Hierarchical Average Fusion with GM-PHD Filters Against FDI and DoS Attacks

Hao Yang, Tiancheng Li*, Junkun Yan, *Senior Member, IEEE*, Víctor Elvira, *Senior Member, IEEE*

***Abstract*—We address the multisensor multitarget tracking problem based on a hierarchical sensor network. In this setup, there is a fusion center, several cluster heads, and many sensors. Each sensor runs a Gaussian mixture probability hypothesis density (PHD) filter. The sensors send their locally calculated Gaussian components to the local cluster head in the presence of false data injection (FDI) and denial-of-service (DoS) attackers. We propose a hybrid PHD averaging fusion framework that consists of two parts: one uses the arithmetic average (AA) fusion to compensate for information shortage due to DoS and the other uses the geometric average (GA) fusion to suppress false information due to FDI. By integrating the respective zero forcing and avoiding behaviors of the two average fusion approaches, our proposed hybrid fusion scheme is proven resilient to both FDI and DoS attacks. Experimental results illustrate that our proposed algorithm can provide reliable tracking performance against FDI and DoS attacks.**

***Index Terms*—PHD filter, network attack, average fusion.**

I. Introduction

MULTISENSOR multitarget tracking based on the random finite set (RFS) has attracted great attention in the last decade [1], [2]. Recent mathematical models allow for realistic sensor network structures and more challenging communication environments. In this letter, we consider the hierarchical structure that is usually composed of several clusters of sensors. This type of network has been increasingly deployed due to its flexibility, robustness, and low communication affordability [3], [4]. As shown in Fig. 1, all sensors are connected to a unique cluster head (CH) within their cluster. The CHs fuse the information from local sensors and then send the result to the fusion center (FC) for the global estimate. The communication between CHs and the FC is commonly considered trustable, as they are typically carried out through dedicated wired communication channels. In contrast, the low-cost remote sensors and their CHs are usually linked by wireless lines, which are prone to a number of malicious attacks and may lead to unreliable estimates [5].

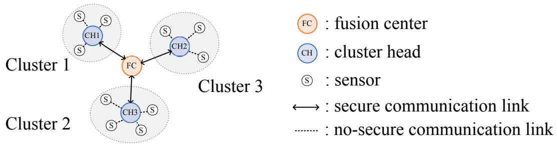


Fig. 1. Illustration of the considered hierarchical sensor network.

We consider attacks on communication links [6], [7]. Two of the most common and representative types of adversarial attacks are the false data injection (FDI) [8]–[10] and the denial-of-service (DoS) jamming attack [11]–[13]. FDI attackers intentionally hijack the data packets from communication links and inject false data packets. In contrast, DoS attackers deliberately block communications by jamming the transmission channel, which will cause packet loss. They correspond to false alarms and miss detections, the most concerning technical challenges in the multitarget tracking problem, respectively. Most existing studies address attack detection and mitigation in the data level, such as the data fusion algorithm [14] to combat FDI attacks and the event-triggered strategy [15] to deal with DoS attacks. Recent works have attempted to cope with attacks in the estimate/posterior level. For example, the FDI injected data are incorporated in the factor graph that describes the statistical structure of the tracking problem. This leads to a belief propagation approach [16] to both FDI and DoS attacks. Based on the RFS framework, the geometric average (GA) fusion approach is used to suppress the random set attacks [5], [17]. Moreover, the arithmetic average (AA) fusion is proven more robust than the GA fusion in the case of data substitution [18]. However, these methods address only packet substitution or injection but not packet loss, using only a single fusion algorithm.

In this paper, we deal with hybrid FDI and DoS attacks by simultaneously employing the AA and GA fusion approaches. In particular, we propose a hybrid average fusion framework for multitarget tracking based on the hierarchical sensor network. This framework makes use of the complementary zero-avoiding and zero-forcing strengths of both AA and GA fusion [19]–[22]: using AA fusion to compensate for information shortage and the GA fusion to suppress false information. To be more specific, we investigate two implementations for the hybrid fusion, namely AA-then-GA and GA-then-AA fusion. The test-bed filter is the Gaussian mixture probability hypothesis density (GM-PHD) filter [23].

The letter is organized as follows. Preliminaries and problem formulation are given in Section II. The proposed AA-then-GA and GA-then-AA fusion frameworks are presented in Section III. Simulation is given in Section IV and conclusion in Section V.

H. Yang and T. Li are with the Key Lab of Information Fusion Technology, School of Automation, Northwestern Polytechnical University, Xi’an 710072, China (e-mail: haoyoung@mail.nwpu.edu.cn; t.c.li@nwpu.edu.cn).

J. Yan is with the National Laboratory of Radar Signal Processing, Xidian University, Xi’an, China (e-mail: jkyan@xidian.edu.cn).

V. Elvira is with the School of Mathematics, University of Edinburgh, UK (email: victor.elvira@ed.ac.uk).

The work is supported in part by the *National Natural Science Foundation* of China (Grant No. 62071389 and 62071345), the *Natural Science Basic Research Program* of Shaanxi (2023JC-XJ-22) and the Fundamental Research Funds for the Central Universities, China. The work of V. E. is supported by ARL/ARO under grant W911NF-22-1-0235.

II. Preliminaries and Problem Formulation

A. System Model

Let us consider that there are N_k targets in the region of interest (ROI) at time k, modeled by an RFS $\mathbf{X}_k = \{\mathbf{x}_{k,1}, \cdots, \mathbf{x}_{k,N_k}\}$ with the random cardinality $N_k = |\mathbf{X}_k|$ [24]. Each target at time $k-1$ may continue to exist or disappear at the next time k with each probability. States of newborn targets are modeled by a Poisson RFS with intensity $\varepsilon_k(\mathbf{x}_k)$.

The considered network structure is shown in Fig.1. Consider that there are N_s sensors and N_h CHs, each CH $h \in \mathcal{H} = \{1, 2, \cdots, N_h\}$ receives Gaussian components (GCs) from $\mathcal{S}_h$, a subset of the sensor set $\mathcal{S} = \{1, 2, \cdots, N_s\}$. The communication links between CHs and FC are considered secure, while the links in clusters are considered vulnerable to be attacked [5]. Given a target with state $\mathbf{x}_k$, sensor s either detects it with probability $p_{s,k}^D$ and generates a measurement $\mathbf{z}_{s,k} \in \mathbf{Z}_{s,k}$ or fails to detect it with probability $1-p_{s,k}^D$, where $\mathbf{Z}_{s,k}$ is the RFS of measurements received by sensor s. For brevity, we omit the notation k in the following.

Based on the standard procedure [23], the GM-PHD obtained synchronously in each sensor s can be written as $f_s(\mathbf{x}) \approx \sum_{i=1}^{J_s} \alpha_s^{(i)} \mathcal{G}\left(\mathbf{x}; \mathbf{m}_s^{(i)}, \mathbf{P}_s^{(i)}\right)$, where $\mathcal{G}(\mathbf{x}; \mathbf{m}, \mathbf{P})$ is referred to a GC with mean $\mathbf{m}$ and covariance $\mathbf{P}$, J_s denotes the number of GCs, and $\alpha_s^{(i)}$ is the weight of the i-th GC [23].

B. FDI and DoS Attacks

Different from [16], we pay special attention to attacks in the estimate/posterior level in this work. The sensors transmit their GCs to CHs through some no-secure communication links. To model the impact of FDI and DoS attacks, we denote by Θ_s the set of GCs generated by the sensor s. γ_s^{FDI} and γ_s^{DoS} are attack indicators, $\gamma_s^{\text{FDI}}/\gamma_s^{\text{DoS}} = 1$ indicates that sensor s is attacked by FDI or DoS attacks, respectively. From the view of the receiver, the set of attacked GCs can be given by

$$\Theta_s^{'} = \Theta_s \bigcup \Theta_s^{\text{FDI}} \setminus \Theta_s^{\text{DoS}}, \tag{1}$$

where Θ_s^{FDI} is the set of false GCs injected by FDI attackers ($\Theta_s^{\text{FDI}} = \varnothing$ when $\gamma_s^{\text{FDI}} = 0$) and Θ_s^{DoS} is the set of lost packets due to DoS attacks ($\Theta_s^{\text{DoS}} = \varnothing$ when $\gamma_s^{\text{DoS}} = 0$) [5].

Furthermore, if an attacker was powerful enough to invade the device and modify the message directly, we can approximately express it by a combination of the above two attacks. For instance, considering the case when an attacker alters the message to a degree where it is utterly unrelated to the original, we would have $\Theta_s^{\text{DOS}} = \Theta_s$ and $\Theta_s^{\text{FDI}} \neq \varnothing$. We further assume that the concerning FDI GCs deviate from the target GCs for the maximum impact on the estimate.

C. AA/GA Fusion and Alpha Divergence

Given PHD $f_s(\mathbf{x})$ and fusion weights $\omega_s > 0$ of sensor s, by minimizing two different directions of the weighted Kullback-Leibler divergence (KLD), the AA and GA fusions have their respective forms [19], [22], [25]–[27]

$$f_{\text{AA}}(\mathbf{x}) = \sum_{s\in\mathcal{L}} \omega_s f_s(\mathbf{x}), \tag{2}$$

$$f_{\text{GA}}(\mathbf{x}) \propto \prod_{s\in\mathcal{L}} (f_s(\mathbf{x}))^{\omega_s}, \tag{3}$$

where $\sum_{s\in\mathcal{L}} \omega_s = 1$, $\mathcal{L} \subset \mathcal{S}$, which is a subset of sensors that participate in the fusion and the result of (3) needs to be specified with the cardinality in order to get the PHD for which we apply the cardinality average approach [21].

Notably, the KLD is a member of the alpha divergence $D_\alpha(f||g) = \frac{4}{1-\alpha^2}\left(1 - \int f(\mathbf{x})^{\frac{1+\alpha}{2}} g(\mathbf{x})^{\frac{1-\alpha}{2}} \delta\mathbf{x}\right)$, where $\alpha \in \mathbb{R}$ is a continuous parameter. When $\alpha \to 1$, the alpha divergence converges to KLD $D_{KL}(f||g)$, and when $\alpha \to -1$, it converges to $D_{KL}(g||f)$ [28]–[31].

D. Zero-Forcing/Avoiding

The concept of zero-forcing/avoiding behavior can be briefly given as follows [22], [30].

Definition 1 (zero-forcing behavior). If $\exists f_s(\mathbf{x}) = 0$, $s \in \mathcal{L}$, then $g(\mathbf{x}) = 0$.

Definition 2 (zero-avoiding behavior). If $\exists f_s(\mathbf{x}) > 0$, $s \in \mathcal{L}$, then $g(\mathbf{x}) > 0$.

Lemma 1. Different from the multitarget probability distribution (MPD) in [22], we discuss it in the PHD domain [32]. Denote the nonzero-interval $\Omega_s^o = \{\mathbf{x} \in \Omega_s^o : f(\mathbf{x}) \neq 0\}$, and the zero-interval $\Omega_s^c = \{\mathbf{x} \in \Omega_s^c : f(\mathbf{x}) = 0\}$. We have:

1) if $f_{\text{GA}}(\mathbf{x}) \neq 0$, then $\mathbf{x} \in \bigcap_{s\in\mathcal{L}} \Omega_s^o$.
2) if $f_{\text{AA}}(\mathbf{x}) \neq 0$, then $\mathbf{x} \in \bigcup_{s\in\mathcal{L}} \Omega_s^o$.

Proof. See AppendixA □

III. Proposed Method

A. Hybrid Fusion: AA-then-GA and GA-then-AA

Given that the rates of false alarm and missed detection in the local filter are insignificant, the GA fusion can suppress false information more effectively, but it is also more susceptible to information shortage. Meanwhile, the AA fusion can cope with information shortage more efficiently, but it is less capable of filtering out false information [19]. Motivated by these observations, we aim to integrate the complementary strength of both fusion methods while avoiding their weaknesses. Given fusion weights ω_h of cluster h, there are two alternative solutions:

Proposition 1 (AA-then-GA fusion). AA fusion is carried out in CHs and GA fusion in the FC, as shown in Fig.2(a), yielding

$$f_{\text{AA-GA}}(\mathbf{x}) \propto \prod_{h\in\mathcal{H}} \left(f_{\text{AA}}^h(\mathbf{x})\right)^{\omega_h}, \tag{4}$$

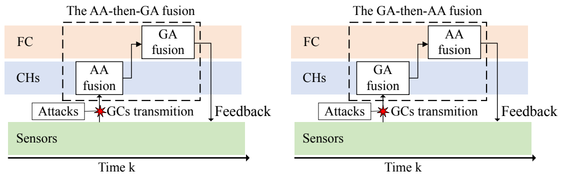
where $f_{\text{AA}}^h(\mathbf{x})$ is the AA fusion result of cluster h, c.f (2).

Proposition 2 (GA-then-AA fusion). GA fusion is carried out in CHs and AA fusion in the FC, as shown in Fig.2(b), yielding

$$f_{\text{GA-AA}}(\mathbf{x}) = \sum_{h\in\mathcal{H}} \omega_h f_{\text{GA}}^h(\mathbf{x}), \tag{5}$$

where $f_{\text{GA}}^h(\mathbf{x})$ is the GA fusion result of cluster h, c.f (3).

The fusion weight of clusters in this work is designed as $\omega_h = \dfrac{|\mathcal{S}_h|}{N_s}$. Obviously, $\sum_{h\in\mathcal{H}} \omega_h = \dfrac{1}{N_s} \sum_{h\in\mathcal{H}} |\mathcal{S}_h| = 1$.



(a) The AA-then-GA fusion. (b) The GA-then-AA fusion.

Fig. 2. Illustration of the proposed hybrid fusion framework

B. Zero-Forcing/Avoiding Behavior Analysis

We model the impact on the nonzero-interval and investigate whether the proposed fusion approach can deal with FDI and DoS attacks. According to (1), for attacked sensor s, the nonzero-interval is changed into $\Omega_s^{o'}$ because of FDI and DoS attacks, which can be given by

$$\Omega_s^{o'} = \Omega_s^o \bigcup \Omega_s^f \setminus \Omega_s^d, \tag{6}$$

where Ω_s^o is the original nonzero-interval before attacks, Ω_s^f is the false state set, and Ω_s^d is the lost state set.

Lemma 2. For the AA-then-GA fusion, if $f_{\text{AA-GA}}(\mathbf{x}) \neq 0$, then $\mathbf{x} \in \psi_{\text{AA-GA}}\left(\Omega_s^o, \Omega_s^f, \Omega_s^d\right) \triangleq \bigcap_{h\in\mathcal{H}}\left(\bigcup_{s\in\mathcal{S}_h}\left(\Omega_s^o \bigcup \Omega_s^f \setminus \Omega_s^d\right)\right)$.

For the GA-then-AA fusion, if $f_{\text{GA-AA}}(\mathbf{x}) \neq 0$, then $\mathbf{x} \in \psi_{\text{GA-AA}}\left(\Omega_s^o, \Omega_s^f, \Omega_s^d\right) \triangleq \bigcup_{h\in\mathcal{H}}\left(\bigcap_{s\in\mathcal{S}_h}\left(\Omega_s^o \bigcup \Omega_s^f \setminus \Omega_s^d\right)\right)$.

Proof. See Appendix B. □

Definition 3 (effective attack). An effective attack is launched if $\psi\left(\Omega_s^o, \Omega_s^f, \Omega_s^d\right) \neq \psi\left(\Omega_s^o\right)$. To be more specific, an effective FDI attack is launched if

$$\psi\left(\Omega_s^o, \Omega_s^f\right) \neq \psi\left(\Omega_s^o\right), \tag{7}$$

and an effective DoS attack is launched if

$$\psi\left(\Omega_s^o, \Omega_s^f\right) \neq \psi\left(\Omega_s^o\right). \tag{8}$$

Lemma 3. For the AA-then-GA fusion, an effective FDI attack is launched when $\bigcap_{h\in\mathcal{H}}\left(\bigcup_{s\in\mathcal{S}_h}\Omega_s^f\right) \neq \varnothing$, while an effective DoS attack is launched when $\bigcup_{h\in\mathcal{H}}\left(\bigcap_{s\in\mathcal{S}_h}\Omega_s^d\right) \neq \varnothing$.

Proof. See Appendix C. □

Lemma 4. For the GA-then-AA fusion, an effective FDI attack is launched when $\bigcup_{h\in\mathcal{H}}\left(\bigcap_{s\in\mathcal{S}_h}\Omega_s^f\right) \neq \varnothing$, while an effective DoS attack is launched when $\bigcap_{h\in\mathcal{H}}\left(\bigcup_{s\in\mathcal{S}_h}\Omega_s^d\right) \neq \varnothing$.

Proof. The proof is omitted here since it follows along the same line as the proof of Lemma 3. □

Remark 1. According to Lemma 3 and 4, it is difficult for FDI or DoS attackers to satisfy the conditions for launching an effective attack to the proposed hybrid fusion fusion approach, demonstrating that our proposed hybrid fusion approaches are resilient to both FDI and DoS attacks.

IV. Simulation

We considered a sensor network that comprises 24 sensors, divided into 8 clusters with 3 sensors in each and the ROI is given by $[-1\text{km}, 1\text{km}] \times [-1\text{km}, 1\text{km}]$ as shown in Fig.3. The newborn target intensity function is $\varepsilon_k(\mathbf{x}) = \sum_{i=1}^4 \lambda_i \mathcal{G}(\mathbf{x}; \mathbf{m}_i, \mathbf{Q})$, where $\lambda_1 = \lambda_2 = \lambda_3 = \lambda_4 = 0.05$, $\mathbf{m}_1 = [0\text{m}, 0\text{m/s}, 0\text{m}, 0\text{m/s}]^T$, $\mathbf{m}_2 = [-500\text{m}, 0\text{m/s}, -500\text{m}, 0\text{m/s}]^T$, $\mathbf{m}_3 = [0\text{m}, 0\text{m/s}, 500\text{m}, 0\text{m/s}]^T$, $\mathbf{m}_4 = [500\text{m}, 0\text{m/s}, -500\text{m}, 0\text{m/s}]^T$, $\mathbf{Q} = \text{diag}\{400\text{m}^2, 100\text{m}^2/\text{s}^2, 400\text{m}^2, 100\text{m}^2/\text{s}^2\}$. The target intensity function spawn from the target $\mathbf{u}$ is given by $b_k(\mathbf{x}|\mathbf{u}) = 0.05 \cdot \mathcal{G}(\mathbf{x}; \mathbf{u}, \mathbf{Q}_r)$, where $\mathbf{Q}_r = \text{diag}\left\{100\text{m}^2, 400\text{m}^2/s^2, 100\text{m}^2, 400\text{m}^2/s^2\right\}$. The target survival probability is 0.99 and the survival targets follow a nearly constant velocity motion, i.e. $\mathbf{x}_k = \mathbf{F}\mathbf{x}_{k-1} + \mathbf{G}\mathbf{u}_k$, where $\mathbf{F} \in \mathbb{R}^{4\times 4}$ and $\mathbf{G} \in \mathbb{R}^{4\times 2}$, given by [33, Eq. (14)]. The process noise $\mathbf{u}_k \sim \mathcal{G}\left(\text{u}; \mathbf{0}_2\text{m/s}^2, 10\mathbf{I}_2\text{m}^2/\text{s}^4\right)$ and the sampling interval $\Delta = 1$s.

The observation model is the same as given in [34, Eq. (31)], where $\mathbf{v}_{k,1}$ and $\mathbf{v}_{k,2}$ are mutually independent zero-mean Gaussian noise with the same standard deviation of 20 m. Clutters are uniformly distributed with clutter intensity $\kappa_k = 10/\left(2000^2\right)$. Denote the attack rates $\delta_{\text{FDI}} \triangleq \left|\Theta_s^{\text{FDI}}\right|$, and $\delta_{\text{DoS}} \triangleq \left|\Theta_s^{\text{DoS}}\right|$ for the FDI and DoS attacks, respectively. $P(\delta_{\text{FDI}} = \delta_i) = \frac{1}{2}$ and $P(\delta_{\text{DoS}} = \delta_i) = \frac{1}{2}$, where $\delta_i = 1, 2$. The injected GCs are randomly selected from the false GC set $\mathcal{A} = \{\mathcal{G}(\mathbf{x}; \mathbf{m}_j, \mathbf{Q}_a), j = 1, 2, 3\}$, where $\mathbf{m}_1 = [0\text{m}, 0\text{m/s}, 0\text{m}, 0\text{m/s}]^T$, $\mathbf{m}_2 = [-800\text{m}, 0\text{m/s}, -800\text{m}, 0\text{m/s}]^T$, $\mathbf{m}_3 = [800\text{m}, 0\text{m/s}, 800\text{m}, 0\text{m/s}]^T$, $\mathbf{Q}_a = \text{diag}\{100\text{m}^2, 100\text{m}^2/\text{s}^2, 100\text{m}^2, 100\text{m}^2/\text{s}^2\}$.

A. Performance under FDI Attacks

The proposed hybrid fusion approaches are compared with the AA-then-AA fusion (AA fusion in both CHs and the FC) and GA-then-GA fusion (GA fusion in both CHs and the FC). In addition, we implement a non-cooperative (NC) protocol that adopts no inter-node interaction. The optimal subpattern assignment (OSPA) distance [35] is used to evaluate the estimation error with cutoff parameter $c = 1000$ m and order parameter $p = 2$. We fix the false alarm rate as 5 and the detection probability as 0.95. Fig. 4(a) shows the network OSPA error performance under FDI attacks, with attack probability varying from 0 to 0.3 during the communication between sensors and CHs. It indicates that the proposed AA-then-GA and GA-then-AA fusion get lower OSPA errors in comparison with the other methods, regardless of the attack probability.

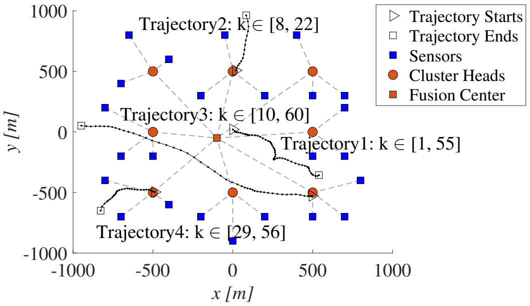
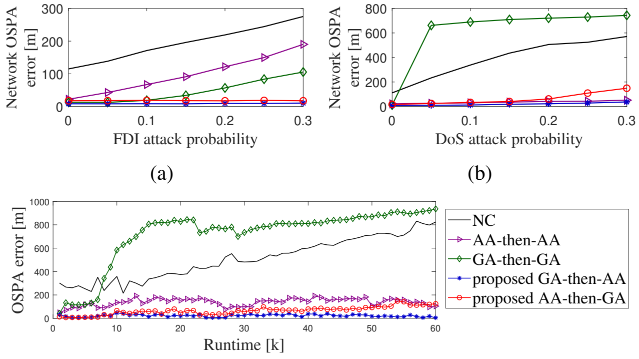


Fig. 3. The hierarchical sensor network topology and the trajectories of four targets with starting and ending times noted.



(a) (b)

(c)

Fig. 4. OSPA errors under different attacks: (a) FDI attacks. (b) DoS attacks. (c) hybrid FDI and DoS attacks.

B. Performance under DoS Attacks

In this case, we perform the abovementioned approaches under DoS attacks with attack probability varying from 0 to 0.3. The false alarm rate and detection probability are the same as the previous case. Fig. 4(b) shows the network OSPA error performance under DoS attacks. The results show that the GA-then-GA fusion performs badly and even becomes ineffective under DoS attacks, due to the cardinality inconsistency problem of the GA fusion [36], [37]. The GA-then-AA, AA-then-GA, and AA-then-AA approaches perform well under DoS attacks. However, the AA-then-AA approach achieves slightly better performance than the AA-then-GA approach, which confirms that the AA fusion has an advantage in dealing with information shortage [19].

C. Performance under Hybrid Attacks

In this case, we evaluate the average OSPA errors over 100 runs in which both attacks happen concurrently, with 0.2 attack probabilities fixed for each. Besides, one sensor is injected a false GC $a_0 = 0.5 \cdot \mathcal{G}(\mathbf{x};\mathbf{m}_0,\mathbf{Q}_a)$ with probability 0.2, where $\mathbf{m}_0 \sim \mathcal{G}(\mathbf{m};\mathbf{x}_{k,1},\mathbf{Q}_m)$ and $\mathbf{Q}_m = \text{diag}\{100\text{m}^2, 100\text{m}^2/\text{s}^2, 100\text{m}^2, 100\text{m}^2/\text{s}^2\}$ from time 30 to 40. From time 40 to 50, the mean of $\mathbf{m}_0$ deviates from the target $\mathbf{x}_{k,1}$ with a constant offset $[20\text{m/s}, 0\text{m/s}^2, 20\text{m/s}, 0\text{m/s}^2]^T$ per filtering step. The result is given in Fig.4(c), which demonstrates that our approaches are superior to AA-then-AA and GA-then-GA fusion when the network faces both forms of attacks simultaneously. We also note that the performance of the AA-then-GA and GA-then-AA depends on the network topology, which will be discussed in our future work.

V. Conclusion

In this letter, two fusion approaches to GM-PHD filter cooperation based on the hierarchical sensor network, namely AA-then-GA and GA-then-AA fusion, are proposed to deal with false information and information shortage caused by FDI and DoS attacks, respectively. Zero-forcing/avoiding behavior of the proposed approach has been analyzed. The numerical results demonstrated the effectiveness of our proposed algorithm which is proven resilient to both FDI and DoS attacks.

Appendix A
Proof of Lemma 1

Proof. For the GA fusion, $f_{\text{GA}}(\mathbf{x}) \propto \prod_{s\in\mathcal{L}} (f_s(\mathbf{x}))^{\omega_s}$, if $f_{\text{GA}}(\mathbf{x}) \neq 0$, we have $f_s(\mathbf{x}) \neq 0$, then $\mathbf{x} \in \bigcap_{s\in\mathcal{L}} \Omega_s^o$. For the AA fusion, consider the contrapositive: "if $\mathbf{x} \notin \bigcup_{s\in\mathcal{L}} \Omega_s^o$, then $f_{\text{AA}}(\mathbf{x}) = 0$", when $\mathbf{x} \notin \bigcup_{s\in\mathcal{L}} \Omega_s^o$, $f_s(\mathbf{x}) = 0$, then $f_{\text{AA}}(\mathbf{x}) = \sum_{s\in\mathcal{L}} \omega_s f_s(\mathbf{x}) = 0$. □

Appendix B
Proof of Lemma 2

Proof. For the AA-then-GA fusion, in the CH h where the AA fusion is performed, from Lemma 1, if $f_{\text{AA}}^h(\mathbf{x}) \neq 0$, then $\mathbf{x} \in \bigcup_{s\in\mathcal{S}_h} \Omega_s^{o'} = \bigcup_{s\in\mathcal{S}_h} \left(\Omega_s^o \bigcup \Omega_s^f \setminus \Omega_s^d\right)$. In the FC where the GA fusion is performed, from Lemma 1, if $f_{\text{AA-GA}}(\mathbf{x}) \neq 0$, then $\mathbf{x} \in \bigcap_{h\in\mathcal{H}} \left(\bigcup_{s\in\mathcal{S}_h} \left(\Omega_s^o \bigcup \Omega_s^f \setminus \Omega_s^d\right)\right)$.

For the GA-then-AA fusion, in the CH h where the GA fusion is performed, from Lemma 1, if $f_{\text{GA}}^h(\mathbf{x}) \neq 0$, then $\mathbf{x} \in \bigcap_{s\in\mathcal{S}_h} \Omega_s^{o'} = \bigcap_{s\in\mathcal{S}_h} \left(\Omega_s^o \bigcup \Omega_s^f \setminus \Omega_s^d\right)$. In the FC, perform the AA fusion where Lemma 1 is performed, if $f_{\text{GA-AA}}(\mathbf{x}) \neq 0$, then $\mathbf{x} \in \bigcup_{h\in\mathcal{H}} \left(\bigcap_{s\in\mathcal{S}_h} \left(\Omega_s^o \bigcup \Omega_s^f \setminus \Omega_s^d\right)\right)$. □

Appendix C
Proof of Lemma 3

Proof. For the AA-then-GA fusion, according to Lemma 2 and Definition 3, an effective FDI attack is launched when

$$\bigcap_{h\in\mathcal{H}} \left(\bigcup_{s\in\mathcal{S}_h} \left(\Omega_s^o \bigcup \Omega_s^f\right)\right) \neq \bigcap_{h\in\mathcal{H}} \left(\bigcup_{s\in\mathcal{S}_h} \Omega_s^o\right). \tag{9}$$

Given that rates of false alarm and missed detection in the local filter are insignificant, we use Ω^o to approximate Ω_s^o. (9) is approximately equivalent to

$$\bigcap_{h\in\mathcal{H}} \left(\bigcup_{s\in\mathcal{S}_h} \left(\Omega^o \bigcup \Omega_s^f\right)\right) \neq \Omega^o. \tag{10}$$

The left hand side (LHS) of (10) can be further derived as

$$\begin{aligned} \text{LHS} &= \bigcap_{h\in\mathcal{H}} \left(\Omega^o \bigcup \left(\bigcup_{s\in\mathcal{S}_h} \Omega_s^f\right)\right) \\ &= \Omega^o \bigcup \left(\bigcap_{h\in\mathcal{H}} \left(\bigcup_{s\in\mathcal{S}_h} \Omega_s^f\right)\right) \neq \text{RHS (right hand side)}. \end{aligned}$$

The injected GCs usually have different means from the original GCs, i.e., $\Omega^o \bigcap \Omega_s^f = \varnothing$, so $\Omega^o \bigcap \left(\bigcap_{h\in\mathcal{H}} \left(\bigcup_{s\in\mathcal{S}_h} \Omega_s^f\right)\right) = \varnothing$, we have $\bigcap_{h\in\mathcal{H}} \left(\bigcup_{s\in\mathcal{S}_h} \Omega_s^f\right) \neq \varnothing$.

For the AA-then-GA fusion, according to Lemma 2 and Definition 3, an effective DoS attack is launched when

$$\bigcap_{h\in\mathcal{H}} \left(\bigcup_{s\in\mathcal{S}_h} \left(\Omega_s^o \setminus \Omega_s^d\right)\right) \neq \bigcap_{h\in\mathcal{H}} \left(\bigcup_{s\in\mathcal{S}_h} \Omega_s^o\right). \tag{11}$$

Use Ω^o to approximate Ω_s^o, we have

$$\bigcap_{h\in\mathcal{H}} \left(\bigcup_{s\in\mathcal{S}_h} \left(\Omega^o \setminus \Omega_s^d\right)\right) \neq \Omega^o. \tag{12}$$

The LHS of (12) can be further derived as

$$\begin{aligned} \text{LHS} &= \bigcap_{h\in\mathcal{H}} \left(\bigcup_{s\in\mathcal{S}_h} \left(\Omega^o \bigcap \overline{\Omega_s^d}\right)\right) \\ &= \bigcap_{h\in\mathcal{H}} \left(\Omega^o \bigcap \left(\bigcup_{s\in\mathcal{S}_h} \overline{\Omega_s^d}\right)\right) \\ &= \Omega^o \bigcap \left(\bigcap_{h\in\mathcal{H}} \left(\bigcup_{s\in\mathcal{S}_h} \overline{\Omega_s^d}\right)\right) \\ &= \Omega^o \bigcap \overline{\left(\bigcup_{h\in\mathcal{H}} \left(\bigcap_{s\in\mathcal{S}_h} \Omega_s^d\right)\right)} \\ &= \Omega^o \setminus \left(\bigcup_{h\in\mathcal{H}} \left(\bigcap_{s\in\mathcal{S}_h} \Omega_s^d\right)\right) \neq \text{RHS}. \end{aligned} \tag{13}$$

Since $\Omega_s^d \subseteq \Omega^o$, $\bigcup_{h\in\mathcal{H}} \left(\bigcap_{s\in\mathcal{S}_h} \Omega_s^d\right) \subseteq \Omega^o$, we have $\bigcup_{h\in\mathcal{H}} \left(\bigcap_{s\in\mathcal{S}_h} \Omega_s^d\right) \neq \varnothing$. □

References

[1] B.-N. Vo, M. Mallick, Y. Bar-shalom, S. Coraluppi, R. Osborne, R. Mahler, and B.-T. Vo, "Multitarget tracking," in *Wiley Encyclopedia of Electrical and Electronics Engineering*. John Wiley & Sons, 2015.

[2] T. Li, K. Da, H. Fan, and B. Yu, "Multisensor random finite set information fusion advances, challenges, and opportunities," in *Secure and Digitalized Future Mobility*, Y. Cao, O. Kaiwartya, and T. Li, Eds. Boca Raton: CRC Press, 2022, ch. 3, pp. 32–63.

[3] H. Song, W.-A. Zhang, and L. Yu, "Hierarchical fusion in clustered sensor networks with asynchronous local estimates," *IEEE Signal Processing Letters*, vol. 21, no. 12, pp. 1506–1510, 2014.

[4] W.-A. Zhang and L. Shi, "Sequential fusion estimation for clustered sensor networks," *Automatica*, vol. 89, pp. 358–363, 2018.

[5] N. Forti, G. Battistelli, L. Chisci, S. Li, B. Wang, and B. Sinopoli, "Distributed joint attack detection and secure state estimation," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 96–110, 2017.

[6] F. Sun, Z. Zhao, Z. Fang, L. Du, Z. Xu, and D. Chen, "A review of attacks and security protocols for wireless sensor networks," *Journal of Networks*, vol. 9, no. 5, p. 1103, 2014.

[7] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," 2006.

[8] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter," *IEEE transactions on control of network systems*, vol. 1, no. 4, pp. 370–379, 2014.

[9] A. Sargolzaei, K. Yazdani, A. Abbaspour, C. D. Crane III, and W. E. Dixon, "Detection and mitigation of false data injection attacks in networked control systems," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4281–4292, 2019.

[10] L. Guo, H. Yu, and F. Hao, "Optimal allocation of false data injection attacks for networked control systems with two communication channels," *IEEE Transactions on Control of Network Systems*, vol. 8, no. 1, pp. 2–14, 2020.

[11] H. Zhang, Y. Qi, J. Wu, L. Fu, and L. He, "Dos attack energy management against remote state estimation," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 1, pp. 383–394, 2016.

[12] C. De Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Transactions on Automatic Control*, vol. 60, no. 11, pp. 2930–2944, 2015.

[13] T. Park, D. Cho, H. Kim *et al.*, "An effective classification for dos attacks in wireless sensor networks," in *2018 Tenth international conference on ubiquitous and future networks (ICUFN)*. IEEE, 2018, pp. 689–692.

[14] C. Yang, L. Feng, H. Zhang, S. He, and Z. Shi, "A novel data fusion algorithm to combat false data injection attacks in networked radar systems," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 125–136, 2018.

[15] N. Zhao, P. Shi, W. Xing, and C. P. Lim, "Event-triggered control for networked systems under denial of service attacks and applications," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 69, no. 2, pp. 811–820, 2021.

[16] Y. Yu and Y. Liang, "Multisensor-multitarget tracking based on belief propagation against false data injection attacks and denial of service attacks," *Digital Signal Processing*, vol. 126, p. 103502, 2022.

[17] ——, "Secure multitarget tracking over decentralized sensor networks with malicious cyber attacks," *Digital Signal Processing*, vol. 117, p. 103132, 2021.

[18] L. Gao, G. Battistelli, and L. Chisci, "Resilience of multi-object density fusion against cyber-attacks," in *2022 11th International Conference on Control, Automation and Information Sciences (ICCAIS)*. IEEE, 2022, pp. 7–12.

[19] T. Li, H. Fan, J. García, and J. M. Corchado, "Second-order statistics analysis and comparison between arithmetic and geometric average fusion: Application to multi-sensor target tracking," *Information Fusion*, vol. 51, pp. 233–243, 2019.

[20] G. Koliander, Y. El-Laham, P. M. Djurić, and F. Hlawatsch, "Fusion of probability density functions," *Proceedings of the IEEE*, vol. 110, no. 4, pp. 404–453, 2022.

[21] T. Li, F. Hlawatsch, and P. M. Djurić, "Cardinality-consensus-based phd filtering for distributed multitarget tracking," *IEEE Signal Processing Letters*, vol. 26, no. 1, pp. 49–53, 2018.

[22] K. Da, T. Li, Y. Zhu, and Q. Fu, "Gaussian mixture particle jump-markov-cphd fusion for multitarget tracking using sensors with limited views," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 6, pp. 605–616, 2020.

[23] B.-N. Vo and W.-K. Ma, "The gaussian mixture probability hypothesis density filter," *IEEE Transactions on signal processing*, vol. 54, no. 11, pp. 4091–4104, 2006.

[24] R. P. Mahler, *Statistical multisource-multitarget information fusion*. Artech House Norwood, MA, USA, 2007, vol. 685.

[25] K. Da, T. Li, Y. Zhu, H. Fan, and Q. Fu, "Kullback-leibler averaging for multitarget density fusion," in *International Symposium on Distributed Computing and Artificial Intelligence*. Springer, 2019, pp. 253–261.

[26] T. Li, Y. Song, E. Song, and H. Fan, "Arithmetic average density fusion - part I: Some statistic and information-theoretic results," *Information Fusion*, vol. 104, p. 102199, 2024.

[27] W. Yi, G. Li, and G. Battistelli, "Distributed multi-sensor fusion of phd filters with different sensor fields of view," *IEEE Transactions on Signal Processing*, vol. 68, pp. 5204–5218, 2020.

[28] S. M. Ali and S. D. Silvey, "A general class of coefficients of divergence of one distribution from another," *Journal of the Royal Statistical Society: Series B (Methodological)*, vol. 28, no. 1, pp. 131–142, 1966.

[29] S.-i. Amari, "Differential geometry of statistical models," *Differential-Geometrical Methods in Statistics*, pp. 11–65, 1985.

[30] T. Minka *et al.*, "Divergence measures and message passing," Citeseer, Tech. Rep., 2005.

[31] C. M. Bishop and N. M. Nasrabadi, *Pattern recognition and machine learning*. Springer, 2006, vol. 4, no. 4.

[32] T. Li, R. Yan, K. Da, and H. Fan, "Arithmetic average density fusion - part III: Heterogeneous unlabeled and labeled RFS filter fusion," *IEEE Transactions on Aerospace and Electronic Systems*, 2023, dOI: 10.1109/TAES.2023.3334223.

[33] X. R. Li and V. P. Jilkov, "Survey of maneuvering target tracking. part i. dynamic models," *IEEE Transactions on aerospace and electronic systems*, vol. 39, no. 4, pp. 1333–1364, 2003.

[34] T. Li, J. M. Corchado, and S. Sun, "Partial consensus and conservative fusion of gaussian mixtures for distributed phd fusion," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 5, pp. 2150–2163, 2018.

[35] D. Schuhmacher, B.-T. Vo, and B.-N. Vo, "A consistent metric for performance evaluation of multi-object filters," *IEEE transactions on signal processing*, vol. 56, no. 8, pp. 3447–3457, 2008.

[36] J. Wei, F. Luo, S. Chen, and J. Qi, "Robust fusion of gm-phd filters based on geometric average," *Signal Processing*, vol. 206, p. 108912, 2023.

[37] M. Üney, J. Houssineau, E. Delande, S. J. Julier, and D. E. Clark, "Fusion of finite-set distributions: Pointwise consistency and global cardinality," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 6, pp. 2759–2773, 2019.