ニュースリリース

令和４年７月２６日

報道機関　各位

国立大学法人　電気通信大学

暗号化制御システムの最適な設計法を提案

【ポイント】

＊暗号化制御システムのセキュリティ指標を提案した
＊セキュリティと制御性能の関係を明らかにすることに成功
＊最適な鍵長と制御器の設計法を考案
＊制御理論と暗号理論の分野を融合した初の成果

【概要】

電気通信大学大学院情報理工学研究科博士後期課程２年の寺西郁氏（日本学術振興会特別研究員）、定本知徳助教、小木曽公尚准教授らの研究グループは、制御系を設計する制御理論に暗号理論のセキュリティ概念を導入した「暗号化制御システム[1]」の最適な設計法を提案しました。このような融合研究は制御理論分野では初めてであり、また暗号理論分野からみても制御理論に応用した初の成果となります。

暗号化制御は準同型暗号[2]を用いて制御システムの動作を秘匿化する次世代制御技術です。研究グループは今回、暗号化制御システムに用いる暗号の鍵長[3]と制御器の最適な設計法を提案しました。まず、暗号化制御システムのセキュリティを評価する指標を開発し、さらに暗号化制御システムのセキュリティと鍵長・制御性能との関係を明らかにしました。その上で開発した指標に基づき、最適な鍵長と制御器の設計アルゴリズムを提案しました。

この成果により、既存の制御システムの制御性能を損なうことなく暗号化制御アルゴリズムを導入し、システムのセキュリティを向上できるようになると期待されます。

本研究の成果は制御理論分野のトップジャーナル「IEEE Transactions on Automatic Control」に掲載されました。

【背景】

物理層と計算層を連携させたサイバーフィジカルシステムは、コストの削減や効率の向上に寄与し、システムの信頼性や持続可能性を飛躍的に改善すると見込まれることから、電力網や輸送、製造、ヘルスケアなどさまざまな分野で注目されています。

一方、その利点と引き換えに、サイバーフィジカルシステムはしばしばセキュリティの脅威に直面します。主要なセキュリティ脅威の一つは盗聴攻撃です。盗聴攻撃はシステムの機密情報を不正に開示しようとする攻撃であり、攻撃者は取得した機密情報を元に効果的にシステムに悪影響を及ぼします。

この盗聴攻撃への対策の一つに暗号を用いる方法があります。暗号化制御は、準同型暗号を用いて制御器のパラメータとネットワーク上の信号を暗号化し、制御システムの動作を秘匿化したまま運用する次世代制御技術です。暗号化制御を用いることで、サイバーフィジカルシステムのセキュリティを向上させることができると期待されています。

しかしながら、これまで暗号理論と制御理論には、盗聴などの攻撃から保護しながら、望ましい制御性能を満たすサイバーフィジカルシステムを構築する体系的な方法論はありませんでした。従来の研究では、暗号システムを制御システムに導入した事例はありましたが、暗号の鍵長をどの程度の大きさにすれば、所望の期間制御システムを守れるのかは明らかにされていません。したがって、暗号化制御システムにおいて暗号の鍵長と制御器の設計方法は体系化されていないのが現状です。そこで本研究では、この困難な問題に取り組み、特定の期間において制御システムを保護するための最適な鍵長と制御器の設計手法を提案することを目指しました。

【手法】

最初に、暗号化制御のフレームワークにおいて、サンプル同定複雑度とサンプル解読時間と呼ばれる二つの新しい概念を提案しました。前者は制御システムの同定精度とデータ数の関係を明示的に示し、後者は暗号の鍵長とシステム同定に用いるデータの解読時間の関係を示します。これら二つの扱いやすい新しい概念に基づき、制御システムを特定の寿命内、かつ特定の精度においてシステム同定を防ぐための最適な鍵長と、制御パフォーマンスを最大化するための最適な制御器の両方を設計する体系的な方法を提案しました。

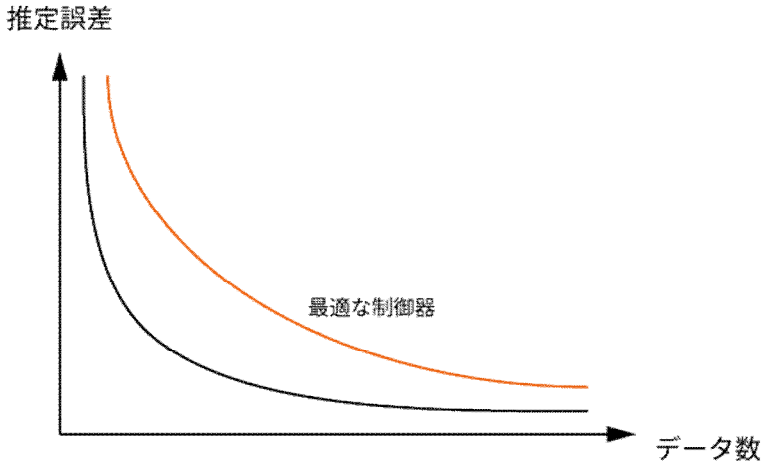

図１　サンプル同定複雑度

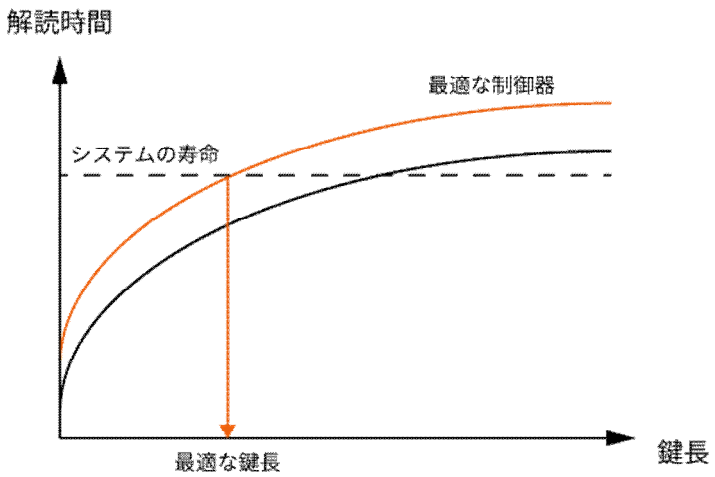

図２　サンプル解読時間

【成果】

暗号化制御システムの最適な鍵長と制御器の設計法を提案しました。スーパーコンピュータ「富岳」と同程度の計算能力をもつ攻撃者から５０年間システムを保護するという設定の下、数値例によりその有効性を確認しました。提案アルゴリズムと動的鍵準同型暗号を組み合わせることにより、従来の暗号化制御システムと比べて鍵長を４５０bit 削減することができました。この結果から、従来と同程度のセキュリティレベルなら計算時間を短縮することができ、また同程度の計算時間ならばセキュリティレベルを向上させることができることを示しました。

【今後の期待】

暗号化制御システムの最適な鍵長と制御器の設計法を提案し、暗号化制御システムの設計を体系化することに成功しました。応用面では、既存の制御システムの制御性能を損なうことなく暗号化制御アルゴリズムを導入でき、システムのセキュリティを向上させることができると期待されます。

（論文情報）

雑誌名：「IEEE Transactions on Automatic Control」

論文タイトル: Designing Optimal Key Lengths and Control Laws for Encrypted Control Systems based on Sample Identifying Complexity and Deciphering Time

著者：Kaoru Teranishi, Tomonori Sadamoto, Aranya Chakrabortty, Kiminao Kogiso

DOI 番号：10.1109/TAC.2022.3174691

（外部資金情報）

本研究は、科学研究費基盤研究(B)22H01509(2022-2024)、および特別研究員奨励費 JP21J22442 の助成を受けて行いました。

（用語説明）

[1]暗号化制御システム：準同型暗号により制御パラメータと信号の両方が暗号化された制御システム

[2]準同型暗号：暗号文のまま加算や乗算などの演算が可能な暗号方式

[3]暗号の鍵長：暗号文の強度を決定するパラメータ。一般に鍵長が長いほど解読されにくい暗号文になる

【連絡先】

＜研究内容に関すること＞

電気通信大学 大学院情報理工学研究科

准教授　小木曽公尚

Tel：042-443-5392　　E-Mail：kogiso@uec.ac.jp

＜報道に関すること＞

電気通信大学　総務企画課　広報係

Tel： 042-443-5019　 Fax： 042-443-5887

E-Mail：kouhou-k@office.uec.ac.jp