国立大学法人
電気通信大学
Unique & Exciting Campus

平成 30 年 11 月 30 日

報道各社御中

国立大学法人電気通信大学

制御アルゴリズムを暗号文だけで構成（秘匿化）できる技術を世界に先駆けて開発

制御信号やパラメータ改ざんなど高度化するサイバー攻撃への防御を有効かつ安価に実現できることに

この度、本学 小木曽 公尚 准教授（大学院情報理工学研究科）が、新たな暗号化制御技術に関する研究成果を 12 月、米国で開催される国際学会で発表することになりました。

ポイント

1. 小木曽准教授は、無線を使った自動制御システムの心臓部である**制御アルゴリズムを暗号文だけで構成（秘匿化）できる技術を世界に先駆けて開発**しました。

2. 本技術によって、制御信号やパラメータ改ざんなどのサイバー攻撃の検知が容易になり**高度化するサイバー攻撃への防御を自動車はじめ各分野の産業界が有効かつ安価に実現**できます。

3. 本技術は、2018 年 12 月 17 日～19 日に米国フロリダ州マイアミで開催される国際学会 **The 57th IEEE Conference on Decision and Control** で発表します。

【Who】

小木曽 公尚 （こぎそ・きみなお） 博士（工学）
電気通信大学大学院 情報理工学研究科 機械知能システム学専攻 准教授
（ http://kjk.office.uec.ac.jp/Profiles/67/0006602/profile.html ）

【What】

IEEE Control Systems Society が主催する旗艦会議で発表します。

会議名：

The 57th IEEE Conference on Decision and Control*

＊システムと制御の理論・応用の発展を目的に、1962 年から続く IEEE Control Systems Society のフラッグシップカンファレンスです。
https://cdc2018.ieeecss.org

発表題目：

「暗号化制御システムのための動的鍵管理方式によるサイバー攻撃予防および検知法」
（Attack Detection and Prevention for Encrypted Control Systems by Application of Switching-Key Management）
https://css.paperplaza.net/conferences/conferences/CDC18/program/CDC18_ContentListWeb_3.html#wea03_06

【Whom】 発表内容の対象者

学術:

学会員（研究者と企業や研究所等に所属する専門家）

産業:

セキュリティに切迫した解決策を求めている国内外の企業。適用先としては、車載制御システム、ドローンなどがあります。このほか、電気・上下水・石油・ガス・化学・医薬品・組立製造業界で利用される産業制御システムなどが対象になります。

【Why】 背景

インターネット社会でサイバー攻撃に対する有効な防御技術の開発は喫緊の課題です。特に、サイバー空間と物理空間をまたぐ制御システムでは、悪意のある情報操作が電子機器やロボットを介して物理的な影響を与えることができます。これまでに、通信路での秘匿化技術は、情報通信分野において非常に活発に研究開発が進んでいます。しかし、制御アルゴリズムや通信路まで含んだ制御システム全体を秘匿化対象とする研究は数少ないのが実情でした。

【How】

暗号化制御技術の特徴:

暗号化制御とは、制御アルゴリズムを秘密計算で実現した制御技術のことで、小木曽准教授らの研究グループが世界に先駆けて発表した制御システムの秘匿化技法です。

この秘密計算では、公開鍵暗号の乗法準同型性を利用しており、制御プログラム（制御器）内の信号情報及びパラメータを暗号化したまま処理できるようになります。さらに、制御器内部は暗号文の情報しかありませんので、不正アクセスによる信号やパラメータへの改ざん攻撃に対してリアルタイムで検知ができるようになります。

暗号化制御は、産業界で広く使われている PID 制御やオブザーバなどの制御アルゴリズムを暗号化実装することができますので、広範な制御アルゴリズムに適用することができます。また、既存の暗号化通信技術（セキュアな通信プロトコル）との併用も可能です。

既存の技術との違い:

制御アルゴリズムに秘密計算を応用し、制御信号及びパラメータを暗号化させた実装方法は今回が初めてです。通信路上の信号を秘匿化する暗号化通信技術は、すでに数多く報告されています。しかし、この従来技術では秘密鍵を制御器内部に置く必要があるため、制御システムが脆弱となる弱点がありました。

今後:

技術の普及と標準化を促進するために電気通信大学発ベンチャー企業を立ち上げる予定。それに先がけ、2018 年 9 月、準備チームを結成し、本学インキュベーション施設に入居しました。

【問合せ先】

研究に関して:

電気通信大学大学院 情報理工学研究科 機械知能システム学専攻

准教授 小木曽 公尚 kogiso@uec.ac.jp

報道に関して:

電気通信大学総務課広報室広報係

電話:042-443-5019 FAX:042-443-5887

E-mail: kouhou-k@office.uec.ac.jp