Abstract

Now days the Internet is exposed to a span of web threats, So the attack on its infrastructure poses a great challenge in its expansion. In the modern world various types of attacks are discovered on the Internet. IP spoofing is one of the major threats in the network security. Hackers use this to hide their identity or to perform an attack. IP spoofing used for many attacks like denial of service, SYN flooding and man in the middle attacks etc. It is necessary to capture or block the spoofer to defend against these attacks. Different IP trace back mechanisms are used for finding the spoofer's identity. IP trace back scheme is a way used to catch the real path of web packets requiring a longer search so, a new hybrid IP trace back scheme is used with efficient packet logging aiming to have a fixed storage requirement for each router in packet logging without the need to refresh the logged tracking information and to achieve zero false positive and false negative rates in attack-path reconstruction. The hybrid IP trace back scheme compare with other related research in the aspects of storage requirement, computation, and accuracy.
References


Index Terms

Computer Science Networks
Keywords

New hybrid IP trace back, CAIDA’s, distributed denial of service attack, packet logging, packet marking.