DYNAMIC MALICIOUS PACKET DROPPING WITH BOTTLENECK

Srinivas Rao S
Department of Physics, S.V.K.P. & Dr.K.S.Raju A &S College,Penugonda.

Sridhar G
Department of Maths, S.V.K.P. & Dr.K.S.Raju A &S College,Penugonda.

Abstract--We consider the problem of detecting whether a compromised router is maliciously manipulating its stream of packets. In particular, we are concerned with a simple yet effective attack in which a router selectively drops packets destined for some Victim. Unfortunately, it is quite challenging to attribute a missing packet to a malicious action because normal network congestion can produce the same effect. Modern networks routinely drop packets when the load emporarily exceeds their buffering capacities. Previous detection protocols have tried to address this problem with a user-defined threshold: too many dropped packets imply malicious intent. However, this heuristic is fundamentally unsound; setting this threshold is, at best, an art and will certainly create unnecessary false positives or mask highly focused attacks. Packet Loss ratio is among the most important metrics for identifying poor network conditions, since it affects data throughput performance and the overall end-to-end data transfer quality. An application for enhancing the security of packets in transit has been proposed. The end to end packet loss and delay is estimated in addition to providing the security to the packets. The objective of our simulation studies done in Java language is to estimate the amount of data that has been lost and the delay incurred. Encryption and decryption has been provided Dynamically. The existing methods indicate certain disadvantages in Poisson based tools. Simulation results demonstrate the effectiveness of the proposed method in terms of packet loss, delay, and encryption

Introduction

The networks are groups of devices that communicate between each other without the support of centralized infrastructure. Although, this technology is promising, some challenges are slowing its development and deployment. Devices in ad hoc networks are in general limited in battery power, CPU and capacity. As a consequence, these devices transmission ranges are limited which make them relying on each other to forward their packets to destination. With devices with limitations in memory and CPU, one can also image limitations in services and security. The factors mentioned earlier, namely the absence of central infrastructure and the devices limitations, have made ad hoc networks more vulnerable to frauds and attacks ranging from passive eavesdropping to active interfering. In fact, an intruder can compromise a node in the network and may eavesdrop on the communications or drop for instance packets, which is supposed to forward them further, to carry out a denial of service attack. If a packets dropping attack occurs, the node sending the packets may misunderstand the reason behind this problem as it might be caused by a broken connection, a hardware limitation such as buffer congestion or a malicious intention. In this case, the packets sender cannot take the right decision and thus will expose himself to a real menace. we develop a Dynamic detection protocol (DDP) 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. We believe our protocol is the first to automatically predict congestion in a systematic manner and that it is necessary for making any such network fault detection practical. Once a router has been compromised in such a fashion, an attacker may interpose on the traffic stream and manipulate it maliciously to attack others—selectively dropping, modifying, or rerouting packets. In the Network every node is a potential victim in the sense that it might be compromised and used to disrupt the network. However, nodes with a bottleneck character attract more interest in being compromised because of the services they can provide. Securing the network in this situation is a critical task because a compromised bottleneck node can eavesdrop on a significant number of communications or even carry out simultaneous denial of service attacks. The aim of this paper is to develop a defense mechanism to face denial of service caused by packet dropping. To be more precise, we suggest a technique that allows a source node to distinguish between what is malicious and spurious regarding a packet dropping performed by its next hop node that is a bottleneck node and which the source node is relying on to forward the packets to their destination. This mechanism requires the support of the destination node. In fact, the destination node is observing the packets that the intermediate bottleneck node is forwarding and when it detects a misbehavior, it notifies the source node. The latter, in turn and based on some information that he has about this intermediate node, estimates the natural congestion level at this node and compare it with the received information. If they mismatch, the intermediate node is declared to be an intruder. Our mechanism can be applied as a monitoring technique for ad hoc network models similar to the ones investigated herewith and which build trust between the impact of a set of TCP packet dropping attack patterns on FTP file transfer was investigated. In addition, a statistic-based approach to detect malicious attacks was proposed. In a

statistic approach is also suggested to detect whether bottleneck nodes are maliciously dropping packets. Even the objectives and the models studied in this paper and in are similar, the used techniques differ in two major points. First of all and contrary to (n which, the destination is in charge of determining whether the bottleneck is an intruder, our model assumes that this task is achieved by the source nodes. This makes, in particular, our technique a means for neighborhood monitoring for reputation-based protocols such as CONFIDANT as mentioned earlier. Secondly, our approach is not statistic-based as in), but uses a deterministic model to detect malicious packet dropping.

DDP Protocol

The protocol used maintains log in each router stating the information about each packet that passes through it. If the actual behavior deviates from the predicted behavior, then a failure has occurred. we consider the properties and overhead of protocol χ.

There are two steps in showing the accuracy and completeness of χ. assume the administrative ability to assign and distribute cryptographic keys to sets of nearby routers.

Detecting router test

This is based on the well-known Z-test4 [10]. Let N be the no. of packets lost due to malicious access. For those N packets, let be the mean of qs(t). Let be the mean of ps and be the mean of qp(t). The packet loss occurs only when X > qlim-qp-ps. The Z test score is: $Z = ((qlim- - -\mu)/(\sigma\sqrt{n}))$.

Evaluation

We evaluate mainly the performance according to the following metrics. *Control overhead:* The control overhead is defined as the ratio between total number of packets to be sent to the total number of received data packets. *Average end-to-end delay:* .The end-to-end-delay is the average time taken by data packets to reach from the sources to the destinations. This includes all the delays caused during route acquisition, buffering and processing at intermediate routers, etc.

Average Packet Delivery Ratio: This is the fraction of the data packets generated by the sources that are delivered to the destination. This evaluates the ability of the protocol to discover routes.

Router Reliability: The node reliability is calculated by the packet delivery ratio of that particular router. If the ratio is high means reliability is also high.

Conclusion

To the best of our knowledge, this paper is the first serious attempt to distinguish between a router dropping packets maliciously and a router dropping packets due to congestion. Previous work has approached this issue using a static user-defined threshold, which is fundamentally limiting. Using the same framework as our earlier work (which is based on a static user-defined threshold) [4], we developed a compromised router detection protocol χ that dynamically infers, based on measured traffic rates and buffer sizes, the number of congestive packet losses that will occur. We evaluated the effectiveness of protocol χ through an implementation and deployment in a small network. We show that even fine-grained attacks, such as stopping a host from opening a connection by discarding the SYN packet, can be detected.

References

[1] 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.

[2] 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.

[3] L. Subramanian, V. Roth, I. Stoica, S. Shenker, and R. Katz, "Listen and Whisper: Security Mechanisms for BGP," Proc.
First Symp. Networked Systems Design and Implementation (NSDI '04), Mar. 2004.

[4] S. Kent, C. Lynn, J. Mikkelson, and K. Seo, "Secure Border Gateway Protocol (Secure-BGP)," IEEE J. Selected Areas in
Comm., vol. 18, no. 4, pp. 582-592, Apr. 2000. Longman Publishing Co. Inc., 1992.

[5] " Securing Routing in Open Networks Using Secure Traceroute ", Gaurav Mathur, Venkata N. Padmanabhan ,Daniel R. Simon,Microsoft Research, July 2004

[6] S. Cheung and K.N. Levitt, "Protecting Routing Infrastructures from Denial of Service Using Cooperative Intrusion Detection," Proc. Workshop on New Security Paradigms (NSPW '97), pp. 94-106, 1997.

[7] 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.

[8] R. White. Deployment Considerations for Secure Origin BGP (soBGP), draft-white-sobgp-bgp-deployment-01.txt. Draft, Internet Engineering Task Force, June 2003