

Resilient Multi-Agent Target Localization and Tracking via BAG-Aware Mutual Information Maximization under False Data Injection Attacks

Bibek Adhikari* Samrat Chaulagain* Kamesh Subbarao*

** Department of Mechanical and Aerospace Engineering,
The University of Texas at Arlington, Arlington, TX 76019 USA
(e-mail: bibek.adhikari@mavs.uta.edu, sxc9808@mavs.uta.edu,
subbarao@uta.edu).*

Abstract: Cooperative multi-agent networks deployed for target localization and tracking remain critically vulnerable to malicious cyber attacks, since a single compromised agent can corrupt the centralized target belief and mislead the estimation process across the entire network. This paper presents a resilient multi-agent target localization and tracking framework under a limited agent sensing range and false-data injection (FDI) attacks. The proposed method combines information-based navigation for target search and posterior target state uncertainty reduction, Bayesian attack graph (BAG) based attack detection for probabilistic identification of the compromised agents, and reachable set-guided recovery that guides the uncompromised agents to relocalize the target when the sole localizing agent is attacked. The framework preserves the network's localization capability after an attack by trust-gating compromised sensing information and guiding attack-immune agents toward a dynamically constructed recovery set representing the new target belief using a Linear Quadratic Regulator (LQR). Simulation validates that the proposed framework maintains a robust tracking performance under FDI attacks, demonstrating the potential for resilient autonomy in safety-critical applications.

Keywords: Multi-Agent Network, Target Tracking, Mutual Information Maximization, Bayesian Attack Graph, Particle Filter, False Data Injection

1. INTRODUCTION

Cooperative multi-agent network have advanced in autonomous systems in the field of localization and tracking. In recent years, such networks have been employed in applications such as autonomous surveillance (Patrino et al., 2022), environmental monitoring (Kravari et al., 2025), and threat localization and neutralization (Saeed et al., 2020). Target tracking through a multi-agent network enables the system to share information among agents via a centralized or decentralized framework. Localization under an agent's sensing range constraint introduces complexity to the network, requiring the target position to be inferred cooperatively from the combination of presence and absence of observations. Under these conditions, agents must actively coordinate their movement to gradually reduce a shared uncertainty of the target state, scanning the area until enough observations are obtained to localize the target with certainty. Particle filter-based approach for cooperative localization is a well-suited framework for systems with unknown target motion models and nonlinear measurements, relying solely on weighted information about the target state (Hoffmann

and Tomlin, 2010). However, when these systems are deployed in adversarial environments, they become vulnerable to cyber-physical attacks such as sensor tampering, false data injection, and Denial-of-Service (DoS) attacks (Duo et al., 2022).

In particular, FDI attacks represent a threat where adversaries inject malicious data into the system, often by taking control of certain agents or by tampering with their communication channels, resulting in invalid measurements. The system with centralized belief is highly vulnerable to these attacks, especially since a single compromised agent can corrupt the entire distribution of the target state, which propagates to other agents in the network. In particle-filter estimation of the target state under FDI attacks, the attacked agents' target estimates could be treated as trusted positions, leading the entire network to pursue the ghost target. The situation is further complicated if the sole initial localizing agent is attacked by the malicious target.

To mitigate cyber-physical attacks, recent research has focused on secure estimation and resilient filtering strategies that aim to detect and isolate compromised nodes (Chen et al., 2019). Bayesian attack graphs provide a probabilistic framework for modeling the propagation of cyber attacks across a network by exploiting dependencies among nodes and have been used for security assessment and in-

* The authors gratefully acknowledge the support from ARO Grant W911NF-23-1-0174

ference of compromise in networked systems (Frigault and Wang, 2008; Muñoz-González et al., 2019). Recent work has further developed BAG-based MMSE monitoring and attack detection under imperfect observations (Kazemina-jafabadi and Imani, 2023), as well as BAG-aware resilient target tracking in multi-agent systems (Chaulagain and Subbarao, 2026).

The rest of the paper is formulated as follows. Section 2 presents the objective and problem statement, while Section 3 presents modeling and analysis of the graph network, target, sensing agent, and measurement model. Section 4 formulates the methodology of the work. The simulation and experimental setups are described in Section 5, and the paper concludes in Section 6.

2. PROBLEM STATEMENT

The paper addresses a multi-agent network tasked with localizing and tracking a dynamic intruder target in a bounded search space. The agents are equipped with a sensor of limited measuring range. A particle filter is employed in the system to represent the target belief and estimate the target state based on the measurements from the sensing agents. The mutual information between the target and the sensor observation is used to navigate inside the search space to localize the target. The control objective of the system is to compute a control input that arranges agents' positions, maximizing the mutual information, which leads to future observations that minimize the target uncertainty.

The paper further addresses a resilient cooperative localization and tracking of the target in the presence of false data injection into the localizing agent through the target. The challenge arises when the sole localizing agent gets compromised, providing biased or inconsistent observation, jeopardizing the system's particle belief. The mission objective is to localize the target under the influence of FDI while preventing the attack from degrading the system's performance, and continue to preserve a bounded posterior belief around the moving target, corresponding to persistent tracking. The contribution of the paper is a unified resilient framework that combines mutual information-based target localization, Bayesian attack graph-based compromise detection, and reachable-set-guided recovery for robust relocalization and tracking.

3. SYSTEM MODELING AND ANALYSIS

The global coordinate system is a fixed reference frame represented as $I = \{O_I, X_I, Y_I, Z_I\}$.

3.1 Target Model

Let $\mathbf{x}_T = [x_T \ y_T \ \dot{x}_T \ \dot{y}_T]^\top$ be the state of the target in inertial frame in the search domain $\mathcal{X}$, such that $\mathbf{x}_T \in \mathcal{X}$, whose model is represented as:

$$\dot{\mathbf{x}}_T(t) = \mathbf{A}_T \mathbf{x}_T(t) + \mathbf{B}_T \boldsymbol{\nu}_T(t), \quad (1)$$

with

$$\mathbf{A}_T = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \in \mathbb{R}^{4 \times 4}, \quad \mathbf{B}_T = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \in \mathbb{R}^{4 \times 2},$$

where $\mathbf{A}_T$ and $\mathbf{B}_T$ are the system and input matrix of the target model, respectively, at time t , and $\boldsymbol{\nu}_T$ is the random acceleration disturbance such that $\boldsymbol{\nu}_T \sim \mathcal{N}(\mathbf{0}, \boldsymbol{\Sigma}_{\boldsymbol{\nu}_T}) \in \mathbb{R}^2$ is modeled as the zero-mean Gaussian noise with covariance $\boldsymbol{\Sigma}_{\boldsymbol{\nu}_T}$. The position of the target is denoted in the inertial frame as $\mathbf{p}_T = [x_T \ y_T]^\top$. A prior distribution of the target $p(\mathbf{x}_T(0))$ is known, around which the search domain is created.

3.2 Sensing Agent Model

Consider a set of A sensing agents localizing the target and let $\mathbf{x}_i = [x_i \ y_i \ \dot{x}_i \ \dot{y}_i]^\top \in \mathbb{R}^4$ be the state of i^{th} agent in inertial frame with dynamics given as:

$$\dot{\mathbf{x}}_i(t) = \mathbf{A} \mathbf{x}_i(t) + \mathbf{B} \mathbf{u}_i(t), \quad (2)$$

where $\mathbf{A}$ and $\mathbf{B}$ are the system and input matrices of sensing agents respectively, and $\mathbf{u}_i(t)$ is the control input of i^{th} agent at time t with

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \mathbf{B} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, \mathbf{u}_i(t) = \begin{bmatrix} a_{x_i} \\ a_{y_i} \end{bmatrix},$$

where a_{x_i} and a_{y_i} are the acceleration control inputs. The position of the i^{th} agent is denoted in the inertial frame as $\mathbf{p}_i = [x_i \ y_i]^\top$, whereas its heading is denoted as ψ_i about the Z_I axis.

3.3 Measurement Model

Let $\mathbf{z}_i$ be the measurement made by the i^{th} sensing agent, measuring the range from the agent to the target, and its bearing. The measurements of the target are obtained only when the target lies within the sensor's maximum range. The range measurement is represented as:

$$z_i^r(k) = \|\mathbf{p}_i(k) - \mathbf{p}_T(k)\| + \epsilon_i^r(k), \quad (3)$$

$$\epsilon_i^r \sim \mathcal{N}(0, \sigma_r^2). \quad (4)$$

The bearing measurement from the agent to the target is expressed as:

$$z_i^\theta(k) = \arctan\left(\frac{y_T(k) - y_i(k)}{x_T(k) - x_i(k)}\right) + \epsilon_i^\theta(k), \quad (5)$$

$$\epsilon_i^\theta \sim \mathcal{N}(0, \sigma_\theta^2), \quad (6)$$

where $\epsilon_i^r(k)$ and $\epsilon_i^\theta(k)$ are the range and bearing measurement noise of i^{th} sensing agent respectively at time step k , with the Gaussian distribution of zero-mean and variance σ_r^2 and σ_θ^2 respectively. The aggregate measurement for i^{th} sensing agent at time step k is represented as $\mathbf{z}_i(k) = [z_i^r(k) \ z_i^\theta(k)]^\top \in \mathbb{R}^2$. The particle-wise likelihood used for belief update incorporates both range and bearing measurements, which is the probability of the current measurement conditioned on the n^{th} particle being the true target state. Assuming independent measurement noise, the likelihood of the n^{th} particle for the i^{th} agent is expressed as:

$$L_i^n(k) = p(\mathbf{z}_i(k) | \mathbf{x}_T = \tilde{\mathbf{x}}_T^n(k)), \quad (7)$$

where $\tilde{\mathbf{x}}_T^n$ denote the state of the particle.

3.4 False Attack Injection Model

The attack is triggered when an agent breaches the target's attack range (R_{atk}). It is assumed that the target's attack range is smaller than the agents' sensing range. Once an agent is compromised, false data is injected into its sensor, which is additive to its true measurement. The measurement of the compromised agent is modeled as:

$$z_{i,\text{atk}}^r(k) = z_i^r(k) + \alpha_i(k), \quad (8)$$

where $\alpha_i(k) \sim \mathcal{N}(b, \sigma_\alpha^2)$ denotes the false-data injected into compromised agent, with mean b and variance σ_α^2 .

4. METHODOLOGY

4.1 Mutual Information Maximization

Mutual information is evaluated between the target state and range measurement. The measurement entropy is approximated using a discretized grid $z^r \in [z_{\min}^r, z_{\max}^r]$ with spacing Δz^r . The optimal control input to plan the next agent state is calculated by optimizing mutual information represented as:

$$\mathbf{u}_{m_i}^*(k) = \arg \max_{\mathbf{u}_{m_i} \in \mathcal{U}_i} I(\mathbf{x}_T; z_i^r(k) | \mathcal{Z}_{k-1}^r), \quad (9)$$

with

$$I(\mathbf{x}_T; z_i^r(k) | \mathcal{Z}_{k-1}^r) = H(z_i^r(k) | \mathcal{Z}_{k-1}^r) - H(z_i^r(k) | \mathbf{x}_T, \mathcal{Z}_{k-1}^r), \quad (10)$$

where $\mathcal{Z}_{k-1}^r = \{\mathbf{z}^r(0), \dots, \mathbf{z}^r(k-1)\}$ represents the range measurement history up until k . The entropy of measurement given the measurement history and entropy of measurement given the target state and measurement history are respectively expressed as:

$$H(z_i^r(k) | \mathcal{Z}_{k-1}^r) = - \sum_{z_i^r \in \mathcal{Z}^r} \left(\left(\sum_{n=1}^N w^n(k) l_i^n(k) \right) \cdot \log \left(\sum_{n=1}^N w^n(k) l_i^n(k) \right) \right) \Delta z^r, \quad (11)$$

$$H(z_i^r(k) | \mathbf{x}_T(k), \mathcal{Z}_{k-1}^r) = - \sum_{z_i^r \in \mathcal{Z}^r} \left(\sum_{n=1}^N (w^n(k) l_i^n(k) \cdot \log(l_i^n(k))) \right) \Delta z^r, \quad (12)$$

where $l_i^n = p(z_i^r | \mathbf{x}_T = \tilde{\mathbf{x}}_T^n)$ is the particle-wise measurement likelihood used for control step utilizing range measurement, and w^n is the weight of the n^{th} particle. The derivation of the respective entropy terms are presented in our earlier work (Adhikari and Subbarao, 2025).

4.2 Localization of target

The differential Gaussian entropy of the target state conditioned on the measurement history is used to quantify the uncertainty of the target probability distribution, which is expressed as:

$$H(\mathbf{x}_T | \mathcal{Z}_k^r) = \frac{1}{2} \log((2\pi e)^d \det(\mathbf{\Sigma}_k)), \quad (13)$$

where e and d denote the Euler's number and dimension of the target state respectively, and $\mathbf{\Sigma}$ represents the posterior covariance estimated from the particle belief.

The posterior belief of the target state increasingly concentrates as the agents receive informative observations, leading to a decrease in posterior differential Gaussian entropy. Once the entropy drops below a predetermined threshold corresponding to an acceptable degree of uncertainty, the target can be deemed localized, and converging to a constant value below the threshold signifies the active tracking of the target. Subsequent measurements are then used to maintain a bounded posterior belief around the target state, corresponding to persistent tracking.

4.3 Bayesian Attack Graph Network

To capture cyber-attack propagation over the multi-agent network, Bayesian attack graph is employed. The BAG is represented by a tuple, represented as:

$$\mathcal{G}_{\text{BAG}} = (\mathcal{V}, \mathcal{E}, \mathcal{T}, \mathcal{P}),$$

where, $\mathcal{V} = \{1, 2, \dots, A\}$ is the set of sensing agents, $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ is the set of directed edges, $\mathcal{T}$ denotes the node types, and $\mathcal{P}$ denotes the exploit probabilities. An edge $(i, j) \in \mathcal{E}$ indicates that compromise of agent i can lead to compromise of agent j . Each agent has binary compromise state $s_j(k) \in \{0, 1\}$, and the network state is

$$\mathbf{s}(k) = [s_1(k) \ s_2(k) \ \dots \ s_A(k)]^\top \in \{0, 1\}^A. \quad (14)$$

A subset $\mathcal{V}_c \subseteq \mathcal{V}$ is vulnerable to direct external attack, where each $j \in \mathcal{V}_c$ is assigned external exploit probability ρ_j . Each edge $(i, j) \in \mathcal{E}$ is assigned internal exploit probability ρ_{ij} . Nodes are classified as AND or OR types. The BAG evolves as the binary-state Markov process, and the conditional probability of node j depends on its node type and the previous compromise state $\mathbf{s}(k-1)$. Once compromised, a node is assumed to remain compromised for the rest of the mission. To infer the hidden compromise states, binary monitoring observations are introduced. Let $y_j(k) \in \{0, 1\}$ denote the monitoring output for agent j , where $y_j(k) = 1$ indicates a detected compromise. The exploit probability calculation and observation model follows (Chaulagain and Subbarao, 2026).

Compromised agents may be missed with probability q_{miss} , while healthy agents do not generate false alarms. The joint observation vector is

$$\mathbf{y}(k) = [y_1(k) \ y_2(k) \ \dots \ y_A(k)]^\top.$$

Let

$$\mathbf{\Omega} = [\mathbf{s}^1, \mathbf{s}^2, \dots, \mathbf{s}^{2^A}] \in \{0, 1\}^{A \times 2^A} \quad (15)$$

denote the set of all possible network compromise configurations. The posterior and predictive belief vectors are defined as:

$$\begin{aligned} \mathbf{\Pi}_{k|k}(i) &= p(\mathbf{s}(k) = \mathbf{s}^i | \mathbf{y}(1:k)), \\ \mathbf{\Pi}_{k|k-1}(i) &= p(\mathbf{s}(k) = \mathbf{s}^i | \mathbf{y}(1:k-1)), \end{aligned} \quad (16)$$

for $i = 1, 2, \dots, 2^A$. The state transition matrix $\mathbf{M}_k \in \mathbb{R}^{2^A \times 2^A}$ is

$$(\mathbf{M}_k)_{ij} = p(\mathbf{s}(k) = \mathbf{s}^i | \mathbf{s}(k-1) = \mathbf{s}^j), \quad (17)$$

which gives the predictive update

$$\mathbf{\Pi}_{k|k-1} = \mathbf{M}_k \mathbf{\Pi}_{k-1|k-1}. \quad (18)$$

Given $\mathbf{y}(k)$ at time k , the likelihood vector is

$$(\mathbf{T}_k(\mathbf{y}(k)))_i = p(\mathbf{y}(k) | \mathbf{s}(k) = \mathbf{s}^i), \quad (19)$$

and the posterior update is

$$\Pi_{k|k} = \frac{\mathbf{T}_k(\mathbf{y}(k)) \circ \Pi_{k|k-1}}{\|\mathbf{T}_k(\mathbf{y}(k)) \circ \Pi_{k|k-1}\|_1}, \quad (20)$$

where $\circ$ denotes the Hadamard (element-wise) product and $\|\cdot\|_1$ denotes the ℓ_1 -norm. The optimal minimum mean-square-error estimate of the compromise state is

$$\hat{\mathbf{s}}^{\text{MMSE}}(k) = \text{round}(\Omega \Pi_{k|k}), \quad (21)$$

where the $\text{round}(\cdot)$ maps each entry to the nearest binary value (Kazeminajafabadi and Imani, 2023). This estimate defines the trust variable used in the resilient particle-filter update as:

$$\gamma_i(k) = \begin{cases} 1, & \hat{s}_i^{\text{MMSE}}(k) = 0, \\ 0, & \hat{s}_i^{\text{MMSE}}(k) = 1. \end{cases} \quad (22)$$

4.4 Target Reachable Region Approximation

Once the BAG detects an attack at time k_d a recovery set is initialized using the last trusted target-belief mean prior to the detected compromise. The last trusted instant is estimated retrospectively from the stored range-residual history of the compromised agent as:

$$r_i(k) = |z_i^r(k) - \bar{z}_i^r(k)|, \quad k_t = \max\{k < k_d : r_i(k) < r_{\text{th}}\}, \quad (23)$$

where $r_i(k)$ denotes the residual of i^{th} agent, r_{th} is the residual threshold, and $\bar{z}^r$ is the estimated range measurement from the particle mean. Assuming the target speed is bounded by v_T^{max} , the feasible post-attack target reachable position is represented by a reachable set as:

$$\mathcal{R}(k) = \left\{ \mathbf{p}_T \in \mathbb{R}^2 : \|\mathbf{p}_T - \boldsymbol{\mu}(k_t)\| \leq R_0 + ((k - k_t)v_T^{\text{max}}\Delta t) \right\}, \quad (24)$$

where $\boldsymbol{\mu}(k_t)$ denotes the target-belief mean, and R_0 is the initial recovery radius reflecting uncertainty at the last trusted instant. A new set of particles is generated inside a set representing the feasible target position post attack detection.

4.5 Linear Quadratic Regulator Guidance

A LQR guidance law is used when an agent is outside an informative sensing configuration, particularly during particle-sparse event and recovery-set entry phase. During particle-sparse event, agents' lookahead state is the particle-belief mean. For recovery-set entry phase, recovery agents are guided into the set with particle-belief mean being the lookahead point. Once sufficient local particle support is observed, the agents switch from LQR guidance to mutual-information-maximizing search within the recovery region. Similarly, during this phase, the desired state for compromised agents is selected to move the agent away from the target attack region. The guidance law is represented as:

$$\mathbf{u}_{g_i}(k) = -\mathbf{K}_g(\mathbf{x}_i(k) - \mathbf{x}_{d,i}(k)), \quad (25)$$

where $\mathbf{x}_{d,i} = [x_{d,i} \ y_{d,i} \ \dot{x}_{d,i} \ \dot{y}_{d,i}]^\top$ is the desired state composed of lookahead position $\mathbf{p}_{d,i}$ and zero desired velocity, and $\mathbf{K}_g$ is LQR feedback gain obtained from discrete-time LQR design. The inter-agent and agent-target collision is avoided using the collision avoidance constraint (Adhikari and Subbarao, 2025).

Algorithm 1 Multi-Agent Target Localization

```

1: Inputs: Search Space  $\mathcal{X}$ ,  $\mathcal{G}_{\text{BAG}}$ , initial BAG belief  $\Pi_{1|0}$ , initial agent states  $\mathbf{x}_i(0)$ , entropy threshold  $H_{\text{th}}$ .
2: for  $k = 1, 2, \dots$  do
3:   if  $z_i^r(k) \leq R_{\text{atk}}$  then
4:     initiate attack
5:   Propagate attack using BAG
6:   Obtain sensor measurements:  $\mathbf{z}_i(k)$ 
7:   Observe cyber monitoring output  $\mathbf{y}(k)$ 
8:   BAG update:  $\Pi_{k|k}$  using Eq. (20)
9:   BAG prediction:  $\Pi_{k+1|k}$  using Eq. (18)
10:  BAG attack detection:  $\hat{\mathbf{s}}^{\text{MMSE}}(k)$  using Eq. (21)
11:  Assign trust:  $\gamma_i(k)$  using Eq. (22)
12:  Update particle weights:  $w_n(k)$  using Eq. (26)
13:  Compute posterior entropy:  $H(\mathbf{x}_T|\mathcal{Z}_k^r)$  using Eq. (13)
14:  if  $H(\mathbf{x}_T|\mathcal{Z}_k^r) < H_{\text{th}}$  for  $\tau$  consecutive steps then
15:    Declare target localized
16:    Continue posterior update for target tracking
17:  if attack detected then
18:    Estimate  $k_t$  using Eq. (23)
19:    Construct  $\mathcal{R}(k)$  using Eq. (24)
20:    if  $i$  is a compromised agent then
21:      Control update:  $\mathbf{u}_{g_i}(k)$  using Eq. (25) with  $\mathbf{p}_{d,i}(k) \leftarrow \mathbf{p}_i(0)$ 
22:    Agent control update:
23:    if sufficient local particle available then  $\mathbf{u}_{m_i}(k)$  using Eq. (9)
24:    else  $\mathbf{u}_{g_i}(k)$  using Eq. (25) with
25:      if attack detected then  $\mathbf{p}_{d,i}(k) \leftarrow \boldsymbol{\mu}(k_t)$ 
26:      else  $\mathbf{p}_{d,i}(k) \leftarrow \boldsymbol{\mu}(k)$ 

```

4.6 Trust-Gated Particle Filter Update

Following attack detection, the particle filter update is conditioned on the agent's trust status. Measurements from trusted agents are used to evaluate the likelihood, while those from compromised agents are excluded. As a result, posterior weight updates and particle resampling rely only on trusted agents, thereby preventing the corrupted data from degrading the target belief and enabling relocalization and tracking of the target using trusted agents. The normalized particle weights are updated as:

$$w^n(k) = w^n(k-1) \prod_{i=1}^A (L_i^n(k))^{\gamma_i(k)}. \quad (26)$$

5. SIMULATION AND RESULTS

A planar multi-agent target localization framework is adopted within a bounded search space, where four agents (1-4 from left to right) are initialized inside the domain to localize and track the target. The communication topology used in this paper is shown in Fig. 1. In the associated BAG, Agent 2 and Agent 3 are designated as AND nodes with zero external vulnerability, thereby making them attack-immune throughout the mission. Whereas Agent 1 and Agent 4 are OR nodes, also labeled as attack-prone agents, with external attack vulnerability as well as internal attack propagation through communication channels, effectively making them both prone to attack in case either is compromised. Particles representing the

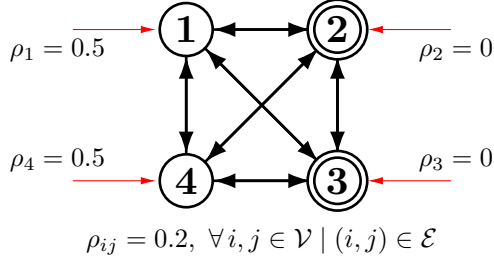


Fig. 1. Communication network of the four-agent system. Double-circled agents denote AND nodes, while single-circled agents denote OR nodes.

target belief are generated inside the search space. The simulation parameters are shown in Table 1. Figure 2 represents the mission evolution of multi-agent target localization. Figure 2a illustrates the initial setup of the framework, where agents are navigating inside the search space to maximize the mutual information. The initial localization of the target is seen in Fig. 2b, where Agent 4 localizes the target. It is further observed from the Fig. 2c that, after the target is localized, the false data is injected into the localizing agent, resulting in the spread of the particle belief over time. Figure 2d displays the recovery-set formation after the BAG detection, which bounds the target. Since BAG detects the FDI into Agent 4 and Agent 1, measurements from these respective agents are trusted during particle filter update. Post-set creation, the compromised agent goes outside the target's attacking range, and the attack-immune agents are commanded into the set to relocalize the target as seen in Fig. 2e. The framework enables mutual information maximization once it observes the particles inside the observing range of the sensing agent, and if not, the guidance law is used to guide the agent to the particle-belief mean. The relocalization of the target is observed in Fig. 2f, where both attack-immune agents relocalize the intruder as seen from the shrinkage of the particle-belief.

To evaluate the system's performance, a Monte Carlo study was conducted over multiple randomized target initial positions. The runs were separated into two classes: Class-I, where an attack-immune agent localizes the target initially, and no further recovery set is created or required, and Class-II, where an attack-prone agent localizes the target initially, and a recovery set is created to relocalize the target. Out of 250 Monte Carlo runs, 146 runs were Class-I, 104 runs were Class-II, and none of them were unsuccessful, denoting a robust localization framework, within the tested simulation conditions. The final median target-localization times for Class-I and Class-II were 39 s and 52 s respectively. To validate the effectiveness of the proposed framework, a comparison is drawn against a conventional mutual-information-based target localization framework without BAG-based attack detection and the subsequent steps it enables.

For each class, the root-mean-square error (RMSE) of the target position and the posterior differential Gaussian entropy of the target belief were aggregated using the median. Figure 3 illustrates that the target-position RMSE for Class-I converges to approximately 0 m, faster than for Class-II, which is consistent with the shorter median target-localization time. Similarly, Fig. 4 illustrates that the median posterior differential Gaussian entropy of the

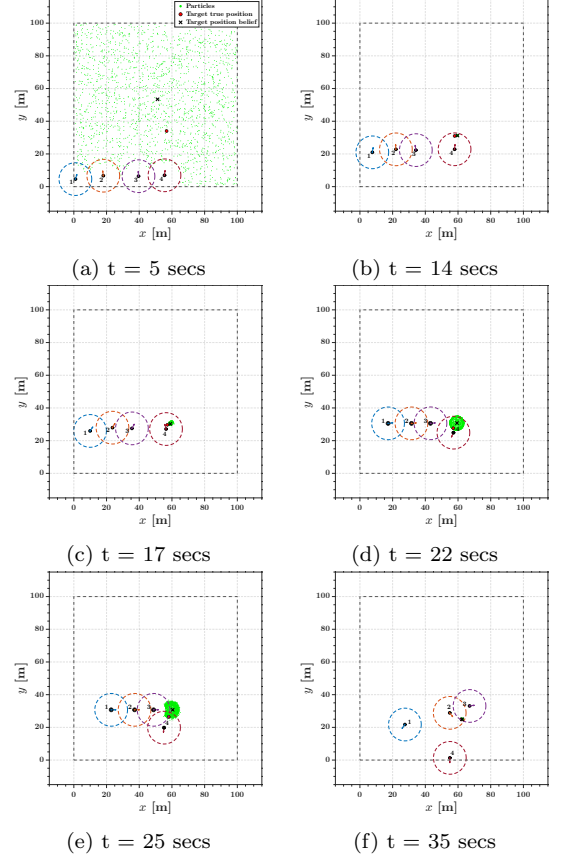


Fig. 2. Mission evolution for target localization using MAN under FDI-attacks: (a) Target search, (b) Initial target localization, (c) FDI attack onset, (d) Recovery-set generation, (e) Post-set recovery maneuver, and (f) Cooperative relocalization. The colored circles represent the agents, and surrounding dashed circles indicate their maximum sensing ranges.

particle-belief converges to a constant value below the entropy threshold faster for Class-I compared to Class-II, as the recovery set is created in Class-II, which expands the entropy post-attack and re-shrinks the belief, thereby requiring more time for relocalization. Additionally, Fig. 3 and 4 compare proposed framework against conventional approach, under which the entropy is observed to remain relatively low despite the high RMSE, indicating that the agents chase a corrupted target belief with unwarranted confidence while the true target escapes.

Figure 5 illustrates the posterior differential Gaussian entropy of target state belief with time relative to initial target-localization, obtained by shifting the Monte Carlo run so the initial localization instant is set to $t = 0$ s. The plot examines the uncertainty evolution of the target estimate after the first localization across two outcome classes. For Class-I the entropy decreases significantly at the instant of the first localization of the target and then converges to a constant value signifying target localization. Similarly, for Class-II, the posterior entropy drops at the time of first localization via attack-prone agents, which spikes back due to the FDI to the sole localizing agent. The entropy then decays to a constant value post-relocalization of the target via attack-immune agents during the recovery phase, signifying the relocalization of the target.

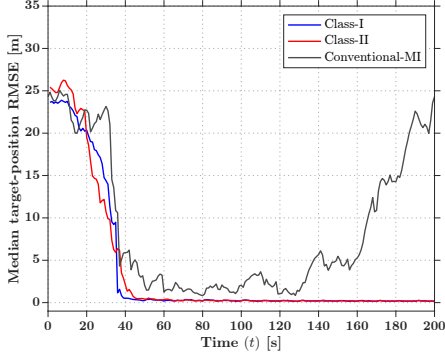


Fig. 3. Median target-position RMSE

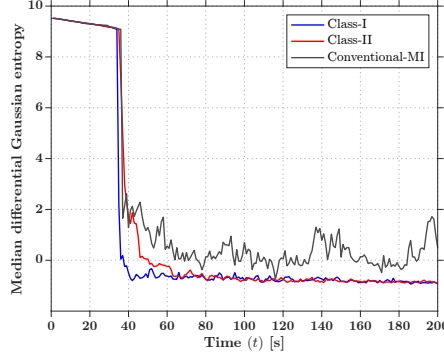


Fig. 4. Median posterior differential Gaussian entropy of target belief

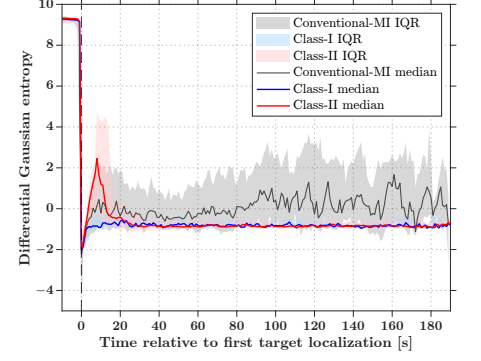


Fig. 5. Posterior differential Gaussian entropy of target-state belief against the relative time for initial target localization

Table 1. Simulation parameters

Parameter	Symbol	Value
Number of particles	N	1500
Target accel input cov	Σ_{ν_T}	$\mathbf{I}_2$
Meas. range std dev	σ_r	0.20 m
Meas. bearing std dev	σ_θ	3°
FDI attack std dev	σ_α	2 m
FDI attack mean	b	15 m
Maximum sensor range	$z_{\max}$	10 m
Agent max speed	$v_{\max}$	1.5 m/s
Target max speed	$v_{T_{\max}}$	0.5 m/s
Agent max accel	$a_{\max}$	0.75 m/s^2
MI grid step	Δz^r	0.25 m
MI time step	dt	1 s
Differential entropy threshold	H_{th}	0
LQR state error penalty	$\mathbf{Q}$	$\text{diag}([10, 10, 5, 5])$
LQR control effort penalty	$\mathbf{R}$	$0.5 \mathbf{I}_2$

6. CONCLUSIONS

The paper presented a resilient multi-agent target localization and tracking framework operating under limited agents' sensing range and FDI attacks. The proposed framework combined mutual information-based navigation and target search, BAG-based attack detection, and reachable set guided recovery to localize the target, and continued target tracking. The result illustrated that the proposed framework maintained localization performance even after the FDI attack on the system. Monte Carlo analysis presented two distinct localization classes: a scenario in which an attack-immune agent localized the target initially, achieving lower median localization time, compared to the scenario where an attack-prone agent localized the target initially, necessitating recovery set formation and relocalization of the target through the attack-immune agent, resulting in higher localization time, and establishing that BAG-based detection is necessary for relocalization under FDI attacks. These results illustrate the effectiveness of the proposed framework and support its relevance for the resilient target-localization applications. Future work includes incorporating sUAV dynamics for the agent to track a dynamic target and extending the framework to a decentralized system with communication constraints.

REFERENCES

- Adhikari, B. and Subbarao, K. (2025). *Optimizing Multi-Agent Network for Target Localization Using Mutual Information Maximization*. doi:10.2514/6.2025-2611.
- Chaulagain, S. and Subbarao, K. (2026). *Resilient Collaborative Target Tracking Using BAG-aware Distributed Kalman Filtering Under Stealthy FDI Attacks*. doi: 10.2514/6.2026-0666.
- Chen, Y., Kar, S., and Moura, J.M.F. (2019). Resilient distributed estimation: Sensor attacks. *IEEE Transactions on Automatic Control*, 64(9), 3772–3779. doi: 10.1109/TAC.2018.2882168.
- Duo, W., Zhou, M., and Abusorrah, A. (2022). A survey of cyber attacks on cyber physical systems: Recent advances and challenges. *IEEE/CAA Journal of Automatica Sinica*, 9(5), 784–800. doi:10.1109/JAS.2022.105548.
- Frigault, M. and Wang, L. (2008). Measuring network security using bayesian network-based attack graphs. In *2008 32nd Annual IEEE International Computer Software and Applications Conference*, 698–703.
- Hoffmann, G.M. and Tomlin, C.J. (2010). Mobile sensor network control using mutual information methods and particle filters. *IEEE Transactions on Automatic Control*, 55(1), 32–47. doi:10.1109/TAC.2009.2034206.
- Kazeminajafabadi, A. and Imani, M. (2023). Optimal monitoring and attack detection of networks modeled by bayesian attack graphs. *Cybersecurity*, 6(1), 22.
- Kravari, K., Roussi, M., Ladomenou, K., Thysiadou, A., and Chalaris, M. (2025). Intelligent agent-based control of distributed sensor networks for environmental monitoring and disaster prediction. *Engineering Proceedings*, 104(1). doi:10.3390/engproc2025104038.
- Muñoz-González, L., Sgandurra, D., Barrère, M., and Lupu, E.C. (2019). Exact inference techniques for the analysis of bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, 16(2), 231–244.
- Patrinopoulou, N., Daramouskas, I., Meimetis, D., Lappas, V., and Kostopoulos, V. (2022). A multi-agent system using decentralized decision-making techniques for area surveillance and intruder monitoring. *Drones*, 6(11). doi:10.3390/drones6110357.
- Saeed, I.A., Selamat, A., Rohani, M.F., Krejcar, O., and Chaudhry, J.A. (2020). A systematic state-of-the-art analysis of multi-agent intrusion detection. *IEEE Access*, 8, 180184–180209.