論 文 内 容 の 要 旨

博士論文題目　　分散型サービス妨害攻撃における攻撃ノード追跡手法に関する研究

氏　　名　　大江　将史

（論文内容の要旨）（1200 字程度）

インターネットにおける脅威の一つである分散型サービス妨害攻撃への被害を最小限にするためには，可能な限り短時間に攻撃パケットが通過した経路を特定し，攻撃ノードの位置を明らかにする技術が必要である．現在は，送信元アドレスが擬装された攻撃パケットの追跡をルータ毎にモニタリング機能などを使用して手作業でおこなっている．このために，攻撃フローと攻撃ノードの特定には時間を要する点が問題となっている．

この問題の解決策として，IP トレースバック技術が提案されている．IP トレースバックは，攻撃フローの真の送信元を特定する技術である．しかしながら，既存の手法は，インターネット全体での同一手法が適用されることを前提としているため，さまざま運用ポリシーを持った組織の集合で成り立っているインターネット上での運用を考慮していない．

そこで，本研究では，さまざまな組織で構成されるインターネット上での運用を前提とした「階層型トレースバック機構」を提案した．本提案手法は，インターネットでの経路制御が，AS (Autonomous System)間と AS 内にわけて EGP (Exterior Gateway Protocol)と IGP (Interior Gateway Protocol)の二つに階層化されている点に着目し，攻撃フローの通過する AS の特定を行う「Exterior IP (eIP) トレースバック機構」と AS 内部において攻撃フローが通過するルータの特定を行う「Interior IP(iIP) トレースバック機構」の 2 つに分離したアーキテクチャとなっている．eIP トレースバックは，攻撃フローの AS を短時間に特定することを目的とする．AS の特定は，フィルタリングなどによる大まかな分散型サービス妨害攻撃への対策を可能とする．また，iIP トレースバックは，AS 内における攻撃ノードの特定を目的とする．攻撃ノードの特定によって，攻撃ノードの分離や遮断等の対策が可能となる．提案手法は，既存の手法では出来なかった実インターネット上での分散型サービス妨害攻撃に対する効果的な対策を実現する．

本研究では，本提案手法の実現可能性を明らかにするために，1.アーキテクチャの定義と必要な技術の特定と評価，2.実インターネットでの提案手法の実現可能性を明らかにするために実装を用いた検証を行った．1.では，実インターネットでの本提案手法を用いた追跡過程とその目標条件を定めた．2.では，実証実験に向けてのプロトタイプ実装についてのアーキテクチャ設計，通信プロトコルの定義，連携に必要な API を定め提案手法の実装を行った．そして，本実装は，50 程度の AS 規模をエミュレートした環境上で十分な追跡性能を有することを確認した．

以上の結果より，本提案手法は，分散型サービス妨害攻撃に対して有効な手法であることが明らかになった．

氏名　　大江　将史

（論文審査結果の要旨）

インターネットの脅威である分散型サービス妨害攻撃は，攻撃者がインターネット上に設置した攻撃ノードから大量のパケットを被害ノードへ送信することによって，被害ノードにおけるWWWやFTPといったインターネット・サービスを妨害する攻撃手法である．この攻撃への対策手法として，本論文では，実インターネットの運用に適合したアーキテクチャを持った階層型IPトレースバック手法の提案と評価をおこない，その有効性を示している．その主な研究成果を以下に示す．

1. 既存研究における共通の問題点として，1．攻撃ノード特定に注力した研究で，被害ノードでの早急な被害緩和についての考慮が十分ではない点，2．インターネットの運用構造を十分考慮していない点を示し，既存研究は，実インターネットでの運用が困難であることを論じている．
2. 既存問題を解決した階層型IPトレースバック手法を提案した．これは，経路制御機構に沿って，AS間トレースバック(eIPトレースバック)とAS内IPトレースバック(iIPトレースバック)の２段階に分けてパケットの経路を特定する手法となっている．eIPトレースバックは，攻撃ノードの存在するASを高速に特定し，iIPトレースバックは，攻撃ノードの存在するAS内で攻撃ノードの位置を特定する．このことから，提案手法は既存研究の持つ問題点を解決している．
3. 提案手法の有効性の検証を行うためにインターネットをエミュレーションした環境下で実験を行っている．エミュレーション環境は，AS規模ランキングの上位50ASの接続を再現や，FreeBSDやZebra-BGP，そして，実在する攻撃ツールなどを利用による実環境を考慮したものとなっており，その環境上での実験結果は，十分な性能を示すものであった．
4. 提案手法の費用対効果やその展開方法，提案手法に対する攻撃への防御手法などの実運用を想定した場合における提案手法の評価について述べ，実インターネットでの運用が十分可能なものになっていることを示すものであった．

以上のことから，本論文は，インターネットの運用機構を十分に考慮した対策手法を提案しその評価，そして有効性を示すことによって，IPトレースバック技術が，分散型サービス妨害攻撃への対策として有効であり，また，その発生の抑止力となる技術であることを明らかにした．したがって，博士（工学）の学位論文として価値のあるものと認める．