CERIAS

The Center for Education and Research in Information Assurance and Security

Secure Distributed Consensus Control for Multi-Robot Systems

Sangjun Lee and Byung-Cheol Min

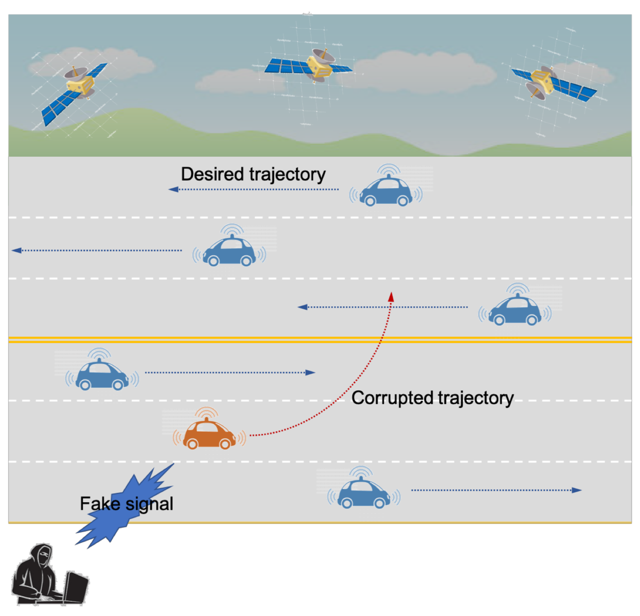
SMART Lab, Department of Computer and Information Technology, Purdue University

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.

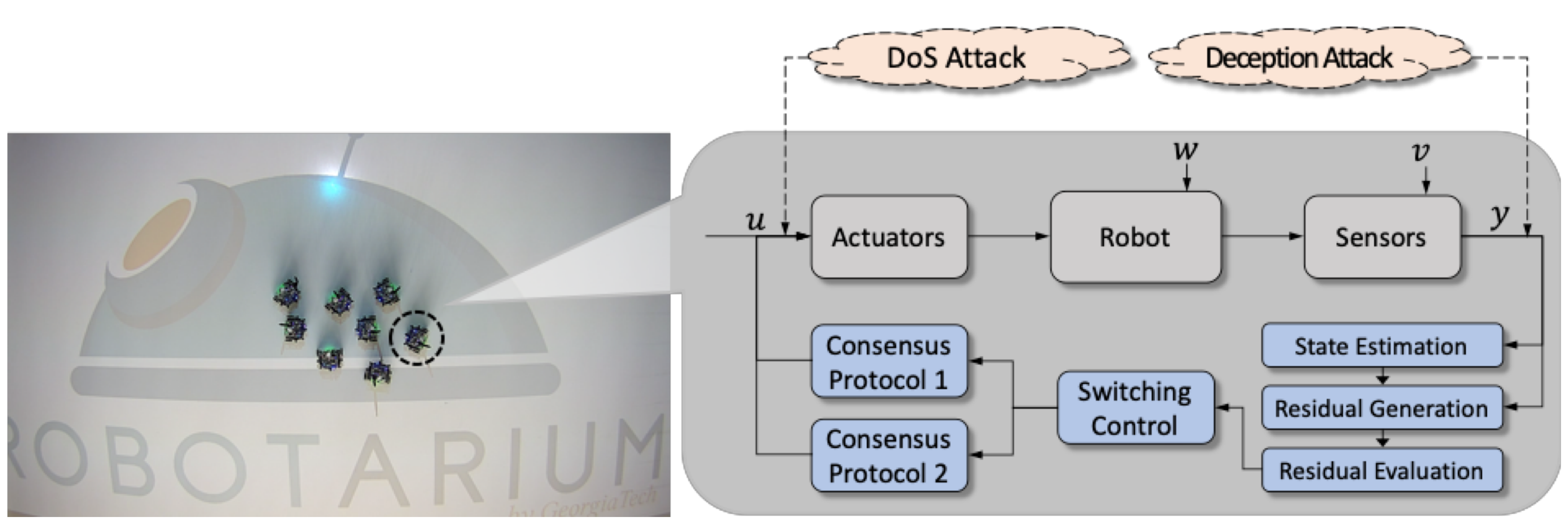
- Illustration of a signal spoofing attack



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

Threat Model

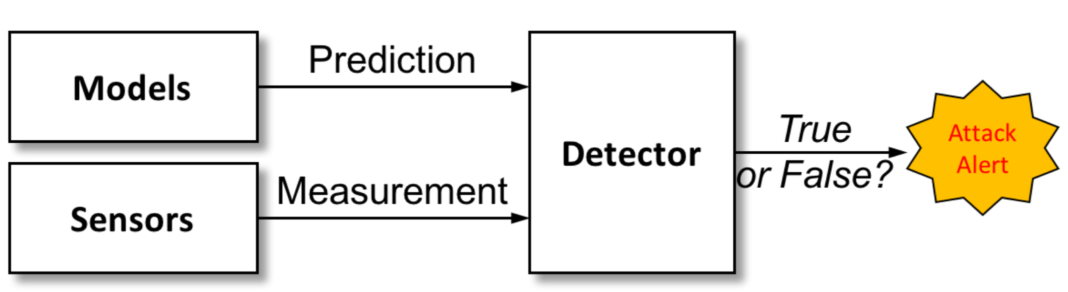
- ***Deception attack:*** the possibility of compromising *the integrity* of control packets or measurements, altering the behavior of sensors and actuators.
- ***Denial of Service (DoS) attack:*** compromise *the availability* of resources by jamming the communication channel.



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

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.

Countermeasurement Against Attacks

- **Switching Consensus Control** to achieve $\lim_{k\to\infty}\|x_i - x_j\| = 0$

  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.

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

Minimize the negative effects of attacks.

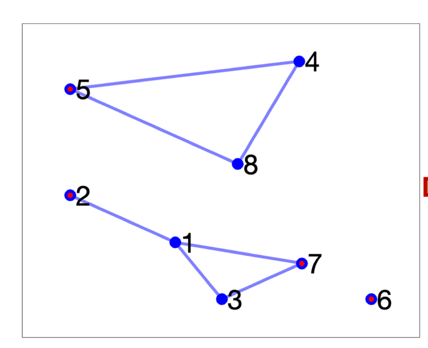
  Consensus Protocol 2: If any of robots is identified under *DoS attack*, reassign the compromised robots as followers by reconfiguring the communication topology.

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

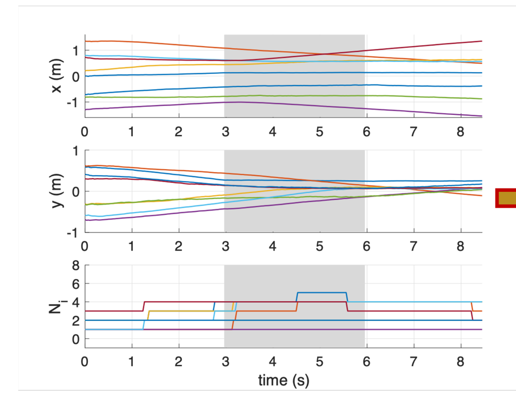
Make the leaders to guide the followers.

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**

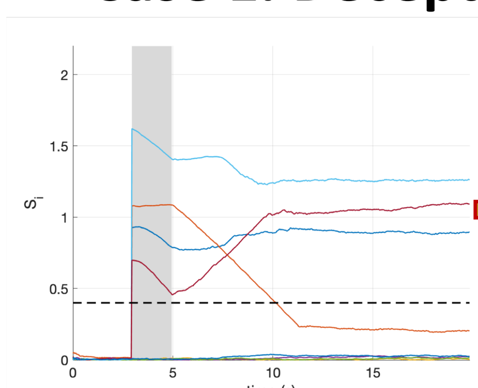


The attacks caused the disconnection of the communication link

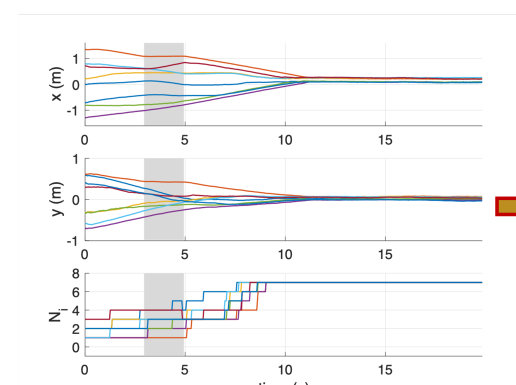


Consensus failed

- **Case 1. Deception Attacks**

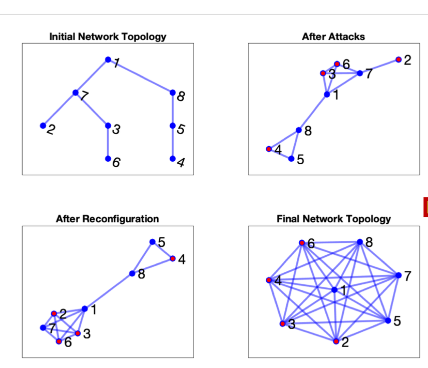


The detection scheme identified significant changes of the residuals that crossed the threshold

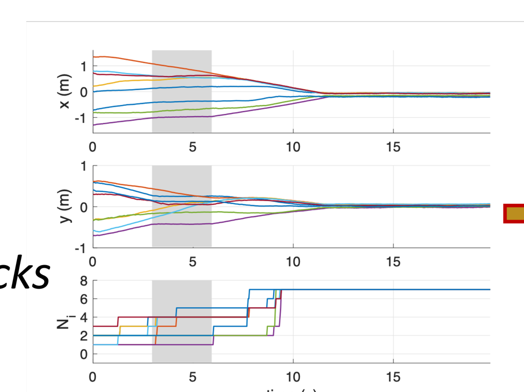


Consensus achieved

- **Case 2. DoS Attacks**



The compromised robots start following the leaders after attacks



Consensus achieved

*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.*

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

- S. Lee and B.-C. Min, "Distributed Direction of Arrival Estimation-aided Cyberattack Detection in Networked Multi-Robot Systems," *2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, Madrid, Spain, October 2018, pp. 6168-6173
- S. Lee, Y. Cho, and B.-C. Min, "Attack-Aware Multi-Sensor Integration Algorithm for Autonomous Vehicle Navigation System," *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC),* Banff, Canada, October 2017, pp. 3739-3744.

PURDUE UNIVERSITY Discovery Park

CERIAS