Secure State Reconstruction Over Networks Subject to Attacks

Task 2.3: Short-time-scale Active Learning in Adaptive, Self-aware IoBTs

IoBT REIGN

DEVCOM ARMY RESEARCH LABORATORY

Yanwen Mao, *UCLA*; Suhas Diggavi, UCLA; Christina Fragouli, UCLA; and Paulo Tabuada, *UCLA*;

Point of Contact: Yanwen Mao, *UCLA*, yanwen.mao@ucla.edu

Objectives

- In order to increase resiliency and survivability of IoBTs in adversarial environments, we address the problem of secure state reconstruction in the presence of sensor and network attacks.
- We consider IoBTs deployed to localize enemy's assets (e.g., trucks, soldiers) notwithstanding attacks on its sensors and communication links.

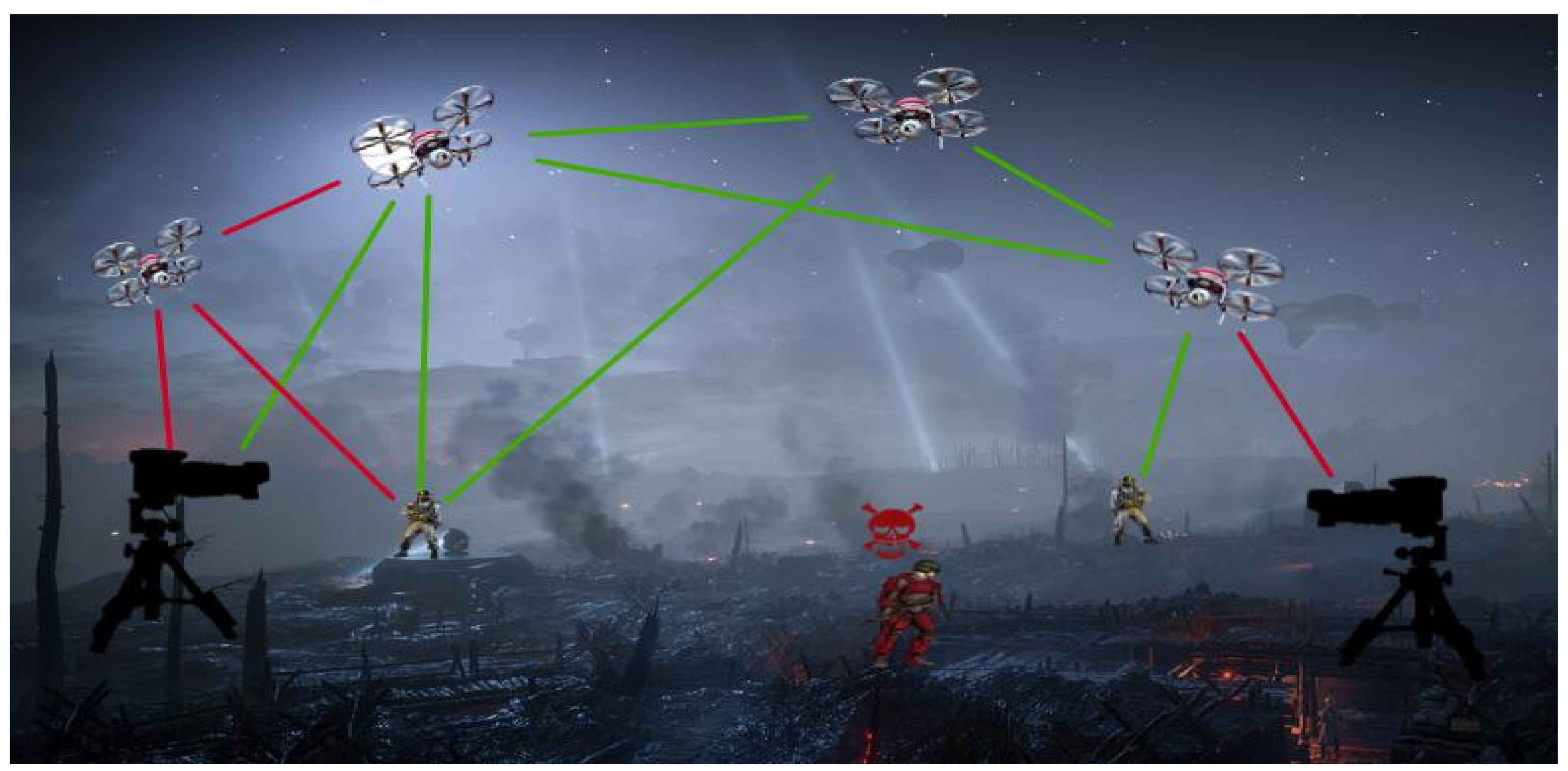


Fig.1: Localization of enemy's asset in presence of malicious sensors.

Problem Formulation

- We model the dynamics of an object as a linear system:

$$\mathrm{x}(t+1) = A\mathrm{x}(t) \qquad (2.1)$$

$$y_i(t) = C_i\mathrm{x}(t) + e_i(t), \quad i = 1, \ldots, p\,, \qquad (2.2)$$

where $\mathrm{x}(t)$ is the state of an enemy's asset (e.g., location and velocity), $y_i(t)$ is the i-th node's measurement, and e_i models how an attack changes the i-th's node measurement.

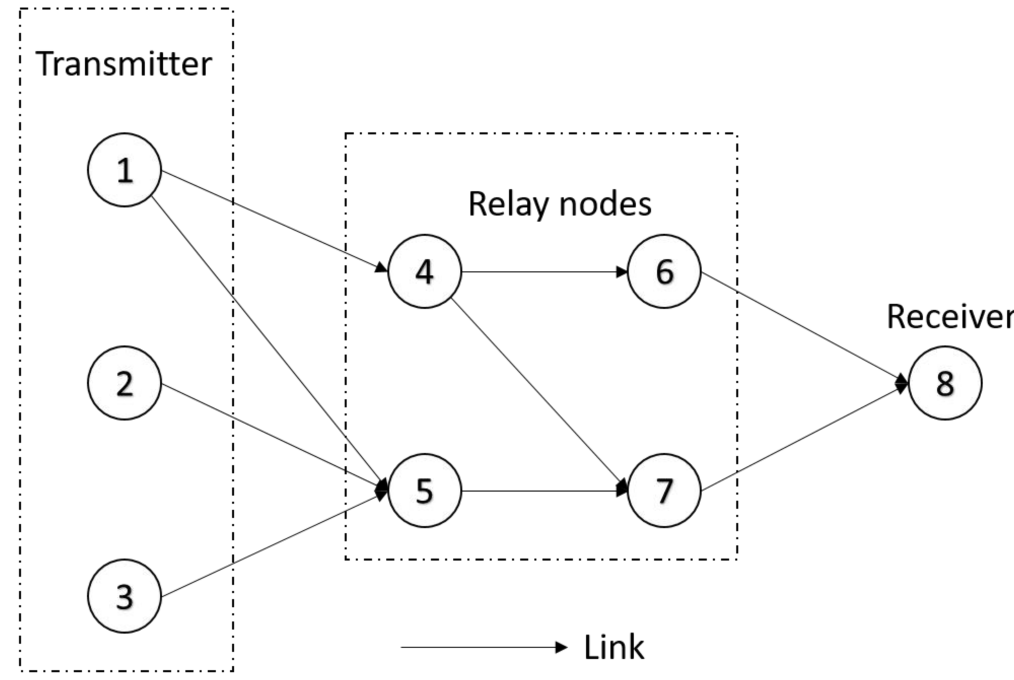


Fig.2: Illustration of model: Transmitter nodes send measurements to the receiver via a communication network composed of relay nodes and links.

- We assume that at most f_1 links and f_2 nodes (including both trasmitter nodes and relay nodes) are attacked.
- The ***secure state reconstruction*** problem asks if we can reconstruct the state x at the receiver from messages received from the receiver's neighbors, despite the attacks on links and nodes.

Definitions

P - the set of transmitters	V - the set of relay nodes
E - the set of links	$C_Q = [C_{q1}^T \vert C_{q2}^T \vert \ldots \vert C_{qr}^T]^T$

- A set $S \subseteq P$ is said to be a critical set if $(A, C_{P/S})$ is not observable.
- Consider a critical set S. A set $H_S \subseteq (P \cup V \cup E)$ is called a mix cut with respect to (w.r.t.) S if removal of $H_S \cap (V \cup E)$ disconnects the receiver and $H_S \cap P$.
- Implications of mix cut: removal of all nodes and links in a mixed cut will prevent the receiver to obtain information from part of the state.

Key Result

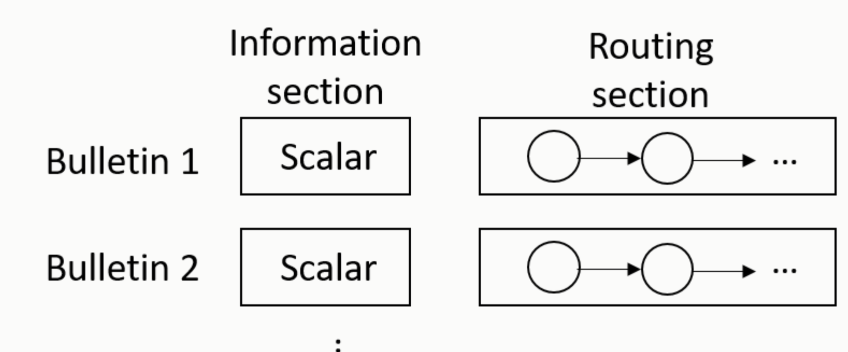
- The secure state-reconstruction problem is solvable if and only if for every critical set S and every mix cut w.r.t. S, H_S, the following bounds are satisfied:

$$\mathrm{L}(H_S) > 2f_1 \text{ or } \mathrm{N}(H_S) > 2f_2,$$

where L and N denote the links and nodes in the mix-cut H_S, respectively.

Steps in State Reconstruction

- The ***key idea*** to reconstruct the state is motivated by the flooding algorithm: each node broadcasts its measurement, any message it receives, and its identifier.
- Message format: Each message is composed of several bulletins. Each bulletin has 2 sections: the information section and the routing section, illustrated as below:



- Our approach is composed of three steps:
  1. The receiver stacks the values in the information section of all bulletins whose routing section values are the same.
  2. The receiver picks a set $L \subseteq (P \cup V \cup E)$ of f_1 links and f_2 nodes, removes any vector obtained in step (1) whose routing section contains at least 1 element in L.
  3. The receiver then checks if there exists a state x that explains all remaining vectors. If so, this x is the state, otherwise go back to step 2 and pick another L.