Distributed Multiple Attacks Detection via Consensus AA-GMPHD Filter

Chaoqun Yang, *Member, IEEE*, Xianghui Cao, *Senior Member, IEEE*, Lidong He, *Member, IEEE*, and Heng Zhang, *Member, IEEE*

***Abstract*—This article is concerned with the problem of multiple attacks detection (MAD) for distributed sensor networks (SNs) under multiple malicious attacks. The goal of this article is to develop an effective method capable of simultaneously detecting multiple attacks in distributed SNs. By integrating the theories of random finite set (RFS), fusion rules, and consensus, a novel distributed filter named consensus arithmetic average Gaussian mixture probability hypothesis density (AA-GMPHD) filter is proposed in this article, which can achieve the simultaneous detection of multiple attacks in the context of distributed SNs. The main contribution of this article, lies in the proposed consensus AA-GMPHD filter that solves the MAD problem in distributed SNs for the first time. Simulation experiments confirm the effectiveness of the proposed filter for the distributed MAD problem in the context of distributed SNs.**

***Index Terms*—Arithmetic average (AA) fusion, consensus, distributed sensor networks (SNs), multiple attacks detection (MAD), probability hypothesis density (PHD) filter.**

List of Abbreviations

AA	Arithmetic average.
AA-GMPHD	Arithmetic average Gaussian mixture probability hypothesis density.
DL	Deep learning.
GCI	Generalized covariance intersection.
GM	Gaussian mixture.
GMPHD	Gaussian mixture probability hypothesis density.
MAD	Multiple attacks detection.
OSPA	Optimal subpattern assignment.
PHD	Probability hypothesis density.
RFS	Random finite set.
SMC	Sequential Monte Carlo.
SN	Sensor network.

Manuscript received 14 April 2023; accepted 19 July 2023. This work was supported in part by the Start-Up Research Fund of Southeast University under Grant RF1028623002; in part by the National Natural Science Foundation of China under Grant 61973163, Grant 92067111, and Grant 61873106; and in part by the Fundamental Research Funds for the Central Universities under Grant MCCSE2023B02. This article was recommended by Associate Editor J. A. Lozano. *(Corresponding author: Xianghui Cao.)*

Chaoqun Yang is with the School of Automation, Southeast University, Nanjing 210096, China (e-mail: ycq@seu.edu.cn).

Xianghui Cao is with the School of Automation and the School of Cyber Science and Engineering, Southeast University, Nanjing 210096, China (e-mail: xhcao@seu.edu.cn).

Lidong He is with the School of Automation, Nanjing University of Science and Technology, Nanjing 210094, China (e-mail: lidonghe@njust.edu.cn).

Heng Zhang is with the School of Computer Engineering, Jiangsu Ocean University, Lianyungang 222000, China (e-mail: zhangheng@jou.edu.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSMC.2023.3298646.

Digital Object Identifier 10.1109/TSMC.2023.3298646

I. Introduction

NOWADAYS, SNs have found widespread applications in various fields, e.g., industrial processes monitoring [1], [2], intelligent transportation [3], [4], localization, tracking [5], [6], etc. Although SNs usually have a variety of topologies for different applications or scenarios, generally speaking, according to whether a central authority (i.e., fusion center) exists or not, the topologies of SNs fall into three categories: 1) centralized; 2) decentralized; and 3) distributed [7], [8]. In centralized topology, individual sensors have to communicate with a central authority to communicate with each other [9]. In decentralized topology, there are multiple authorities that serve as a central authority for a subsection of sensors [10]. Distributed topology, refers to a network topology where each sensor can communicate with one another without going through a central authority [11]. In comparison with the SNs with centralized or decentralized topologies, the main differences of the distributed SNs lie in the lack of the central authority and the feature that they are composed of equal and interconnected sensors. Thus, the distributed SNs are more flexible, transparent, scalable, and fault tolerant [12].

Since SNs are being incorporated into more and more critical infrastructure hardware and applications, their security is becoming a pressing issue, and it is of great importance to protect them from malicious attacks by detecting these attacks accurately and quickly. In addition, from the perspective of malicious attackers, in their pursuit of increasing the likelihood of success and maximizing the impact of their attacks, they tend to employ a cooperate strategies, simultaneously launching multiple attacks [13]. For example, on 7 February 2022, Vodafone Portugal suffered from multiple cyber attacks, resulting in mobile networks offline overnight [14]. Based on the white paper recently released by Sophos, the problem of multiple attackers has emerged as a prominent and imminent threat [15], [16]. Thus, it is urgent to deal with the problem of MAD for SNs.

Moreover, from the perspective of the SN's supervisor, it is also meaningful to accurately detect multiple attacks. First, global detection of multiple attacks plays a pivotal role in comprehending and profiling the behaviors of attackers, which

not only aids in the detection and prediction of attacks but also contributes significantly to mitigating the damage to the SN [17]. Second, the global detection of multiple attacks also provides the direction for designing defensive strategies against potential attacks. However, it is much more difficult to detect multiple attacks simultaneously in a distributed SN. The reasons are twofold, on the one hand, due to the lack of central authority, the only way the distributed SN's supervisor can get global detection information is through individual sensors, but it is intractable for individual sensors to achieve the comprehensive detection of multiple attacks. On the other hand, for the MAD problem, both the number of attacks and all of the attacked sensors need to be accurately and simultaneously detected.

Although numerous studies have been dedicated to attack detection for SNs or other similar systems so far [18], [19], [20], [21], [22], [23], most of them are carried out in the context of centralized or decentralized topologies. As a contrast, few existing methods have been proposed to cope with the problem on how to detect an attack in the distributed SNs. Moreover, it is also worth noting that rare work has investigated the MAD problem for distributed SNs.

Motivated by this, this article devotes to developing an effective MAD algorithm to simultaneously multiple attacks in distributed SNs. To this end, we first inherit our previous idea of detecting multiple attacks by means of the RFS theory [24], and utilize the PHD filter to obtain the local detections of individual sensors. Second, we introduce AA fusion rule to cope with the problem on how to fuse local detections. Third, consensus is exploited at individual sensors to achieve the agreement on the global detection over the entire distributed SNs.

By integrating the theories of RFS, fusion rules and consensus, we propose a novel distributed filter named consensus AA-GMPHD filter for the distributed MAD problem. In comparison with the existing works on distributed attacks detection [25], [26], [27], [28], [29], [30], the proposed filter is not only capable of simultaneously detecting the number of attacks and individual attacked sensors but also does not require the knowledge of the entire topologies, which is suitable for the distributed SNs. In comparison with the existing works on distributed RFS-based fusion [12], [31], the proposed filter overcomes cardinality inconsistency [32], and poses obvious advantages in computation efficiency, which is suitable for distributed SNs composed of sensors with limited sensing and processing capabilities.

In summary, the main contribution of this article lies in the proposed consensus AA-GMPHD filter that solves the MAD problem in distributed SNs for the first time. Meanwhile, to the best of our knowledge, the proposed consensus AA-GMPHD filter is the first work on distributed detection algorithms against multiple attacks.

The remainder of this article is organized as follows. Section II provides a brief overview of related work. Section III presents the preliminaries on notations description and the RFS theory. Section IV formulates the distributed MAD problem by means of the RFS theory. Section V describes the proposed consensus AA-GMPHD filter in detail. Numerical simulations are provided in Section VI, followed by conclusions in Section VII.

II. Related Work

Numerous studies have been dedicated to attack detection for SNs or other similar systems so far [18], [19], [20]. However, most of them are carried out in the context of centralized or decentralized topologies. As a contrast, up to now, few existing methods have been proposed to cope with distributed attack detection. According to the target of attacks, these methods can be divided into three categories: 1) the methods against the attacks targeting the network layer; 2) the methods against the attacks targeting the physical layer; and 3) the methods against the attacks targeting both the network layer and the physical layer.

For the methods against the attacks targeting the network layer, Boem et al. studied the problem of detecting cyber attacks in communication links for distributed control system, and designed a distributed detection architecture that does not require the knowledge of the global topologies [25]. In the designed architecture, cyber attacks are formulated as faults in communication links, and a threshold-based local detection scheme is developed, and consensus-based control is used to improve the accuracy of detection. Gallo et al. proposed a distributed architecture capable of detecting attacks for linear large scale systems, which consists of two models, i.e., a Luenberger observer for estimating the state of local subsystems and a bank of unknown-input observer for estimating the states of neighboring subsystems [26]. By combining the estimated results from the two models, the proposed architecture is capable of detecting cyber attacks targeting communication layers.

For the methods against the attacks targeting the physical layer, Shi et al. proposed [27] a distributed data-driven method to detect stealthy false data injection attack in multi-area interconnected power systems. In this method, each area first estimates the local state of the entire system via distributed state estimation algorithms, and then the estimated local state is taken as the input of a trained neural network to detect the stealthy false data injection attack. Rathore and Park [28], a fog-based framework for distributed attack detection in Internet of Things (IoT) systems was proposed. By analyzing the data from each IoT device, the fog node connected to the IoT device is capable of detecting attacks on this IoT device.

For the methods against the attacks targeting both the network layer and the physical layer, Adepu and Mathur [29] proposed a distributed attack detection method by means of the concept of "process invariant." Unlike most existing methods that rely on state estimation, the proposed method is based on the observation of real-time systems and the consistent relationships between state variables. Guan and Ge [30] proposed a distributed attack detection estimator to cope with the problem of joint attack detection and secure estimation when both the network layer and the physical layer are under attacks. The proposed estimator first runs a two-step mechanism to detect the attacks targeting the physical layer, and

then uses the compensated measurements to alleviate the effect caused by the attacks targeting the network layer.

Although the above work has advanced the study of distributed attack detection significantly, there are still some limitations. First, the mentioned work is referred to as "distributed," but the system topologies considered in most of them are not exactly matched the definition of distributed topologies, sensors or nodes in the considered system topologies are not completely equal. Second, except for the remarkable works in [25], [26], and [27], most of them still require the knowledge of the entire topologies, which is usually inaccessible for distributed SNs. Meanwhile, it is also worth noting that little work has been done on the MAD problem for SNs or other similar systems. Among them, Li et al. [13] first addressed this problem and proposed an algebraic approach to detect multiple attacks aiming at communication channels. The works in [24] copied with the simultaneous detection of the number of attacks and the attacked sensors. Nevertheless, the systems considered in [13] and [24] are based on centralized topologies. As far as the authors' know, there is rare research on the MAD problem for the SNs or other similar systems with distributed topologies. In a word, the above limitations motivate our research on the MAD problem for distributed SNs.

III. Preliminaries

A. Notations

Throughout this article, we use the following notations. Scalars and variables are denoted by small letters (e.g., x). matrices are represented by capital letters (e.g., H). RFSs are represented by capital Greek letters (e.g., Ω). Spaces are represented by blackboard bold letters (e.g., $\mathbb{X}$). The floor function that outputs the greatest integer that is no more than x is denoted by $\lfloor x \rfloor$. $\mathbb{N}(x; m, P)$ represents the Gaussian probability density function (PDF) with mean m and covariance P.

B. RFS Theory

In essence, an RFS like $\Omega = \{x_1, x_2, \ldots, x_n\}$ can be treated as a set-valued random variable [33]. Given the following definition of set integral:

$$\int f(\Omega)d\Omega = f(\emptyset) + \sum_{n=1}^{\infty} \frac{1}{n!} \int f(\{x_1, \ldots, x_n\})dx_1 \cdots dx_n \tag{1}$$

the statistical characteristics of the RFS Ω can be entirely captured by its multiobject PDF $f(\Omega)$ with $\int f(\Omega)d\Omega = 1$. Usually, the number of the elements in the RFS Ω, denoted as $|\Omega|$, is called the cardinality of Ω.

A Poisson RFS is an RFS with

$$\begin{aligned} f(\Omega) &= e^{-\lambda} \prod_{x\in\Omega} \lambda p(x) \\ &= e^{-\int v(x)dx} \prod_{x\in\Omega} v(x) \end{aligned} \tag{2}$$

where λ denotes the expected cardinality of Ω, $p(x)$ is the independent identically distributed (IID) PDF that all elements subject to, and $v(x) = \lambda p(x)$ is the PHD of the Poisson RFS Ω [32], [33]. According to (2), one can find that the multiobject PDF of an Poisson RFS only depends on its PHD. Thus, a Poisson RFS is completely characterized by its PHD [32]. The propagation of Poisson RFSs in the multiobject Bayesian estimation is at the core of the PHD filter [32], in which the posterior multiobject state is assumed to follow a Poisson RFS. The PHD filter will be introduced in the following sections.

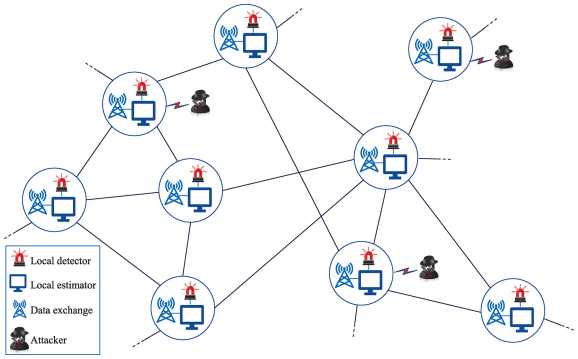

Fig. 1. Illustration of a distributed SN under multiple attacks.

IV. RFS-Based Problem Formulation

As shown in Fig. 1, consider a distributed SN, which consists of numerous heterogeneous and geographically distributed sensors connected by wireless communication links [12], [31]. Thereinto, each sensor has the limited capacities of local detection, local estimation, and data exchange with its neighbors, whereas it has no knowledge of the entire topology.

For simplicity, each sensor is identified by an ordered index j, where $j \in \mathbb{X}$ and $\mathbb{X}$ is the discrete space for all sensors' indices. This SN can be abstractly described by a directed graph $\mathcal{G} = (\mathcal{N}, \mathcal{A})$. Thereinto, $\mathcal{N}$ and $\mathcal{A}$ represent the set of sensors and the set of communication links, respectively, $|\mathcal{N}|$ denotes the number of sensors, and $(i, j) \in \mathcal{A}$ means that sensor j can receive data from sensor i. For each sensor j, $\mathcal{N}^{(j)} = \{i \in \mathcal{N} : (i, j) \in \mathcal{A}\}$ is called its in-neighbors, in particular, $\mathcal{N}^{(j)} \setminus j$ denotes its in-neighbors without itself.

On the other hand, as shown in Fig. 1, aiming at disrupting the above SN, suppose that multiple malicious attackers are employed to launch multiple attacks on different sensors in this SN. In what follows, we assume that all of these attackers have limited energy resource and can launch attacks with a cooperate or uncooperative way.

A. RFS-Based Formulation for Multiple Attackers' Behaviors

Similar to [24], the behaviors of these attackers are supposed to satisfy the following reasonable assumptions.

A1: At each time step, each attacker only has two states, active or dormant. The former means that it is launching an attack at the current time step, while the latter means that it does not launch an attack. Due to the limited energy resource [34], [35], [36], the number of the active attackers is time-varying at each time step.

A2: From the perspective of the efficient utilization of the limited energy resource, at each time step, each attacker will

only attack no more than one sensor, and these attackers will not simultaneously attack the same sensor at the same time [24]. According to this assumption, one can find that the number of the attacked sensors equals to the number of attacks (active attackers) at each time step.

A3: The transition between active state and dormant state satisfies the following statements. On the one hand, for each active attacker at the current time step, it will become dormant with probability $1-p_s$, or survive and keep active with probability p_s at the next time step. On the other hand, for each dormant attacker at the current time step, it also has a probability to become a newborn active attacker,[1] or still keeps dormant at the next time step.

Let $x_{i,k} \in \mathbb{X}$ denote the index of the sensor attacked by the ith active attacker at time step k, then the set of all of the attacked sensors at this time step can be modeled by an RFS

$$\Sigma_k = \{x_{1,k}, x_{2,k}, \ldots, x_{n(k),k}\} \tag{3}$$

$$= \Theta_k(\Sigma_{k-1}) \cup \Gamma_k. \tag{4}$$

It follows that $|\Sigma_k| = n(k)$, representing the number of the attacked sensors. From *A2*, $n(k)$ can be also taken as the number of attacks (active attackers) at this time step. According to *A3*, (4) holds true since Σ_k can be divided into two categories: 1) the sensors attacked by the surviving attackers, $\Theta_k(X_{k-1})$ and 2) those attacked by the newborn attackers, Γ_k.

For each surviving attacker, assume that its attack behavior (i.e., its attacked sensors versus time) follows an integral discrete Markov stochastic process. For example, a linear discrete Gaussian stochastic process

$$x_{i,k} = \lfloor F x_{i,k-1} + v_k \rfloor \tag{5}$$

where F is the transition matrix and v_k is the Gaussian process noise with zero mean and covariance Q.

B. RFS-Based Formulation for Reports at Each Sensor

Suppose that each sensor has the limited capacities of local detection, local estimation, and data exchange with its neighbors. In particular, for monitoring purposes, each sensor j is equipped with a local detector to detect whether it suffers from attacks or not. If detected, it will report its index to its local estimator for further analysis. More precisely, if it is under an attack launched by the ith attacker, then its report is

$$z_k^{(j)} = H x_{i,k} = j \tag{6}$$

where H is the measurement matrix that can be taken as the identity matrix. If no detection, its report can be treated as an empty set. Thus, if an attack aiming at sensor j happens, the report can be formulated by the following RFS:

$$\Phi_k^{(j)} = \begin{cases} \emptyset, & \text{with probability } 1-p_d^{(j)} \\ \{z_k^{(j)}\}, & \text{with probability } p_d^{(j)} \end{cases} \tag{7}$$

where $p_d^{(j)}$ is the detection rate of the local detector. For simplicity, assuming that all detectors share the same detection rates, i.e., $p_d^{(j)} = p_d$.

[1]It will be treated as a newborn attacker even it ever was active in the past.

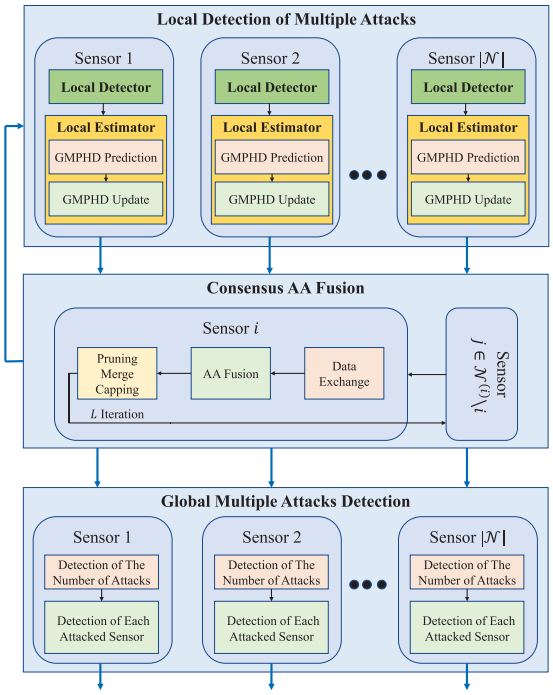

Fig. 2. Schematic of the proposed consensus AA-GMPHD filter.

Due to the lack of all of the reports over the entire SN, it is impossible for individual sensors to obtain the accurate detections of multiple attacks only depending on their individual reports. Therefore, to simultaneously detect multiple attacks, a distributed MAD algorithm is indispensable.

V. Proposed Consensus AA-GMPHD Filter

In this section, we present a novel distributed algorithm named consensus AA-GMPHD filter for MAD. As illustrated in Fig. 2, the proposed filter consists of three procedures, i.e., local detection of multiple attacks, consensus AA fusion, and global MAD.

A. Local Detection of Multiple Attacks

For any sensor j at time step k, based on the reports $\Phi_k^{(j)}$ from its local detector, the objective of its local estimator is to detect multiple attacks over the entire SN $\mathcal{G}$. Since the information about attacks is completely capsuled by the RFS Σ_k and the corresponding multiobject PDF, this objective is equivalent to the posterior estimation of the multiobject PDF of Σ_k conditioned on $\Phi_k^{(j)}$, i.e., $\pi_k^{(j)}(\Sigma_k|\Phi_k^{(j)})$. Unfortunately, due to the abstract set integration, it is intractable to directly calculate $\pi_k^{(j)}(\Sigma_k|\Phi_k^{(j)})$. Thus, as one of the RFS-based filters, the PHD filter, which recursively estimates the first moment (also called the PHD) of $\pi_k^{(j)}(\Sigma_k|\Phi_k^{(j)})$, is introduced [37].

Generally speaking, there are two implementations for the PHD filter, i.e., SMC implementation and GM implementation. The former uses lots of particles to represent PHDs, whereas the latter uses a linear combination of Gaussian components to represent PHDs. Usually, the number of required Gaussian components is far smaller than the number of required particles for a given PHD, leading to lower-computation burden that

the GM implementation poses. Therefore, due to the limited computation capacity and energy resource of individual sensors, the PHD filter with GM implementation (also called the GMPHD filter) is considered in what follows. Specifically, the following GMPHD filter that includes prediction and update steps, is carried out at the jth sensor.

Prediction: At time step $k-1$, for sensor j, given the posterior PHD $v_{k-1}^{(j)}(x)$ with the GM form

$$v_{k-1}^{(j)}(x)=\sum_{a=1}^{I_{k-1}^{(j)}} w_{k-1}^{(a)}\mathbb{N}\left(x;m_{k-1}^{(a)},P_{k-1}^{(a)}\right) \tag{8}$$

where $w_{k-1}^{(a)}$ is the weight of the ath Gaussian component, $m_{k-1}^{(a)}$ and $P_{k-1}^{(a)}$ are the mean and covariance of the ath Gaussian component, respectively, and $I_{k-1}^{(j)}$ is the number of Gaussian components. Then, the predicted PHD $v_{k|k-1}^{(j)}(x)$ is also a GM form given by [37]

$$v_{k|k-1}^{(j)}(x)=v_{s,k|k-1}^{(j)}(x)+\gamma_k(x) \tag{9}$$

where

$$\begin{aligned}
v_{s,k|k-1}^{(j)}(x)&=p_s\sum_{a=1}^{I_{k-1}^{(j)}} w_{k-1}^{(a)}\mathbb{N}\left(x;m_{s,k|k-1}^{(a)},P_{s,k|k-1}^{(a)}\right)\\
m_{s,k|k-1}^{(a)}&=Fm_{k|k-1}^{(a)}\\
P_{s,k|k-1}^{(a)}&=Q+FP_{k-1}^{(a)}F^T
\end{aligned}$$

and $\gamma_k(x)$ denotes the PHD of the birth RFS Γ_k, both F and Q are defined in (5). In particular, $\gamma_k(x)$ is also supposed to be the following GM form:

$$\gamma_k(x)=\sum_{a=1}^{I_r} w_{r,k}^{(a)}\mathbb{N}\left(x;m_{r,k}^{(a)},P_{r,k}^{(a)}\right). \tag{10}$$

Update: Suppose that the predicted PHD $v_{k|k-1}^{(j)}(x)$ is given in (9), with the GM form

$$v_{k|k-1}^{(j)}=\sum_{a=1}^{I_{k|k-1}^{(j)}} w_{k|k-1}^{(a)}\mathbb{N}\left(x;m_{k|k-1}^{(a)},P_{k|k-1}^{(a)}\right). \tag{11}$$

After receiving the reports $\Phi_k^{(j)}$, $v_k^{(j)}(x)$ still is a GM form calculated as [37]

$$v_k^{(j)}(x)=(1-p_d)v_{k|k-1}^{(j)}(x)+\sum_{z\in\Phi_k^{(j)}} v_{d,k}^{(j)}(x;z) \tag{12}$$

where

$$\begin{aligned}
v_{d,k}^{(j)}(x;z)&=\sum_{a=1}^{I_{k|k-1}^{(j)}} w_k^{(a)}(z)\mathbb{N}\left(x;m_k^{(a)}(z),P_k^{(a)}\right)\\
w_k^{(a)}(z)&=\frac{p_d w_{k|k-1}^{(a)}q_k^{(a)}(z)}{\kappa_k(z)+p_d\sum_{b=1}^{I_{k|k-1}^{(j)}} w_{k|k-1}^{(b)}q_k^{(b)}(z)}\\
q_k^{(a)}(z)&=\mathbb{N}\left(z;Hm_{k|k-1}^{(a)},HP_{k|k-1}^{(a)}H^T+R\right)\\
m_k^{(a)}(z)&=m_{k|k-1}^{(a)}+K_k^{(a)}\left(z-Hm_{k|k-1}^{(a)}\right)\\
P_k^{(a)}&=\left[I-K_k^{(a)}H\right]P_{k|k-1}^{(a)}\\
K_k^{(a)}&=P_{k|k-1}^{(a)}H^T\left[HP_{k|k-1}^{(a)}H^T+R\right]^{-1}
\end{aligned}$$

where H is defined in (6), R denotes the covariance of measurement noise, and κ_k denotes the PHD of clutter measurements at time step k. In particular, from the report model (7), it follows that no measurement noise and clutter measurements exist among the reports. Thus, let $R=0$ and $\kappa_k=\text{eps}$.

B. Consensus AA Fusion

As mentioned before, due to the lack of all of the reports over the entire SN, it is impossible for individual sensors to achieve the accurate global detections of multiple attacks unless their local detections are fused. In this section, we first present the adopted fused rule, followed by the method on how to achieve the global detection via the consensus theory.

For local PHDs, there exist two fusion rules: 1) AA [38], [39] and 2) GCI [40]. Although both them have reasonable interpretations from the view of minimizing discrimination of information [32], in comparison with the GCI fusion rule, the AA fusion rule poses the following two advantages: 1) it poses smaller computational complexity since it can be taken as the linear weighted mean of the local multiobject PDFs and 2) it is more suitable for fusing local multiobject PDFs defined within different fields-of-views (FoVs). For example, if there exists a local multiobject PDF $f^{(i)}(\Sigma)=0$ at a specific sensor i, then the GCI fused multiobject PDF $\bar{f}(\Sigma)=0$ even if $f^{(j)}(\Sigma)\neq 0$ for all $j\in\mathcal{N}, j\neq i$, while it can be seen that the AA fused multiobject PDF $\bar{f}(\Sigma)\neq 0$ in this case. Considering the fact that the sensors always have limited computational capacities and most sensors are under no attack at each time step, resulting in $f^{(i)}(\Sigma)=0$ for most sensors, the AA fusion rule is more appropriate for the distributed MAD problem. Specifically, the AA fusion rule for local PHDs is as follows.

Lemma 1: If the local multiobject PDF $f^{(i)}(\Sigma)$ is the multiobject PDF of a Poisson RFS, shown in (2), with cardinality $\lambda^{(i)}$, PDF $p^{(i)}$, and PHD $v^{(i)}=\lambda^{(i)}p^{(i)}$, then the AA fused multiobject PDF $\bar{f}(\Sigma)$ still is the multiobject PDF of a Poisson RFS, and is characterized by $\bar{\lambda}$ and $\bar{p}$ given as follows [32]:

$$\bar{\lambda}=\sum\nolimits_{i\in\mathcal{N}}\omega^{(i)}\lambda^{(i)},\quad \bar{p}(x)=\frac{\sum_{i\in\mathcal{N}}\omega^{(i)}\lambda^{(i)}p^{(i)}}{\sum_{j\in\mathcal{N}}\omega^{(j)}\lambda^{(j)}} \tag{13}$$

and the corresponding AA fused PHD is

$$\bar{v}(x)=\sum\nolimits_{i\in\mathcal{N}}\omega^{(i)}v^{(i)}(x). \tag{14}$$

In particular, if $\omega^{(i)}=1/|\mathcal{N}|$, (14) is simplified to the unweighted AA fused PHD $\bar{v}(x)=1/|\mathcal{N}|\sum_{i\in\mathcal{N}}v^{(i)}(x)$.

Cardinality Inconsistency: In practice, only (14) needs to be conducted for the fusion of local PHDs. The reasons are twofold.

1) As mentioned before, a Poisson RFS is completely characterized by its PHD [32].
2) The fused cardinality in (13) is inconsistent.

For instance, in a special case in which two sensors with different FoVs exist, if one sensor detects no attack, leading to

$\lambda^{(1)} = 0$, while the other sensor detects a real attack, leading to $\lambda^{(2)} = 1$, then the fused cardinality in (13) turns to be $\bar{\lambda} = \omega^{(2)} \leq 1$, resulting in an over-conservative fused cardinality. In fact, in this case, $\bar{\lambda} = 1$ is more reasonable since the two sensors have different FoVs. On the contrary, if only (14) is computed, the problem of cardinality inconsistency can be alleviated. The reason is that the fused cardinality can be extracted by counting the Gaussian components with high weights in the fused PHD, instead of being directly computed via (13).

For the distributed SN $\mathcal{G}$, due to the lack of central processor, it is impossible to directly calculate the AA fused PHD via (14). Fortunately, consensus can be used to achieve distributed averaging over a distributed topology by allowing each sensor to iteratively update and exchange local information with its in-neighbors [12], [31]. In the context of MAD, consensus is utilized to perform distributed computation for the global unweighted AA fused PHD over all sensors $i \in \mathcal{N}$.

To this end, suppose that, at time step k, each sensor i starts with its local PHD $v_k^{(i)}(x)$ as the initial iterated PHD $v_{k,0}^{(i)}(x)$, and calculates the lth consensus iteration of the local PHD as

$$v_{k,l+1}^{(i)}(x) = \sum\nolimits_{j\in\mathcal{N}^{(i)}} \omega^{(i,j)} v_{k,l}^{(j)}(x) \quad \forall i \in \mathcal{N} \tag{15}$$

where $w^{(i,j)}$ is the consensus weight satisfying

$$\begin{aligned} w^{(i,j)} &\geq 0 \quad \forall i,j \in \mathcal{N} \\ 1 &= \sum_{j\in\mathcal{N}^{(i)}} w^{(i,j)} \quad \forall i \in \mathcal{N} \\ w^{(i,j)} &= \frac{1}{1+\max\{|\mathcal{N}^{(i)}|, |\mathcal{N}^{(j)}|\}}, i \in \mathcal{N}, j \in \mathcal{N}^{(i)} \setminus i \\ w^{(i,i)} &= 1 - \sum_{j\in\mathcal{N}^{(i)}\setminus i} w^{(i,j)}. \end{aligned}$$

If the topology of the distributed SN $\mathcal{G}$ is strongly connected, then it has been proved that the consensus iteration (15) trends to the unweighted AA fused PHD [12], [31]

$$\lim_{n\to\infty} v_{k,n}^{(i)}(x) = \frac{1}{|\mathcal{N}|} \sum\nolimits_{i\in\mathcal{N}} v^{(i)}(x). \tag{16}$$

In brief, the second step of the proposed filter, i.e., consensus AA fusion, can be summarized as follows: given an appropriate iteration number L, each sensor i performs consensus iteration. In each iteration l, each sensor i sends its information, i.e., the main components of its local GMPHD, including $\{w_{k,l}^{(a)}, m_{k,l}^{(a)}, P_{k,l}^{(a)}\}_{a\in\{1:J_{k,l}^{(i)}\}}$, to its in-neighbors $j \in \mathcal{N}^{(i)} \setminus i$, and waits until it receives information from them. Then, each sensor i performs the consensus AA fusion (15) over $\mathcal{N}^{(i)}$. Note that most of sensors are under no attack, to improve computational efficiency, $v_{k,l}^{(j)}(x)$ whose cardinality equals to zero can be omitted in (15). After consensus, to limit the increasing number of Gaussian components, the steps of pruning, merge and capping are necessary, which can be found in [37] for details.

C. Global Multiple Attacks Detection

After consensus, the PHD of each sensor has achieved the consensual global PHD. Given a threshold τ, each sensor picks up all the Gaussian components with $w_k^{(a)} > \tau$ in the consensual global PHD, and takes the integer that is closest to the sum of the weights of the picked Gaussian components as the consensual cardinality $\hat{n}_k$. Meanwhile, the consensual cardinality is treated as the detected number of attacks over the entire SN $\mathcal{G}$.

For each sensor, selecting $\hat{n}_k$ Gaussian components with highest weights. For each selected Gaussian component $\{(w_k^{(a)}, m_k^{(a)}, P_k^{(a)})\}$, the index of the attacked sensor can be taken as the integer which is nearest to the first element of $m_k^{(a)}$.[2]

In summary, to detect multiple attacks, at each time step k, each sensor i in this SN carries out in parallel, beginning with its previous local PHD, producing its new consensus PHD at the end of consensus iteration, and extracting the detection information of multiple attacks. Specifically, the schematic of the proposed consensus AA-GMPHD filter is illustrated in Fig. 2, and the corresponding pseudo-code is shown in Algorithm 1.

Algorithm 1 Consensus AA-GMPHD Filter for Distributed MAD

for sensor $i = 1, \ldots, |\mathcal{N}|$ **do**
  Initialization
end for
for time step $k = 1, 2, \cdots$ **do**
  Procedure 1: Local Detection of Multiple Attacks
  for sensor $i = 1, \ldots, |\mathcal{N}|$ **do**
    Input: Local report of sensor i
    Local GMPHD prediction via (9)-(10)
    Local GMPHD update via (11)-(12)
  end for
  Procedure 2: Consensus AA Fusion
  for $l = 1, \ldots, L$ **do**
    for sensor $i = 1, \ldots, |\mathcal{N}|$ **do**
      Data exchange
      Consensus AA fusion (15) over $\mathcal{N}^{(i)}$
      Pruning, merge and capping, see [37]
    end for
  end for
  Procedure 3: Global Multiple Attacks Detection
  for sensor $i = 1, \ldots, |\mathcal{N}|$ **do**
    The detection of the number of attacks
    The detection of each attacked sensor
    Output: The number of total attacks and the indices of the attacked sensors over the entire distributed SN
  end for
end for

D. Performance Analysis

1) Security Analysis: According to [41], cyber attacks can be divided into three categories, i.e., availability, integrity, and confidentiality attacks. The availability attacks is to make data unavailable by disrupting communication networks, which include jamming and denial of service (DoS) attacks. The integrity attacks, such as false data injection attacks, are to inject false data or control commands in sensors or communication networks. The confidentiality attacks may happen at any part of SNs, including eavesdropping, and the combination of DoS and integrity attacks.

[2]The vector $m_k^{(a)}$ may has different rows, while the first element is the estimated index of the attacked sensor.

Obviously, not all of the above attacks can be detected by the proposed filter. In fact, the kinds of the attacks which can be detected by the proposed filter need to simultaneously satisfy the following two conditions, the first is that the attacks are targeting the sensors, rather than the communication links between sensors, which means that only the integrity attacks and confidentiality attacks are satisfactory. The second is that, neglecting the aspect of missing detection, the attacks is unable to evade the local detectors installed on individual sensors, which further means that only the integrity attacks and confidentiality attacks that cannot escape from the local detector can be detected.

2) Complexity Analysis: It has been shown that the complexity of the PHD filter is $\mathcal{O}(mn)$ [12], [37], where m and n are the number of reports and the number of attackers, respectively. As far as the proposed filter is concerned, Note that each sensor has to operate local PHD filter and the number of its reports does not exceed 1 at each time step, then the computational complexity for the local PHD filter is clearly independent of the number of sensors, and can be expressed as $\mathcal{O}(n)$. Moreover, one can find that the consensus AA fusion for each sensor requires $\mathcal{O}(Ld)$ computations, where L is the consensus iteration number and d is the degree of this sensor. Thus, the computational complexity is $\max\{\mathcal{O}(n), \mathcal{O}(Ld)\}$.

3) Relationship Between Detection Performance and The Number of Attackers: Theoretically speaking, the number of attackers does not affect the detection performance of the proposed filter. However, in the specific implementation of the proposed filter, the following two factors are affected by the number of attackers, consequently, indirectly affecting the detection performance. The first is the number of Gaussian components used to represent PHDs. Since the information of attackers is represented by the corresponding PHDs, the increase of the number of attackers means the increase of the complexity of PHDs, which means that more Gaussian components are needed to represent PHDs. The second is the convergence rate of consensus AA fusion, the increase of the number of attackers means the increase of the complexity of PHDs, consequently, affecting the convergence rate of consensus AA fusion shown (15).

VI. Numerical Experiments

In this section, the performances of the proposed filter for MAD are assessed via numerical experiments over two distributed SNs.

A. Parameters Settings

As illustrated in Figs. 3 and 4, the number of sensors in the two SNs are 30 and 57, respectively, and the two SNs are with the topologies of the IEEE 30-bus system and IEEE 57-bus system, respectively. The lines in the two SNs represent the communication links, which means that the two sensors connected by one line can exchange their local detection information with each other. Meanwhile, the local detector equipped by each sensor is the χ detector, and the detection rate is set to $p_d = 0.99$.

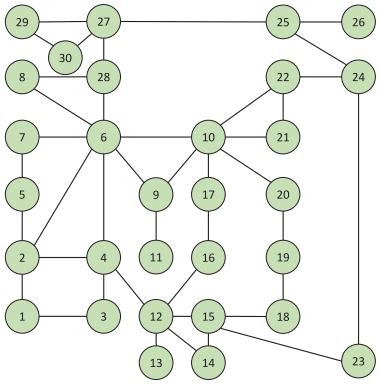

Fig. 3. Distributed SN with the topology of the IEEE 30-bus system.

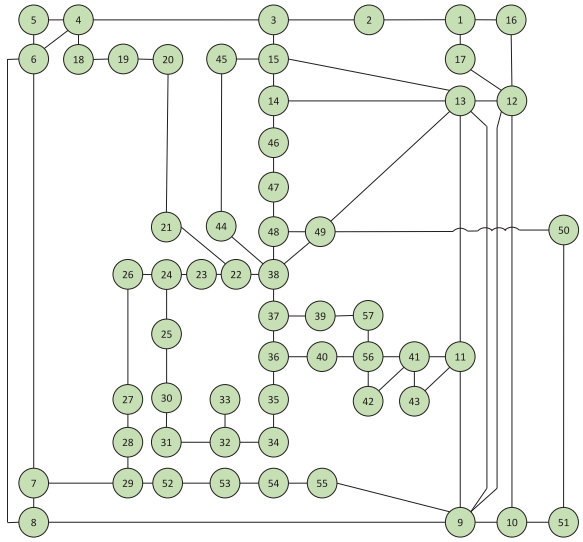

Fig. 4. Distributed SN with the topology of the IEEE 57-bus system.

Suppose there exist six attackers who share the same linear attack behaviors following (5) with:

$$F = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

and

$$Q = \begin{bmatrix} 0.1^2 & 0 \\ 0 & 0.1^2 \end{bmatrix}.$$

For all of the attackers, they will launch multiple attacks on different sensors in the two SNs. Without consideration of missing detection, these attacks are assumed to be detected by the χ^2 detectors equipped by individual sensors. The persistent attack duration of these attackers are 1–30, 5–30, 8–30, 15–30, 20–30, and 25–30 time steps, respectively.

Meanwhile, suppose that these attackers share the same surviving probability $p_s = 0.9$, and newborn model Γ_k. The PHD of the newborn model Γ_k with the GM form (10) is assumed to be described as follows: The number of Gaussian components is $I_r = 2$; For each Gaussian component, $w_{r,k}^{(a)} = 0.001$, and the first element of $m_{r,k}^{(a)}$ follows an integral uniform distribution between 1 and $|\mathcal{N}|$, where $|\mathcal{N}| = 30$ and $|\mathcal{N}| = 57$

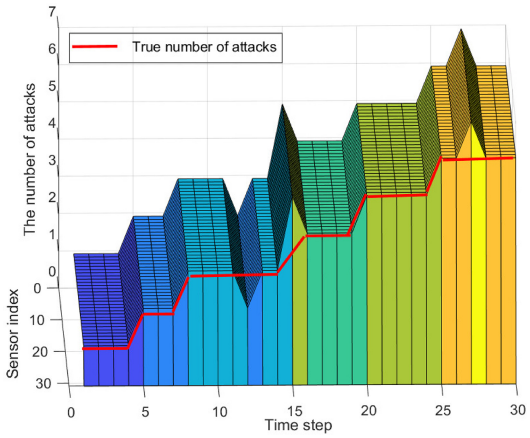

Fig. 5. Detection results of the number of attacks of all sensors via the proposed filter for the distributed SN with the topology of the IEEE 30-bus system over one trial.

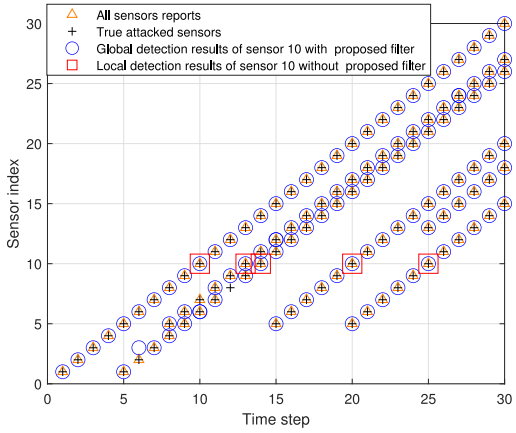

Fig. 6. Detection results of the attacked sensors of sensor 10 in the distributed SN with the topology of the IEEE 30-bus system over one trial.

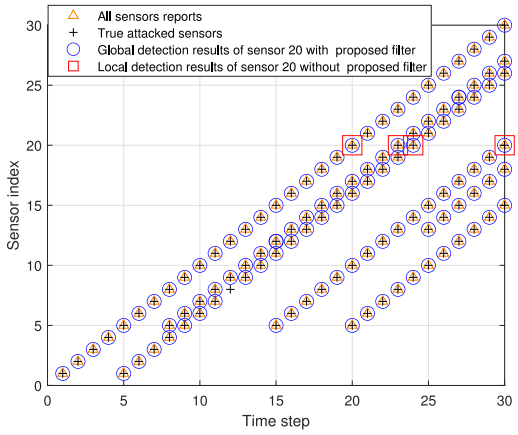

Fig. 7. Detection results of the attacked sensors of sensor 20 in the distributed SN with the topology of the IEEE 30-bus system over one trial.

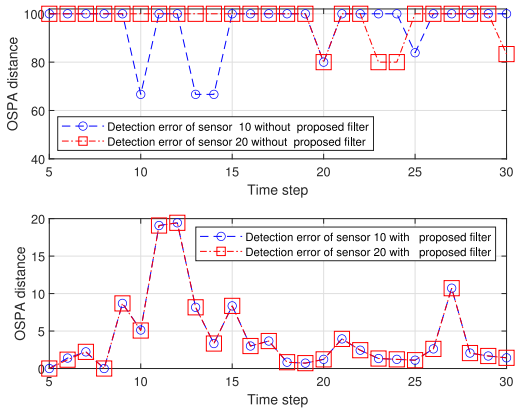

Fig. 8. Detection error (OSPA distance) for the distributed SN with the topology of the IEEE 30-bus system over 100 MC trials.

for the two SNs, respectively, and

$$P_{r,k}^{(a)} = \begin{bmatrix} 10 & 0 \\ 0 & 10 \end{bmatrix}.$$

In the proposed filter, the local GMPHD filter with the maximum allowable number of Gaussian components $I = 20$ for each PHD is adopted. The number of consensus iteration L and the threshold τ are set to 50 and 0.01, respectively. Similar to [24] and [31], the OSPA distance [42] with $p = 1$ and $c = 100$ is taken as the performance metric to evaluate the detection error of MAD.

B. Simulation Results

For the distributed SNs shown in Figs. 3 and 4, the proposed filter is executed in parallel in each sensor, and the global detection results (i.e., the number of attacks and the indices of attacked sensors over the entire SN) are extracted via the third step of the proposed filter (i.e., global MAD).

For the distributed SN with the topology of the IEEE 30-bus system, simulation results are shown in Figs. 5–8 . Thereinto, Fig. 5 presents all sensors' detection results of the number of attacks via the proposed filter. From Fig. 5, it can be seen that the detection results of all sensors have converged to a consensual value at each time step. Moreover, the consensual value exactly equals to the true number of attacks in most time.

Since the detection results of all sensors have converged, we randomly choose the detection performance of two sensors (sensors 10 and 20) to demonstrate the effectiveness of the proposed filter. Specifically, Figs. 6 and 7 present the detection performance of the attacked sensors of the two sensors, respectively. As shown by the red rectangular symbols in the two figures, the two sensors without the proposed filter can only detect the attacks launched on themselves in a very short time, and fail to detect multiple attacks over the entire SN. On the contrary, after performing the proposed filter, as shown by the blue circular symbols, it follows that the two sensors achieve the detection of multiple attacks over the entire SN.

Next, the averaged detection error over 100 Monte Carlo (MC) trials is illustrated in Fig. 8. As Fig. 8 shows, the detection error of the sensors without the proposed filter versus time always is high (more than 60), because they fail to detect any attack unless they themselves are under attack. As a comparison, the sensors with the proposed filter achieve much smaller detection error (no more than 20), further confirming the advantages of the proposed filter on distributed MAD.

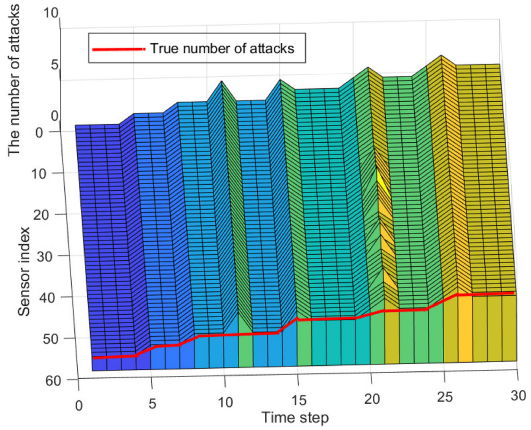

Fig. 9. Detection results of the number of attacks of all sensors via the proposed filter for the distributed SN with the topology of the IEEE 57-bus system over one trial.

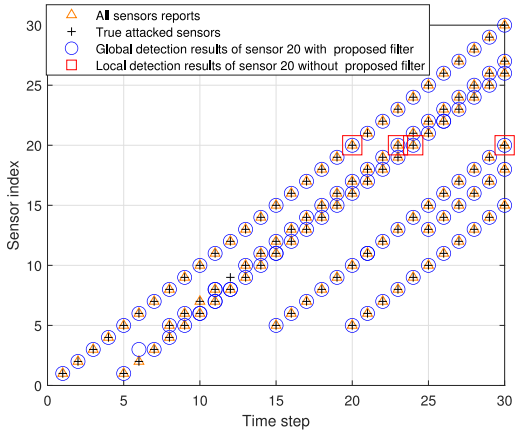

Fig. 11. Detection results of the attacked sensors of sensor 20 in the distributed SN with the topology of the IEEE 57-bus system over one trial.

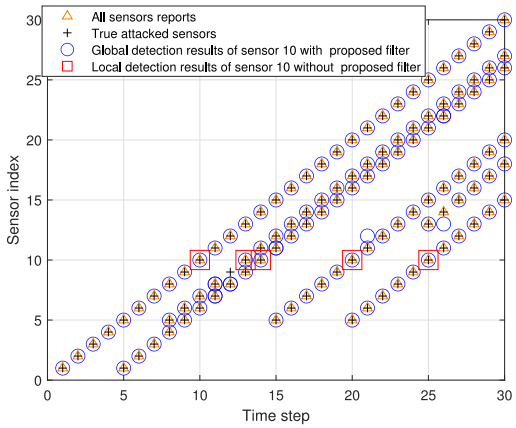

Fig. 10. Detection results of the attacked sensors of sensor 10 in the distributed SN with the topology of the IEEE 57-bus system over one trial.

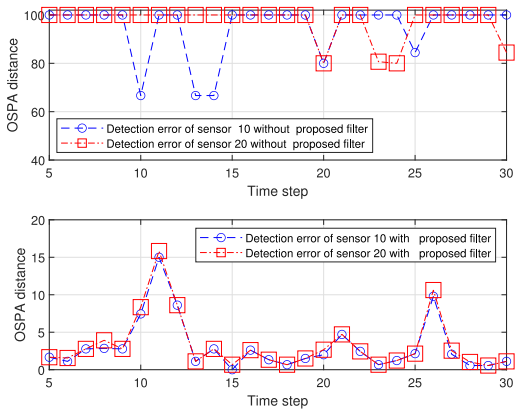

Fig. 12. Detection error (OSPA distance) for the distributed SN with the topology of the IEEE 57-bus system over 100 MC trials.

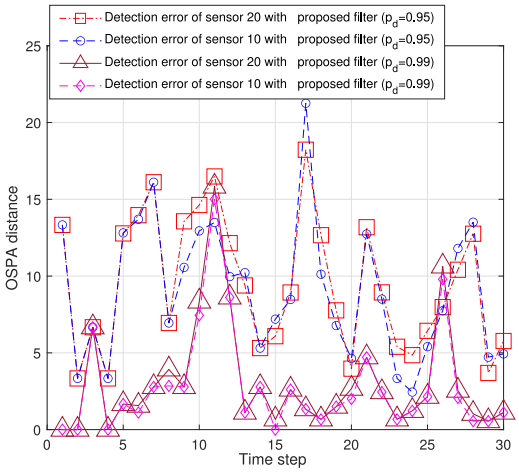

Fig. 13. Detection error (OSPA distance) for the distributed SN with the topology of the IEEE 57-bus system over 100 MC trials, where p_d are 0.95 and 0.99, respectively.

To assess the effectiveness of the proposed filter under the case of large-scale SNs with distributed topologies, the distributed SN with the topology of the IEEE 57-bus system is considered, and simulation results are shown in Figs. 9–12. Thereinto, Figs. 9–11 present the detection performance of the attacked sensors over one trial, and Fig. 12 presents the averaged detection error over 100 MC trials. Comparing Figs. 5–8 and Figs. 9–12, it can be seen that the detection performance for the two distributed SNs is similar, which implies that the proposed filter shows robustness with network sizes and network topologies.

To further verify the effectiveness of the proposed filter, different initial conditions are set. Specifically, the detection rate of each sensor p_d decreases from 0.99 to 0.95, and other settings are the same as before. The results over 100 MC trials are shown in Fig. 13. From Fig. 13, it can be seen that the detection error increases when p_d decreases. It is reasonable since the lower the value of p_d, the more attacks will escape from detection.

VII. Conclusion

This article has addressed a fundamental issue in the distributed SNs, i.e., how to detect multiple attacks aiming at different sensors in a distributed way. By means of the theories of RFS, fusion rules and consensus, this problem has been cast in a distributed PHD filter, and a novel filter named consensus AA-GMPHD filter has been proposed to solve

this problem. Numerical experiments concerning with the distributed SNs with the topologies of the IEEE 30-bus and IEEE 57-bus systems have been investigated, which verifies the effectiveness of the proposed filter for distributed MAD.

In the future work, two possible research directions will be considered.

1) Although the proposed filter aims at coping with the problem of distributed MAD, it also provides a promising perspective to handle some tough problems, such as distributed multiple target tracking and distributed data fusion. Thus, we will consider how to use the proposed filter to handle the above problems.
2) The types of attacks that can be detected by the proposed filter are still limited. Thus, we will pay attention to the research on the detection of multiple more sophisticated and stealthy attacks.

REFERENCES

[1] J. Liu et al., "Frame-dilated convolutional fusion network and GRU-based self-attention dual-channel network for soft-sensor modeling of industrial process quality indexes," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 9, pp. 5989–6002, Sep. 2022.

[2] X. Yin, Z. Li, L. Zhang, and M. Han, "Distributed state estimation of sensor-network systems subject to Markovian channel switching with application to a chemical process," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 6, pp. 864–874, Jun. 2018.

[3] L. Chen and P. Chou, "BIG-CCA: Beacon-less, infrastructure-less, and GPS-less cooperative collision avoidance based on vehicular sensor networks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 46, no. 11, pp. 1518–1528, Nov. 2016.

[4] C. Zhou, Y. Gu, X. Fan, Z. Shi, G. Mao, and Y. D. Zhang, "Direction-of-arrival estimation for coprime array via virtual array interpolation," *IEEE Trans. Signal Process.*, vol. 66, no. 22, pp. 5956–5971, Nov. 2018.

[5] C. Chang, G. Chen, G. Yu, T.-L. Wang, and T.-C. Wang, "TCWTP: Time-constrained weighted targets patrolling mechanism in wireless mobile sensor networks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 45, no. 6, pp. 901–914, Jun. 2015.

[6] Z. Zhang, Z. Shi, C. Zhou, C. Yan, and Y. Gu, "Ziv-Zakai bound for compressive time delay estimation," *IEEE Trans. Signal Process.*, vol. 70, pp. 4006–4019, Jun. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9794611

[7] Y. Chen, S. Kar, and J. M. F. Moura, "The Internet of Things: Secure distributed inference," *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 64–75, Sep. 2018.

[8] A. Buonviri, M. York, K. LeGrand, and J. Meub, "Survey of challenges in labeled random finite set distributed multi-sensor multi-object tracking," in *Proc. IEEE Aerosp. Conf.*, Big Sky, MT, USA, Mar. 2019, pp. 1–12.

[9] "Centralized network." Accessed: Apr. 1, 2023. [Online]. Available: https://csrc.nist.gov/glossary/term/centralized_network

[10] "Decentralized network." Accessed: Apr. 1, 2023. [Online]. Available: https://csrc.nist.gov/glossary/term/decentralized_network

[11] "Distributed network." Accessed: Apr. 1, 2023. [Online]. Available: https://csrc.nist.gov/glossary/term/distributed_network

[12] C. Fantacci, B.-N. Vo, B.-T. Vo, G. Battistelli, and L. Chisci, "Consensus labeled random finite set filtering for distributed multi-object tracking," 2015, *arXiv preprint:1501.01579*.

[13] Y. Li, H. Voos, M. Darouach, and C. Hua, "An algebraic detection approach for control systems under multiple stochastic cyber-attacks," *IEEE/CAA J. Automatica Sinica*, vol. 2, no. 3, pp. 258–266, Jul. 2015.

[14] C. Cimpanu. "Cyberattack brings down Vodafone Portugal mobile, voice, and TV services." Accessed: Feb. 8, 2022. [Online]. Available: https://therecord.media/cyberattack-brings-down-Vodafone-Portugal-mobile-voice-and-tv-services/

[15] M. Wixey, "Multiple attackers: A clear and present danger," A Sophos X-Ops Active Adversary, Abingdon, U.K., White Paper, pp. 1–23, Aug. 2022.

[16] K. Townsend. "Cyberattack victims often attacked by multiple adversaries: Research." Accessed: Aug. 2022. [Online]. Available: https://www.securityweek.com/cyberattack-victims-often-attacked-multiple-adversaries-research

[17] R. Katipally, L. Yang, and A. Liu, "Attacker behavior analysis in multi-stage attack detection system," in *Proc. 7th CSIIRW Conf.*, Oak Ridge, TN, USA, Oct. 2011, pp. 1–4.

[18] S. I. Popoola, B. Adebisi, M. Hammoudeh, G. Gui, and H. Gacanin, "Hybrid deep learning for botnet attack detection in the Internet-of-Things networks," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4944–4956, Mar. 2021.

[19] D. Yin, L. Zhang, and K. Yang, "A DDoS attack detection and mitigation with software-defined Internet of Things framework," *IEEE Access*, vol. 6, pp. 24694–24705, Apr. 2018.

[20] W. Yan, L. K. Mestha, and M. Abbaszadeh, "Attack detection for securing cyber physical systems," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8471–8481, Oct. 2019.

[21] S. Tan, J. M. Guerrero, P. Xie, R. Han, and J. C. Vasquez, "Brief survey on attack detection methods for cyber-physical systems," *IEEE Syst. J.*, vol. 14, no. 4, pp. 5329–5339, Dec. 2020.

[22] J. Zhang, L. Pan, Q. Han, C. Chen, S. Wen, and Y. Xiang, "Deep learning based attack detection for cyber-physical system cybersecurity: A survey," *IEEE/CAA J. Automatica Sinica*, vol. 9, no. 3, pp. 377–391, Mar. 2022.

[23] X. Xie, C. Wei, Z. Gu, and K. Shi, "Relaxed resilient fuzzy stabilization of discrete-time Takagi–Sugeno systems via a higher order time-variant balanced matrix method," *IEEE Trans. Fuzzy Syst.*, vol. 30, no. 11, pp. 5044–5050, Nov. 2022.

[24] C. Yang, Z. Shi, H. Zhang, J. Wu, and X. Shi, "Multiple attacks detection in cyber-physical systems using random finite set theory," *IEEE Trans. Cybern.*, vol. 50, no. 9, pp. 4066–4075, Sep. 2020.

[25] F. Boem, A. J. Gallo, G. Ferrari-Trecate, and T. Parisini, "A distributed attack detection method for multi-agent systems governed by consensus-based control," in *Proc. IEEE CDC*, Melbourne, VIC, Australia, Dec. 2017, pp. 5961–5966.

[26] A. J. Gallo, M. S. Turan, F. Boem, T. Parisini, and G. Ferrari-Trecate, "A distributed cyber-attack detection scheme with application to DC microgrids," *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3800–3815, Sep. 2020.

[27] J. Shi, S. Liu, B. Chen, and L. Yu, "Distributed data-driven intrusion detection for sparse stealthy FDI attacks in smart grids," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 3, pp. 993–997, Mar. 2021.

[28] S. Rathore and J. Park, "Semi-supervised learning based distributed attack detection framework for IoT," *Appl. Soft Comput.*, vol. 72, pp. 79–89, Nov. 2018.

[29] S. Adepu and A. Mathur, "Distributed attack detection in a water treatment plant: Method and case study," *IEEE Trans. Depend. Secure Comput.*, vol. 18, no. 1, pp. 86–99, Jan./Feb. 2021.

[30] Y. Guan and X. Ge, "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 4, no. 1, pp. 48–59, Mar. 2018.

[31] G. Battistelli, L. Chisci, C. Fantacci, A. Farina, and A. Graziano, "Consensus CPHD filter for distributed multitarget tracking," *IEEE J. Sel. Topics Signal Process.*, vol. 7, no. 3, pp. 508–520, Jun. 2013.

[32] L. Gao, G. Battistelli, and L. Chisci, "Multiobject fusion with minimum information loss," *IEEE Signal Process. Lett.*, vol. 27, pp. 201–205, 2020.

[33] C. Yang, F. Li, Z. Shi, R. Lu, and K. Choo, "A crowdsensing-based cyber-physical system for drone surveillance using random finite set theory," *ACM Trans. CPS*, vol. 3, no. 4, pp. 1–22, Oct. 2019.

[34] J. Qin, M. Li, L. Shi, and X. Yu, "Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks," *IEEE Trans. Autom. Control*, vol. 63, no. 6, pp. 1648–1663, Jun. 2018.

[35] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 3023–3028, Nov. 2015.

[36] L. Li, H. Zhang, Y. Xia, and H. Yang, "Security estimation under denial-of-service attack with energy constraint," *Neurocomputing*, vol. 292, no. 31, pp. 111–120, May 2018.

[37] B.-N. Vo and W.-K. Ma, "The Gaussian mixture probability hypothesis density filter," *IEEE Trans. Signal Process.*, vol. 54, no. 11, pp. 4091–4104, Nov. 2006.

[38] T. Li, J. M. Corchado, and S. Sun, "Partial consensus and conservative fusion of gaussian mixtures for distributed PHD fusion," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 5, pp. 2150–2163, Oct. 2019.

[39] T. Li, F. Hlawatsch, and P. M. Djurić, "Cardinality-consensus-based PHD filtering for distributed multitarget tracking," *IEEE Signal Process. Lett.*, vol. 26, no. 1, pp. 49–53, Jan. 2019.

[40] D. Clark, S. Julier, R. Mahler, and B. Ristić, "Robust multi-object sensor fusion with unknown correlations," in *Proc. SSPD*, London, U.K., Sep. 2010, pp. 1–5.
[41] W. Duo, M. Zhou, and A. Abusorrah, "A survey of cyber attacks on cyber physical systems: Recent advances and challenges," *IEEE/CAA J. Automatica Sinica*, vol. 9, no. 5, pp. 784–800, May 2022.
[42] D. Schuhmacher, B.-T. Vo, and B.-N. Vo, "A consistent metric for performance evaluation in multi-object filters," *IEEE Trans. Signal Process.*, vol. 56, no. 8, pp. 3447–3457, Aug. 2008.

Chaoqun Yang (Member, IEEE) received the B.Sc. degree in marine technology from Xiamen University, Xiamen, China, in 2015, and the Ph.D. degree in information science and electronic engineering from Zhejiang University, Hangzhou, China, in 2019.

From 2019 to 2022, he was an Engineer with the Nanjing Research Institute of Electronics Technology, Nanjing, China. Since 2022, he has been an Associate Professor with the School of Automation, Southeast University, Nanjing. His research interest concentrates on multitarget tracking, radar signal processing, cyber security, and information fusion.

Dr. Yang was the Session Co-Chair and received the Best Organizers Award of the International Conference on Autonomous Unmanned Systems in 2022. He also serves as an Associate Editor for *IET Wireless Sensor Systems* and a Guest Editor for *Internet Technology Letters*.

Xianghui Cao (Senior Member, IEEE) received the B.S. and Ph.D. degrees in control science and engineering from Zhejiang University, Hangzhou, China, in 2006 and 2011, respectively.

From 2012 to 2015, he was a Senior Research Associate with the Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL, USA. He is currently a Professor with the School of Automation, Southeast University, Nanjing, China. His current research interests include cyber–physical' systems, wireless network performance analysis, wireless networked control, and network security.

Prof. Cao was a recipient of the Best Paper Runner-Up Award from ACM MobiHoc in 2014 and the First Prize of Natural Science Award of Ministry of Education of China in 2017. He also serves as an Associate Editor for *ACTA Automatica Sinica* and IEEE/CAA JOURNAL OF AUTOMATICA SINICA.

Lidong He (Member, IEEE) received the B.Eng. degree in mechanical engineering from Zhejiang Ocean University, Zhoushan, China, in 2005, the master's degree in control theory and control engineering from Northeastern University, Shenyang, China, in 2008, and the Ph.D. degree in control science and engineering from Shanghai Jiao Tong University, Shanghai, China, in 2014.

In the fall of 2010 and 2011, he was a visiting student with The Hong Kong University of Science and Technology, Hong Kong. From 2014 to 2016, He was a Postdoctoral Researcher with Zhejiang University, Hangzhou, China. In 2016, He joined the School of Automation, Nanjing University of Science and Technology, Nanjing, China, and is currently an Associate Professor. His research interests include secure estimation and control for cyber physical systems and its application in unmanned systems.

Dr. He is an active reviewer for many international journals.

Heng Zhang (Member, IEEE) received the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2015.

He was a Research Fellow with Western Sydney University, Sydney, NSW, Australia, from 2017 to 2018. His research interests include security and privacy in cyber–physical systems and control and optimization theory.

Dr. Zhang is an editorial board member of several academic journals, including *IET Wireless Sensor Systems*, *EURASIP Journal on Wireless Communications and Networking*, and *KSII Transactions on Internet and Information Systems*. He is also the Guest Editor of the *Journal of The Franklin Institute* and *Peer-to-Peer Networking and Applications*.