2010年7月1日
株式会社日立製作所

10ギガビット/秒のブロードバンド上でP2P型ファイル共有ソフトのトラヒックを検知するソフトウェアを開発

情報漏えいなどに対するネットワークセキュリティの向上に貢献

株式会社日立製作所(執行役社長:中西 宏明／以下、日立)は、このたび、10ギガビット／秒のブロードバンド上で、Winny、Winnyp、PerfectDarkなど7種類のP2P(Peer to Peer)[*1]型ファイル共有ソフト(以下、P2Pソフト)のトラヒックを、平均99.78%の高精度で検知するソフトウェアを開発しました。

本ソフトウェアは、これまで検知できなかったブロードバンド上に占めるP2Pソフトのトラヒック[*2]が把握できるため、悪質なウイルスによる情報漏えいやデータの違法公開など、ネットワークセキュリティ上の問題を解決するキーテクノロジーとしての貢献が期待されます。

近年、新たな通信ネットワークの方式としてP2Pソフト通信技術が大きな期待を集めています。P2Pは利用者間を直接つないで音声や画像ファイルなどを交換できるため、その利便性が評価される一方、悪質なウイルスによる情報漏えいが大きな社会問題になるなど、セキュリティ対策が課題となっていました。P2Pソフトは、トラヒックを隠ぺいするために暗号化されている場合が多く、従来の侵入検知システム(IDS)[*3]で主に採用されているパターンマッチング(平文比較)[*4]方式では、そのトラヒックの有無を特定することが困難でした。

さらに、検知可能な帯域幅と検知精度は、トレードオフの関係にあるため、通信パケット[*5]の復号処理など、解析に多くの処理を要するP2Pソフトのトラヒックは、ブロードバンド上での検知が課題とされてきました。

このような背景から、日立は、ブロードバンド上で、Winny、Winnyp、PerfectDarkなど、国内における利用者の90%以上をカバーする[*6]7種類のP2Pソフトのトラヒックを平均99.78%の高精度で検知するソフトウェアを開発しました。開発した技術の概要は以下の通りです。

(1) ファースト・パケット・パスフィルタ技術

P2Pソフトによるトラヒックの多くは、TCP(Transmission Control Protocol)[*7]コネクションにおける最初の1パケットに検知すべき特徴を含んでいます。この特徴に着目し、ブロードバンド上でリアルタイムにP2Pソフトのトラヒックを検知するにあたり、すべてのパケットを検査するのではなく、最初の1パケットを抽出する「ファースト・パケット・パスフィルタ技術」を開発しました。これにより、ブロードバンド上におけるP2Pソフトのトラヒックが効率よく検知できるようになりました。

(2) 高精度検知技術

検知精度向上のため、P2Pソフトのトラヒックを高精度に検知するディープ・パケット・インスペクション(以下、DPI)[*8]方式を採用した、高精度検知技術を開発しました。また、暗号化されたトラヒックを、暗号モジュールにより確実に検知します。さらに検知処理手順を、複雑なプログラミングを用いずに、テキスト形式のスクリプトとして実行することで、7種類のP2Pソフトを1つのソフトで検知し、新たなP2Pソフトの検知にも柔軟に対応します。

開発したソフトウェアの実証実験を、独立行政法人情報 通信研究機構(NICT)北陸リサーチセンターの運用するインターネットシミュレータ「StarBED」において行いました。実験では 12 コアのアプリケーションプロセッサを備えた装置に、本ソフトウェアを実装し、ブロードバンド上で 7 種類の P2P ソフトのトラヒックを平均 99.78%の高精度で検知することを確認しました。

今後は、P2P の検知から制御まで、一貫した対策ができるソフトウェアの実用化を目指し、ネットワークセキュリティの向上に貢献していきます。

なお、本ソフトウェアは、総務省委託研究「ネットワークを通じた情報流出の検知及び漏出情報の自動流通停止のための技術開発」(2007 年度から 2009 年度)の成果です。

■用語

*1 P2P(Peer to Peer):ネットワーク上で端末間を直接接続し、データを送受信する方式。

*2 トラヒック:通信網を通過する情報の流れのこと。

*3 侵入検知システム(IDS: Intrusion Detection System): ネットワークを流れる通信データを監視して、不正行為を検知・通知するシステム。

*4 パターンマッチング(平文比較): 予め定義されたパターンが、検査対象データに含まれているか否かを判定する方式。

*5 パケット: コンピュータがネットワークを通じて相互に通信するための伝送単位。

*6 社団法人コンピュータソフトウェア著作権協会「ファイル共有ソフトの利用に関する調査(2009 年)」の結果より算出。
7 種類の P2P ソフト(Winny、Winnyp、Perfect Dark、Bit torrent、LimeWire、WinMX、Share)

*7 TCP(Transmission Control Protocol):インターネットやイントラネットで標準的に使われる通信プロトコル(手順)。

*8 DPI(ディープ・パケット・インスペクション):パケットの内容を解析して検査を行う方式。

■照会先

株式会社日立製作所 システム開発研究所 企画室 [担当:塚越]
〒215-0013 神奈川県川崎市麻生区王禅寺 1099 番地
電話 044-959-0325(直通)