可抑制DDoS網路攻擊的方法

夏怡樺,王俊鑫
資訊工程學系
資訊學院
chwang@chu.edu.tw

摘要

分散式阻斷服務攻擊（Distributed Denial of Service, DDoS）中大量封包造成嚴重的網路安全問題，如擁塞頻寬、主機資源耗盡等，許多學者提出防禦的研究方法，利用路由器功能的提昇，達到追蹤攻擊來源的目的，提昇路由器的功能依其成本多寡及必要性有：簡單易提昇的像是可對封包標記（Marking）、透過通隧（Tunneling）將封包轉送到其他路由器，成本較高的如使用過濾器將攻擊封包過濾（Filtering）…等，IP封包追蹤法多藉由路由器容易升級的功能，著重在蒐集必要資訊後重建出攻擊路徑。本篇方法欲採用標記、通隧、過濾等功能的路由器，在網路中及早的過濾掉攻擊封包而減少網路的負擔。我們使用有通隧功能（Tunneling-enabled router）的路由器，將經過封包轉送至過濾器做過濾，藉著標記功能（Marking-enabled router）的路由器協助劃分攻擊區域，互補減低通隧的缺點，使通隧啟動率降低，讓攻擊封包在網路中佔據頻寬的影響降到最低。模擬實驗結果顯示在最差情況下仍然可以減少20%的網路負擔，而在有標記功能路由器的幫助下，更可以減少帶有通隧功能路由器的啟動率達27.5%。

關鍵字：DDoS