Secure Distributed Consensus Control for Multi-Robot Systems

Sangjun Lee and Byung-Cheol Min

SMART Lab, Department of Computer and Information Technology, Purdue University

**Motivation**

- Multi-robot systems is commonly operated through supervisory control in unprotected communication channels.
- Applications run on an open source framework that is fully accessible to unauthorized users.

These natures makes itself more vulnerable to cyberthreats.

- Illustration of a signal spoofing attack

**Threat Model**

- **Deception attack**: the possibility of compromising the integrity of control packets or measurements, altering the behavior of sensors and actuators.
- **Denial of Service (DoS) attack**: compromise the availability of resources by jamming the communication channel.

If there is an attack, actuators would not be able to respond to the robot correctly, which may lead to disastrous consequences.

**Countermeasure Against Attacks**

- **Switching Consensus Control** to achieve \( \lim_{t \to \infty} ||x_i - x_j|| = 0 \)

**Consensus Protocol 1**: If any of robots is identified under deception attack, assign more weight to the robots in normal operation than the compromised robots.

\[ u_k = \sum_{j=1}^{N} a_{ij} (x_i - x_j) \]  

Minimize the negative effects of attacks.

**Consensus Protocol 2**: If any of robots is identified under DoS attack, reassign the compromised robots as followers by reconfi guring the communication topology.

\[ u_{k,f} = \sum_{j=1}^{N} a_{ij} (x_i - x_j) \]  

Make the leaders to guide the followers.

**Research Questions**

1) Is a robot able to identify attacks solely?
2) If so, is the robot able to counteract them?

**Experimental Validation**

- While the team is trying to reach consensus at a common point, two types of attacks are injected into 4 arbitrarily selected robots when the global clock reached 3 seconds.

- **Case 0. Deception Attacks without the countermeasure**

  The attacks caused the disconnection of the communication link

- **Case 1. Deception Attacks**

  The detection scheme identified significant changes of the residuals that crossed the threshold

- **Case 2. DoS Attacks**

  The compromised robots start following the leaders after attacks

The proposed countermeasure enabled the robot team to reach consensus at a common point without losing any robots and connectivity in the presence of more than one robot under attacks.

**Threat Identification**

- **Model-based identification Scheme**

  Robot’s dynamics model allow us to predict it’s normal behaviors.

An attack will cause deviations at the physical layer, resulting unexpected alterations (Prediction ≠ Measurement).

- **Detection Mechanism**

  Identifying the alterations is to distinguish between two hypotheses: \( H_0 \) – the normal case, \( H_1 \) – the abnormal case where a change has taken place.

**Acknowledgement**

This work was supported by Award No. 2017-R2-CX-0001, awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice.

**References**