ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Mitigation of Denial of Service Attack Using Token Bucket Filtering

G. Rakshitha [1], S. Muthukumar [2]

M.E Student (CSE), Sree Sowdambika College of Engineering, Chettikurichi, Aruppukottai, Virudhunagar District, Tamil Nadu ,India [1]

Associate Professor & head of the Department (CSE), Sree Sowdambika College of Engineering, Chettikurichi, Aruppukottai, Virudhunagar District, Tamil Nadu, India [2]

ABSTRACT: Now-a-days, Denial-of-Service (DoS) attacks are identified as the most dangerous threats to the any network because of its resource constrained property. DoS have various types to issue the integrity, availability, and security of any network architecture. There are several processes are presented to remove the DoS attack which are not so effective. Thus, it is necessary to detect and reduce the DoS attack. For that we proposed a system that requires Token Bucket Algorithm (TBA) to eliminate DoS attack. Simulation is performed in NS-2 and the results are demonstrated and compared to existing techniques.

KEYWORDS: Denial-of-Service (DoS), Token Bucket Algorithm, Token.

I. INTRODUCTION

A wireless sensor network (WSN) comprises of thousands of spatially distributed independent devices utilizing sensors to screen physical or environmental conditions. A WSN framework consolidates a gateway node that gives remote link to the wired network and appropriated nodes.

A Denial of Service attack (DoS) is a sort of web oriented attack which looks to disturb the ordinary operation of the focused on computer network. This attack tries to make the resources of computer networks unavailable to its clients. A DOS assault is basically a consolidated push to keep computers from filling in and also they ought to, regularly from a remote area over the web. Various number of accommodated system attacks, so that bringing denial of service for clients of the focused on framework. The surge of incoming messages to the objective framework basically compels it to shut down, in this way refusing service to the framework to authorized clients. The most widely recognized technique for system attacks is to transmit a mass immersion of unending requests for outside communication to the system target. These frameworks are overflowed with requests for data from non-clients, and frequently non-guests to the site.

An effective protective mechanism for DoS attack is primary to distinguish and maintain as fast as possible. In order to accomplish this, researchers require a mysterious comprehension of dynamics of the data packets, traces of network traffic which can portray reasonable information, attributes of the attack traffic, statistics of packet flow, a network platform at where they can run their trials with no complexities. DoS defense assessment can give a huge advancement in the state of the art for DoS defense assessment and a critical step towards a typical assessment strategy. The prompt task of DoS defense is to give tremendous data transfer capacity to authorized clients when there is an attack. Regrettably most recent defense techniques can't effectively recognize and filter out the traffic of the attack. The proposed technique is to find the network anomalies, establish the framework at dispersed routers, recognize the attack packets, and then filter them. Hence the real traffic throughput is enhanced and attack traffic throughput is decreased.

The proposed Token Bucket Algorithm (TBA) can perform well in relieving DoS attack traffic exactly and successfully.

II. RELATED WORKS

There have been proposed numerous techniques for DoS defense attack over past few decades [1-6]. These existing techniques attempt to reduce the communication overhead and increase the security of the system.
Hop-count filtering is a casualty based arrangement depending on the factor that the number of hops between source node and destination is accidentally demonstrated by the TTL field in IP data packets [7, 9, and 15]. Connecting the source IP with the factual number of hops in order to achieve the destination could be utilized as a kind of perspective to survey the legitimacy of the guaranteed IP source. NSD is a type of switch based defense system [8, 11]. All systems on the web are grouped into two sets: neighbors and strangers. The neighbor systems are those whose data packets attain the assigned switch without going through whatever other signing switch.
Alternate networks, those whose data packets attain the assigned switch by other signing switches, are viewed as more odd networks. DefCOM gives added usefulness to existing defense services so they could work together in DDoS recognition and reaction however a progressively assembled overlay [13, 14]. Pushback is a technique for protecting against distributed denial-of-service (DDoS) attacks [12]. DDoS assaults are dealt with as a congestion control issue, but since most types of congestion is brought on by malicious hosts not performing end-to-end congestion control, the issue must be taken care of by the switches. There are some functionalities are contributed to every switch to identify and specially drop data packets that most likely belong to the attacks. The authors in [3] use game theory to propose a progression of optimal puzzle-based strategies for addressing progressively complex flooding attack situations. The result idea of Nash equilibrium is utilized in a as a part of a prescriptive manner, where the protector assumes his part in the result as an ideal protect against judicious attackers. This study finishes in an approach for addressing distributed attacks from an obscure number of sources.

III. PROPOSED TECHNIQUE

In order to obtain the objective of this paper, we have presented a technique named Token bucket Algorithm (TBA) for detection and reduction of denial of services attack. The token bucket is type of algorithm employed in data packet switched computer networks and telecommunications networks. It can be needed to assure that data transmissions, in the form of data packets, suit to fixed boundaries on bandwidth and burstiness (a measure of the unevenness or variations in the traffic flow). The token bucket algorithm can be utilized in either traffic shaping or traffic policing. In traffic policing, nonconforming data packets might be discarded by dropping or may be minimized in priority (for downstream traffic management functions to drop if there is congestion). In traffic shaping, data packets are delayed until they conform. Traffic policing and traffic shaping are usually employed to preserve the network against excess or excessively bursty traffic. We are demonstrating our simulation result with the help of the Network Simulator (NS-2) with various parameters.

3.1. Token Bucket:

- ✓ For congestion control, the Token Bucket Algorithm is applied at network router.
- ✓ Depending on the burst size, the Token Bucket Algorithm varies the output rate.
- ✓ In this algorithm, tokens are held in the buckets and a token is added with a data packet for transmission. When it reaches its destination the host captures the token and destroys it.
- ✓ Tokens are produced by a clock at the rate of one token per sec.
- ✓ In order to send large burst, available host capture and preserve the tokens up to the maximum size of the bucket.

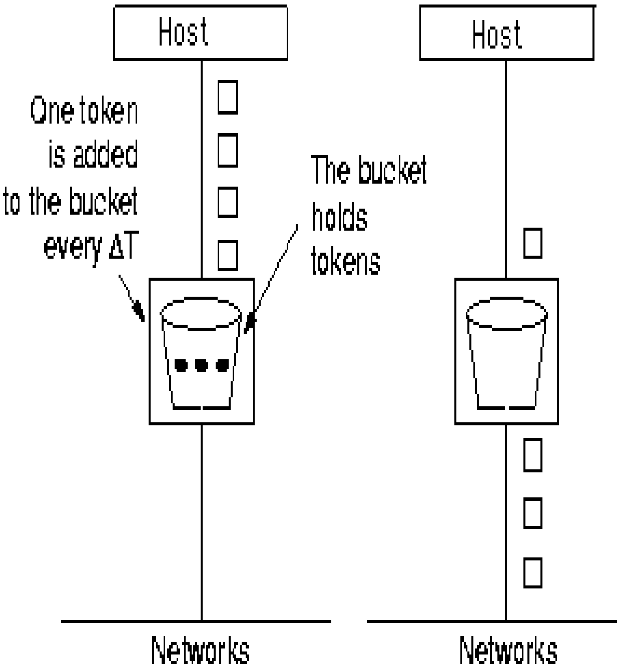

Figure 1: Operation of Token Bucket Algorithm

IV. EXPERIMENTAL RESULTS

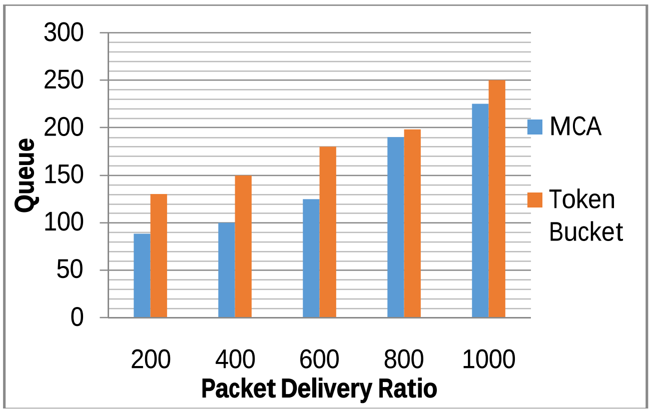

Fig-2 Performance Comparison Between Multivariate Complexity Analysis and Token Bucket Algorithm Parameters of Packet Delivery Ratio vs. Queue

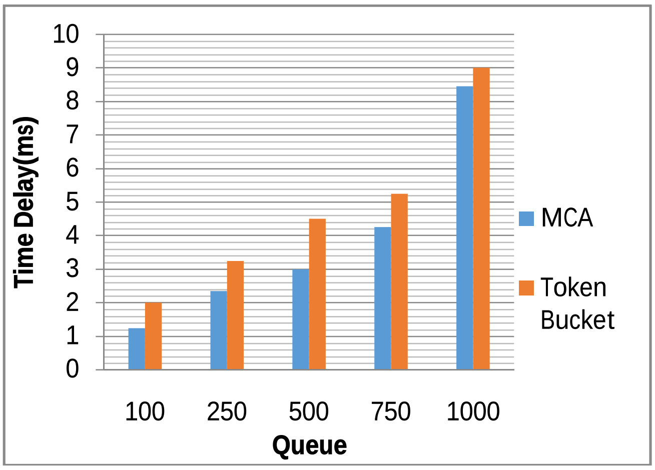

Fig-3 Performance Comparison between Multivariate Complexity Analysis and Token Bucket Algorithm Parameters of Queue and Time Delay in ms

V. CONCLUSION

Thus, we proposed a technique to prevent the network from Denial-of-Service (DoS) using Token Bucket Algorithm (TBA). We also presented architecture for client server to avoid DoS attack. The complete elimination of dos attack is impracticable. This paper will show simulation of different affected parameter under Dos Attack and can become quite significant.

REFERENCES

[1] John Brainard and Ari Juels, “Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks”, Proceedings of the Network and Distributed Systems Security Symposium, February 1999.
[2] Jin, G., Wang, H., and Shin, K. G, “Hop-count filtering: an effective defense against spoofed DDoS traffic”, In Proceedings of the 10th ACM conference on Computer and communication security. Washington D.C., USA, 2003.
[3] Mehran S. Fallah, “A Puzzle-Based Defense Strategy against Flooding Attacks Using Game Theory”, 2006
[4] Boldizs´ar Bencs´ath Istv´an Vajda Levente Butty´an, “A Game Based Analysis of the Client Puzzle Approach to Defend Against DoS Attacks”, July 2003
[5] Antonio Challita, Mona El Hassan, Sabine Maalouf, Adel Zouheiry, “A Survey of DDoSDefense Mechanisms”, 2004.
[6] Ioannidis, J. and Bellovin, S. M., “Implementing pushback: Router-based defense against DDoS attacks”, NDSS Conference Proceedings, 2002.
[7] Tuomas Aura, Pekka Nikander, and Jussipekka Leiwo, “DOS-resistant Authentication with Client Puzzles”, Proceedings of the International Workshop on Security Protocols, April 2000.
[8] “Denial of Service Resistance in Authentication Protocols”, Indo-Australian CIP Project March 23, 2009
[9] John Nagle, "On packet switches with infinite storage" , December 1985.
[10] N. U. Ahmed, Qun Wang, “Systematic approach to model the token bucket algorithm in computer networks”, July 2002
[11] George Oikonomou, Jelena Mirkovic, Peter Reiher, Max Robinson, “A Framework for a Collaborative DDoS Defense” , 2006
[12] Najwa Aaaraj, Sleiman Itani, and Darine Abdelahad, “ Neighbor Stranger Discrimination (NSD) A New Defense Mechanism against DDoS Attacks”, 2004
[13] Jelena Mirkovic, Peter Reiher, “A Taxonomy of DDoS Attack and DDoS Defense mechanisms”, 2004
[14] Jieren Cheng, Jianping Yin, Yun Liu, Zhiping Cai, and Min Li, “DDoS Attack Detection Algorithm Using IP Address Features”, FAW 2009
[15] Tae Hwan Kim, Dong Seong Kim, Sang Min Lee, and Jong Sou Park, “Detecting DDoS Attacks Using Dispersible Traffic Matrix and Weighted Moving Average”, 2009