

IoT を支える知的ネットワークセキュリティ技術

情報科学研究科
情報工学専攻

教授 永山 忍 NAGAYAMA, Shinobu

教員情報



キーワード ネットワークセキュリティ、FPGA 実装、設計自動化、機械学習による不正侵入検知

研究シーズの概要

インターネットに繋がるモノが増えるほど、ハッキングや個人情報漏洩などの危険が高まり、セキュリティ対策が不可欠になります。しかし、対策をすればするほど、利便性が損なわれ、反対に利便性を重視すると安全性が損なわれることがあります。本研究では、安全性と利便性の両立を目指し、様々な観点で研究を行っております。特に近年では、ネットワークから危機への不正アクセスを機械学習により検知する方法およびそのハードウェア実装について研究しております。

研究シーズの詳細

◆研究例◆

ネットワーク上の不正アクセスは、過去の不正アクセスパターンを分析・ルール化することにより、検出でき、ゲートウェイで通信を事前にチェックすることで、水際で不正アクセスを検知できます。ルール化された不正アクセスパターンは、正規言語で表現されていることが多く、チェックには正規表現マッチングが行われます。

このチェックは正常な通信に対しても行われるので、このチェックに時間を要するとゲートウェイで通信が滞ってしまいます。そのため、安全性と利便性の両立のために専用ハードウェアによる高速化が必要になります。また不正アクセスのパターンは次々出現しますので、新たなパターンでハードウェアを更新できるプログラマブルな構成も必要になります。

これまでに、決定グラフや特殊なオートマトンを用いた設計法を提案し、新たなパターンに対する柔軟性と高速性を兼ね備えたハードウェアの設計に成功しています。

ルールベースの不正アクセス検知手法は、ルール化された不正アクセスについては確実に検知できますが、ルール化されていない新しいタイプの不正アクセスを検知できない点やルール化自体が難しい点などの欠点があります。

そこで、機械学習により明確なルールを用いずに検知する手法が使われています。様々な機械学習の中でランダムフォレストが、その単純性と検知精度の高さから注目を集めており、本研究でもランダムフォレストを用いたシステムの開発を行っております。

ランダムフォレストは、複数の決定木から構成されており、複数の決定木を使って様々な観点で通信を調べることにより不正アクセスを検知しています。そのため、入念にチェックすればするほど、決定木の数が増え、計算量が大きくなります。ハードウェア化することで、各決定木で並列にチェックができるので、高速なチェックが可能になります。

応用例・セールスポイント

近年、スマートハウス、スマートメーター、自動車など様々なものがネットに繋がりはじめていますが、こういった小物はセキュリティ対策が軽視されがちです。しかし、小さな情報がパズルのように合わさると大きな情報漏洩に繋がる恐れがあり危険です。コストやユーザの手間を最小限に抑えつつ安全対策を目指す様々な応用分野に研究成果を適用可能です。

本研究は、他大学や企業と共同で行っているテーマもあり、共同研究の実績があります。基礎研究の性質上、汎用性の高い成果が多く、様々な応用分野にカスタマイズでき、適用可能です。ネットワークセキュリティに限らず、「処理の高速化」、「設計手順の単純化」、「機械学習の応用」などについて興味のある場合にも、研究成果を適用可能だと考えております。

【問い合わせ先】 広島市立大学 地域共創センター 〒731-3194 広島市安佐南区大塚東 3-4-1 (情報科学部棟別館 1F)
TEL:082-830-1764 / FAX:082-830-1555 / E-mail:ken-san@m.hiroshima-cu.ac.jp