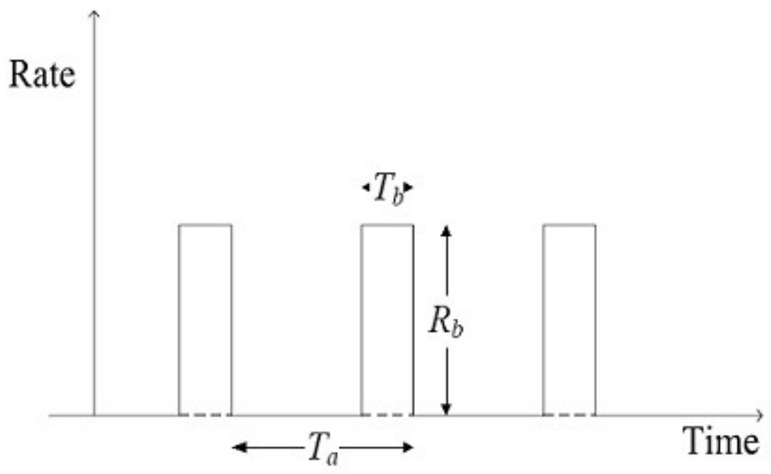
Chống tấn công từ chối dịch vụ tốc độ thấp vào giao thức TCP bằng các cải tiến cơ chế quản lý hàng đợi tích cực

Kiều Minh Việt, Nguyễn Đại Thọ, Nguyễn Thanh Thủy
Trường Đại học Công nghệ, Đại học quốc gia Hà Nội

Giới thiệu

Tấn công từ chối dịch vụ tốc độ thấp vào giao thức TCP (LDoS – xem hình 1) là hình thức tấn công từ chối dịch vụ phân tán (DDoS) mới hiện nay, đã được giới thiệu lần đầu tiên bởi Aleksandar Kuzmanovic và Edward W. Knightly năm 2003 trong bài báo [1]. LDoS khai thác điểm yếu của giao thức TCP đó là sử dụng giá trị thời gian chờ phát lại gói tin nhỏ nhất minRTO là hằng số bằng 1 giây. Chống LDoS trở nên khó khăn hơn so với chống DDoS thông thường vì LDoS gửi gói tin với tốc độ trung bình thấp nên nó tránh được sự phát hiện của các bộ giám sát mạng (chủ yếu phát hiện bất thường dựa trên sự bùng nổ gói tin vào mạng).

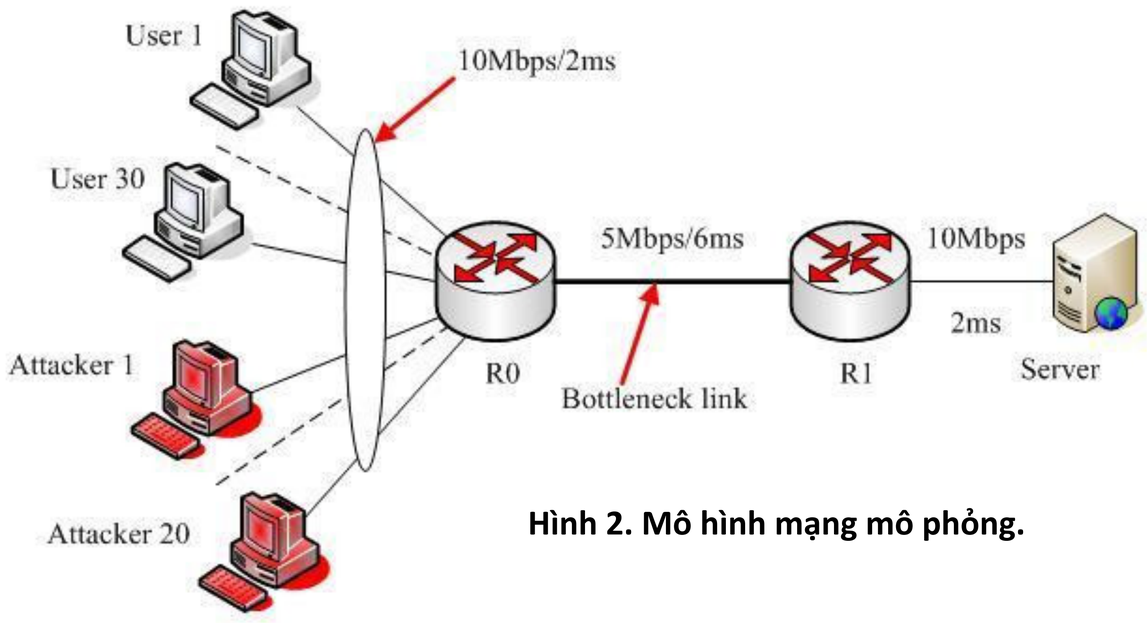


Hình 1. Tấn công LDoS.

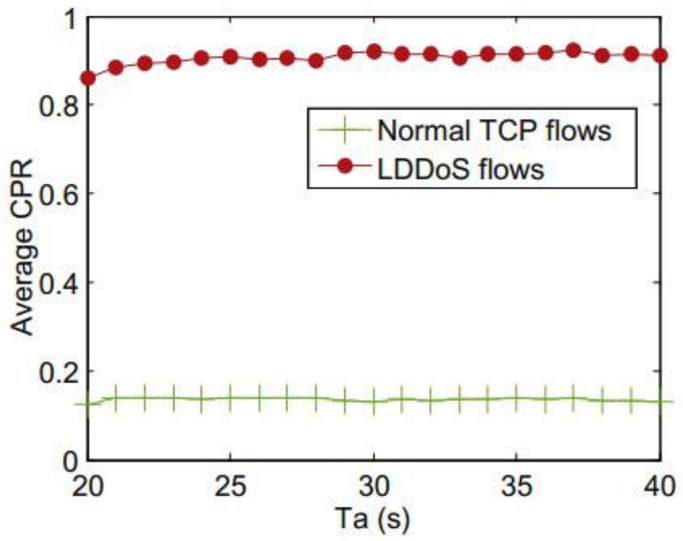
Trong hình 1: Ta là chu kỳ tấn công (Ta ~ minRTO); Tb là khoảng thời gian LDoS phát gói tin tốc độ cao vào mạng (Tb ~ RTT thời gian đi về của gói tin); Rb là tốc độ phát gói tin.

Mục tiêu nghiên cứu và mô hình mạng

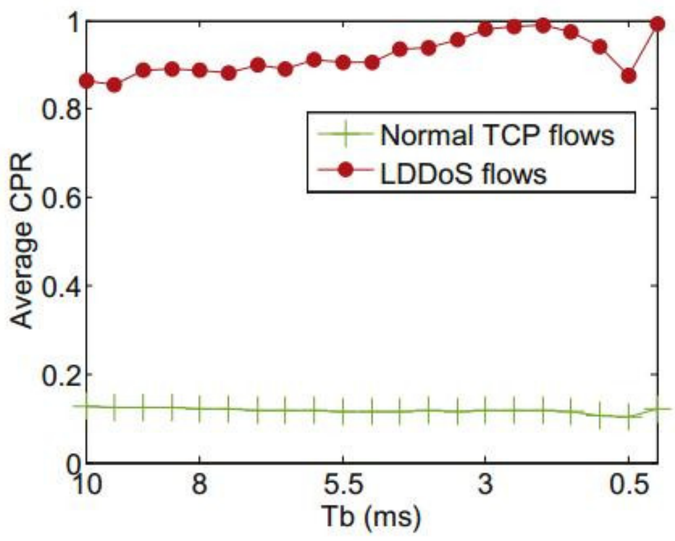
Nghiên cứu đưa ra độ đo mới Congestion Participation Rate (CPR) để phân biệt dòng TCP thông thường và dòng tấn công LDoS, cải tiến thuật toán quản lý hàng đợi RED (Random Early Detection – xem bài báo [2]) để chống LDoS. Mô hình mạng mô phỏng xây dựng bằng phần mềm NS-2 thể hiện ở hình 2.



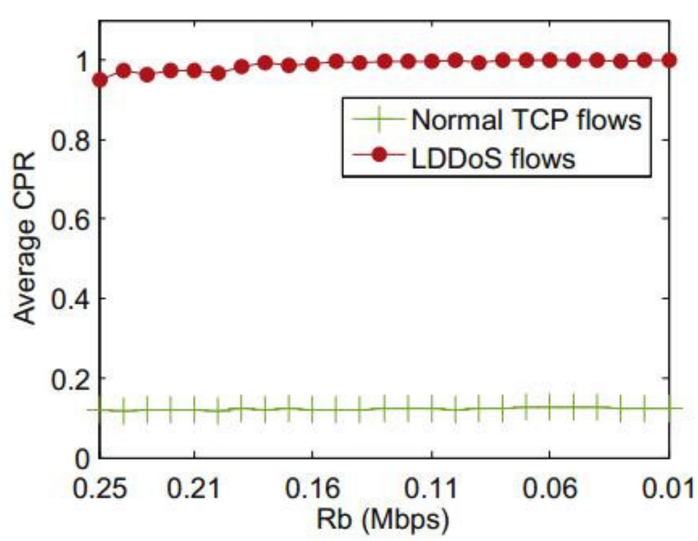
Hình 2. Mô hình mạng mô phỏng.



Hình 3a. Biến thiên Ta trong [20, 40] (s); Tb = 200 ms; Rb = 5 Mbps.



Hình 3b. Biến thiên Tb trong [0.1, 10] (ms); Ta = 1 s; Rb = 5 Mbps.



Hình 3c. Biến thiên Rb trong [0.01, 0.25] (Mbps); Ta = 1 s; Tb = 200 ms.

Kết quả

- CPR trung bình của 30 dòng TCP thông thường nhỏ hơn so với CPR trung bình của 20 dòng tấn công LDoS (xem các hình 3a, 3b, 3c).
- Dựa trên giá trị CPR của từng dòng, thuật toán có thể loại bỏ gói tin của các dòng tấn công LDoS và cho đi qua gói tin của các dòng TCP thông thường.
- Kết quả so sánh hiệu năng của thuật toán với thuật toán quản lý hàng đợi đơn giản DropTail sẽ được đưa ra trong thời gian sắp tới.

Tài liệu tham khảo

[1] Kuzmanovic A., Knightly E.W. (2003), "Low-Rate TCP-Targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephants)", *Proceedings of ACM SIGCOMM.*

[2] Floyd S., Jacobson V. (1993), "Random Early Detection Gateways for Congestion Avoidance", *IEEE/ACM Transactions on Networking, 1 (4), pp. 397-413.*

[3] Changwang Zhang, Zhiping Cai, Weifeng Chen, Xiapu Luo, Jianping Yin (2012), "Flow level detection and filtering of low-rate DDoS".