Detection Techniques against DDoS attacks: A Comprehensive Review

Volume 96 - Number 5

Year of Publication: 2014

Authors:
Shaveta Gupta
Dinesh Grover
Abhinav Bhandari

Abstract

Distributed Denial of Service (DDoS) attacks have also become a problem for users of computer systems connected to the Internet. So defending internet from these attacks has become the need of the hour. There are three solutions against DDoS attacks: Prevention, Detection and Reaction. Detection is one of the key steps in defending against DoS/ DDoS attacks. There are some challenges that has to face while adopting any of the detection technique. If attacks can be detected close to attack sources, attack traffic can be filtered before it wastes any network bandwidth. A good detection technique should have short detection time, low false positive rate, low false negative rate but high normal packet survival ratio. This review paper provides the comparative analysis of various detection techniques with their corresponding advantages and disadvantages.

References

- Stephen Specht, Ruby Lee,"Taxonomies of distributed Denial of Service Networks
Detection Techniques against DDoS attacks: A Comprehensive Review

- Rajesh Kumar, "An Introduction to DDoS – Distributed Denial of Service attack"; March 15, 2011.
- Keunsoo Lee, Juhyun Kim, Ki Hoon Kwon, Younggoo Han, Sehun Kim, "DDoS attack detection method using cluster analysis." Volume 34 Issue 3, April 2008, Pages 1659–1665
- Saman Taghavi Zargar, Member, IEEE, James Joshi, Member, IEEE, and David Tipper, Senior Member, IEEE, "A survey of defense mechanisms against distributed denial of service flooding attacks." IEEE Communications Survey & Tutorials accepted for publication 11 Feb, 2013.

Index Terms

Computer Science
Security
Keywords
- DDoS Attacks
- False positive rate
- Detection Techniques.