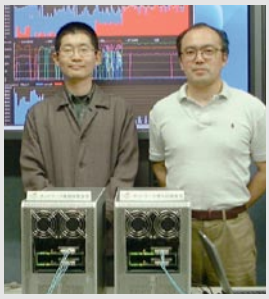
大規模ネットワークの防御システムを実現

侵入検知ルールの変更に素早く対応、100ギガbpsにも拡張可能



戸田 賢二
とだ けんじ（右）
k-toda@aist.go.jp
情報技術研究部門
兼 男女共同参画室 室長代理
（つくばセンター）

産総研入所以来、並列計算機やネットワークのアーキテクチャ研究に従事しています。現在は、高性能実時間組込システムの研究開発を中心テーマとしており、ハードウェアによるセキュリティシステム、高性能画像処理装置などの応用研究を展開中です。

片下 敏宏
かたした としひろ（左）
t-katashita@aist.go.jp
情報技術研究部門 特別研究員
（つくばセンター）

2006年筑波大学大学院システム情報工学研究科卒業、博士（工学）。ネットワークセキュリティシステムを中心に、アプリケーション重視の組み込み機器応用を研究テーマとしています。主としてシステム設計、回路設計、FPGAデバイスに関する研究に従事しています。

関連情報：

- 情報技術研究部門実時間組込システム研究班
  http://unit.aist.go.jp/itri/attacker_brief/rtes-index.html
- 共同研究者
  山口喜教、前田敦司（筑波大学）
- プレス発表
  2007年2月20日「サイバー攻撃から大規模ネットワークを防御するシステムの実現」
- 模擬試験装置は、経済産業省の地域新生コンソーシアム研究開発事業による研究「パターンマッチング回路の超高速化とフィルタリング装置への応用」（H16～H17年度）の研究成果を発展させたものです。

サイバー攻撃への対処

プロバイダをはじめ企業や学校などの組織ネットワークへのサイバー攻撃は、サービス不能やホームページの改ざん、情報漏洩など甚大な被害をもたらします。その被害を抑えることが、組織の信用を高めるだけでなく、利用者を被害から守るという点からも重要です。

サイバー攻撃を検知するシステムとしては、シグネチャ方式の「Snort」と呼ばれるシステムが知られています。しかし、Snortで、組織の基幹ネットワークに利用される10ギガビットイーサネットの通信データを漏れなく検査することは困難でした。

ネットワーク侵入防御装置の開発

シグネチャ方式では、既知の侵入・攻撃のデータベース（検知ルール）中の文字列と通信データをひとつひとつ照合するパターンマッチング処理で検査を行います。私たちは、この照合を高速化するハードウェアを開発しました。すなわち、非決定性オートマンによって複数の照合を並行して行わせて高速化し、回路の共有で大幅にコンパクト化したのです。このことにより、1225種類の侵入・攻撃に対応して、10ギガビットイーサネットの通信データを漏れなく検査する侵入防御装置の開発に成功しました。

この装置には、FPGAという論理回路が書き換え可能なLSIを用い、さらにルールをもとに回路を生成するプログラムも開発しました。この出力をFGPAに書き込むことで、検知ルールの変更や追加にもすばやく対応できます。また、検出した侵入・攻撃やネットワーク速度の情報をリアルタイムに通知するほか、明らかな侵入や攻撃である通信データは除去することもできます（図1）。

ネットワーク模擬攻撃装置も開発

開発した防御装置は、10ギガbpsという非常に高い処理性能を持つため、これを試験する装置がなく、デバッグや詳細な性能評価が困難でした。そこで、10ギガビットイーサネットの回線速度で攻撃用の通信データを生成・送出するネットワーク模擬攻撃装置を開発しました。

この装置は、通信データの送出と同時に試験対象からの出力を監視して、通信データの中から攻撃データだけが検出・除去され、通常のデータは通過していることを検証する機能をもっています。

10ギガbpsの速度を実現するため、ネットワーク物理層チップをハードウェアで直接制御する機能をもたせ、独自に開発したハッシュテーブル方式による通信データの検証機能を搭載しました。ハッシュテーブルを用いることで、ハードウェアの削減と通信データ記録の高速化を達成しています。

模擬攻撃装置を用いて10ギガビットイーサネットの回線速度で実験した結果、防御装置はすべての攻撃を正しく遮断し、無害な通信データだけを通過させました。これによって私たちが開発した検知ハードウェアの処理速度と機能を実証できました（図2）。このシステムは100ギガbpsの処理速度にも拡張が可能です。

今後の予定

これらの装置は、小型で低消費電力（50W程度）ですので、大規模ネットワークのセキュリティを向上させ、安心安全なIT社会の実現に大きく寄与することが期待できます。

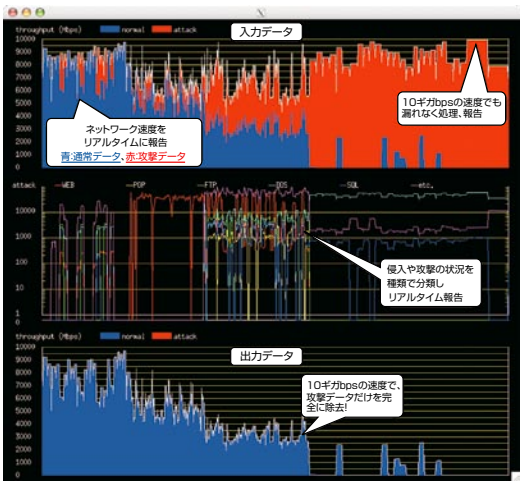


図1　侵入防御装置で検出されたサイバー攻撃の通知画面

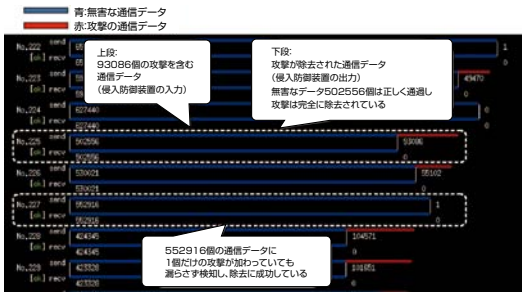


図2　模擬攻撃装置による侵入防御装置のテスト結果