Low rate TCP denial-of-service attack detection at edge routers

Publisher: IEEE

Abstract:
Low rate TCP denial-of-service attacks are a new type of DoS attacks that are carefully orchestrated to exploit the fixed minimum TCP RTO property and thereby deny services to legitimate users. This type of attacks is different from traditional flood-based attacks and hence conventional solutions to detect these attacks are not applicable. We propose a novel approach to detect these attack flows at edge routers. A flow exhibiting a periodic pattern is marked malicious if its burst length is greater than or equal to RTTs of other connections with the same server and its time period is equal to the fixed minimum RTO. A carefully designed light weight data structure is proposed to store the necessary flow history at edge routers. Simulation results show that such flows can be detected by our proposed approach, which does not require any modification to TCP congestion control algorithms like randomizing the fixed minimum RTO.

Published in: IEEE Communications Letters (Volume: 9 , Issue: 4 , April 2005)
Page(s): 363 - 365
Date of Publication: 04 April 2005
ISSN Information:
INSPEC Accession Number: 8396585
DOI: 10.1109/LCOMM.2005.1413635
Publisher: IEEE

SECTION I.

Introduction

The Internet has become an integral part of various commercial activities like online banking, online shopping, etc. Denial-of-Service *(DoS)* attacks are becoming a major threat to the Internet infrastructure integrity. Protocol development is influenced by various factors such as scalability, availability, and ease of transition. It is difficult to envision loop holes during the protocol development stage that may be exposed to future security breaches. In this paper, we address the problem of identifying DoS attacks caused by protocol exploits. We introduce a scheme to detect a low rate TCP DoS attack which exploits the fixed minimum RTO property of TCP implementations [1]. This fixed minimum RTO introduces a vulnerability of synchronizing other TCP flows to timeout at the time scale of the attack flow. Also, to evade traditional detection systems, the average rate of the attack flow is kept low. This is done by sending high rate bursts for short intervals that are repeated periodically. Hence, there is a need to constantly monitor flows that exhibit periodicity. As a packet traverses from the source towards its destination, it can take any available route depending upon parameters like network congestion and route failures. Routers look at the header information to forward packets onto the next hop. Most attacks are launched by exploiting some vulnerabilities, and it is possible to identify such attacks at routers if we analyze each flow by monitoring parameters exploited in the attack. Routers are playing a significant role in provisioning QoS and security; they will be required to perform higher layer functions such as application based traffic classification, and maintaining per flow information. In general, the proposed detection system will modify the Internet layer structure as shown in Fig. 1, where edge routers will perform the transport layer function of maintaining some connection parameters. The rest of this letter is organized as follows. Section II briefly describes existing solutions to the problem. Section III describes an implementation

scenario. Section IV describes the proposed detection system. Section V presents simulation results, followed by conclusions in Section VI.

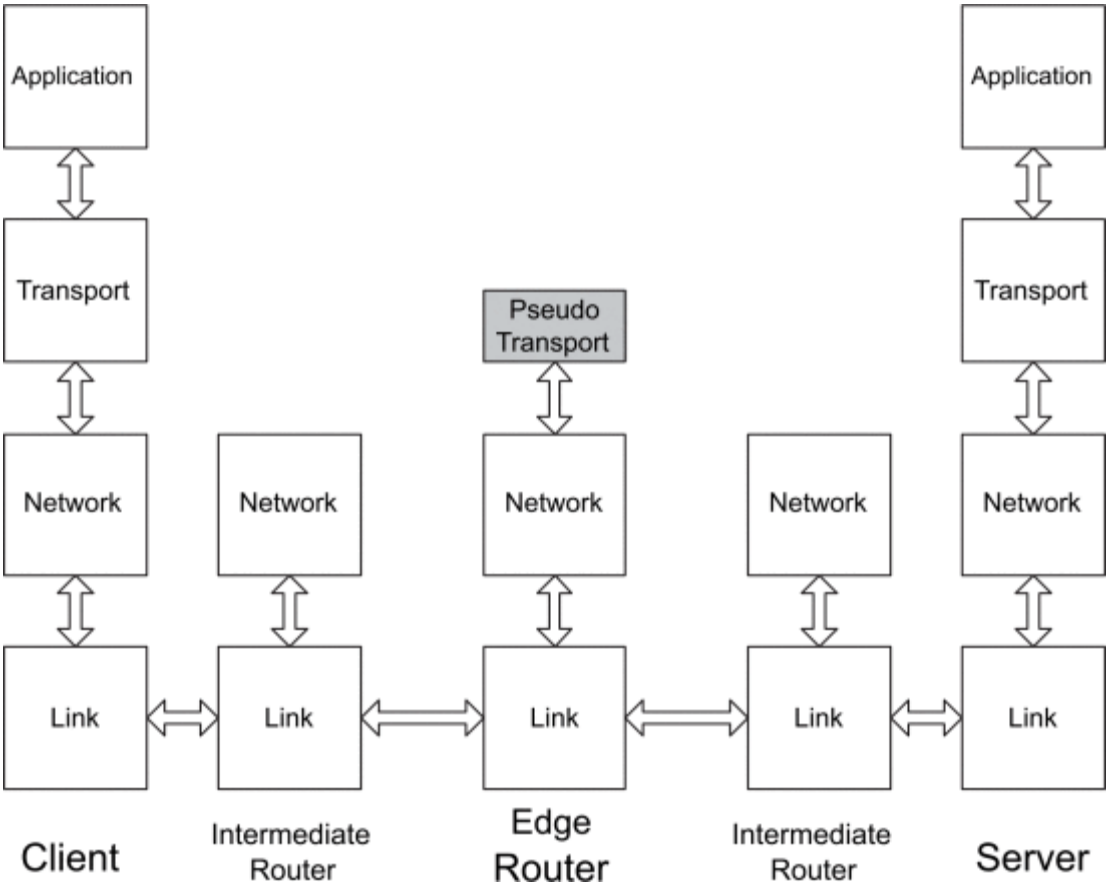

Fig. 1.
A new layer structure.

View All

SECTION II.

Existing Solutions

In [2], a scheme is proposed to mitigate the low rate DoS attack by randomizing the fixed minimum RTO value used in the TCP implementations. Apart from this scheme, to our best knowledge, no other viable solutions have been proposed to combat this type of attacks. Randomizing the fixed minimum RTO seems to be an immediate solution, but the main issue is whether such an approach should be adopted. Randomizing the fixed minimum RTO will reduce the TCP connection performance in the absence of an attack. It is shown in [3] that an unnecessary TCP timeout results in loss of useful throughput, and TCP begins a new *slow start*. TCP will also require a long time to adapt its RTT estimate after every timeout, since the RTTs of retransmitted packets are not measured [4]. The fixed minimum RTO of one second was selected because it eliminated unnecessary timeouts [3]. In [5], a router based low rate TCP DoS detection approach is proposed. It uses the autocorreleation property to detect periodic attack flows, and is required to be implemented at multiple routers along the path from source to destination. Hence, we propose a novel scheme that does not introduce any modification

to the TCP congestion control mechanism like randomizing the fixed minimum RTO and can be implemented at a single edge router.

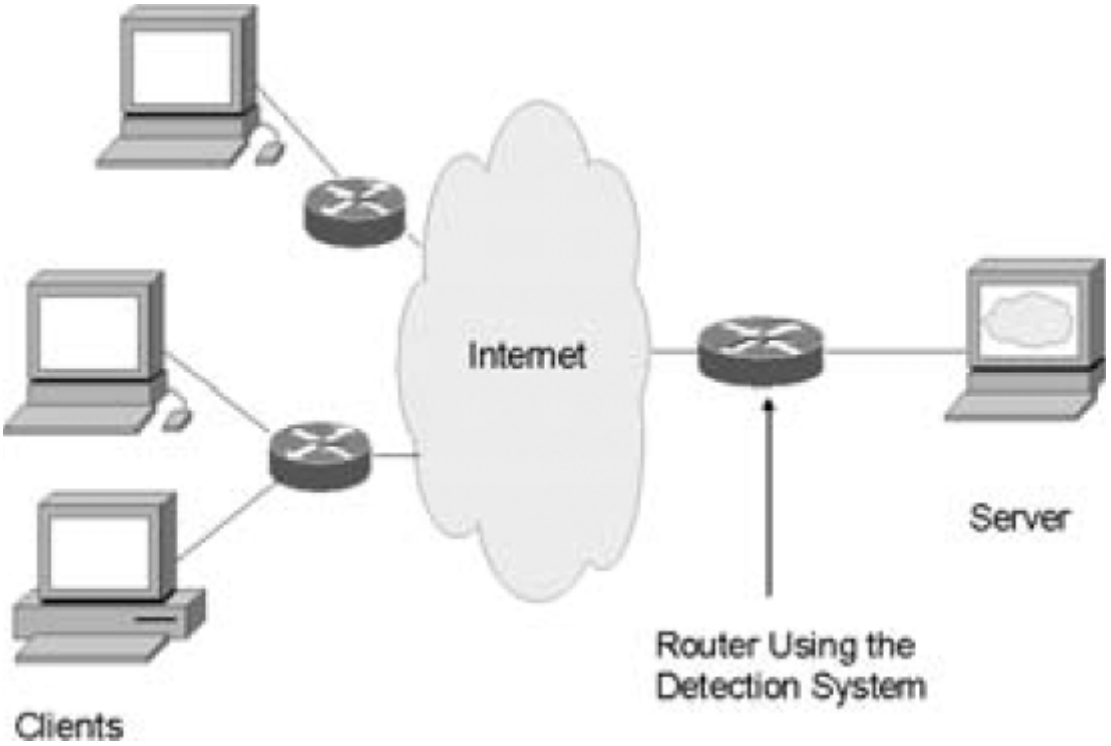

Fig. 2.
Proposed detection system deployed at an edge router.

View All

SECTION III.

Typical Example

A network scenario in Fig. 2 is shown to explain where our proposed detection system is deployed. It shows edge routers connecting a local area network to the Internet with typical client server connections. Each edge router acts as an entry and exit point for traffic originating from that local area network; essentially all incoming and outgoing traffic will pass through this point. The proposed detection system can be deployed at the edge routers of a local area network in which the server is present. For illustrative purposes, we assume that all clients are outside the local area network in which the server is present, so that the detection system can monitor all flows connecting to the server.

SECTION IV.

Detection System Architecture

Fig. 3 shows the basic layout of the system. It has three basic blocks, namely, flow classifier, object module, and filter. Each block functions as follows:

- The flow classifier module classifies packets based on the flow ID by means of a combination of the IP source address, IP source port, IP destination address, and IP destination port. Flow information is obtained from these packets, and packets

are forwarded as usual by the routing mechanism resulting in no additional delay apart from the lookup delay.

- The object module consists of various objects for each flow that is monitored. Detailed explanation is given in the next sub-section. A flow is monitored until it is considered normal.

- The filter is used to block flows that are identified as malicious by the object module.

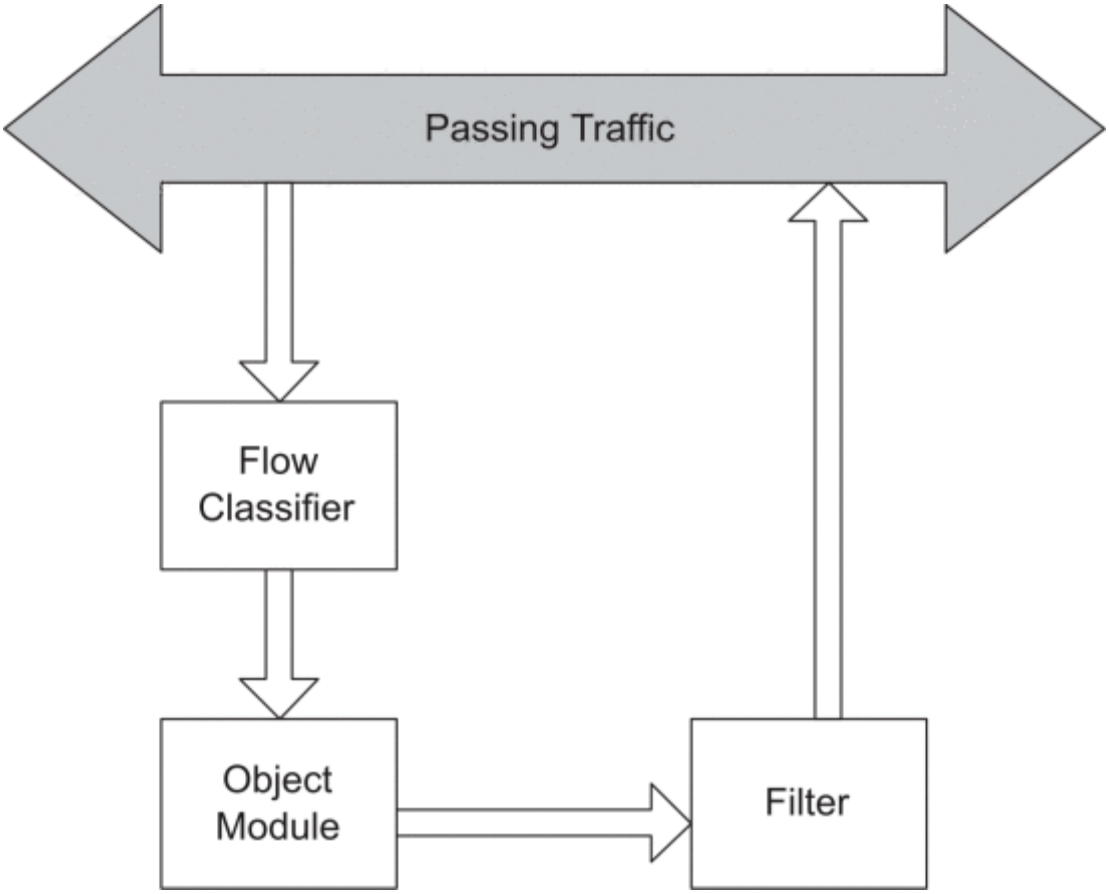

Fig. 3.
Architecture of the system.

View All

A. Highlights of Object Module

Consider a DoS attack which tries to exploit protocol shortcomings. The object module maintains per flow information by creating objects per flow called *flow objects*. A thin data structure layer is designed to keep track of these flow objects. It maintains only those parameters which are exploited in the attack. This thin structure keeps separate track of information about flows classified as malicious. This information is then relayed to the filter module. Advantages of the object module over other proposed solutions are highlighted below.

- Different types of protocol attacks can be detected by changing parameters that should be maintained by the thin data structure layer.

- Effective control mechanism can easily be introduced in the Internet architecture by adding functionalities to routers.

- The detection system is distributed, and can be implemented as an add-on module at edge routers.

- The proposed detection system relies on verifying the *actual intent* of a flow.

- False positives of this detection system are significantly reduced as compared to the traditional IDS as it does not rely on *"signature or pattern matching techniques"*. The proposed system is used for online detection of malicious flows.

- The proposed scheme can work in conjunction with an IP traceback scheme [6] to provide an effective solution to mitigate distributed denial of service attacks.

- The object module provides a significant advantage over other solutions by making efficient use of resources. After a flow is classified as normal, flow objects are destroyed, and occupied memory is released.

B. Low Rate TCP Denial-oj-Service Attack Detection

Consider a periodic stream in which the burst length is greater than or equal to RTTs of other connections with the same server, and the time period is equal to the fixed minimum RTO. An attack flow satisfying these two important conditions can cause denial of service to other TCP flows [1]. The flow objects maintain the arrival times of packets at the edge router in the pseudo transport layer. The malicious flow detection sub-module of the object module computes the time difference of consecutive packets of each flow. The submodule computes the average high and average low of the time difference values. The average high value of the time difference repeats periodically for the attack flow; other flows do not exhibit this property. The malicious flow detection submodule then estimates the burst length of a flow based on the packet arrival times, and compares it with the relative RTTs of other flows connected to the same server. The relative RTT of each connection is computed by the sub-module from the packet arrival times maintained for both source and destination side packets. In a similar way, the time period is estimated, and compared with the fixed minimum RTO of one second. A flow meeting the above two conditions is marked as malicious. The above detection criteria can detect attack flow with period (T=1sec) which is the ideal attack flow criterion that will inflict the maximum damage, i.e., by denying service to the maximum number of connections. In order to detect quasi periodic attack flows, the average high of the time difference to be compared is in the range of $(T+\Delta t)-(L+\Delta L)$, where for example Δt can vary between -0.2 to 0.2, T=1sec is constant (minRTO), L is the burst length computed by our detection system, and ΔL is the deviation of the burst length. The Δt and ΔL are configurable parameters of the detection system.

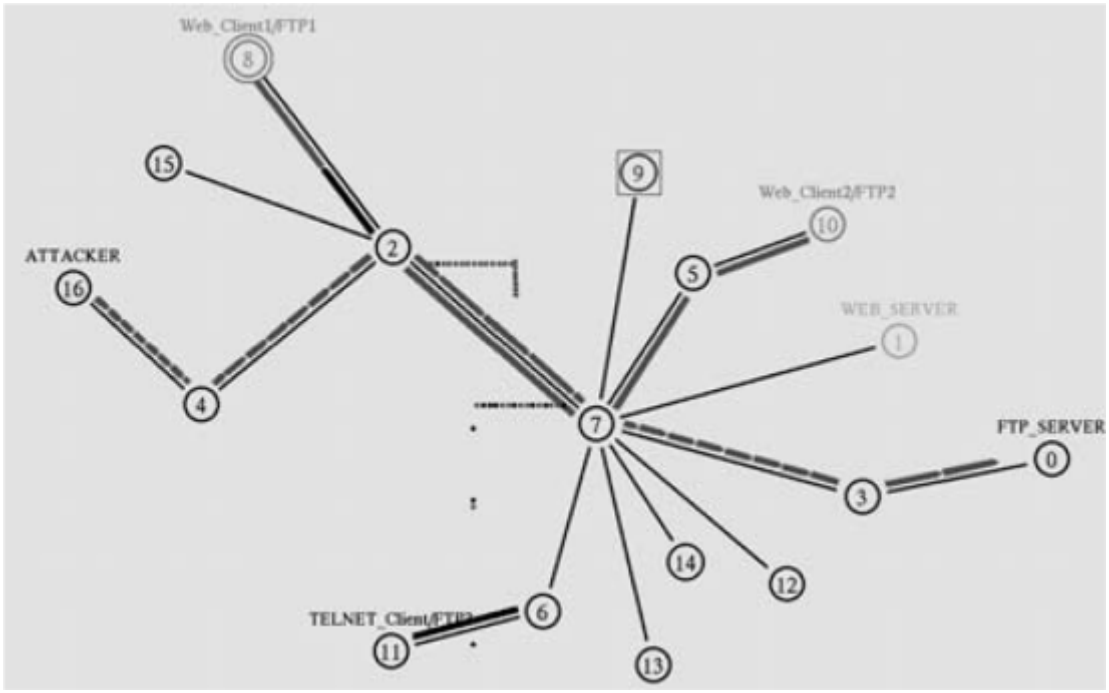

Fig. 4.
Experimental topology.

View All

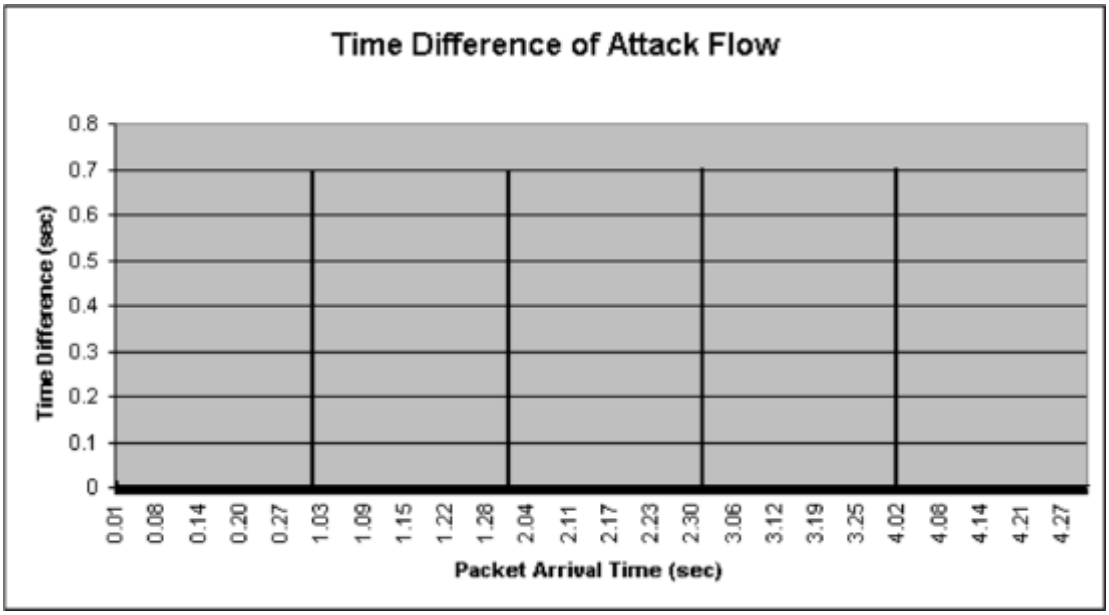

Fig. 5.
Time difference of attack flow.

View All

SECTION V.

Simulation Results

We used NS2 [7] to demonstrate the performance of our proposed detection scheme. The experimental topology is shown in Fig. 4. As specified earlier, we compute the time difference of consecutive packets. Figs. 5–7 show plots of this time difference for three different types of flows. Note that the attack traffic shows periodicity in the time difference while HTTP and FTP traffic lacks periodicity. This is the first step in distinguishing the attack flow from other flows. In the second step, the time period (T) of the attack flow is compared with the fixed minimum RTO, and the inter-burst length (L) of the attack flow is compared with RTTs of other flows connected to the same server. If T is found approximately equal to one second, and L is found approximately equal to RTTs of other connections, we conclude that the flow is malicious.

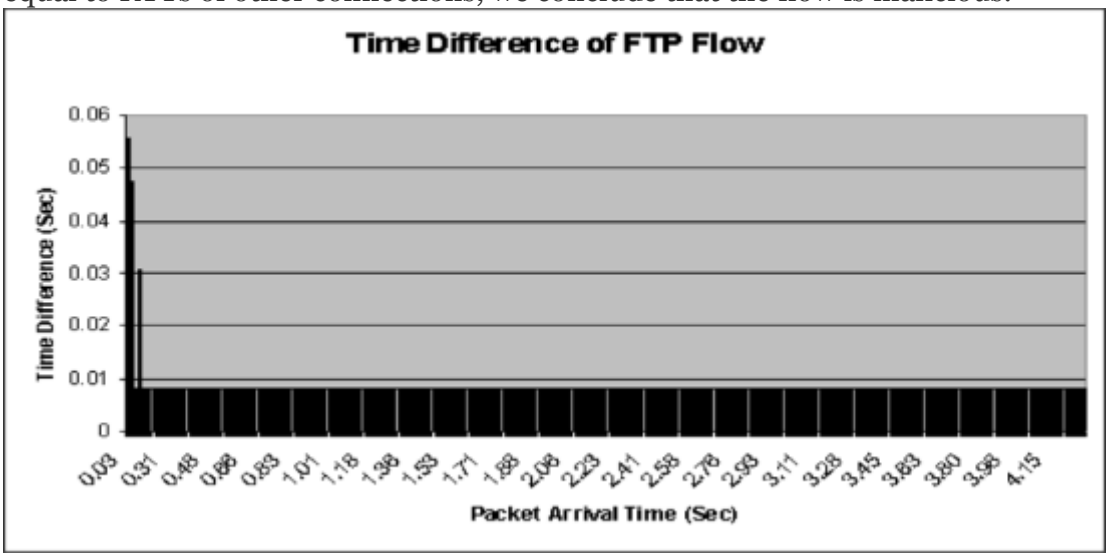

Fig. 6.
Time difference of FTP flow.

View All

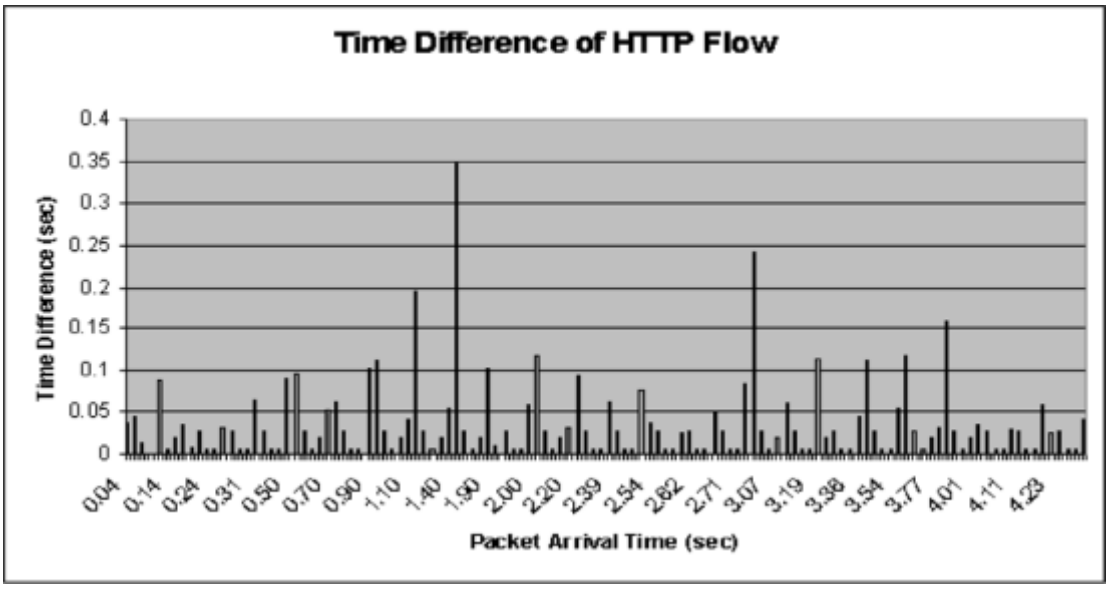

Fig. 7.

Time difference of HTTP flow.

View All

SECTION VI.

Conclusion and Future Work

We have proposed a new detection scheme against the low rate TCP DoS attacks that can detect the low rate TCP DoS attack at edge routers. The detection scheme is easily deployable. The focus of this letter is to present the framework of the proposed detection concept that will prompt more relevant follow up research activities. We also plan to investigate the applicability of this proposal to detect worm propagation in which the application layer exploits are used to launch an attack or infect hosts.