An Efficient Response Time for Shrew Attack Protection in Mitigating Low-Rate Tcp-Targeted Attacks

S. Ganesan[#1], B.Loganathan[*2]
[#1]M.Phil. Scholar
[#1]PG & Research Department of Computer Science
[#1]Government Arts College, Coimbatore-18, Tamilnadu, India.
*[*2]Associate Professor*
*[*2]PG & Research Department of Computer Science*
*[*2]Government Arts College, Coimbatore-18, Tamilnadu, India.*

***Abstract*--- This paper presents a simple priority-tagging filtering mechanism, called SAP (Shrew Attack Protection), which protects well-behaved TCP flows against low-rate TCP-targeted Shrew attacks. In this scheme, a router maintains a simple set of counters and keeps track of the drop rate for each potential victim. If the monitored drop rates are low, all packets are treated as normal and equally complete to be admitted to the output queue and only dropped based on the AQM (Active Queue Management) policy when the output queue is full. SAP keeps tagging victim packets as high priority until their drop rate is below the fair drop rate. By preferentially dropping normal packets to protect high-priority packets, SAP can prevent low rate TCP-targeted Shrew attacks from causing a well-behaved TCP flow to lose multiple consecutive packets repeatedly. This simple strategy protects well-behaved TCP flows away from near zero throughputs (due to slow start) under an attack.**

***Keywords*---- Shrew attack, differential tagging, fair drop rate.**

I. INTRODUCTION

As SAP focuses on protecting TCP flows against Shrew attacks, we envision that SAP is used in conjunction with other systems that are more effective for different types of network attacks [2]. In fact, SAP can help such systems by providing more information when some of the monitored applications experience unusual high packet drop rates. Since keeping the information about per-flow state is typically prohibitive for a router to maintain, SAP aggregates flows and maintains statistics for each aggregate. While different levels of aggregation obviously lead to different performance trade-off between accuracy and memory/computation requirements, this approach uses the application-level granularity to identify potential victims.

Specifically, identify the application of a packet based on the value of destination port field in the TCP/IP header (regardless of the source and destination IP addresses) and maintain drop rate statistics for each port. Due to this aggregation, SAP may not be able to fully protect legitimate traffic from attack flows all the time. Furthermore, some attackers may try to evade SAP by using multiple destinations ports or exploit SAP by manipulating the drop rate of particular ports.[2]

The approach illustrates a number of attack scenarios when SAP is employed, and present experiment results where SAP performs well in these adversarial scenarios. In these experiments, SAP can effectively protect victims from Shrew attacks whereas an AQM scheme alone (e.g., RED) cannot.
In particular, in simulations involving a mix of normal TCP flows and a BGP session, show that a Shrew attack can cause the BGP session to close and

increase the drop rate of normal TCP traffic to near 100%, resulting in degradation in the performance of normal TCP traffic to near zero throughputs.[2] When employ SAP, the drop rate of normal TCP traffic only increased by 1.1%, allowing normal TCP traffic to retain most of their throughput, and we observe that the BGP session remained active with no loss in performance. Also consider a number of adversarial scenarios, and we demonstrate that SAP performs well when multiple destination ports have a drop rate higher than the fair drop rate. In addition, evaluate performance of SAP when regular DDoS attacks use ports that SAP wants to protect. [4] In this scenario, SAP protects legitimate TCP flows from getting zero throughput or session closing.

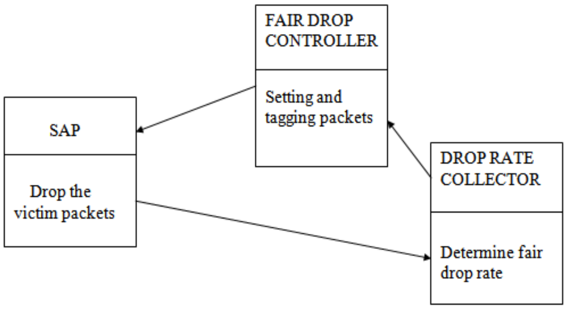

Fig.1 SAP Architecture

II. PROBLEM DEFINITION

A. SAP METHODOLOGY

SAP neutralize Shrew attack by controlling drop rates of TCP flows at the application aggregate level and use of differential packet prioritization. Drop Rate collector monitors application aggregates. Employ a hash of flow description fields in the packet. [2]

Fair Drop Rate controller uses a single fair drop rate adjusted dynamically. Differential Tagging module, tag victim TCP packets as high priority to lower victim's drop rate. Tagged packets are passed to the priority AQM module in router for preferential packet dropping mechanism. SAP is treated as a form of traffic management mechanism and ensures all application flows experience similar drop rates when going through the same network link by using multiple classes/tagging on flow level. [2]

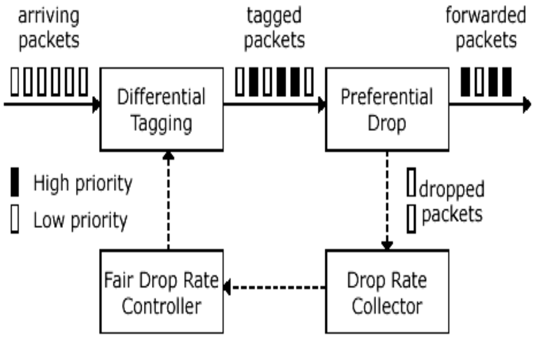

Fig.2 SAP Flow [2]

For each aggregate (e.g., destination port), maintain two set of counters (for arrival and drop). SAP is implemented, only 216 = 65536 distinct destination ports are feasible. Number of applications need to be monitored are much smaller in practice and it is used to protect all legitimate TCP-based protocols.[2]

B.PROBLEMS OF EXISTING FRAME WORK

- SAP does not measure exploited bandwidth rate.
- Response time of attack mitigation is not measured using SAP.
- Bandwidth efficiency level should be static.

III. ANALYSIS OF THE PROPOSED SYSTEM

The proposed system presents a extend SAP the port based mechanism to allocate appropriate bandwidth rate and to reduce response time for attack mitigation. Improve SAP a destination port based mechanism to allocate bandwidth rate for transmission and reduce response time for attack mitigation. In proposed work new blocks introduced are Drop rate collector, Delay rate controller and Bandwidth rate specified. Drop and delay rate collector measures the number of packets dropped at the specified time. Time of drop is sent to the delay rate controller. Delay rate controller sends the time of appropriation of delivery for dropped packets. Delay rate controller intimates the differential tagging for packets to be forwarded.

Bandwidth rate specifies block identify data rate to be prioritized. In differential tagging based on the bandwidth rate allocation the data packets are appropriate to the destination node. Response rate of attack mitigation is improved with delay sensitivity and bandwidth appropriation.

A. ADVANTAGES OF PROPOSED FRAME WORK

- To allocate appropriate bandwidth rate in TCP flow sessions.
- To reduce response time for attack mitigation.
  Shrew attack exploits TCP's
- Retransmission timeout mechanism.

The proposed system involves the concept of improving the SAP for destination port based mechanism to allocate bandwidth rate for transmission and reduce response time for attack mitigation. In the existing system, SAP is a destination-port-based mechanism requires a small number of counters to find potential victims. Since the SAP preferentially admits packets from victims with high drop rates to output queue. So the proposed system uses SAP architecture to minimize the bandwidth rate and response time.

IV. SOLUTION FRAMEWORK

i) Delay and Drop Rate Controller
ii) Delay Rate Controller
iii) Fair Drop Rate Controller

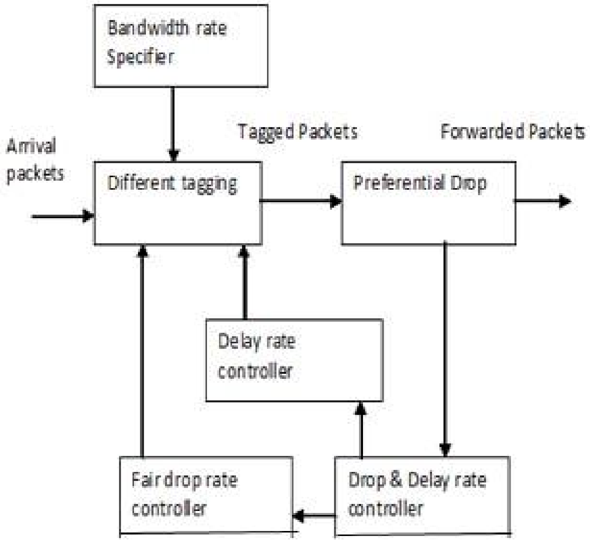

Fig.3 Energy Efficiency of SAP

A. DELAY AND DROP RATE CONTROLLER

In SAP it considers mainly to neutralize a shrew attack by controlling the drop rates of TCP flows. The drop rates of application aggregates based on which SAP identifies potential victims are monitor by drop rate collector. The fair drop rate is determined by SAP. It starts to project the victims by tagging their TCP packet as high priority to lower the victim Drop rates.

B. DELAY RATE CONTROLLER

Drop rates of application like aggregates based on which SAP identifies potential victims are monitor by Drop rate collector. By this drop rate collector , we easily find out the packet drop rate hence we find and detect the packet drop by reducing the rate of

C.FAIR DROP RATE CONTROLLER

In this framework we find out the average of total drop rates from the drop rate collector. Now we set our fair drop rate with the help of the average drop rate from the drop rate collector. In which, corresponding flow we set the minimum drop rate in the drop rate controller.

i) Average of drop rate > minimum drop rate =>fair drop rate=avg of drop rate.

ii) Average of drop rate < minimum drop rat =>fair drop rate=minimum of drop rate.

V. CONCLUSION

This proposed approach introduced a simple Shrew attack protection mechanism called SAP. SAP provides network operators with a broad first line of proactive defense against Shrew attacks, significantly neutralizing their impact. By monitoring the drop rates of potential victims, SAP prevents consecutive packet drops for a victim, which observes for well-behaved TCP flows under a Shrew attack. SAP achieves this through differentiated tagging of victims' packets and preferential admission to the output queue. Unlike other existing mechanisms, SAP focuses on protecting victims without explicitly identifying attackers.

SAP is a port-based victim-detection scheme and readily deployed on top of existing router mechanisms, as SAP does not rely on any proprietary packet header information or sophisticated signal analysis techniques. The result shows that SAP is able to stop the crippling BGP attack scenario identified. More broadly, our results show that SAP is also effective in allowing TCP flows in general to recover their throughput under a Shrew attack. [2]

REFERENCES

[1] M. Allman and V. Paxson, "*On estimating end-to-end network path properties*," in Proc. ACM SIGCOMM, [1999].

[2] C. W. Chang, S. Lee, B. Lin, and J. Wang, "*The taming of the shrew: Mitigating low-rate TCP-targeted attack*," in Proc. IEEE ICDCS, [2009].

[3] Y. Chen, Y.-K. Kwok, and K. Hwang, "*Filtering shrew DDoS attacks using a new frequency-domain approach*," in Proc. IEEE LCN Workshop Netw. Security, 2005.

[4] C.-M. Cheng, H. Kung, and K.-S. Tan, "*Use of spectral analysis in defense against DoS attacks*," in Proc. IEEE GLOBECOM, 2002.

[5] Cisco Systems, "*Distributed Weighted Random Early Detection*."

[6] "*Official port number defined by IANA (Internet Assigned Numbers Authority)."*

[7] Cisco Systems, "*WRED and MDRR on the Cisco 12000 Series Internet outer with a Mix of Unicast, Multicast, and Voice Traffic Configuration Example*."

[8] D. Clark and W. Fang, "*Explicit allocation of best-effort packet delivery service*," IEEE/ACM Trans. Networking, vol. 6, no. 4, 1998.

[9] M. A. El-Gendy, A. Bose, and K. G. Shin, "*Evolution of the Internet QoS and support for soft real-time applications*," Proc. IEEE, 2003.

[10] T. D. Feng, R. Ballantyne, and L. Trajkovic, "*Implementation of BGP in a network simulator," in Applied Telecommun. Symp.*, 2004.

[11] S. Floyd and K. Fall, "*Promoting the use of end-to-end congestion control in the internet*," IEEE/ACM Trans. Networking, 1999.

[12] M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, "*Reduction of quality (RoQ) attacks on Internet end systems*," in Proc. IEEE INFOCOM, 2005.

[13] C. Hopps, "*Analysis of an equal-cost multi-path algorithm*," RFC 2992 (Informational), Nov. 2000.

[14] A. Kuzmanovic and E. W. Knightly, "*Low-rate TCP-targeted denial of service attacks (The shrew vs. the mice and elephants)*," in Proc. ACM SIGCOMM, 2003.

[15] Y. K. Kwok, R. Tripathi, Y. Chen, and K. Hwang, "*HAWK: halting anomalies with weighted choking to rescue well-behaved TCP sessions from shrew DoS attacks," in International Conf. Computer Netw. Mobile Computing*, 2005.

[16] X. Luo and R. K. C. Chang, "*On a new class of pulsing denial-of-service attacks and the defense*," in Proc. Netw. Distributed Syst. Security Symp., 2005.

[17] R. Mahajan, S. Floyd, and D. Wetherall, "*Controlling high-bandwidth flows at the congested router*," in Proc. International Conf. Netw. Protocols, 2001.

[18] M. Roesch, "*Snort—lightweight intrusion detection for networks*," in Proc. LISA '99: 13th USENIX Conf. Syst. Administration, pp. 229-238, Berkeley, CA, USA, 1999. USENIX Assoc.

[20] M. Rupinder, L. Ioannis, H. S. Jamal, S. Nabil, N. Biswajit, and B. Jozef, "*Empirical study of buffer management scheme for diffserv assured forwarding PHB*," in ICCCN, 2000.

[21] A. Shevtekar, K. Anantharam, and N. Ansari, "*Low rate TCP denialof- service attack detection at edge routers*." IEEE Commun. Lett., Apr.2005.

[22] S. M. Specht and R. B. Lee, "*Distributed denial of service: taxonomies of attacks, tools, and countermeasures*," in Proc. International Conf. Parallel Distributed Computing Syst., 2004.