THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Remote Path Identification using Packet Pair Technique to Strengthen the Security for Online Applications

R. Abinaya
PG Scholar, Department of CSE, M.A.M College of Engineering
Tiruchirappalli, Tamil Nadu, India
V. Pugazhenthi
Associate Professor, Department of CSE, M.A.M College of Engineering
Tiruchirappalli, Tamil Nadu, India

Abstract:
As the technology grows in size, complexity connections, new applications and service requirements necessitate the development of suitable end-to-end tools that monitor and measure the properties of the paths become essential. In particular, the effective evaluation and measurement of the capacities along paths are of realistic interest. In fact, the end-to-end path capacity estimation in networks is much more important. Since the measurements are performed in any environment, end-hosts might try to change these measurements to increase their gain in the network, which leads to a wide range of bandwidth manipulation attacks such as packet loss, delay in packets, impersonation attacks and cross traffic, etc. This project aims to detect these security threats against bottleneck bandwidth estimation using the packet-pair technique. The security levels are adaptively enhanced for video files in packet pair technique. It further implements an algorithm for remote path identification using the distribution of packet-pair dispersions and evaluates its accuracy, robustness and potential use of online applications. This is achieved by the verifier checks the prover's claimed or assumed identity by measuring the path without active cooperation from the prover.

Key words: *Network measurements, bandwidth manipulation, packet pair, probing and security.*

1. Introduction

The Internet is largely a commercial infrastructure in which users pay for their access to an Internet Service Provider (ISP) and from there on the global Internet. The Network measurements enable Internet-based systems, to acquire reliable estimates of the network in order to ensure the QoS and performance of their online services. The performance level of these network connections is based on their bit rate, or network bandwidth, since the additional bandwidth normally means higher throughput and better quality of service. In such an environment, bandwidth monitoring becomes a critical operation. Users need to check whether they get the required bandwidth that they pay for and whether the network that they using are sufficiently provisioned. Bottleneck bandwidth measurements are gaining increasing importance in many wide-area Internet systems and services including multicast trees, content distribution and P2P systems.

Bottleneck bandwidth [9] refers to the maximum throughput that a flow between two end hosts can achieve, when there is no other competing traffic load. The performance and QoS of most Internet services are based on their bandwidth capacities mainly due to this fact. The bottleneck bandwidth techniques can be classified in two categories: the one-packet and the packet-pair technique. The techniques are well understood and can provide exact estimates under certain conditions. In one packet and packet pair techniques, probe packets are exchanged between the verifier and the prover to extract estimates of the network bandwidth characteristics. The one-packet methods are based on the assumption that the end-to-end transmission delay is proportional to the probe packet size.

The packet-pair technique predicts the difference in arrival time of two packets back to back of the same size travelling from the same source to the same destination. The packet-pair technique usage has been recommended as a potential solution to several problems such as network management, end-to-end admission control. Packet-pair measurements are performed in an end-to-end environment, end-hosts are motivated to modify their bottleneck bandwidth in order to increase their gain in the network. The malicious host can change the claimed bandwidth and increase or decrease the bandwidth to increase their benefits in the network. The malicious host captures the network interface delays the packets and sends it in short time with high bandwidth. Otherwise the malicious host claims smaller time dispersion between packet-pairs and consequently inflate its bandwidth. The prover gets the packet and reply the packet to the verifier on it received time. The verifier gets the packet and checks it not in the time it calculated. It again sends the packet on the bottleneck link if it verified time is changed and it confirms malicious prover is on the path. The malicious prover cannot send the packet on same bandwidth they increase or decrease the packet bandwidth. The

verifier also checks the packet size if its size is large transmission delay is occurred and they queued on the bottleneck link. The bottleneck link verifier measures the capacity and time of the link and sends the packets on that link. The same sized packet is sending on that link they are queued and reach the prover and prover send reply to the verifier. If large packet is send it queued on the link, delay and traffic is occurred. For this file is splitted and send it on multiple paths. So delay is reduced and also controls traffic on bottleneck link. The malicious host on the path they did not get the full information and send the content of the file in bottleneck link with minimum delay. The splitted file content is merged on the prover and prover send reply on the time verifier calculated. For example, a malicious host forces to modify the trusted network interface or use bandwidth shapers in order to increase its utility in content distribution networks. While this misbehavior increase its gain in the network and it would also result in performance deterioration in the entire network.

The routers in the path, gain much of their bandwidth by being as simple as possible, slowing the flow to answer the link bandwidth queries is probably not acceptable. The easiest approach to deploy and consequently which we are most interested, is for end hosts to understand link bandwidth by actively probing or passively listening to traffic. As a result, these techniques rely on routers handling ICMP packets consistently, and timely delivery of acknowledgements. These techniques use significant amounts of network bandwidth to perform their measurements and can be slow enough to become impractical for some of the application.

This paper is organized as follows. In Section 2 papers related to my concept. Section 3 Secure packet pair techniques. Section 4 conclusion.

2. Related Works

Measuring the end to end behavior between two hosts can be problematic. This can be easily done by network measurement tool. Network measurement tool is the process of measuring the amount and type of traffic and delay, measuring maximum data throughput and measuring the maximum bandwidth. End to end capacity is measured using MultiQ[1]. [1] is a passive bottleneck detection tool or passive capacity measurement tool. It measures the capacity of multiple congested links along a path from a single flow trace using TCP packet interarrival time. It identifies cross traffic, minimum capacity and capacities of other congested link. [1] Extract the useful information from cross traffic. Capprobe[2] measures the correct capacity of the path and filter out noisy measurements . It also identifies the delay packets using correct measurements it measured. The incorrect capacity caused queuing effects and does not address the malicious provers.

End to end measurements of link bandwidth and available bandwidth in Packet train and packet pair [3]. Both techniques estimate the accurate measurements based on active probing. This Packet pair and packet train shows how cross traffic is interacting with probe packets and identifies mirror effect. The main difference between packet-train and packet pair methods is that one cross-traffic packet affects at least two dispersion values in the packet train, while in the packet pair it only affects one dispersion value. In the packet train the two dispersion values are dependent of each other. This might be exploitable, or perhaps may lead to mistakes in calculations. The packet pair dispersion can be increased or decreased based on whether packet is affected by cross traffic. [4] Measuring link bandwidth is a deterministic model of packet delay. It measures the link bandwidth for the path. It set TTL for large packets it sends on each link. The small packets are queued on the path followed by large packets. These packets have Round Trip Time will form a line whose slope is the inverse of the link bandwidth. Path quality monitor [5] is a effective monitoring technique to estimate packet loss rate, delay exceed threshold. It provides accurate information when intermediate nodes may adversarial drop, modify and inject packets. The malicious prover used cheating strategy in which it always delays/rushes it packets.

[11] Analyzes how correlated distributed events are controlled and estimated can be applied to for network security. Based on this approach, Process Query System (PQS) and have implemented a software, which is able to scan and correlate distributed events according to users high level process description. [13] Shows the effects of network load, cross traffic, variable packet size and probing packet size on the bandwidth distribution of packet pairs. Then the dispersion of long packet trains is considered. The mean of packet train dispersion distribution corresponds to bandwidth metric is referred as Average Dispersion Rate (ADR). It is difficult to measure the capacity of a path with just a few packet pairs.

3. Secure Packet Pair

The two packets are exchanged adjacently in time between verifier and prover using packet pair technique. The verifier and prover connected to the network using router. The verifier measures the prover's path characteristics by exchanging the probe packets with the prover. The prover accepts the bandwidth measured by the verifier and participates in the bandwidth verification process.

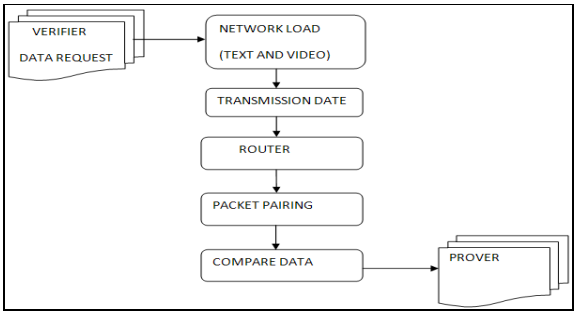

Figure 1: Architecture

4. Network Topology Constructions

Network Topology may consist of the number of routers that are connected with local area networks. Thus, a router can receive data from the nearer router or from the local area network. An edge router receives packets from its local network. A center router receives packets from other routers. The number of routers connected to a one router is called as the degree of a router. This is calculated and stored in a database. The Upstream interfaces of each router also have to be found and stored in the interface table.

5. Packet Pair Technique

To describe the principles behind the packet-pair technique, consider a network path defined by a sequence of consecutive links ρ that connect the verifier to prover. Links are connected via network components (router). The dispersion between two packets after a link refers to the time interval between the entire transmissions of these packets. The prover sends large packet-pairs back-to-back in time with an initial dispersion. Packet-pairs are initially sent with a dispersion Δo, the resulting dispersion measured at the other end of ρ is denoted by Δn. It describes how to mitigate this limitation by filtering out samples that suffer undesirable queuing.

$$\Delta_n = \frac{S}{C_{min}} + d_2^{min} + \sum_{i=min+1}^{n} (d_2^i - d_1^i)$$

In addition, the packet pair property assumes that the two packets are sent close enough in time that they queue together at the bottleneck link. This is very high problem in bandwidth bottleneck links and/or for passive measurement.

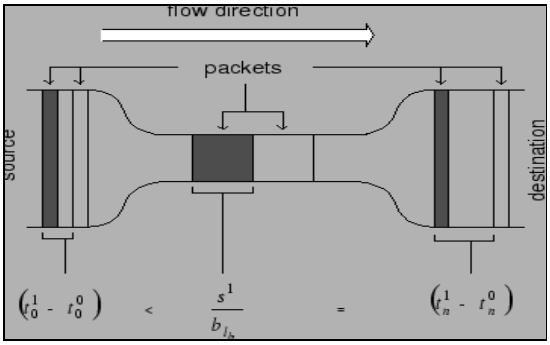

Figure 2: Packet Pair Diagram

The attacker can also reroute probe packets through other bottleneck links to influence the measurements. Packet-pair sent by the verifier to the prover can be used to measures the prover's download bandwidth, provided that the verifier's upload bandwidth is superior than the prover's download capacity and that the prover reply back the verifier's packets with small probes that do not queue at the bottleneck link. The dispersion between the reply packet as determined by the verifier is likely to correspond to the dispersion of the packets sent by the verifier on the downlink path to the prover. A malicious prover can also delay its probes to vary the bandwidth estimates extracted by the verifier. A packet-pair technique was generated without prior security considerations and assumes that end-hosts are trustworthy.

5.1. Peer To Peer Algorithm

This paper provides more security to send the packets using packet pair technique. To send the packets more secure the verifier split the file and send it on multiple paths. So if any malicious person is on the path they will not get full information. These splitted information's are merged on the prover's side. The Peer to Peer routing algorithm is used to send packet more securely. Earlier they send small packet first to the prover. But in this algorithm they collect the verifier request based on time not on the size of the packet. Peer to peer algorithm distributed computing nodes of equal roles or capabilities exchange information directly with each other.

6. Path Identification Techniques

Evaluate an automated Internet path identification system based on the packet-pair dispersion. The verifier checks the prover's claimed or assumed identity by measuring the path. The probe packets can be exchanged in two different directions uplink (up) and downlink (dw). The up mode required provers to initiate the transmission. The dw verifier measures the provers downlink measurements. Then it performs data collection process to extract the measurement parameters that result in more stable path. The impact of measurement time, probing rate and measured duration of extracted features is evaluated. It collects all the data and it select the parameters by doing the measurements to be used in the accuracy testing. Then it identified the better path and allowed to send the packets on that path.

6.1. Real Time Scheduling

Real time network applications depend on schedulers to guarantee the quality of service (QoS). Conventional Real time Schedulers focus on the timing constraints but are less effective in satisfying the security requirements. It proposes an adaptive

security-aware scheduling system for packet switched networks using a real-time multi agent design models. The proposed system combines real time scheduling with security service enhancement. In the Real time Scheduling the priority is given to the person who comes first based on time and sends the file either it is large or small file. First verifier calculates the path capacity and sends the packets by splitting them. To provide more security encryption is used it encrypt the file and it generate the hash key automatically by reading the content in the file. If any malicious person got the file they cannot read it. If they read the file delay is occurred so hash key is changed. The prover gets the file and check the hash key is same they send reply packet to verifier. If any change is made they confirm that it was untrusted person and change the path and reroute the file. The untrusted host on the path will not get full information because they splitted the file content and send on multiple path. In addition we send video file to the prover without splitting the file and any delay on the path. The audio and video files of real time data flows has guaranteed QoS while the packet security levels are adaptively enhanced according to the feedbacks from the congestion control module.

7. Impersonations of Path Identities

Once the Packet has reached the destination after applying the Composing Filtering Algorithm, there it checks whether it has sent from the right upstream interfaces. If any one of the attack is found, then it request for the Path Reconstruction. The process of finding the new path for the same source and the destination in which no attack can be made is called Path Reconstruction.

7.1. Composing Filter Algorithm

The composition algorithm acting a central role in the usage of weighted finite-state transducers to apply finite-state models to inputs and to combine cascaded model. The composition algorithm, which simply matches transitions leaving, paired input states. Some transducers have practical importances that do not compose efficiently in this way. These cases typically create significant numbers of non-co accessible composition states that waste time. For some problems, it is possible to find equivalent inputs that will compose more efficiently, but it is not all the time possible or desirable to do so. Composition filter applied at each composition state during the construction that decides if composition is to continue. It set out to create a general composition filter that blocks every non-co accessible composition state for any input transducers, and then we have only delegated the job of doing a full composition to the filter. The end to end dispersion measured by the verifier

$$\Delta_n = \Delta_0 + \sum_{i=1}^{n} (d_2^i - d_1^i)$$

Where d_1 is first packet, d_2 is second packet, Δo is initial dispersion and Δn is final dispersion. The concept of the composition filters and presents filters that remove useless epsilon paths and push forward labels and weights along epsilon path. This proposes a new type of time-domain direct-form fast filtering algorithm, which composes sum of N/2 product-of-sum terms. The sum consists of the desired present output point and the half partial results of the preceding and succeeding output point. These services require Internet routers to move from simple destination based packet forwarding to a more complex form of forwarding called layer switching. Since the lower bounds indicate that highly efficient algorithms are unlikely for the completely general problem.

8. Conclusion

While using end to end network some problems are arises such as packet delay, impersonation attack and cross traffic is occurred. To overcome this problem packet pair technique is used. Packet pair technique is used to measure the capacity of the path and it give complete scheme for remote path identification to provide more security measurements in end to end networks and analyzes resilience to impersonation attack. A large subset of attacks against the packet-pair technique can be successfully countered. The verifier sends large packets of equal size in multiple paths to reach the prover. The Composing filter algorithm is used to merge the packets send on multiple path in prove and it reduce packet delay and cross traffic. As a by-product, we outlined a number of scenarios where the use of the packet-pair technique may strengthen the security. To motivate for the need of a next-generation Internet that provides secure functionality for network measurements. It briefly discussed the benefits of using trusted network components to secure the use of the packet-pair technique.

9. References

1. S. Katti, D. Katabi, C. Blake, E. Kohler, and J. Strauss, "MultiQ: Automated detection of multiple bottleneck capacities along a path," in Proc. IMC, 2004, pp. 245–250.
2. R. Kapoor, L. Chen, L. Lao,M. Gerla, and M. Y. Sanadidi, "CapProbe: A simple and accurate capacity estimation technique," in Proc. ACM SIGCOMM, 2004, pp. 67–78.
3. Andreas Johnsson, "On the Comparison of Packet-Pair and Packet-Train Measurements",2003.
4. K. Lai and M. Baker, "Measuring link bandwidths using a deterministic model of packet delays," in Proc. ACM SIGCOMM, 2000, pp.283–294.
5. S. Goldberg, D. Xiao, E. Tromer, B. Barak, and J. Rexford, "Path quality monitoring in the presence of adversaries," in Proc. ACM SIGMETRICS 2008, pp. 193–204.
6. C. Dovrolis, P. Ramanathan, and D. Moore, "Packet- dispersion techniques and a capacity-estimation methodology," IEEE/ACM Trans. Netw., vol. 12, no. 6, pp. 963–977, Dec.2004.
7. Pathrate [Online]. Available:http://www.cis.udel.edu/~dovrolis/ bwmeter.html
8. Pathchar [Online]. Available: http://www.caida.org/tools/taxonomy/perftaxonomy.xml\#pathchar

9. G. Karame, D. Gubler, and S. Capkun, "On the security of bottleneck bandwidth estimationtechniques," in Proc. Securecomm, 2009,pp. 121–141.
10. T. Kohno, A. Broido, and K. Claffy, "Remote physical device fingerprinting," IEEE Trans. Dependable Secure Comput.,vol. 2, no. 2, pp. 93–108, Apr./Jun. 2005.
11. G. Jiang and G. Cybenko, "Temporal and spatial distributed event correlation for network security," in Proc. Amer.Control Conf., 2004, pp.996–1001.
12. C. Dovrolis, P. Ramanathan, and D. Moore, "What do packet dispersion techniques measure," in Proc. IEEE INFOCOM,2001, pp. 905–914.
13. C. Dovrolis, P. Ramanathan, and D. Moore, "Packet-dispersion techniques and a capacity-estimation methodology," IEEE/ACM Trans. Netw., vol. 12, no. 6, pp. 963–977, Dec. 2004.
14. R. Sinha, C. Papadopoulos, and J. Heidemann, Fingerprinting Internet Paths Using Packet Pair Dispersion 2006.
15. ShaperProbe [Online]. Available: http://www.cc.gatech.edu/~partha/ diffprobe/shaperprobe.html