氏　名	スバナ　タナセガラン SUBANA THANASEGARAN
学位の種類	博士（工学）
学位記番号	博第821号
学位授与の日付	平成24年3月23日
学位授与の条件	学位規則第４条第１項該当　課程博士
学位論文題目	A Topological Approach to Implement a Conflict Detection System for Time-based Firewall Policies （時間ベースファイアウォールポリシのコンフリクト検出システムの実現へのトポロジカルアプローチ）
論文審査委員	主査　教授　高橋直久 教授　和田幸一 准教授　片山喜章

論文内容の要旨

ファイアウォールはコンピュータセキュリティの防御用のツールの一つである。これは、組織内ネットワークとインターネットの間で出入りするパケットを監視し、決められたルール（フィルタ）に従ってパケットを通過させたり破棄したりする。フィルタの系列（ファイアウォールポリシーという）の設定誤りの一つにフィルタ間の衝突（コンフリクトという）がある。コンフリクトが存在する場合には、決して実行されないフィルタが存在するなど、ファイアウォールポリシーがネットワーク管理者の意志を正しく反映していないことがある。すなわち、セキュリティホールなどの問題が起きる可能性がある。経験豊富な管理者でも多数のコンフリクトを含むファイアウォールポリシーを設定してしまうことがある。

従来，コンフリクト検出法がいくつか提案されているが、これらには次のような問題がある。１）時限付きフィルタを含む時間ベースファイアウォールポリシーのコンフリクト検出に従来手法をそのまま適用すると本来コンフリクトが生じていない場合もコンフリクトが生じていると判定してしまい、管理者の

手間が増えることがある。2）フィルタの数が多くなると計算時間とメモリ量が急激に増大することがある。フィルタの組み合わせにより生じるコンフリクトを検出する場合には、問題が深刻になる。

本研究の目標は、上記問題を解決するコンフリクト検出システムを実現することである。本論文では，このため次の３つの手法を提案し、これらの手法を用いたコンフリクト検出システムの実現法を提示する。①ビットベクタを用いた空間計算法 BISCAL によるコンフリクト検出法。②時間と空間を同時に解析する手法、および、時間を分割して空間的解析を繰り返す手法。③周期的な時間付きフィルタに対する時間に関する効率的なマッピングメカニズム。

第一の研究では，フィルタ間のトポロジーを解析してコンフリクトを検出するため、効率的な空間計算法 BISCAL を提案する。BISCAL はフィルタ集合をビットベクタで表現し、このビットベクタに対する６つの基本演算によりフィルタ間のトポロジーを求める計算法である。BISCAL を使うことで複数のフィルタの組み合わせによる生じるコンフリクトを効率的に検出することができる。本研究では、また、数学的解析と実験的解析により提案システムの有効性を評価する。

第二の研究では、時間ベースファイアウォールポリシーに対して，時間と空間を同時に解析するコンフリクト検出手法を提案する。また、時間軸に関しても空間的解析と同様の手法で時間を分割して，各時間帯ごとに空間的解析を繰り返す手法を開発する。さらに，両者を比較評価する。

第三の研究では、周期的な時限付きフィルタに対して効率的にコンフリクトを検出するために、時間のマッピングメカニズムを提案する。マッピングメカニズムを用いたコンフリクト検出システムは、周期的なフィルタにより生じる繰り返し計算を削除するため、より広範な時間ベースファイアウォールポリシーに適用可能である。

上記３つの研究により、時間ベースファイアウォールポリシーに対して複数のフィルタの組み合わせにより生じるコンフリクトを効率よく検出するシステムの実現法が明らかになり、このようなシステムがネットワーク管理者の負担を軽減するうえでの有効性と問題点が明らかになると期待できる。

論文審査結果の要旨

ファイアウォールはコンピュータセキュリティの防御用のツールの一つである。これは、組織内ネットワークとインターネットの間で出入りするパケットを監視し、決められたルール（フィルタ）に従ってパケットを通過させたり破棄したりする。フィルタの系列（ファイアウォールポリシーという）の設定誤りの一つにフィルタ間の衝突（コンフリクトという）がある。コンフリクトが存在する場合には、決して実行されないフィルタが存在するなど、セキュリティポリシーがネットワーク管理者の意志を正しく反映していないことがある。すなわち、セキュリティホールなどの問題が起きる可能性がある。経験豊富な管理者でも多数のコンフリクトを含むファイアウォールポリシーを設定してしまうことがある。

従来、コンフリクト検出法がいくつか提案されているが、これらには次のような問題がある。1）時限付きフィルタを含む時間ベースファイアウォールポリシーのコンフリクト検出に従来手法をそのまま適用すると本来コンフリクトが生じていない場合もコンフリクトが生じていると判定してしまい、管理者の手間が増えることがある。2）フィルタの数が多くなると計算時間とメモリ量が急激に増大することがある。

本論文では、これらの問題を解決するため、次の３つの手法を提案し、これらの手法を用いたコンフリクト検出システムの実現法を提示している。①ビットベクタを用いた空間計算法 BISCAL によるコンフリクト検出法。②時間と空間を同時に解析する手法、および、時間を分割して空間的解析を繰り返す手法。③周期的な時間付きフィルタに対する時間に関する効率的なマッピングメカニズム。

第一の研究では、フィルタ間のトポロジーを解析してコンフリクトを検出するため、効率的な空間計算法 BISCAL を提案している。BISCAL はフィルタ集合をビットベクタで表現し、このビットベクタに対する６つの基本演算によりフィルタ間のトポロジーを求める計算法である。BISCAL を使うことで複数のフィルタの組み合わせによる生じるコンフリクトを効率的に検出することができる。本研究では、また、数学的解析と実験的解析により提案システムの有効性を評価している。

第二の研究では、時間ベースファイアウォールポリシーに対して、時間と空間を同時に解析するコンフリクト検出手法を提案している。また、時間軸に関しても空間的解析と同様の手法で時間を分割して、各時間帯ごとに空間的解析を繰り返す手法を示している。さらに、両者を比較評価している。

第三の研究では、周期的な時限付きフィルタに対して効率的にコンフリクトを検出するために、時間のマッピングメカニズムを提案している。マッピングメカニズムを用いたコンフリクト検出システムは、周期的なフィルタにより生じる繰り返し計算を削除するため、より広範な時間ベースファイアウォールポリシーに適用可能である。

上記３つの研究により、時間ベースファイアウォールポリシーに対して複数のフィルタの組み合わせにより生じるコンフリクトを効率よく検出するシステムの実現法が明らかになり、このようなシステムがネットワーク管理者の負担を軽減するうえでの有効性と問題点が明らかになると期待できる。

なお、本論文の内容について、３編の論文が国際会議で発表され、２編の論文が学術論文誌へ掲載されている。これらの成果は、平成 21 年度電子情報通信学会の通信ソサイエティ・インターネットアーキテクチャー研究会学生奨励受賞、平成 22 年度情報処理学会東海支部学生論文奨励賞、及び、平成 23 年度堀情報科学振興財団研究助成を受賞するなど関連学会でも高く評価されている。本論文は、今後益々重要となる安心安全なインターネットの実現技術への寄与が大きいことから、本学課程博士の博士（工学）の論文として、十分その価値を有するものと認める。