私的セキュリティポリシを利用した NGN における DoS 対策の研究

A Study of DoS Attack Measures in NGN Using Private Security Policy

情報セキュリティ大学院大学
西川　康宏

要旨

高速インターネットの普及・発達により，企業・組織・個人によるインターネット利用者が増加している．一方で，悪意を持った利用者による不正アクセスも増加しており，不正アクセスによる脅威とトラヒックの増加が，正常なインターネット利用者の妨げとなっている．また NGN（Next Generation Network）においても，インターネットとの接続により，インターネットからの不正アクセスによる脅威とトラヒックの増加が，正常な NGN 利用者の妨げになると考えられる．そこで，本稿では，私的セキュリティポリシを利用した NGN における DoS 対策方法を提案する．本提案方法では，(1) インターネットから NGN に流入する IP パケットを，NGN 出口側のエッジルータで私的セキュリティポリシを利用した異常 IP パケットの検知を行うこと．(2) NGN 入口側のエッジルータでは，異常 IP パケットに対してマーキングを行い，遅延を取り入れた経路ループ付加を行うことに特徴を有する．また，本提案方法の有効性をネットワークシミュレーションにより検証し，本提案方式の私的セキュリティポリシを利用した DoS 攻撃の抑制手法を用いることで，DoS 攻撃の抑制を行うことができ，本提案方式の有効性を確認した．また，本提案方式を利用することで，正規利用者の通信帯域の確保．DoS 攻撃の影響を受けない通信，正規利用者の通信を DoS 攻撃として誤検知しても，IP パケットを廃棄することなく正常に通信を行うことも確認できた．

Abstract

This paper proposes a method against denial of service (DoS) attacks on the Next Generation Network (NGN). Using a private security policy, IP packets flowing from the Internet into the NGN are checked at the edge routers on the NGN exit-side and abnormal IP packets are detected. Then an attack notification is sent to the edge routers on the NGN entrance-side. After that, the entrance-side edge routers put the IP packets marks to show if the IP packets meet the private policy. If the IP packets don't satisfy the policy, the transmission path delay is added to them by applying feedback routing loop along entrance-side edge routers. The feature of method is adding delay to DoS attack packets, while they are conventionally discarded. By letting the end user decide their normality, it can avoid the loss of normal packets due to misrecognition as attack packets. This loss avoidance of normal packets is useful because DoS attack packets are usually meaningless rather than dangerous. The method also eliminates attack-induced congestion and restores service provision. Finally, the above effectiveness is verified by network simulations.