Encrypted Cooperative Control

Encrypted cooperative control for network systems

Invention

Cooperative control in multi-agent systems enable the implementation of a "global" objective through the use of "local" regulatory strategies in networked systems. To account for the coupling of the subsystems or agents within the control, status data are typically exchanged between neighboring agents (see figure). For this purpose, status data is typically exchanged between individual neighboring agents. Calculations are carried out by neighboring agents as shown in the figure below.

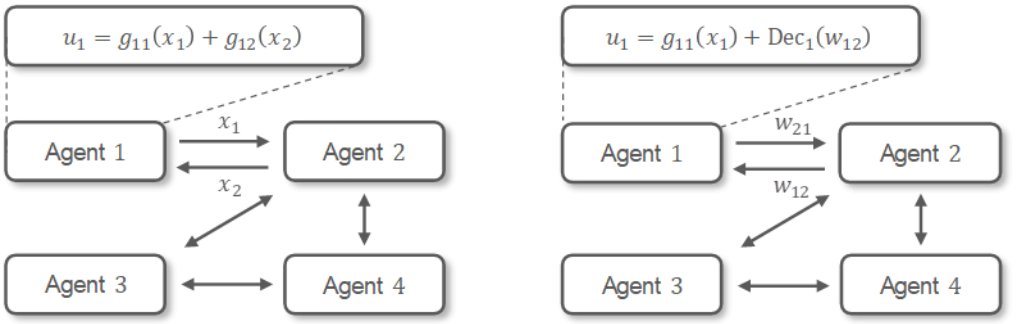

Fig.: Conventional cooperative control based on the exchange of system states x_i (left) and encrypted cooperative control based on the exchange of encrypted control shares w_{ij} (right). It applies $w_{ij} \coloneqq G_{ij}(x_j)$, whereby G_{ij} is an encrypted version of g_{ij}

Often these are sensitive data (for example e.g. in power grids or autonomous vehicle networks), which have to be protected against inspection by third parties such as neighboring agents. It is obvious that encrypted communication of the data does not provide comprehensive protection per se, as the state data on neighbouring agents is processed unencrypted. Therefore, the encrypted cooperative control goes a step further and encrypts the local control algorithms as well. Characteristics of the new technology are a redistribution of the calculation of the local control shares. The secure evaluation of these shares with techniques of homomorphic encryption. The implementation of the technology takes place in two stages. Prior to commissioning of the cooperative regime, portions of the local regulations are identified which depend only on conditions of the neighboring agents. These shares dominate all common cooperative arrangements. For instance, shares are then implemented encrypted on the neighboring agent that the results can only be decrypted by the target agents. During runtime of the control, the encrypted control shares are exchanged between the agents instead of the usual status data. Three security guarantees are thus obtained: (1) the communication is encrypted, (2) neighbor states are protected from inspection and (3) neighboring regulatory shares and strategies are not disclosed.

Commercial Opportunities

The encrypted cooperative regulation significantly increases the data security in distributed control systems and thus addresses a core goal of Industry 4.0. It can be used universally and is not limited to individual applications.

Current Status

A patent application was filed with the German Patent and Trademark Office for the encrypted cooperative regulation. International registrations are still possible. On behalf of the Paderborn University, we offer interested companies the technology for licensing and further development.

An invention of the Paderborn University.

Competitive Advantages

- High data security in multi-agent systems
- Simple integration into consisting cooperative/ distributed control systems
- Wide range of application
- Pioneer for Industry 4.0

Technology Readiness Level

1 2 3 4 5 6 7 8 9

Basic principles observed

Industries

- Electrical Engineering
- Electric Circuits

Ref. No.

5403

Contact

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

PROvendis GmbH
Schlossstraße 11-15
45468 Muelheim an der Ruhr
Germany
www.provendis.info