Encrypted Cooperative Control

Verschlüsselte kooperative Regelungen für vernetzte Systeme

Erfindung

Kooperative Regelungen ermöglichen in vernetzten Systemen die Umsetzung einer „globalen“ Zielsetzung durch den Einsatz „lokaler“ Regelungsstrategien. Um die Kopplung der Teilsysteme oder Agenten innerhalb der Regelung zu berücksichtigen, werden typischerweise Zustandsdaten zwischen benachbarten Agenten ausgetauscht (siehe Abbildung). Häufig handelt es sich dabei um sensible Daten (z.B. in Stromnetzen oder autonomen Fahrzeugverbünden), die vor Einsichtnahme durch Dritte aber auch durch benachbarte Agenten zu schützen sind.

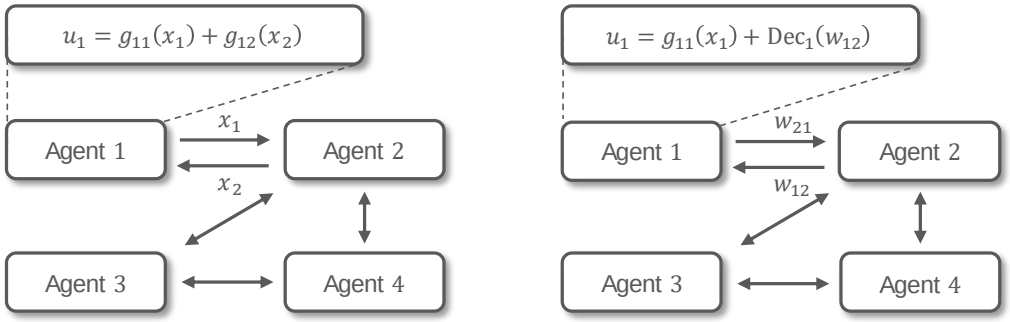

Abbildung: Konventionelle kooperative Regelung basierend auf dem Austausch von Systemzuständen x_i (links) und verschlüsselter kooperative Regelung basierend auf den Austausch verschlüsselter Regelungsanteile w_{ij} (rechts). Es gilt $w_{ij} := G_{ij}(x_j)$, wobei G_{ij} eine verschlüsselte Version von g_{ij} verkörpert

Es ist leicht ersichtlich, dass eine verschlüsselte Kommunikation der Daten für sich genommen keinen umfassenden Schutz bietet, da die Zustandsdaten auf benachbarten Agenten unverschlüsselt verarbeitet werden. Die verschlüsselte kooperative Regelung geht daher einen Schritt weiter und verschlüsselt auch die lokalen Regelungsalgorithmen. Charakteristika der neuen Technologie sind eine Umverteilung der Berechnung der lokalen Regelungsanteile und die sichere Auswertung dieser Anteile mit Techniken der homomorphen Verschlüsselung. Die Implementierung der Technologie erfolgt zweistufig. Vor der Inbetriebnahme der kooperativen Regelung werden Anteile der lokalen Regelungen identifiziert, die nur von Zuständen der Nachbaragenten abhängen. Derartige Anteile dominieren alle gängigen kooperativen Regelungen. Diese Anteile werden anschließend verschlüsselt auf den Nachbaragenten implementiert und zwar derart, dass die Resultate nur von den Zielagenten entschlüsselt werden können. Zur Laufzeit der Regelung werden die verschlüsselten Regelungsanteile anstelle der üblichen Zustandsdaten zwischen den Agenten ausgetauscht. Man erhält somit drei Sicherheitsgarantien: (1.) Die Kommunikation ist verschlüsselt, (2.) Nachbarzustände werden vor Einsichtnahme geschützt und (3.) benachbarte Regelungsanteile und -Strategien werden nicht offengelegt.

Kommerzielle Anwendung

Die verschlüsselte kooperative Regelung erhöht die Datensicherheit in verteilten Regelungssystemen signifikant und adressiert damit ein Kernziel der Industrie 4.0. Sie kann universell eingesetzt werden und ist nicht auf einzelne Anwendungen festgelegt.

Aktueller Stand

Für die verschlüsselte kooperative Regelung wurde beim Deutschen Patent- und Markenamt eine Patentanmeldung eingereicht. Internationale Anmeldungen sind noch möglich. Im Namen der Universität Paderborn bieten wir interessierten Unternehmen die Technologie zur Lizenznahme und zur Weiterentwicklung an.

Eine Erfindung der Universität Paderborn.

Vorteile

- Hohe Datensicherheit für vernetzte Systeme
- Einfache Integration in bestehende kooperative / verteilte Regelungen
- Universelles Einsatzgebiet
- Wegbereiter der Industrie 4.0

Technologie-Reifegrad

1 2 3 4 5 6 7 8 9

Beobachtung und Beschreibung des Funktionsprinzips

Branche(n)

- Elektrotechnik
- Elektrische Schaltungen

Ref.-Nr.

5403

Kontakt

Andreas Brennemann
E-Mail: ab@provendis.info
Tel.: +49(0)208-94105-33

PROvendis GmbH
Schloßstraße 11-15
45468 Mülheim an der Ruhr
Deutschland
www.provendis.info