(1139-4)

【AI・ロボット技術分野】

仮訳

ロボットへの悪意ある攻撃を停止させる新しいサイバーアルゴリズム
（オーストラリア）

2023 年 10 月 12 日

オーストラリアの研究者らが、無人の軍事ロボットに対する中間者攻撃（MitM）を数秒で停止させるアルゴリズムを開発した。

チャールズ・スタート大学と南オーストラリア大学（UniSA）の人工知能（AI）専門家が、ディープラーニング（深層学習）ニューラルネットワークを使って人間の脳の振る舞いをシミュレートする実験において、ロボットのオペレーティングシステム(ROS)を訓練し、MitM による盗聴サイバー攻撃の特徴を学習させた。攻撃者は、ROS で進行中の通信、つまりデータの転送の中断を狙い撃ちする。

UniSA と チャールズ・スタート大学の AI 研究者らが.実験で使用した GVR-BOT

米軍の戦闘用地上車両のレプリカを用いてリアルタイムに試験したアルゴリズムでは、悪意のある攻撃を 99%防御することに成功。2%を下回る偽陽性率により、同システムの有効性を確立し、その効果を実証した。

本研究の結果は、IEEE Transactions on Dependable and Secure Computing にて発表されている。

UniSA の自律システム研究者である Anthony Finn 教授によると、このアルゴリズムは、サイバー攻撃の検出に世界中で使用されている他の認識技術よりも優れているという。

Charles Sturt Artificial Intelligence and Cyber Futures Institute の Finn 教授と Fendy Santoso 博士は、米国陸軍フューチャーコマンド(AFC)との協力で、GVR-BOT 地上車両に対する MitM 攻撃を再現し、攻撃を認識するように ROS を訓練した。

「ロボットオペレーティングシステム (ROS) は非常に高度にネットワーク化されているため、データ侵害や電子ハイジャックの影響を大変受けやすいのです」 と Finn 教授は説明する。

「ロボット工学、オートメーション、モノのインターネット (IoT) の革新を特徴とするインダストリー4.0 の到来により、協働するロボットの必要性が高まっています。それには、センサー、アクチュエーター、コントローラーが、クラウドサービスを介して相互に通信し、情報を交換する必要があるのですが、ここでの欠点はサイバー攻撃に対して非常に脆弱であることです」。

「しかし、幸いなことに、コンピューティングの速度が数年毎に倍増し、デジタル攻撃からシステムを守るための高度な AI アルゴリズムを開発して実装することが可能になっているのです」。

Santoso 博士によると、その大きな利点と広範な利用にもかかわらず、暗号化されたネットワークトラフィックデータと、システムの完全性チェック機能の制限のために、ROS はそのコーディングスキームにおいてセキュリティの問題をほとんど無視しているという。

「ディープラーニングのおかげで、私たちの侵入検知フレームワークは堅牢で高精度なものになっています」と Santoso 博士は言う。「このシステムは、ROS のような大規模かつリアルタイムのデータ駆動システムを保護するのに最適な、大規模なデータセットを扱うことができるのです」。

Finn 教授と Santoso 博士は、地上ロボットよりも高速で複雑なダイナミクスを持つドローンを含む様々なロボティックプラットフォームにおいて、この侵入検知アルゴリズムの試験実施を計画している。

10 月は、サイバーセキュリティー意識向上月間である。

Statista によると、2023 年にロボット市場は 370 億米ドルに達すると予測されている。サービスロボットは市場の大半を占めており、軍用、民間用、農業用、産業用、捜索救助や医療分野等の他のロボットの使用は世界中で増加している。

訳：NEDO（担当　技術戦略研究センター）

出典：本資料は、オーストラリア連邦・南オーストラリア大学(UniSA)の記事“New cyber algorithm shuts down malicious robotic attack ”(https://www.unisa.edu.au/media-centre/Releases/2023/new-cyber-algorithm-shuts-down-malicious-robotic-attack/) を翻訳したものである。
(Reprinted with permission of University of South Australia (UniSA))