dynamically infers the precise number of congestive packet losses that will occur. Once the congestion ambiguity is removed, subsequent packet losses can be safely attributed to malicious actions.

In [2], a protocol was developed that detects and reacts to routers that drop or misroute packets. The protocol WATCHERS is based on the principle of conservation of flow in a network: all data bytes sent into a node, and not destined for that node, are expected to exit the node. WATCHERS track this flow, and detect routers that violate the conservation principle. The WATCHERS has several advantages over existing network monitoring techniques. The WATCHERS protocol impact on router performance and WATCHERS' memory requirements are reasonable for many environments. However, the WATCHERS protocol had many limitations in both its traffic validation mechanism and in its control protocol.

Author α: M.Tech (CSE) Aurora's Technological and Research Institute, Hyderabad, India. E-mail : Vinnu.ncs@gmail.com
Author Ω: Associate Professor, ATRI, Uppal, Hyderabad, AP. Email : varacse@gmail.com

The problem of detecting routers [3] [4] [5] with incorrect packet forwarding behaviour and the design space of protocols that implement such a detector is explored. A protocol that is likely inexpensive enough for practical implementation at scale is presented. A prototype system called Fatih that implements this approach on a PC router is explained.

The algorithms [6] that form the basis of the protocols such as OSPF, RIP, and IEGP are not secure, however, and have even been compromised by routers that did not follow the respective protocols correctly.

Robust routing requires [7] [8] not only a secure routing protocol but also well-behaved packet forwarding. To this end, the paper proposes an approach to robust routing in which routers, assisted by end hosts, adaptively detect poorly performing routes that appear suspicious, and use a secure trace route protocol to attempt to detect an offending router. This approach complements efforts that focus on securing the routing protocol itself. The secure trace route is a general technique with wide applicability, and is presently investigating it in the context of multi-hop wireless networks.

The paper [9] considers the impact of systemic noncongestion related packet loss on the effectiveness, fairness, and efficiency of parallel TCP transmissions. The results indicate that parallel connections are effective at increasing aggregate throughput, and increase the overall efficiency of the network bottleneck. In the presence of congestion related losses, parallel flows steal bandwidth from other single Stream flows. A simple modification is presented that reduces the fairness problems when congestion is present, but retains effectiveness and efficiency.

RED gateways [10] [11] keep the average queue size low while allowing occasional bursts of packets in the queue. During congestion, the probability that the gateway notifies a particular connection to reduce its window is roughly proportional to that connection's share of the bandwidth through the gateway. RED gateways are designed to accompany a transport-layer congestion control protocol such as TCP. The RED gateway has no bias against busty traffic and avoids the global synchronization of many connections decreasing their window at the same time. Simulations of a TCP/IP network are used to illustrate the performance of RED gateways.

Random Exponential Marking [12] [13], aims to achieve both high utilization and negligible loss and delay in a simple and scalable manner. The key idea is to decouple congestion measure from performance measure such as loss, queue length, or delay. While congestion measure indicates excess demand for bandwidth and must track the number of users, performance measure should be stabilized around their targets independent of the number of users.

All the above related work only presents the detection of malicious router and provides an alternate method to avoid malicious router. This paper goes an extra step to detect the malicious router and also regularize the packet losses so that the confidence in the packet transmission is maintained. This helps in critical applications being implemented, especially those applications that require data integrity.

III. Regularization of Packets

In a network, the packets are sent from a source router to destination router through the intermediate routers. A routing table exists for every router. The routing table maintains the source, destination and route of the packets in the network. It is frequently updated with the latest information.

In the proposed system, the router works in three modes - Mode 1, Mode 2, and Mode 3. The router can work in any one of the three modes individually by setting the router properties. These properties are set manually. When a router property is set to Mode 1, there is no differentiation of the packet loss. It may be due to overflow or may be due to maliciousness of the router.

In mode 2, based on the traffic parameters such as router buffer load (inflow), router buffer capacity, network bandwidth, queue size etc, a dynamic threshold is set. This threshold is used to remove the ambiguity between the packet loss due to congestion and router maliciousness. Also, a single queue is used to maintain the packets at the router.

In mode 3, along with the differentiation of the packet loss due to congestion and router maliciousness, the packets are also regularized. Unlike the mode 2, there are two queues maintained at each of the router–Accepted Queue (AQ) and Rejected Queue (RQ).

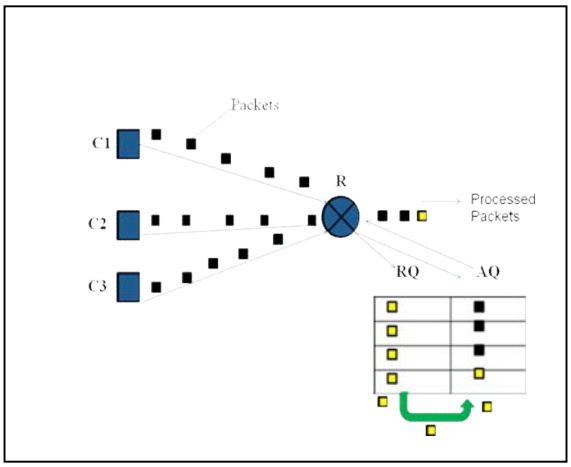

Figure 1 : Router working on mode 3

In the above figure 1 where the router works on mode 3, C1, C2, C3 are the client which sends packets

(P) to the router (R). Two queues, AQ – Accept Queue and RQ – Reject Queue are maintained at each router. Based on the below algorithm – Conditional Packet Buffering (CPB) - at the router, the packets are sent to either the AQ or RQ. A packet consists of attributes like the packet id, source and destination address, packet lifetime etc. The router Consider the packet's life time from its attributes and performs the below algorithm as follows

a) Conditional Packet Buffering (CPB) Algorithm

Sum (Packet Process Time and Current Waiting Time) > Packet Lifetime = RQ

Sum (Packet Process Time and Current Waiting Time) < Packet Lifetime = AQ

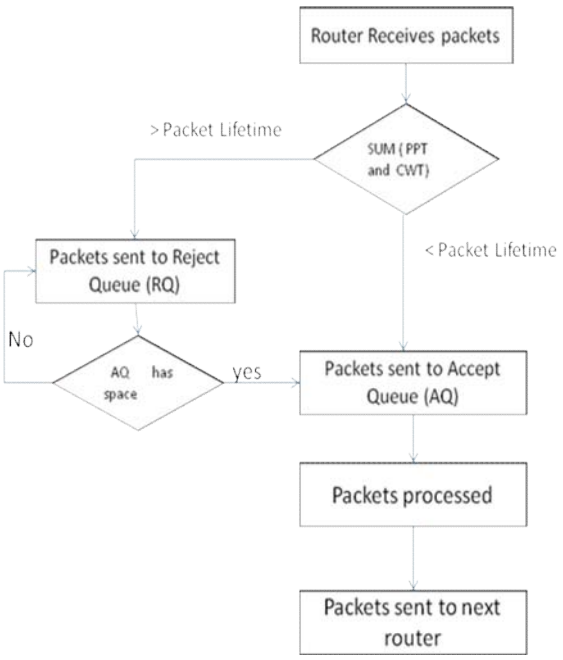

Figure 2 : Flow chart for CPB Algorithm

The router takes the current waiting time and the packet process time of the packets which are in the buffer and does the summation of the packet process time and current waiting time. If the summed up value is greater than the packet's life time then the router send the packet to the Reject Queue (RQ). If the summed up value is less than the packet's life time then the router send the packet to the Accept Queue (AQ). If at any time, the AQ is either empty or has place to accommodate a packets to process, the router takes the packets from RQ which has less lifetime and sends it to the AQ where the packets are processed and sends them towards the destination.

Table I : Comparission With Existing Solution

Status	Mode 1	Mode 2	Mode 3
Total packets sent to router	1000	1000	1000
Total packets processed(throughput)	608	629	680
Total packets dropped	392	43	51
Total Packets maliciously dropped	0	328	269

The above table which gives information that existing solution which is represented in mode 1 and mode 2 and the proposed solution in mode 3 in which the total packets processed are more i.e., throughput is increased.

IV. Performance Analysis

In existing solution the ambiguity between the packet loss due to congestion and maliciousness of the router is determined in which the throughput of the router is less. In the proposed solution along with the differentiation of the packet loss due to congestion and maliciousness of the router, the packets are regularized where the throughput is increased compared to the existing solution. The benchmark results after executing the algorithm in the three different modes shows the increase in the throughput of the router packet processing. From below graph I can conclude that mode 3 has high throughput than mode 1 and mode 2.

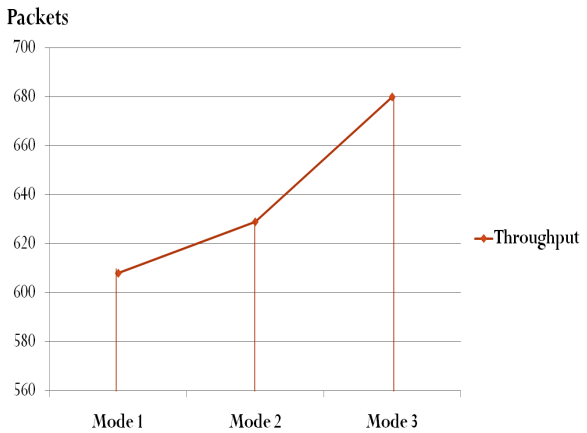

Figure 3 : Throughput increase at the router in three different modes Mode 1, Mode 2 – Existing Solution and Mode 3 – Proposed Solution

V. Conclusion

This paper makes an attempt to propose a solution to increase the throughput of the routers in the network by taking into consideration the packets that may have been dropped due to congestion or maliciousness of the router. The packet loss is thus minimized by regularizing.

Acknowledgment

I would like to thank Sr.Asst.Prof G. Varalakshmi, Sr. Asst.Prof A. Poongodai and Prof D. Sujatha (Aurora's Technological and Research Institute, Hyderabad, India) for their careful reading and valuable suggestions. I would also like to thank the anonymous referees for their helpful comments and suggestions to improve this work.

References References Referencias

1. Alper T. M Zrak, Student Member, IEEE, Stefan Savage, Member, IEEE, and. Keith Marzullo, Member, "Detecting Malicious Packet Losses" IEEE-26 Feb 2009.
2. K.A. Bradley, S. Cheung, N. Puketza, B. Mukherjee, and R.A. Olsson,"Detecting Disruptive Routers: A Distributed Network Monitoring Approach," Proc. IEEE Symp. Security and Privacy (S&P '98), pp. 115-124, May 1998.
3. A.T. Mizrak, Y.-C. Cheng, K. Marzullo, and S. Savage, "Detecting and Isolating Malicious Routers," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 3, pp. 230-244, July-Sept. 2006.
4. S. Cheung and K. Levitt, "Protecting Routing Infrastructures from Denial of Service Using Cooperative Intrusion Detection," Proc. New Security Paradigms Workshop, 1997.
5. D. Taylor, "Using a Compromised Router to Capture Network Traffic," unpublished technical report, July 2002, http://www.netsys.com/library/papers/GRE_sniffing.PDF.
6. M.T.Goodrich, "Efficientand and Secure Network Routing Algorithms", Jan. 2001.
7. V.N. Padmanabhan and D. Simon, "Secure Trace route to Detect Faulty or Malicious Routing," SIGCOMM Computer Comm. Rev., vol. 33, no. 1, pp. 77-82, 2003.
8. S. Kent and R. Atkinson. "Security Architecture for the Internet Protocol", RFC 2401, November 1998
9. T.J. Hacker, B.D. Noble, and B.D. Athey, "The Effects of Systemic Packet Loss on Aggregate TCP Flows," Proc. ACM/IEEE Conf. Supercomputing (SC '02), pp. 1-15, 2002.
10. S. Floyd and V. Jacobson, "Random Early Detection Gateways for Congestion Avoidance," IEEE/ACM Trans. Networking (TON '93), vol. 1, no. 4, pp. 397-413, 1993.
11. K. Bala. I. Cidon. and K. Sohraby. "Congestion control for high speed packet switched networks," in Proc. INFOCOM '90. pp. 52CL526, 1990.
12. S. Athuraliya, S. Low, V. Li, and Q. Yin, "REM: Active Queue Management," IEEE Network, vol. 15, no. 3, pp. 48-53, 2001.
13. S. Athuraliya and S. H. Low," Optimization Flow Control, II: Implementation.Submitted for publication, http:// netlab.caltech.edu, May 2000.
.