IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 10, 2017, accepted May 29, 2017, date of publication June 8, 2017, date of current version June 27, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2713807

Distributed Secure Estimation Over Wireless Sensor Networks Against Random Multichannel Jamming Attacks

YANPENG GUAN[1] **AND XIAOHUA GE**[2]

[1]Department of Automation, Shanxi University, Taiyuan 030006, China
[2]School of Software and Electrical Engineering, Swinburne University of Technology, Melbourne, VIC 3122, Australia

Corresponding author: Xiaohua Ge (xge@swin.edu.au)

This work was supported in part by the National Natural Science Foundation of China under Grant 61603232 and in part by the Key Project of Natural Science Foundation of Zhejiang Province, China, under Grant LZ13F030001.

ABSTRACT This paper addresses the distributed secure estimation problem over wireless sensor networks subject to random multichannel jamming attacks. Each sensor's measurement is divided into n_y (the dimension of measurement signal) components and transmitted via n_y relevant wireless channels. The attacker is an active adversary in the sense that sensors' measurements through wireless transmission channels are randomly dropped if the corresponding channels are successfully jammed. By employing a piecewise homogeneous Markov chain, a sophisticated two-level switching multichannel jamming attack model is developed. From the perspective of the attacker, this attack model is promising and makes the wireless channels highly vulnerable, because the attacker can randomly and arbitrarily decide when and where to launch the attacks. We then focus our attention on the secure estimation of a target signal with the caveat that some of the measurements can be incomplete induced by the attacks. A system theoretic framework is then developed to cast the network-based security problem into an H_∞ estimation theory problem of a piecewise homogeneous Markov jump system. Criteria for analyzing H_∞ estimation performance and designing resilient estimators against noises and attacks are also presented. The effectiveness of the proposed results is illustrated through a military F404 aircraft engine system.

INDEX TERMS Distributed secure estimation, jamming attack, wireless sensor network, piecewise homogeneous Markov chain, multichannel transmission.

I. INTRODUCTION

Recent advances in hardware and wireless communication technologies have enabled the development and application of wireless sensor networks (WSNs) in a widespread areas, such as military (battlefield surveillance), health (elderly patient wellness monitoring) and environment (chemical detection in a contaminated environment). Generally, a WSN consists of a large number of smart sensor devices that are spatially deployed either very close to the phenomenon or inside the region of interest [1]. These sensors are usually powered by finite battery and possess data sensing, data processing and communication capabilities. As indicated in [2], a critical issue in WSNs is to design an efficient distributed collaborative signal processing algorithm to track a target through noisy and unreliable network environment. Furthermore, the core part in collaborative signal processing lies in the distributed estimation or filtering, which has aroused ever-increasing research interest over the past several years. We refer the reader to [3]–[7] and many references therein for related work.

The broadcast nature of the wireless transmission medium renders WSNs vulnerable to various malicious attacks [8]. This is because WSNs rely on deployed energy-constrained sensors to cooperatively perform an overall task by broadcasting data with the neighboring sensors. As a result, sensors' data can be potentially manipulated by cyber attacks. Typical attacks can be roughly classified as eavesdropping attacks [9], [10], node capture attacks [8], [11], stealthy attacks [12], false data injection attacks [13]–[15], denial-of-service (DoS) attacks, etc. Thereinto, DoS attacks, which aim to prevent sensors' data from reaching their destinations, rendering the data unavailable, have been widely studied in the literature, see, e.g., [16]–[18]. As a typical DoS technique, jamming attacks [19]–[21] are well-known threats as they disrupt the radio frequencies on the wireless communication channels and lead to channel congestions [22]. Besides, from the attacker's viewpoint, jamming attacks require little prior knowledge about the system/target and do not need any special hardware to launch them. Whereas, they seriously threaten WSNs operating reliably in real time. Hence, how to assess the trustworthiness of sensors' data makes the security a challenging issue in WSNs. Although the study of a jamming attack is not new, its impact on a distributed estimation protocol is significant due to the fact that the corrupted sensor data will be propagated and disseminated in an epidemic way over a WSN [23]. To the best of the authors' knowledge, the distributed estimation problem over WSNs in the presence of *random multichannel jamming attacks* has not been adequately addressed yet. In contrast to deterministic or constant jamming, the difficulty may lie in that random multichannel jamming attacks are cost effective as the attackers can randomly and arbitrarily choose when to launch the attacks and which specific channels to jam, but also hard to track and remove by detectors and estimators due to their random jamming behaviors. Consequently, these attacks pose new challenges to the WSN-based application development and make the distributed secure estimation problem much more complicated, which motivates the present study.

Different from the traditional information theoretic studies on secure communication which mainly involve the protection of data, such as adopting frequency hopping or spread spectrum communication, locating and bypassing the jamming area, rerouting traffic and implementing prioritized transmission [24], [25], in this paper, we will focus on investigating the distributed estimation performance under the random multichannel jamming attacks from the system theoretic perspective. Unlike most previous studies which are mainly devoted to passively detecting and eliminating the malicious attacks [21], we will then develop a distributed secure estimation framework which pro-actively admits and utilizes the corrupted sensor measurement.

The main contributions of this work are summarized as follows: i) *A sophisticated two-level switching multichannel jamming attack model will be developed.* More specifically, the attack model involves two levels of switching. At the low level, a Markov chain is introduced to model random jamming, where the state space of the Markov chain corresponds to all possible modes of attacks. At the high level, the variations of the transition probabilities of the low-level Markov chain fall into two categories: deterministic average dwell time switching and stochastic switching. This provides a sophisticated model for the attacker to intelligently implement the random jamming without being easily detected or corrected. We will focus on jamming attacks in sensor measurement transmission channels. This is particularly important because sensors need to first measure the target signal, then compute estimations and further share their estimations with the neighboring sensors. In other words, the corrupted sensor measurements will be propagated among the neighboring sensors; ii) *A refined system theoretic framework to address the distributed secure estimation problem in the presence of random multichannel jamming attacks in WSNs will be presented.* The WSN-based security problem will be mapped into an H_∞ estimation theory problem based on the stochastic stability of a piecewise homogeneous Markov jump system. Thus, the framework enables one to study stability and performance analysis issues of WSNs under such attacks; and iii) *Novel criteria for analyzing secure estimation performance and designing distributed secure estimators will be established.* We will analytically and numerically investigate the impact of the considered two-level switching multichannel attacks on the estimation performance, and show that under what conditions the resultant estimation error system will converge even in the presence of such attacks.

The rest of this paper is organized as follows. In Section II, the two-level switching multichannel jamming attack model is presented and the distributed secure estimation problem is formulated. Section III presents the performance analysis results on distributed secure consensus estimation in detail. In Section IV, the design criteria on the existence of desired distributed attack-mode-and-variation-dependent consensus estimators are provided. Section V validates the effectiveness of the proposed distributed secure consensus estimation method by considering a military aircraft gas turbine engine system. Finally, Section VI draws a conclusion.

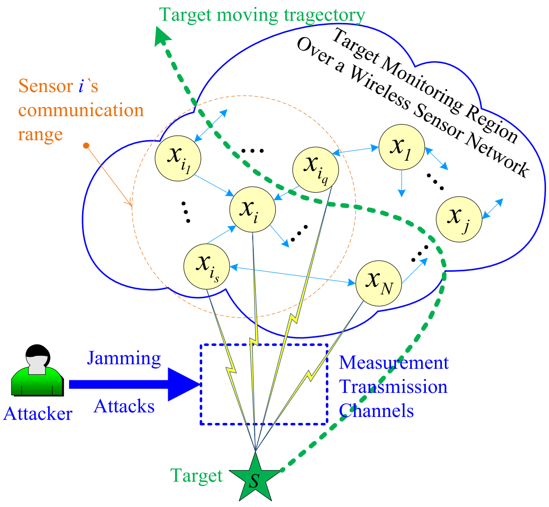


FIGURE 1. A schematic diagram of a distributed secure estimation problem for target tracking over a wireless sensor network subject to jamming attacks on measurement transmission channels.

II. PROBLEM FORMULATION

The system considered for a distributed secure estimation problem of target tracking is composed of N cooperative sensors and a moving target in a monitoring region over a WSN, as shown in Fig. 1.

A. NOTATIONS

Throughout the paper, we use $\mathbb{R}^n$ to denote the n-dimensional Euclidean space and $\mathbb{R}^{n\times m}$ to represent the set of all the real

$n \times m$ matrices. For symmetric matrices X and Y, the notation $X \leq Y$ (respectively, $X < Y$) means that $X - Y$ is negative semidefinite (respectively, negative definite). $Pr\{\cdot\}$ represents the occurrence probability of an event. $\mathbb{E}\{\cdot\}$ represents the mathematical expectation of a stochastic variable. $\|\cdot\|$ denotes the induced matrix 2-norm or the Euclidean vector norm as appropriate. $|\cdot|$ denotes the absolute value of a scalar. $\otimes$ stands for the Kronecker product for matrices. $diag\{\cdot\}$ represents a diagonal matrix. $\mathbb{N}$ denotes the set of nonnegative integers. I is an identity matrix with an appropriate dimension. Let asterisk '$*$' denote a term that is induced by symmetry in symmetric block matrices. The superscript 'T' denotes the transpose of a matrix with vectors as a special case. If a matrix is invertible, the superscript '-1' represents the matrix inverse. The symbol $\sum$ denotes the summation of a sequence. The space of square-summable vector functions over $[0, \infty)$ is denoted as $l_2[0, \infty)$ and for any $w(k) \in l_2[0, \infty)$, its norm is given by $\|w(k)\| = \sqrt{\sum_{k=0}^{\infty} w^T(k)w(k)}$. Matrices, if not explicitly stated, are assumed to have appropriate dimensions.

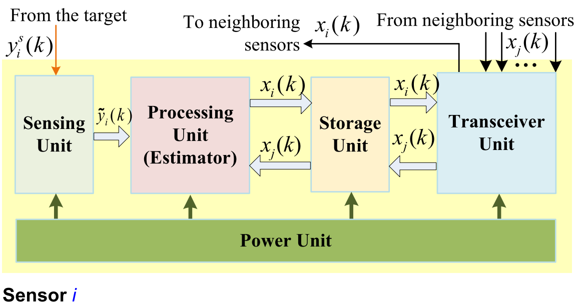


FIGURE 2. A typical architecture of a smart sensor with main components such as sensing unit, processing unit, storage unit, transceiver unit and power unit.

B. A PRESCRIBED COMMUNICATION TOPOLOGY

In a WSN setting, a group of N smart sensor nodes are usually deployed in a monitoring region to cooperatively track the moving target. A typical architecture of such a smart sensor device is depicted in Fig. 2. Each of these smart sensors is equipped with radio transceivers and interconnected via wireless radio channels. Therefore, each sensor may possess a limited communication range due to finite power. In other words, only a subset of sensors can sense the target signal, and that each sensor is capable of sharing its state estimation with a limited fraction of sensors in its communication range, see Fig. 1. The communication topology among these N sensor nodes over a WSN is modeled by a weighted directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$ with $\mathcal{V} = \{1, 2, \cdots, N\}$ denoting an index set of N nodes, $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ representing an edge set of paired nodes and $\mathcal{A} = [a_{ij}] \in \mathbb{R}^{N \times N}$ standing for a weighted adjacency matrix. A directed edge of $\mathcal{G}$ is denoted by (i, j), which means that node i can receive information from node j or node j can send its information to node i. The adjacency elements a_{ij} associated with the directed edges of the graph are positive, i.e., $a_{ij} > 0 \Leftrightarrow (i, j) \in \mathcal{E}$. It is assumed that self-loops are excluded in the graph, i.e., $a_{ii} = 0$, $i \in \mathcal{V}$. Denote $\mathcal{N}_i = \{j \in \mathcal{V} : (i, j) \in \mathcal{E}\}$, then an element of $\mathcal{N}_i$ is called a neighbor of node i. Denote $\mathcal{D} = diag_N^i\{d_i\}$ with $d_i = \sum_{j=1}^{N} a_{ij}$. The Laplacian matrix of the directed weighted graph $\mathcal{G}$ is defined as $\mathcal{L} = [l_{ij}]_{N \times N} = \mathcal{D} - \mathcal{A}$.

C. TARGET DYNAMICS

The target motion is described by a discrete-time linear time-invariant system of the following state-space representation

$$s(k+1) = As(k) + Bw(k), \ s(0) = s_0 \tag{1}$$

$$z^s(k) = Es(k) + Fw(k) \tag{2}$$

for all $k \in \mathbb{N}$, where $s(k) \in \mathbb{R}^{n_s}$ is the state of the target at the k-th time step; $w(k) \in \mathbb{R}^{n_w}$ belonging to $l_2[0, \infty)$ is the exogenous disturbance input; $z^s(k) \in \mathbb{R}^{n_z}$ is the objective output of the target to be estimated. The objective output $z^s(k)$ can be regarded as an the internal measurement of the target and is not transmitted through a communication network, thus it is considered to be secure; s_0 is the initial state of the target; and A, B, E and F are known constant matrices with appropriate dimensions.

The ideal measurement of the target state signal for sensor i is given by

$$y_i^s(k) = C_i s(k), \quad \forall\, i \in \mathcal{V}, \tag{3}$$

where $y_i^s(k) \in \mathbb{R}^{n_y}$ is the external measurement output from the target and needs to be transmitted through a communication network, thus being vulnerable to cyber attacks; and C_i, for all $i \in \mathcal{V}$, are known constant observation matrices with appropriate dimensions.

D. A TWO-LEVEL SWITCHING MULTICHANNEL JAMMING ATTACK MODEL

Sensors in WSNs are often equipped with on-board processors. After receiving measurement from the target signal, each sensor runs an estimator to compute a state estimation of the target signal. In most of the existing results, the measuring of the target is explicitly assumed to be successful as long as the target moves within the monitoring region of a sensor [3], [26], [27], which leads to

$$\tilde{y}_i(k) = y_i^s(k), \quad \forall\, i \in \mathcal{V} \tag{4}$$

at each time step k, where $\tilde{y}_i(k) \in \mathbb{R}^{n_y}$ is the input of estimator i. However, this ideal assumption is not always true in practice when malicious attacks occur in wireless transmission channels. For example, in presence of DoS attacks, the transmission of sensor measurement from the target to remote sensors may be blocked since typical DoS attacks can jam the channels over a WSN. In this sense, the input of an estimator and the ideal measurement output may not be identical.

In the following, we consider the scenario that there is an attacker which degrades the remote estimation performance by jamming the wireless measurement channels between the target and sensors, as shown in Fig. 1. The attacker is an active adversary in the sense that the sensors' measurement will be passively dropped once the attacker successfully jammed the wireless channels. Generally, there are three cases after the attacker launched an attack: *Case (i)* the sensors' measurements of the target signal will successfully arrive at their destinations if the attacker fails to jam the transmission channels. For example, in some circumstances, the attacker has to give up jamming certain channels due to a limited energy budget [16]; *Case (ii)* the sensors' measurement of the target signal will be partially lost if the jamming of transmission channels is not heavy; and *Case (iii)* the sensors' measurement of the target signal will be completely lost if the transmission channels are severely jammed.

Based on the observations mentioned above, we propose the following target measurement model on sensor i under multichannel attacks

$$\tilde{y}_i(k) = \Lambda_i y_i^{sx}(k) + D_i v_i(k), \quad \forall\, i \in \mathcal{V}, \tag{5}$$

where $\Lambda_i \in \mathbb{R}^{n_y \times n_y}$ are prescribed attack model parameter matrices by the attacker, $y_i^{sx}(k) = y_i^s(k) - y_i^x(k)$ and $y_i^x(k)$ is the output of estimator i which will be defined later. In (5), the term $\Lambda_i y_i^x(k)$ is introduced to compensate the effects of malicious attacks against estimation performance and also plays an important role in successfully achieving target tracking. Moreover, $\tilde{y}_i(k)$ is corrupted by a measurement noise $v_i(k) \in \mathbb{R}^{n_w}$ which belongs to $l_2[0,\infty)$. For all $i \in \mathcal{V}$, D_i are known constant matrices with appropriate dimensions. It is assumed that the attack model parameter matrices Λ_i have the following diagonal structure

$$\Lambda_i = diag\{\lambda_{i,1}, \lambda_{i,2}, \cdots, \lambda_{i,n_y}\}, \tag{6}$$

where $\lambda_{i,p} \in [0,1]$ are prescribed constants, $\forall\ p = 1, 2, \cdots, n_y$. Obviously, due to its diagonal feature of Λ_i, the scenario of multichannel attacks is fully incorporated. For each index p, the parameter $\lambda_{i,p}$ can be used to characterize the transmission status of sensor i' measurement output $y_{i,p}^{sx}(k)$ so as to reflect the jamming status of measurement channel p under the attacks. For example, the case $\lambda_{i,p} = 1$ corresponds to the ideal transmission of $y_{i,p}^{sx}(k)$, which means that there is no jamming through channel p and the p-th measurement $y_{i,p}^{sx}(k)$ is successfully delivered to remote estimator i. When $0 < \lambda_{i,p} < 1$, it characterizes the case of partial transmission of $y_{i,p}^{sx}(k)$. In this case, the measurement channel p may be slightly congested. If $\lambda_{i,p} = 0$, however, it reduces to the worst case of outage of the measurement channel p, which means that sensor i's p-th measurement output $y_{i,p}^{sx}(k)$ is completely lost during transmission.

In practical WSNs environments, to incarnate phenomena such as varying network queues and varying network loads, a wireless transmission channel usually needs to have memory or modes [28], [29]. One way to model dependence between different working modes is by letting the wireless transmission channel be governed by the mode of an underlying Markov chain. Then the effects of varying network queues and varying network loads can be modelled by a transition from one mode to another mode of the Markov chain. In this sense, when the measurement outputs are transmitted to remote estimators, wireless transmission channels may possess Markovian characteristics and depend on each working mode of the current network status. On the other hand, the strategy of applying multichannel attacks in (5) is in nature deterministic. Such a deterministic attack policy may lead to an excess energy consumption of the attacker while energy constraint is a natural concern for various types of attackers [16]. Alternatively, the attacker may randomly decide to jam the wireless channels or to sleep in order to save the energy. Besides, under a deterministic attack policy, robust detectors and estimators can be designed to analyze, detect and handle attacks so that a cunning attacker should carefully design his attack strategy to deceive detectors and robust estimators [13]. Hence, in the presence of a smart attacker, some random or more complicated attack policies may pose major difficulties for remote estimators. Motivated by these facts, we modify (5) to a sophisticated target measurement attack model by introducing a random process $\{r_k, k \geq 0\}$ as follows

$$\tilde{y}_i(k) = \Lambda_i^{r_k} y_i^{sx}(k) + D_i v_i(k), \quad \forall\, i \in \mathcal{V}, \tag{7}$$

where

$$\Lambda_i^{r_k} = diag\{\lambda_{i,1}^{r_k}, \lambda_{i,2}^{r_k}, \cdots, \lambda_{i,n_y}^{r_k}\} \tag{8}$$

$$\underline{\lambda}_{i,p}^{r_k} \leq \lambda_{i,p}^{r_k} \leq \overline{\lambda}_{i,p}^{r_k}, \quad \forall\, i \in \mathcal{V}; p = 1, 2\cdots, n_y \tag{9}$$

with $\underline{\lambda}_{i,p}^{r_k}, \overline{\lambda}_{i,p}^{r_k} \in [0,1]$ being known constants. In the sequel, the process $\{r_k, k \geq 0\}$ is described by a discrete-time Markov chain and takes values in the finite set $\mathcal{R} = \{1, 2, \cdots, R\}$ corresponding to all possible modes under attacks. The mode transition probability matrix (TPM) is given as $\Pi^{\sigma_{k+1}} = [\pi_{uv}^{\sigma_{k+1}}]_{R\times R}$ and with transition probabilities (TPs) given by:

$$Pr(r_{k+1} = v | r_k = u) = \pi_{uv}^{\sigma_{k+1}}, \tag{10}$$

where $\pi_{uv}^{\sigma_{k+1}}$ for all $u, v \in \mathcal{R}$ denotes the TP from mode u at time k to mode v at time $k+1$, and $\sum_{v=1}^{R} \pi_{uv}^{\sigma_{k+1}} = 1$ for all $u \in \mathcal{R}$. A simple illustration of of the proposed random multichannel attack model (7) is given in Fig. 3.

Analogous to the process $\{r_k, k \geq 0\}$ which describes the random and time-varying characteristics of the attack model parameter matrices $\Lambda_i^{r_k}$, a switching signal $\{\sigma_k, k \geq 0\}$ is introduced to consider the TP of $\{r_k, k \geq 0\}$ to be of time-varying property. Additionally, $\{\sigma_k, k \geq 0\}$ is assumed to take values in a finite set $\mathcal{S} = \{1, 2, \cdots, S\}$. It should be pointed out that the assumption of time-varying TPs in (10) is partially motivated by the piecewise homogeneous Markov chains studied in [30], where the switching signal σ_k is merely restricted to be a random process. By taking the variations of the TP matrix in the finite set $\mathcal{S}$ into consideration, the attacker can neatly implement his attack policy based on some specific missions. To elaborate this point, the switching signal $\{\sigma_k, k \geq 0\}$ is further considered as the following two categories:

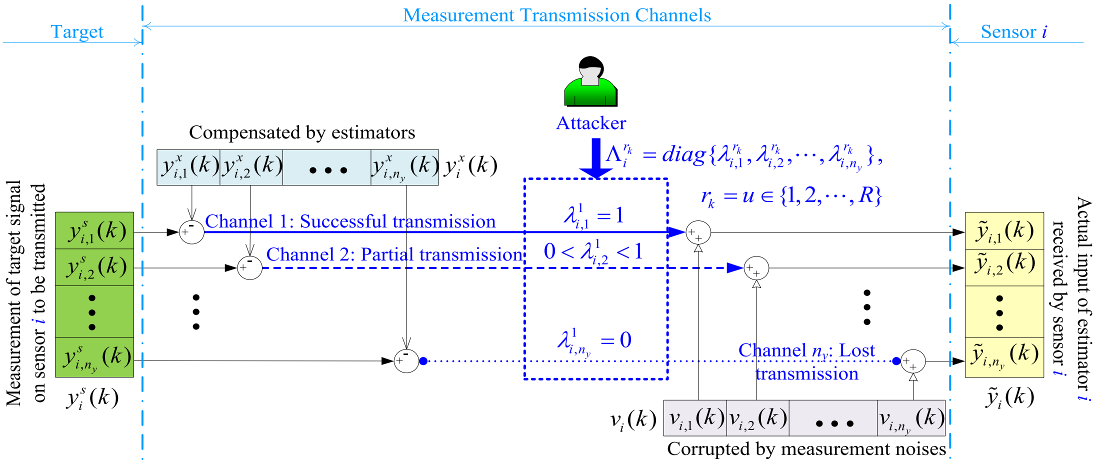

Target
Measurement Transmission Channels
Sensor i
Attacker
$\Lambda_i^{r_k} = diag\{\lambda_{i,1}^{r_k}, \lambda_{i,2}^{r_k}, \cdots, \lambda_{i,n_y}^{r_k}\}$,
$r_k = u \in \{1, 2, \cdots, R\}$
Compensated by estimators
$y_{i,1}^x(k)$ $y_{i,2}^x(k)$ • • • $y_{i,n_y}^x(k)$ $y_i^x(k)$
Measurement of target signal on sensor i to be transmitted
$y_{i,1}^s(k)$
$y_{i,2}^s(k)$
$y_{i,n_y}^s(k)$
$y_i^s(k)$
Channel 1: Successful transmission
Channel 2: Partial transmission
$\lambda_{i,1}^1 = 1$
$0 < \lambda_{i,2}^1 < 1$
$\lambda_{i,n_y}^1 = 0$
Channel n_y: Lost transmission
$v_i(k)$ $v_{i,1}(k)$ $v_{i,2}(k)$ • • • $v_{i,n_y}(k)$
Corrupted by measurement noises
$\tilde{y}_{i,1}(k)$
$\tilde{y}_{i,2}(k)$
$\tilde{y}_{i,n_y}(k)$
$\tilde{y}_i(k)$
Actual input of estimator received by sensor i

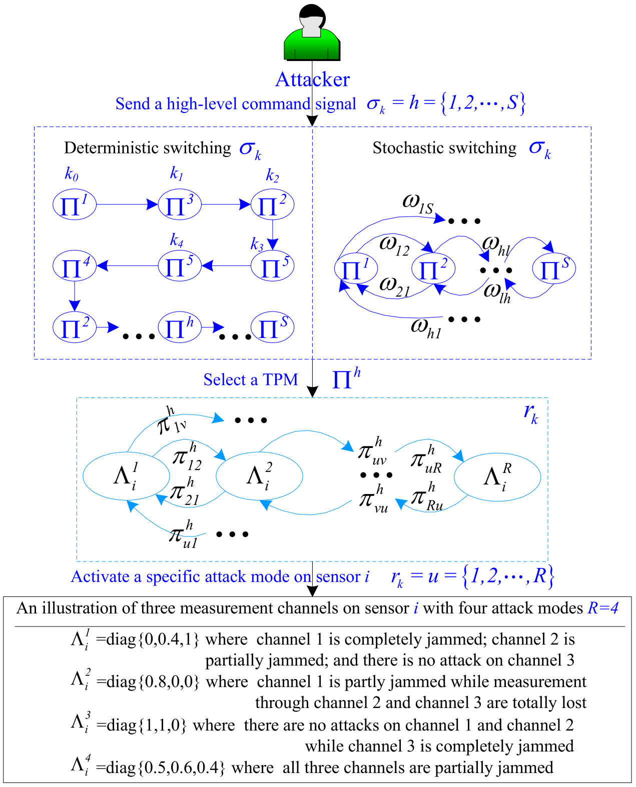
FIGURE 3. A random multichannel jamming attack model governed by a Markov chain $\{r_k, k \geq 0\}$ in measurement transmission channels, where at attack mode $r_k = u = 1$, measurement through transmission channel 1 is successfully sent to remote estimator i; measurement through transmission channel 2 is partially arrived at estimator i; and measurement through transmission channel n_y is completely lost.

- *Deterministic Switching.* In this case, $\{\sigma_k, k \geq 0\}$ is governed by a high-level deterministic switching signal, more specifically, a dwell time switching signal. For a switching time sequence $0 = k_0 < k_1 < k_2 < \cdots$, σ_k is continuous from the right everywhere and may be either autonomous or controlled [31]. When $k \in [k_p, k_{p+1})$, the σ_{k_p}-th TP matrix is active and $\hbar_p = k_{p+1} - k_p$ is called the dwell time of the switching signal σ_k between switching instants k_p and k_{p+1}.
- *Stochastic Switching.* In this case, $\{\sigma_k, k \geq 0\}$ is governed by a high-level homogeneous Markov chain. The TPM of σ_k is defined as $\Omega = [\omega_{hl}]_{S\times S}$ with TPs given by

$$Pr(\sigma_{k+1} = l | \sigma_k = h) = \omega_{hl},$$

where $\omega_{hl} > 0$, $\forall\, h, l \in \mathcal{S}$, denotes the TP from Π^h at time k to Π^l at time $k+1$ and $\sum_{l=1}^{S} \omega_{hl} = 1$ for all $h \in \mathcal{S}$.

Remark 1: Under either deterministic switching or stochastic switching, all the possible cases of Π^1, Π^2, $\cdots$, Π^S with TPs $\pi_{uv}^{\sigma_{k+1}}$ defined in (10) can be encapsulated into a database with σ_k being a high-level command signal assigned by the attacker. At each time step k, the attacker sends a command $\sigma_k = h$, $\forall\, h \in \mathcal{S}$ to select a TPM Π^h so as to carry out the multichannel attacks in (7). For each individual measurement channel p, $\forall\, p = 1, 2, \cdots, n_y$, the attack mode is determined by the Markov chain r_k because the state space $\mathcal{R}$ corresponds to all the possible modes of the multichannel attacks. Therefore, the attacker can allocate different attack modes by taking energy budget into account and construct them into a database indicated by both the Markov chain r_k and the high-level switching signal σ_k. To emphasize such a feature, we refer to (7) as a two-level switching multichannel jamming attack model. The principle of how the attacker carries out such two-level multichannel jamming attacks is demonstrated in Fig. 4.


Attacker
Send a high-level command signal $\sigma_k = h = \{1,2,\cdots,S\}$
Deterministic switching σ_k
k_0 k_1 k_2
Π^1 Π^3 Π^2
k_4 k_3
Π^4 Π^5 Π^5
Π^2 • • • Π^h • • • Π^S
Stochastic switching σ_k
ω_{1S} • • •
ω_{12} ω_{hl}
Π^1 Π^2 • • • Π^S
ω_{21} ω_{lh}
ω_{h1} • • •
Select a TPM Π^h
r_k
π_{1v}^h • • •
Λ_i^1 π_{12}^h π_{21}^h Λ_i^2 π_{uv}^h • • • π_{vu}^h π_{uR}^h π_{Ru}^h Λ_i^R
π_{u1}^h • • •
Activate a specific attack mode on sensor i $r_k = u = \{1,2,\cdots,R\}$

An illustration of three measurement channels on sensor i with four attack modes R=4

Λ_i^1 =diag{0,0.4,1} where channel 1 is completely jammed; channel 2 is partially jammed; and there is no attack on channel 3

Λ_i^2 =diag{0.8,0,0} where channel 1 is partly jammed while measurement through channel 2 and channel 3 are totally lost

Λ_i^3 =diag{1,1,0} where there are no attacks on channel 1 and channel 2 while channel 3 is completely jammed

Λ_i^4 =diag{0.5,0.6,0.4} where all three channels are partially jammed

FIGURE 4. Scheme of two-level switching multichannel jamming attacks.

E. DISTRIBUTED ATTACK-MODE-AND-VARIATION-DEPENDENT CONSENSUS ESTIMATORS

To estimate the state of the target, sensor i is assumed to run a consensus-based estimator of the form

$$x_i(k+1) = Ax_i(k) + G^i_{r_k,\sigma_k}\tilde{x}_i(k) + K^i_{r_k,\sigma_k}\tilde{y}_i(k) \quad (11)$$

$$y_i^x(k) = C_i x_i(k) \quad (12)$$

$$z_i^x(k) = Ex_i(k), \quad (13)$$

where $x_i(k) \in \mathbb{R}^{n_s}$ is the state estimation computed by estimator i; $\tilde{x}_i(k) = \sum_{j\in\mathcal{N}_i} a_{ij}(x_i(k) - x_j(k))$ is a state consensus term of estimator i which guarantees the agreement of the whole sensor network on estimating the target state signal over time; $\tilde{y}_i(k) \in \mathbb{R}^{n_y}$ is the input of estimator i defined in (7); $y_i^x(k) \in \mathbb{R}^{n_y}$ is the measurement output of estimator i; $z_i^x(k) \in \mathbb{R}^{n_z}$ represents an estimation of the target output signal $z^s(k)$; the initial condition of estimator i is $x_i(0) = x_i^0$. For all $r_k = u \in \mathcal{R}$; $\sigma_k = h \in \mathcal{S}$; $i \in \mathcal{V}$, $G_{u,h}^i$ and $K_{u,h}^i$ are the gain matrices to be determined.

Remark 2: Note that the gain matrices G_{r_k,σ_k}^i and K_{r_k,σ_k}^i in (11) arise from the consensus term $\tilde{x}_i(k)$ and the local luenberger-like observer term $\tilde{y}_i(k)$, respectively. From the definition of $\tilde{x}_i(k)$, it is clear that estimator i not only uses its own state estimation $x_i(k)$ but also takes into account state estimation information $x_j(k)$ collected from its all underlying neighbors in $\mathcal{N}_i$. Thus, sensors in the proposed distributed estimation framework are capable of cooperatively monitoring the behavior of the target based only on neighbor-to-neighbor communication, i.e., achieving target tracking in a fully distributed fashion by using only local information of a specific sensor and its neighbors. Generally, information exchanges and intercommunication among a group of sensors can achieve better tracking accuracy, particularly when there exist malicious attacks on sensor measurement channels. From (11), it can be also seen that the proposed estimator i is not only dependent on attack modes r_k but also dependent on TPM variation modes σ_k, which renders our distributed estimators (11) more resilient with regard to security attacks on sensors' measurement. In the following, estimators in the form of (11) are referred to as distributed attack-mode-and-variation-dependent consensus estimators (DACEs).

F. A DISTRIBUTED SECURE CONSENSUS ESTIMATION PROBLEM

For sensor node i, $\forall\, i \in \mathcal{V}$, define a state estimation error vector $e_i^x(k) = s(k) - x_i(k)$ and an output estimation error vector $e_i^z(k) = z^s(k) - z_i^x(k)$. Substituting (7) and (12) into (11) and combining (1), (2) and (13) yield the following estimation error dynamics

$$e_i^x(k+1) = (A - K_{u,h}^i \Lambda_i^u C_i)e_i^x(k) + Bw(k) - K_{u,h}^i D_i v_i(k) + G_{u,h}^i \sum_{j\in\mathcal{N}_i} l_{ij} e_j^x(k) \tag{14}$$

$$e_i^z(k) = Ee_i^x(k) + Fw(k). \tag{15}$$

To simplify subsequent development, we denote $\tilde{e}_x(k) = [e_1^{xT}(k), e_2^{xT}(k), \cdots, e_N^{xT}(k)]^T$, $\tilde{e}_z(k) = [e_1^{zT}(k), e_2^{zT}(k), \cdots, e_N^{zT}(k)]^T$ and $\tilde{v}(k) = [v_1^T(k), v_2^T(k), \cdots, v_N^T(k)]^T$, and let $\tilde{A} = I_N \otimes A$, $\tilde{B} = [B^T, B^T, \cdots, B^T]^T$, $\tilde{C} = diag\{C_1, C_2, \cdots, C_N\}$, $\tilde{D} = diag\{D_1, D_2, \cdots, D_N\}$, $\tilde{E} = I_N \otimes E$, $\tilde{F} = [F^T, F^T, \cdots, F^T]^T$, $\tilde{G}_{u,h} = diag\{G_{u,h}^1, G_{u,h}^2, \cdots, G_{u,h}^N\}$, $\tilde{K}_{u,h} = diag\{K_{u,h}^1, K_{u,h}^2, \cdots, K_{u,h}^N\}$ and $\tilde{\mathcal{L}} = \mathcal{L} \otimes I_N$.

For all $u \in \mathcal{R}$; $i \in \mathcal{V}$, recalling that the attack model parameter matrices Λ_i^u in (14) are unknown, to facilitate further analysis, we define the following matrices

$$\hat{\Lambda}_i^u = diag\{\frac{\overline{\lambda}_{i,1}^u + \underline{\lambda}_{i,1}^u}{2}, \frac{\overline{\lambda}_{i,2}^u + \underline{\lambda}_{i,2}^u}{2}, \cdots, \frac{\overline{\lambda}_{i,n_y}^u + \underline{\lambda}_{i,n_y}^u}{2}\} \tag{16}$$

$$\check{\Lambda}_i^u = diag\{\frac{\overline{\lambda}_{i,1}^u - \underline{\lambda}_{i,1}^u}{2}, \frac{\overline{\lambda}_{i,2}^u - \underline{\lambda}_{i,2}^u}{2}, \cdots, \frac{\overline{\lambda}_{i,n_y}^u - \underline{\lambda}_{i,n_y}^u}{2}\}. \tag{17}$$

Then, one has

$$\Lambda_i^u = \hat{\Lambda}_i^u + \tilde{\Lambda}_i^u \tag{18}$$

for all $u \in \mathcal{R}$; $i \in \mathcal{V}$, where $\tilde{\Lambda}_i^u = diag\{\tilde{\lambda}_{i,1}^u, \tilde{\lambda}_{i,2}^u, \cdots, \tilde{\lambda}_{i,n_y}^u\}$ and $|\tilde{\lambda}_{i,p}^u| \le \frac{\overline{\lambda}_{i,p}^u - \underline{\lambda}_{i,p}^u}{2}$, $\forall\, p = 1, 2, \cdots, n_y$. Thus, we have

$$\|\tilde{\Lambda}_i^u\| \le \check{\Lambda}_i^u \tag{19}$$

for all $u \in \mathcal{R}$; $i \in \mathcal{V}$. Denote $\Lambda_u = diag\{\Lambda_i^u, \Lambda_2^u, \cdots, \Lambda_N^u\}$, $\hat{\Lambda}_u = diag\{\hat{\Lambda}_i^u, \hat{\Lambda}_2^u, \cdots, \hat{\Lambda}_N^u\}$, $\check{\Lambda}_u = diag\{\check{\Lambda}_i^u, \check{\Lambda}_2^u, \cdots, \check{\Lambda}_N^u\}$, $\tilde{\Lambda}_u = diag\{\tilde{\Lambda}_i^u, \tilde{\Lambda}_2^u, \cdots, \tilde{\Lambda}_N^u\}$ and $\check{e}_x(k) = \tilde{\Lambda}_u \tilde{C} \tilde{e}_x(k)$. The estimation error dynamics (14) and (15) can be rewritten in a compact form as follows

$$\tilde{e}_x(k+1) = \mathscr{A}_{u,h}\tilde{e}_x(k) + \mathscr{B}_{u,h}\check{e}_x(k) + \tilde{B}w(k) + \mathscr{D}_{u,h}\tilde{v}(k) \tag{20}$$

$$\tilde{e}_z(k) = \tilde{E}\tilde{e}_x(k) + \tilde{F}w(k), \tag{21}$$

where $\mathscr{A}_{u,h} = \tilde{A} + \tilde{G}_{u,h}\tilde{\mathcal{L}} - \tilde{K}_{u,h}\hat{\Lambda}_u\tilde{C}$, $\mathscr{B}_{u,h} = -\tilde{K}_{u,h}$ and $\mathscr{D}_{u,h} = -\tilde{K}_{u,h}\tilde{D}$ for all $u \in \mathcal{R}$; $h \in \mathcal{S}$.

To proceed with, the following definition with regard to stochastic stability is recalled to describe the main problem of this paper more precisely.

Definition 1: System (20) with $w(k) \equiv 0$ and $\tilde{v}(k) \equiv 0$ is said to be stochastically stable if

$$\mathbb{E}\left\{\sum_{k=0}^{\infty} \|\tilde{e}_x(k)\|^2 |_{s_0, r_0, \sigma_0}\right\} < \infty$$

holds for any initial condition s_0, $r_0 \in \mathcal{R}$ and $\sigma_0 \in \mathcal{S}$.

To quantify the estimation performance, we introduce the following quadratic H_∞ noise attenuation performance index as a system performance metric

$$J_\infty(w, v) = \mathbb{E}\left\{\frac{1}{N}\sum_{k=0}^{\infty}\sum_{i=1}^{N} \|e_i^z(k)\|^2\right\} - \beta\gamma^2 \sum_{k=0}^{\infty} \|w(k)\|^2 - (1-\beta)\gamma^2 \frac{1}{N}\sum_{k=0}^{\infty}\sum_{i=1}^{N} \|v_i(k)\|^2, \tag{22}$$

where $\gamma > 0$ is a prescribed H_∞ performance level and $\beta \in (0, 1)$ is a weighting factor which explicitly explains how the external disturbance $w(k)$ and the measurement noise $v_i(k)$ affect estimation performance separately at a different weighting rate.

Therefore, the distributed secure estimation problem to be addressed in the paper can now be transformed into an H_∞ consensus estimation problem and can be formulated as follows: For given scalars $\gamma > 0$, $\beta \in (0, 1)$ and $\underline{\lambda}_{i,p}^u, \overline{\lambda}_{i,p}^u \in [0, 1]$, $\forall\, u \in \mathcal{R}$, the objective is to design desired DACEs of the form (11)-(13) such that

- *(Stochastic Stability)* Under the two-level multichannel attack model (7) with parameter matrices given by (8) and (9), the resultant estimation error system of the form (20) and (21) with $w(k) \equiv 0$ and $\tilde{v}(k) \equiv 0$ is stochastically stable for any initial condition; and
- *(H_∞ Noise Attenuation Performance)* For all nonzero $w(k)$, $v_i(k) \in l_2[0, \infty)$, $\forall\, i \in \mathcal{V}$, the resultant estimation error system of the form (20) and (21) satisfies the following performance constraint $J_\infty(w, v) < 0$ for zero initial condition.

III. ANALYSIS OF DISTRIBUTED SECURE ESTIMATION PERFORMANCE

In this section, criteria on secure estimation performance analysis for the resultant error system (20) and (21) will be derived. Recalling that a two-level multichannel attack model is proposed in the preceding section, the subsequent analysis procedure is divided into two parts based on a deterministic high-level switching signal $\{\sigma_k, k \geq 0\}$, more precisely, the average dwell time (ADT) switching, and a stochastic high-level switching signal $\{\sigma_k, k \geq 0\}$.

A. DETERMINISTIC HIGH-LEVEL SWITCHING

In this subsection, the variation of the TPMs Π^1, Π^2, $\cdots$, Π^S is subject to a typical class of deterministic switching signal, i.e., the ADT switching. In this case, the number of switches of the TP matrices in a finite interval is bounded and the average time between two consecutive switches is not less than a constant. Note that the concept of ADT was originally proposed in [32] for continuous-time switched systems. For ease development, the definition of ADT in the discrete-time case is recalled as follows.

Definition 2 [31]: For any $k_T \geq k_0$ and any switching signal σ_k, where $k_0 \leq k < k_T$, let $N_\sigma(k_T, k_0)$ denote the switching numbers of σ_k over the interval $[k_0, k_T)$. If $N_\sigma(k_T, k_0) \leq N_0 + (k_T - k_0)/T_a$ holds for $N_0 > 0$ and $T_a > 0$, then N_0 is called the chatter bound and T_a is called the ADT.

Then, the aim is to find a class of ADT switching signals $\{\sigma_k, k \geq 0\}$ to guarantee the stochastic stability and H_∞ performance of the resultant error system (20) and (21). The corresponding result is presented in the following theorem.

Theorem 1 For given scalars $\alpha, \beta \in (0, 1)$, $\gamma > 0$ and $\delta > 1$, under the two-level multichannel attack model (7) with parameter matrices given by (8) and (9), where $\underline{\lambda}^u_{i,p}, \overline{\lambda}^u_{i,p} \in [0, 1]$, $\forall\, u \in \mathcal{R}$ are known scalars, if there exist matrices $P_{u,h} > 0$ of appropriate dimensions and scalars $\rho_u > 0$ such that

$$P_{u,h} \leq \delta P_{u,l}, \quad \forall\, h \neq l \tag{23}$$

$$\Xi_{u,h} = \begin{bmatrix} \Xi^{(1)}_{u,h} & \Xi^{(2)}_{u,h} & \Xi^{(3)}_{u,h} \\ * & -\tilde{P}_{u,h} & 0 \\ * & * & -NI \end{bmatrix} \leq 0 \tag{24}$$

for all $u \in \mathcal{R}$; $h, l \in \mathcal{S}$, where

$$\begin{aligned} \Xi^{(1)}_{u,h} &= diag\{\Xi^{(1,1)}_{u,h}, -\rho_u I, -\beta\gamma^2 I, -(1-\beta)\gamma^2/NI\} \\ \Xi^{(1,1)}_{u,h} &= -(1-\alpha)P_{u,h} + \rho_u \tilde{C}^T \check{\Lambda}_u^T \check{\Lambda}_u \tilde{C} \\ \Xi^{(2)}_{u,h} &= [\tilde{P}_{u,h}\mathscr{A}_{u,h}, \tilde{P}_{u,h}\mathscr{B}_{u,h}, \tilde{P}_{u,h}\tilde{B}, \tilde{P}_{u,h}\mathscr{D}_{u,h}]^T \\ \Xi^{(3)}_{u,h} &= [\tilde{E}, 0, \tilde{F}, 0]^T, \ \tilde{P}_{u,h} = \sum_{v \in \mathcal{R}} \pi^h_{uv} P_{v,h}, \end{aligned}$$

then the resultant estimation error system (20) and (21) is stochastically stable and achieves a prescribed H_∞ performance level γ for any switching signal with ADT satisfying

$$\tau_a > \tau_a^* = -\frac{\ln(\delta)}{\ln(1-\alpha)}. \tag{25}$$

Proof: See Appendix A. □

B. STOCHASTIC HIGH-LEVEL SWITCHING

In this subsection, the variation of the TPMs Π^1, Π^2, $\cdots$, Π^S is governed by a high-level homogeneous Markov chain $\{\sigma_k, k \geq 0\}$. Without loss of generality, it is assumed that $\{\sigma_k, k \geq 0\}$ is independent on $f_{k-1} = \sigma\{r_1, r_2, \cdots, r_{k-1}\}$, where f_{k-1} is a σ-algebra generated by $\{r_1, r_2, \cdots, r_{k-1}\}$ [30]. The following theorem provides a sufficient condition to ensure the stochastic stability of the the resultant error system (20) and (21) with a prescribed H_∞ performance level when the TPMs Π^h for all $h \in \mathcal{S}$ are time varying in the sense of stochastic variation.

Theorem 2 For given scalars $\beta \in (0, 1)$ and $\gamma > 0$, under the two-level multichannel attack model (7) with parameter matrices given by (8) and (9), where $\underline{\lambda}^u_{i,p}, \overline{\lambda}^u_{i,p} \in [0, 1]$, $\forall\, u \in \mathcal{R}$ are known scalars, the resultant estimation error system (20) and (21) is stochastically stable and achieves a prescribed H_∞ performance level γ if there exist matrices $P_{u,h} > 0$ of appropriate dimensions and scalars $\rho_u > 0$ such that

$$\check{\Xi}_{u,h} = \begin{bmatrix} \check{\Xi}^{(1)}_{u,h} & \check{\Xi}^{(2)}_{u,h} & \Xi^{(3)}_{u,h} \\ * & -\check{P}_{u,h} & 0 \\ * & * & -NI \end{bmatrix} \leq 0 \tag{26}$$

for all $u \in \mathcal{R}$; $h \in \mathcal{S}$, where

$$\begin{aligned} \check{\Xi}^{(1)}_{u,h} &= diag\{\check{\Xi}^{(1,1)}_{u,h}, -\rho_u I, -\beta\gamma^2 I, -(1-\beta)\gamma^2/NI\} \\ \check{\Xi}^{(1,1)}_{u,h} &= -P_{u,h} + \rho_u \tilde{C}^T \check{\Lambda}_u^T \check{\Lambda}_u \tilde{C} \\ \check{\Xi}^{(2)}_{u,h} &= [\check{P}_{u,h}\mathscr{A}_{u,h}, \check{P}_{u,h}\mathscr{B}_{u,h}, \check{P}_{u,h}\tilde{B}, \check{P}_{u,h}\mathscr{D}_{u,h}]^T \\ \check{P}_{u,h} &= \sum_{l \in \mathcal{S}} \omega_{hl} \sum_{v \in \mathcal{R}} \pi^l_{uv} P_{v,l}. \end{aligned}$$

Proof: See Appendix B. □

IV. DESIGN OF DISTRIBUTED ATTACK-MODE-AND-VARIATION-DEPENDENT CONSENSUS ESTIMATORS

In this section, criteria for designing desired DACEs of the form (11) will be presented when the TPMs Π^1, Π^2, $\cdots$, Π^S governed by $\{\sigma_k, k \geq 0\}$ are time-varying in the sense of deterministic variation and stochastic variation, respectively. The attack-mode-and-variation-dependent estimator gain parameters $G^i_{u,h}$ and $K^i_{u,h}$, $\forall\ i \in \mathcal{V}; u \in \mathcal{R}; h \in \mathcal{S}$, will be solved out such that the resultant estimation error system (20) and (21) is stochastically stable and has a prescribed H_∞ performance level.

The following theorem provides a criterion on the existence of DACEs (11) in the case of deterministic variation.

Theorem 3 For given scalars $\alpha, \beta \in (0, 1)$, $\gamma > 0$, $\delta > 1$ and $\varrho > 0$, under the two-level multichannel attack model (7) with parameter matrices given by (8) and (9), where $\underline{\lambda}^u_{i,p}, \overline{\lambda}^u_{i,p} \in [0, 1]$, $\forall\ u \in \mathcal{R}$ are known scalars, if there exist matrices $P_{u,h} > 0, X_{u,h}, \bar{G}_{u,h}, \bar{K}_{u,h}$ of appropriate dimensions and scalars $\rho_u > 0$ such that

$$X_{u,h} \le \delta X_{u,l}, \quad \forall\ h \neq l \tag{27}$$

$$\bar{\Xi}_{u,h} = \begin{bmatrix} \Xi^{(1)}_{u,h} & \bar{\Xi}^{(2)}_{u,h} & \Xi^{(3)}_{u,h} \\ * & \varrho^2 \tilde{P}_{u,h} - \varrho X^T_{u,h} - \varrho X_{u,h} & 0 \\ * & * & -NI \end{bmatrix} \le 0 \tag{28}$$

for all $u \in \mathcal{R}; h, l \in \mathcal{S}$, where $\bar{\Xi}^{(2)}_{u,h} = [X^T_{u,h}\tilde{A} + \bar{G}_{u,h}\tilde{\mathcal{L}} - \bar{K}_{u,h}\hat{\Lambda}_u\tilde{C}, -\bar{K}_{u,h}, X^T_{u,h}\tilde{B}, -\bar{K}_{u,h}\tilde{D}]^T$, then the proposed distributed secure consensus estimation problem is solvable by desired DACEs in the form of (11) for any switching signal with ADT satisfying (25). Moreover, the admissible estimator gain parameters in (11) can be given by

$$\tilde{G}_{u,h} = X^{-T}_{u,h}\bar{G}_{u,h}, \tilde{K}_{u,h} = X^{-T}_{u,h}\bar{K}_{u,h}, \ \forall\ u \in \mathcal{R}; h \in \mathcal{S}. \tag{29}$$

Proof: See Appendix C. □

The following theorem presents a criterion on the existence of admissible DACEs with the form (11) for the estimation error system (20) and (21) in the case of stochastic variation of the TPMs $\Pi^1, \Pi^2, \cdots, \Pi^S$.

Theorem 4 For given scalars $\beta \in (0, 1)$, $\gamma > 0$ and $\varrho > 0$, under the two-level multichannel attack model (7) with parameter matrices given by (8) and (9), where $\underline{\lambda}^u_{i,p}, \overline{\lambda}^u_{i,p} \in [0, 1]$, $\forall\ u \in \mathcal{R}$ are known scalars, if there exist matrices $P_{u,h} > 0, X_{u,h}, \bar{G}_{u,h}, \bar{K}_{u,h}$ of appropriate dimensions and scalars $\rho_u > 0$ such that

$$\hat{\Xi}_{u,h} = \begin{bmatrix} \check{\Xi}^{(1)}_{u,h} & \bar{\Xi}^{(2)}_{u,h} & \Xi^{(3)}_{u,h} \\ * & \varrho^2 \check{P}_{u,h} - \varrho X^T_{u,h} - \varrho X_{u,h} & 0 \\ * & * & -NI \end{bmatrix} \le 0 \tag{30}$$

for all $u \in \mathcal{R}; h \in \mathcal{S}$, then the proposed distributed secure consensus estimation problem is solvable by desired DACEs in the form of (11) with gain parameters given by (29).

Proof: The proof is similar to the counterpart in the proof for Theorem 3. □

Remark 3 Based on Theorems 3 and 4, the proposed distributed secure consensus estimation problem can be converted into the following optimization problem

$$\underset{\mathcal{F}}{\text{minimize}}\ (\lambda) \ \text{ subject to (27) and (28) (or (30)),}$$

where $\lambda = \gamma^2$ and $\mathcal{F}$ is the set of all feasible solutions from linear matrix inequalities (LMIs) (27) and (28) in Theorem 3 or (30) in Theorem 4. In this case, by solving the above minimization problem, one can solve out desired resilient DACEs (11), while guaranteeing the stability and the optimal H_∞ performance level $\gamma = \sqrt{\lambda}$ of the resultant estimation error system (20) and (21) under the two-level switching jamming attacks.

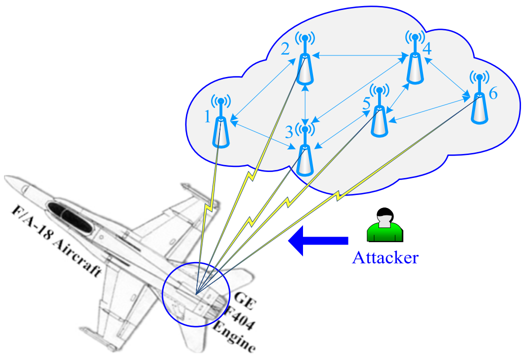


FIGURE 5. Distributed secure estimation for an F404 engine monitoring system under cyber attacks.

V. AN ILLUSTRATIVE EXAMPLE

In this section, to demonstrate the effectiveness and applicability of the proposed secure consensus estimation method, the target model is concerned with a military gas turbine engine, i.e., a GE F404 engine, in operational use with the RAAF fleet of F/A-18 aircraft [35].

Practically, gas turbine engines may be disturbed by uncontrolled external forces, such as wind gusts, gravity gradients, structural vibrations, and sensor noise, which generally degrade the engine system performance. For example, random vibration of aircraft engine system may affect the fatigue life of the engine so that accurate fatigue analysis should be conducted and the engine may be changed inexpensively at an early stage if required. Therefore, one of the objectives in the simulation is to take into account the effects of the external disturbance modeled by $w(k)$ and sensors' noise (measurement noise) indicated by $v_i(k)$ when estimation and assessment of engine condition are performed. On the other hand, to extract engine condition assessment information, an on-board engine monitoring system (EMS) is usually utilized [35]. In the following, we consider that the EMS consists of a group of smart sensors to monitor the engine condition assessment data. Sensors share their measurements among themselves through wireless channels for further analyzing and processing, such as computing estimations of the engine's state signal, as illustrated in Fig. 5. In the simulation, 6 interacting sensors are deployed to form a local interaction network with its topology shown in Fig. 5. Moreover, in a military environment, sensors are not always available to receive exact engine condition assessment information due to the existence of cyber adversaries. Jamming attacks on wireless transmissions and further sensor measurement losses may be present in an F404 engine monitoring system. In this case, how to provide a secure estimation method to track such an aircraft engine system through wireless data transmissions subject to multichannel jamming attacks and noise is important and necessary. We consider the following continuous-time linearized model of the F-404 engine originally presented in [35]

$$\dot{s}(t) = \begin{bmatrix} -1.46 & 0 & 0.2480 \\ 0.1643 & -0.4 & -0.3788 \\ 0.3107 & 0 & -2.23 \end{bmatrix} s(t) + \begin{bmatrix} 0.2 \\ 0.8 \\ -0.2 \end{bmatrix} w(t),$$

where $s(t) = [s^1(t), s^2(t), s^3(t)]^T$ with $s^1(t), s^2(t)$ representing the horizontal position and $s^3(t)$ denoting the altitude of the aircraft, respectively, and $w(t)$ is the external disturbance input. By the zero-order hold equivalent method with a sample period $h = 0.1sec$, a discrete-time model of the engine system is derived in the form of (1) with

$$A = \begin{bmatrix} 0.8673 & 0 & 0.2022 \\ 0.0145 & 0.9608 & -0.0316 \\ 0.0259 & 0 & 0.8032 \end{bmatrix}, B = \begin{bmatrix} 0.0165 \\ 0.0789 \\ -0.0177 \end{bmatrix}.$$

Other system parameters in (2) and (5) are given as $E = [1 \ \ 0 \ \ 1]$, $F = 1$, $C_i = diag\{1 + 0.1i, 1 + 0.1i, 1 + 0.1i\}$, $D_i = [1/i, 1/i, -1/i]^T$, $i \in \mathcal{V} = \{1, 2, \cdots, 6\}$.

It is assumed that there are two attack modes in (7), i.e., $r_k = u \in \{1, 2\}$ and the unknown model parameter matrices Λ_i^u at each attack mode are given as follows:

- On sensor 1, $diag\{1, 0.2, 0\} \leq \Lambda_1^1 \leq diag\{1, 0.5, 0\}$ and $diag\{1, 0.2, 1\} \leq \Lambda_1^2 \leq diag\{1, 0.5, 1\}$;
- On sensor 2, $diag\{0.1, 1, 0\} \leq \Lambda_2^1 \leq diag\{0.6, 1, 0\}$ and $diag\{0.1, 0.4, 0.2\} \leq \Lambda_2^2 \leq diag\{0.5, 0.8, 0.6\}$;
- On sensor 3, $diag\{0, 0.5, 1\} \leq \Lambda_3^1 \leq diag\{0, 0.8, 1\}$ and $diag\{1, 0.3, 0.3\} \leq \Lambda_3^2 \leq diag\{1, 0.8, 0.5\}$;
- On sensor 4, $diag\{0, 0.3, 0\} \leq \Lambda_4^1 \leq diag\{0, 0.7, 0\}$ and $diag\{0.6, 0.5, 1\} \leq \Lambda_4^2 \leq diag\{0.8, 0.9, 1\}$;
- On sensor 5, $diag\{0.4, 0, 0.2\} \leq \Lambda_5^1 \leq diag\{0.9, 0, 0.6\}$ and $diag\{0.3, 0.2, 0.1\} \leq \Lambda_5^2 \leq diag\{0.7, 0.4, 0.3\}$; and
- On sensor 6, $diag\{1, 0.5, 0\} \leq \Lambda_6^1 \leq diag\{1, 0.8, 0\}$ and $\Lambda_6^2 = diag\{1, 1, 1\}$.

As can be seen from the above attack model parameter matrices, the jamming status at mode 1 is more severe than the one at mode 2 since sensors' measurements through some channels may be completely lost due to successful attacks on those channels. Therefore, the attacker can turn off a few attacks at mode 2 in order to save the energy. Regarding how to select a specific attack mode at every time of instant, the attacker may be based on some prescribed tasks related to energy issues or even purely carries out random attacks to deceive detectors and estimators. For simplicity, it is assumed the high-level switching signal has two modes, i.e., $\sigma_k = h \in \{1, 2\}$. Set $\beta = 0.4$ and $\rho = 1$.

In the case of deterministic variation, applying Theorem 3 with $\alpha = 0.01$ and $\delta = 1.02$, it is found that the proposed distributed secure estimation problem is solved by desired DACEs in the form of (11) for any switching signal $\{\sigma_k, k \geq 0\}$ with ADT satisfying $\tau_a > \tau_a^* = 1.9703$. The optimal H_∞ noise attenuation level is given by $\gamma_{min} = 1.6039$. In the case of stochastic variation, applying Theorem 4, we find that the proposed distributed secure estimation problem is solved by desired DACEs in the form of (11) with the optimal H_∞ noise attenuation level given by $\gamma_{min} = 1.6026$. Letting the external disturbance and measurement noise on each sensor node be $w(k) = cos^2(k)/(1 + (k + 1)^2)$ and $v_i(k) = 2e^{-0.1ik}sin(0.4k)$, $\forall \ i \in \mathcal{V}$. It can be verified that $w(k), v_i(k) \in l_2[0, \infty)$. Choose the initial conditions $s_0 = [\pi/5, \pi/6, \pi/8]^T$ and $x_0^i = [rand, rand, rand]^T$, where $rand$ is a random number satisfying (0, 1). In the sequel, for brevity, only the simulation under stochastic high-level switching is provided. Applying the obtained DACEs to the discretized model of the engine system, Fig. 6 illustrates the evolutions of attack modes r_k and variation modes σ_k; Fig. 7 shows the trajectories of the target state $s(k)$ and state estimations $x_i(k)$ on sensors; while Fig. 8 demonstrates the output estimation errors $e_i^z(k)$ on sensors. Hence, it can be seen that the designed DACEs well estimate the target states, which verifies the effectiveness of the proposed distributed secure consensus estimation method.

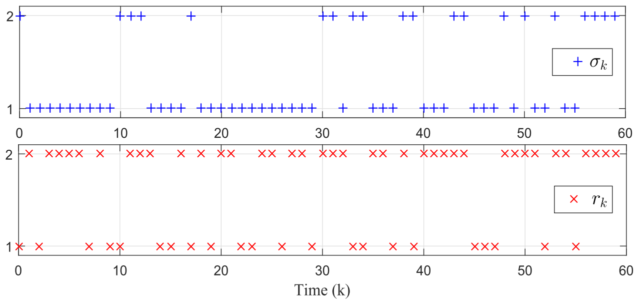


FIGURE 6. Attack modes $\{r_k, k \geq 0\}$ and variation modes $\{\sigma_k, k \geq 0\}$.

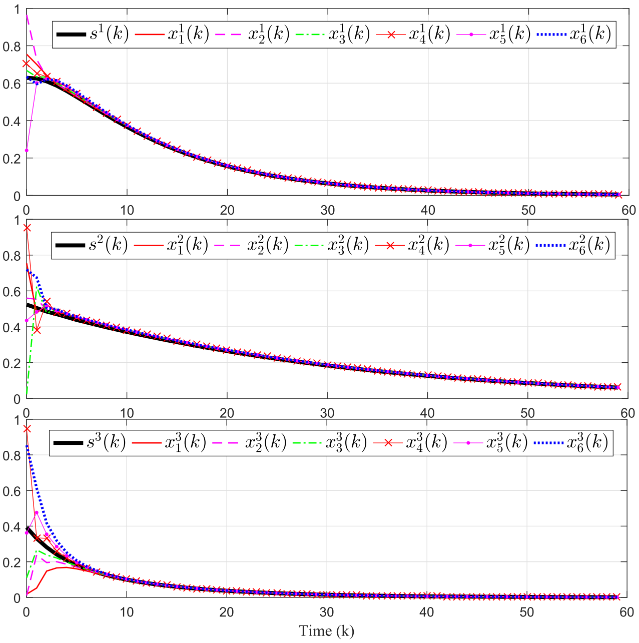


FIGURE 7. The F404 engine state signal $s(k) = [s^1(k), s^2(k), s^3(k)]^T$ and its estimations $x_i(k) = [x_i^1(k), x_i^2(k), x_i^3(k)]^T$, $\forall \ i \in \mathcal{V}$, on each sensor.

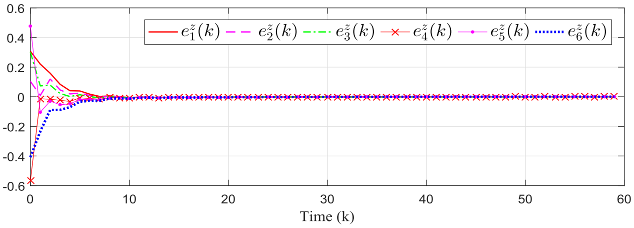


FIGURE 8. The output estimation errors $e_i^z(k) = z^s(k) - z_i^x(k), \forall \in \mathcal{V}$, on each sensor.

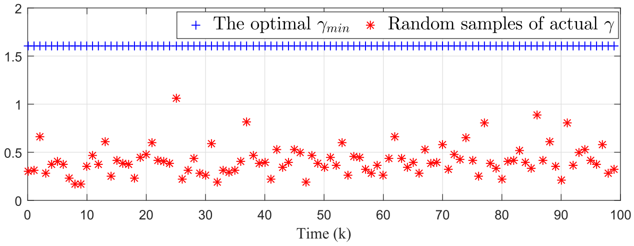


FIGURE 9. Random samples of the actual H_∞ performance level γ.

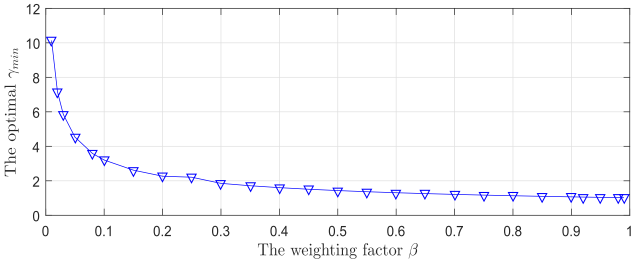


FIGURE 10. Relationship between the weighting factor β and the resultant optimal H_∞ performance level γ_{min}.

We next run additional 100 random simulations on calculating the actual H_∞ performance level due to random switching in the paper, and the simulation results are presented in Fig. 9. It is seen that the H_∞ performance is always guaranteed. Eventually, by choosing different values of the weighting factor β, and applying the corresponding result derived from Theorem 4, we obtain the relationship between β and the minimal value of the weighting average H_∞ performance level γ_{min}, as illustrated in Fig. 10, from which it is shown that one can properly select the weighting factor β to obtain desirable weighting H_∞ performance, thus the introduction of β increases the flexible dimensions in the solution space for the formulated H_∞ optimization problem.

VI. CONCLUSION

The distributed secure estimation problem over wireless sensor networks subject to random multichannel jamming attacks has been studied. Each sensor's measurement has been divided into multiple components according to the dimension of measurement signal and then transmitted via multiple wireless channels. An active adversary has been present to jam sensors' measurement transmission channels. When a specific measurement channel has been successfully jammed, the corresponding measurement has been dropped dependent on the jamming status of the channel. Specifically, a two-level switching attack model has been developed to capture the random attack strategies through multiple measurement channels. Then, distributed attack-mode-and-variation-dependent consensus estimators have been designedly proposed to achieve secure consensus estimation for target tracking. Criteria for designing desired distributed estimators have been also presented to guarantee the stochastic stability of the resultant estimation error system with a prescribed system performance index. An aircraft gas turbine engine system has been borrowed to illustrate the effectiveness of the proposed distributed secure consensus estimation method.

APPENDIX

A. PROOF OF THEOREM 1

The proof is twofold. In the first part, the stochastic stability of the resultant error system will be proved. In the second part of the proof, the H_∞ performance will be considered.

i) Proof of the stochastic stability. Let $w(k) \equiv 0$ and $\tilde{v}(k) \equiv 0$. Consider a Lyapunov functional candidate for the system (20) and (21) of the following quadratic form

$$V(\tilde{e}_x(k), r_k, \sigma_k) = \tilde{e}_x^T(k) P_{r_k,\sigma_k} \tilde{e}_x(k). \tag{31}$$

Then, from the point $(\tilde{e}_x(k) = \tilde{e}_x, r_k = u, \sigma_k = h)$ for all $u \in \mathcal{R}$ and $h \in \mathcal{S}$, calculating the forward difference along the system (20) yields

$$\begin{aligned}\Delta V(\tilde{e}_x, u, h) &= \mathbb{E}\left\{V(\tilde{e}_x(k+1), r_{k+1}, \sigma_{k+1})|_{\tilde{e}_x,u,h}\right\} \\ &\quad - V(\tilde{e}_x, u, h) \\ &= \tilde{e}_x^T(k)\left(\mathscr{A}_{u,h}^T \tilde{P}_{u,h} \mathscr{A}_{u,h} - P_{u,h}\right)\tilde{e}_x(k) \\ &\quad + 2\tilde{e}_x^T(k)\mathscr{A}_{u,h}^T \tilde{P}_{u,h} \mathscr{B}_{u,h} \check{e}_x(k) \\ &\quad + \check{e}_x^T(k)\mathscr{B}_{u,h}^T \tilde{P}_{u,h} \mathscr{B}_{u,h} \check{e}_x(k).\end{aligned} \tag{32}$$

Since $\check{e}_x(k) = \tilde{\Lambda}_u \tilde{C} \tilde{e}_x(k)$, we know from (19) that

$$\begin{aligned}\check{e}_x^T(k)\check{e}_x(k) &= \tilde{e}_x^T(k)\tilde{C}^T \tilde{\Lambda}_u^T \tilde{\Lambda}_u \tilde{C} \tilde{e}_x(k) \\ &\leq \tilde{e}_x^T(k)\tilde{C}^T \check{\Lambda}_u^T \check{\Lambda}_u \tilde{C} \tilde{e}_x(k).\end{aligned} \tag{33}$$

Then, we further obtain

$$\rho_u \tilde{e}_x^T(k)\tilde{C}^T \check{\Lambda}_u^T \check{\Lambda}_u \tilde{C} \tilde{e}_x(k) - \rho_u \check{e}_x^T(k)\check{e}_x(k) \geq 0, \tag{34}$$

where $\rho_u > 0, \forall\, u \in \mathcal{R}$.

Adding the left-hand side of (34) to (32) and letting $\theta(k) = [\tilde{e}_x^T(k), \check{e}_x^T(k)]^T$, one has

$$\Delta V(\tilde{e}_x, u, h) \leq \theta^T(k) \Theta_{u,h} \theta(k), \tag{35}$$

where $\Theta_{u,h} = [\Theta_{u,h}^{(p,q)}]_{2\times 2}$ is a symmetric block matrix with its entries given by $\Theta_{u,h}^{(1,1)} = \mathscr{A}_{u,h}^T \tilde{P}_{u,h} \mathscr{A}_{u,h} - P_{u,h} + \rho_u \tilde{C}^T \check{\Lambda}_u^T \check{\Lambda}_u \tilde{C}$, $\Theta_{u,h}^{(1,2)} = \mathscr{A}_{u,h}^T \tilde{P}_{u,h} \mathscr{B}_{u,h}$, and $\Theta_{u,h}^{(2,2)} = \mathscr{B}_{u,h}^T \tilde{P}_{u,h} \mathscr{B}_{u,h} - \rho_u I$.

Thus, applying Schur complement [33] to (24), it is straightforward to derive that

$$\Delta V(\tilde{e}_x, u, h) \leq -\alpha \tilde{e}_x^T(k) P_{u,h} \tilde{e}_x(k). \tag{36}$$

Adding up $\Delta V(\tilde{e}_x, u, h)$ from k_s to k and taking expectations, it follows from (36) that

$$\begin{aligned}\mathbb{E}&\left\{V(\tilde{e}_x(k), r_k, \sigma_k)|_{\tilde{e}_x(k_s), r_{k_s}, \sigma_{k_s}}\right\}\\ &\leq (1-\alpha)^{k-k_s}\mathbb{E}\left\{V(\tilde{e}_x(k_s), r_{k_s}, \sigma_{k_s})\right\}. \end{aligned}\tag{37}$$

Recalling $P_{u,h} \leq \delta P_{u,l}$, at each switching instant $k = k_s$, one has

$$\mathbb{E}\left\{V(\tilde{e}_x(k_s), r_{k_s}, \sigma_{k_s})\right\} \leq \delta \mathbb{E}\left\{V(\tilde{e}_x(k_s), r_{k_s}, \sigma_{\tilde{k}_s})\right\}. \tag{38}$$

Combining (37) and (38) yields

$$\begin{aligned}\mathbb{E}&\left\{V(\tilde{e}_x(k), r_k, \sigma_k)|_{\tilde{e}_x(k_0), r_{k_0}, \sigma_{k_0}}\right\}\\ &\leq (1-\alpha)^{k-k_s}\delta\mathbb{E}\left\{V(\tilde{e}_x(k_s), r_{k_s}, \sigma_{\tilde{k}_s})|_{\tilde{e}_x(k_0), r_{k_0}, \sigma_{k_0}}\right\}\\ &\leq \cdots \leq (1-\alpha)^{k-k_0}\delta^{N_\sigma(k,k_0)}\mathbb{E}\left\{V(\tilde{e}_x(k_0), r_{k_0}, \sigma_{k_0})\right\}\\ &\leq (1-\alpha)^{k-k_0}\delta^{N_0+\frac{k-k_0}{\tau_a}}\mathbb{E}\left\{V(\tilde{e}_x(k_0), r_{k_0}, \sigma_{k_0})\right\}\\ &= \delta^{N_0}e^{(k-k_0)(\ln(1-\alpha)+\frac{\ln(\delta)}{\tau_a})}\mathbb{E}\left\{V(\tilde{e}_x(k_0), r_{k_0}, \sigma_{k_0})\right\}. \end{aligned}\tag{39}$$

If (25) holds, then we have $\ln(1-\alpha) + \frac{\ln(\delta)}{\tau_a} < 0$, i.e., $e^{\ln(1-\alpha)+\ln(\delta)/\tau_a} < 1$. Denote $\varepsilon = e^{\ln(1-\alpha)+\ln(\delta)/\tau_a}$ and $\eta = \delta^{N_0}$. Then, (39) can be rewritten as

$$\begin{aligned}\mathbb{E}&\left\{V(\tilde{e}_x(k), r_k, \sigma_k)|_{\tilde{e}_x(k_0), r_{k_0}, \sigma_{k_0}}\right\}\\ &\leq \eta\varepsilon^{k-k_0}\mathbb{E}\left\{V(\tilde{e}_x(k_0), r_{k_0}, \sigma_{k_0})\right\}. \end{aligned}\tag{40}$$

Therefore, it follows form (40) that

$$\begin{aligned}\mathbb{E}&\left\{\sum_{k=0}^{N_\sigma(k_T,k)} V(\tilde{e}_x(k), r_k, \sigma_k)|_{\tilde{e}_x(k_0), r_{k_0}, \sigma_{k_0}}\right\}\\ &\leq \eta(1+\varepsilon+\cdots+\varepsilon^{N_\sigma(k_T,k)})V(\tilde{e}_x(k_0), r_{k_0}, \sigma_{k_0})\\ &= \frac{\eta(1-\varepsilon^{N_\sigma(k_T,k)+1})}{1-\varepsilon}V(\tilde{e}_x(k_0), r_{k_0}, \sigma_{k_0}). \end{aligned}\tag{41}$$

Noting that $\varepsilon \in (0, 1)$, thus one has

$$\begin{aligned}\lim_{k_T\to\infty}\mathbb{E}&\left\{\sum_{k=0}^{N_\sigma(k_T,k)} V(\tilde{e}_x(k), r_k, \sigma_k)|_{\tilde{e}_x(k_0), r_{k_0}, \sigma_{k_0}}\right\}\\ &\leq \frac{\eta}{1-\varepsilon}V(\tilde{e}_x(k_0), r_{k_0}, \sigma_{k_0}). \end{aligned}\tag{42}$$

On the other hand, recalling that $V(\tilde{e}_x, u, h) = \tilde{e}_x^T(k)P_{u,h}\tilde{e}_x(k)$, it is easy to obtain

$$\begin{aligned}\lim_{k_T\to\infty}\mathbb{E}&\left\{\sum_{k=0}^{N_\sigma(k_T,k)} V(\tilde{e}_x(k), r_k, \sigma_k)|_{\tilde{e}_x(k_0), r_{k_0}, \sigma_{k_0}}\right\}\\ &\geq \lim_{k_T\to\infty}\mathbb{E}\left\{\sum_{k=0}^{N_\sigma(k_T,k)} \phi\|\tilde{e}_x(k)\|^2|_{\tilde{e}_x(k_0), r_{k_0}, \sigma_{k_0}}\right\}, \end{aligned}\tag{43}$$

where $\phi = \min_{u\in\mathcal{R}, h\in\mathcal{S}}(\lambda_{min}(P_{u,h}))$.

Together with (42) and (43), we have

$$\begin{aligned}\lim_{k_T\to\infty}\mathbb{E}&\left\{\sum_{k=0}^{N_\sigma(k_T,k)} \|\tilde{e}_x(k)\|^2|_{\tilde{e}_x(k_0), r_{k_0}, \sigma_{k_0}}\right\}\\ &\leq \frac{\eta}{\phi(1-\varepsilon)}V(\tilde{e}_x(k_0), r_{k_0}, \sigma_{k_0}) < \infty. \end{aligned}\tag{44}$$

Following Definition 1, the resultant estimation error system with $w(k) \equiv 0$ and $\tilde{v}(k) \equiv 0$ is stochastically stable.

ii) Proof of the H_∞ noise attenuation performance. For all nonzero $w(k)$, $v_i(k) \in l_2[0, \infty)$, $\forall\ i \in \mathcal{V}$, we denote $\tilde{J}(k_s) = \frac{1}{N}\tilde{e}_z^T(k_s)\tilde{e}_z(k_s) - \beta\gamma^2 w^T(k_s)w(k_s) - (1-\beta)\gamma^2/N\tilde{v}^T(k_s)\tilde{v}(k_s)$.

Similar to the discussion in the first part of the proof, it is not difficult to derive from (24) that

$$\Delta V(\tilde{e}_x(k), r_k, \sigma_k) + \mathbb{E}\left\{\tilde{J}(k)\right\} \leq -\alpha\tilde{e}_x^T(k)P_{u,h}\tilde{e}_x(k). \tag{45}$$

Then, we have

$$\begin{aligned}\mathbb{E}&\left\{V(\tilde{e}_x(k+1), r_{k+1}, \sigma_{k+1})|_{\tilde{e}_x, u, h}\right\}\\ &\leq (1-\alpha)\mathbb{E}\left\{V(\tilde{e}_x(k), r_k, \sigma_k)\right\} - \mathbb{E}\left\{\tilde{J}(k)\right\}. \end{aligned}\tag{46}$$

Therefore, for any $\sigma_k = h \in \mathcal{S}$, summing up (46) from k_0 to k yields

$$\begin{aligned}\mathbb{E}&\left\{V(\tilde{e}_x(k), r_k, h)|_{\tilde{e}_x(k_0), r_{k_0}, h}\right\}\\ &\leq (1-\alpha)^{k-k_0}\mathbb{E}\left\{V(\tilde{e}_x(k_0), r_{k_0}, h)\right\}\\ &\quad - \sum_{q=k_0}^{k-1}(1-\alpha)^{k-q-1}\mathbb{E}\left\{\tilde{J}(q)\right\}. \end{aligned}\tag{47}$$

Under zero initial condition, one has that $\mathbb{E}\{V(\tilde{e}_x(k_0), r_{k_0}, h)\} = 0$ and $\mathbb{E}\{V(\tilde{e}_x(k), r_k, h)|_{\tilde{e}_x(k_0), r_{k_0}, h}\} \geq 0$. Thus, we obtain

$$\sum_{k=k_0}^{\infty}\sum_{q=k_0}^{k-1}(1-\alpha)^{k-q-1}\mathbb{E}\left\{\tilde{J}(q)\right\} \leq 0, \tag{48}$$

which means that $\sum_{q=k_0}^{\infty}\tilde{J}(q) < 0$. After simple computation, it is easy to find that $J_\infty(w, v) < 0$ holds for a guaranteed H_∞ performance level γ. This completes the proof. □

B. PROOF OF THEOREM 2

Consider that the Lyapunov functional candidate has the same form of (31). Emanating from the point ($\tilde{e}_x(k) = \tilde{e}_x$, $r_k = u$, $\sigma_k = h$) for all $u \in \mathcal{R}$ and $h \in \mathcal{S}$, we have

$$\begin{aligned}\Delta V(\tilde{e}_x, u, h) &= \mathbb{E}\left\{V(\tilde{e}_x(k+1), r_{k+1}, \sigma_{k+1})|_{\tilde{e}_x, u, h}\right\}\\ &\quad - V(\tilde{e}_x, u, h)\\ &= \tilde{e}_x^T(k+1)\check{P}_{u,h}\tilde{e}_x(k+1)\\ &\quad - \tilde{e}_x^T(k)P_{u,h}\tilde{e}_x(k). \end{aligned}\tag{49}$$

Similar to the proof for Theorem 1, we first prove the stochastic stability and let $w(k) \equiv 0$ and $\tilde{v}(k) \equiv 0$. Then, according to (20) and (34), one can get

$$\begin{aligned}\Delta V(\tilde{e}_x, u, h) \leq \tilde{e}_x^T(k)(&\mathscr{A}_{u,h}^T\check{P}_{u,h}\mathscr{A}_{u,h} + \rho_u\tilde{C}^T\check{\Lambda}_u^T\check{\Lambda}_u\tilde{C}\\ &- P_{u,h})\tilde{e}_x(k) + 2\tilde{e}_x^T(k)\mathscr{A}_{u,h}^T\check{P}_{u,h}\mathscr{B}_{u,h}\check{e}_x(k)\end{aligned}$$

$$\begin{aligned}&+\check{e}_x^T(k)(\mathscr{B}_{u,h}^T\check{P}_{u,h}\mathscr{B}_{u,h}-\rho_u I)\check{e}_x(k)\\ &=\theta^T(k)\check{\Theta}_{u,h}\theta(k),\end{aligned} \tag{50}$$

where $\theta(k)=[\tilde{e}_x^T(k),\check{e}_x^T(k)]^T$ and $\check{\Theta}_{u,h}=[\check{\Theta}_{u,h}^{(p,q)}]_{2\times 2}$ is a symmetric block matrix with its entries given by $\check{\Theta}_{u,h}^{(1,1)}=\mathscr{A}_{u,h}^T\check{P}_{u,h}\mathscr{A}_{u,h}-P_{u,h}+\rho_u\tilde{C}^T\check{\Lambda}_u^T\check{\Lambda}_u\tilde{C}$, $\check{\Theta}_{u,h}^{(1,2)}=\mathscr{A}_{u,h}^T\check{P}_{u,h}\mathscr{B}_{u,h}$, and $\check{\Theta}_{u,h}^{(2,2)}=\mathscr{B}_{u,h}^T\check{P}_{u,h}\mathscr{B}_{u,h}-\rho_u I$. By virtue of Schur complement, it can be seen from (26) that $\check{\Theta}_{u,h}<0$. Thus, one has $\Delta V(\tilde{e}_x(k),r_k,\sigma_k)<0$. Then, following a similar pattern of the proof of [34, Th. 1], it can be shown that $\mathbb{E}\left\{\sum_{k=0}^{\infty}\|\tilde{e}_x(k)\|^2|_{s_0,r_0,\sigma_0}\right\}<\infty$. By Definition 1, it can be concluded that the resultant error system (20) is stochastically stable.

Next, we establish the H_∞ performance for the system (20) and (21) in the case of nonzero $w(k)$, $v_i(k)\in l_2[0,\infty)$, $\forall\, i\in\mathcal{V}$. Denote $\tilde{J}(k)=\frac{1}{N}\tilde{e}_z^T(k)\tilde{e}_z(k)-\beta\gamma^2w^T(k)w(k)-(1-\beta)\gamma^2/N\tilde{v}^T(k)\tilde{v}(k)$.

Then, we have

$$\Delta V(\tilde{e}_x(k),r_k,\sigma_k)+\tilde{J}(k)\leq\check{\theta}^T(k)\tilde{\Theta}_{u,h}\check{\theta}(k), \tag{51}$$

where $\check{\theta}(k)=[\tilde{e}_x^T(k),\check{e}_x^T(k),w^T(k),\check{v}^T(k)]^T$ and $\tilde{\Theta}_{u,h}=[\tilde{\Theta}_{u,h}^{(p,q)}]_{4\times 4}$ is a symmetric block matrix with its entries given by $\tilde{\Theta}_{u,h}^{(1,1)}=\mathscr{A}_{u,h}^T\check{P}_{u,h}\mathscr{A}_{u,h}-P_{u,h}+\rho_u\tilde{C}^T\check{\Lambda}_u^T\check{\Lambda}_u\tilde{C}+\frac{1}{N}\tilde{E}^T\tilde{E}$, $\tilde{\Theta}_{u,h}^{(1,2)}=\mathscr{A}_{u,h}^T\check{P}_{u,h}\mathscr{B}_{u,h}$, $\tilde{\Theta}_{u,h}^{(1,3)}=\mathscr{A}_{u,h}^T\check{P}_{u,h}\tilde{B}$, $\tilde{\Theta}_{u,h}^{(1,4)}=\mathscr{A}_{u,h}^T\check{P}_{u,h}\mathscr{D}_{u,h}$, $\tilde{\Theta}_{u,h}^{(2,2)}=\mathscr{B}_{u,h}^T\check{P}_{u,h}\mathscr{B}_{u,h}-\rho_u I$, $\tilde{\Theta}_{u,h}^{(2,3)}=\mathscr{B}_{u,h}^T\check{P}_{u,h}\tilde{B}$, $\tilde{\Theta}_{u,h}^{(2,4)}=\mathscr{B}_{u,h}^T\check{P}_{u,h}\mathscr{D}_{u,h}$, $\tilde{\Theta}_{u,h}^{(3,3)}=-\beta\gamma^2I+\tilde{B}^T\check{P}_{u,h}\tilde{B}+\frac{1}{N}\tilde{F}^T\tilde{F}$, $\tilde{\Theta}_{u,h}^{(3,4)}=\tilde{B}^T\check{P}_{u,h}\mathscr{D}_{u,h}$ and $\tilde{\Theta}_{u,h}^{(4,4)}=-\frac{(1-\beta)\gamma^2}{N}I+\mathscr{D}_{u,h}^T\check{P}_{u,h}\mathscr{D}_{u,h}$. By Schur complement, it can be readily seen that $\tilde{\Theta}_{u,h}<0$ is equivalent to $\check{\Xi}_{u,h}<0$ in (26). Thus, one has

$$\tilde{J}(k)<-\Delta V(\tilde{e}_x(k),r_k,\sigma_k). \tag{52}$$

Summing up (52) from $k=0$ to $k=k_T$, where $k_T\to\infty$, under zero initial condition that $\mathbb{E}\{V(\tilde{e}_x(0),r_0,\sigma_0)\}=0$ and $\mathbb{E}\{V(\tilde{e}_x(k),r_k,\sigma_k)|_{\tilde{e}_x(0),r_0,\sigma_0}\}\geq 0$, we finally obtain $\sum_{k=0}^{\infty}\tilde{J}(k)<0$, which means that $J_\infty(w,v)<0$ holds. This completes the proof. □

C. PROOF OF THEOREM 3

Preforming a congruence transformation to (24) by $diag\{I,\tilde{P}_{u,h}^{-1}X_{u,h},I\}$ and letting $\bar{G}_{u,h}=\tilde{G}_{u,h}X_{u,h}$ and $\bar{K}_{u,h}=\tilde{K}_{u,h}X_{u,h}$, it is straightforward to have (28) where $\varrho^2\tilde{P}_{u,h}-\varrho X_{u,h}^T-\varrho X_{u,h}$ is replaced by $-\varrho X_{u,h}^T\tilde{P}_{u,h}^{-1}\varrho X_{u,h}$. Recalling that

$$(X_{u,h}-\varrho\tilde{P}_{u,h})^T\tilde{P}_{u,h}^{-1}(X_{u,h}-\varrho\tilde{P}_{u,h})\geq 0 \tag{53}$$

for all $\varrho>0$. Obviously, (53) can be rewritten as

$$-X_{u,h}^T\tilde{P}_{u,h}^{-1}\varrho X_{u,h}\leq\varrho^2\tilde{P}_{u,h}-\varrho X_{u,h}^T-\varrho X_{u,h}, \tag{54}$$

which implies (28). Furthermore, (27) ensures (23) for all $h\neq l$; $u\in\mathcal{R}$; $h,l\in\mathcal{S}$. On the other hand, it is seen from (28) that $\varrho^2\tilde{P}_{u,h}-\varrho X_{u,h}^T-\varrho X_{u,h}<0$. In other words, $X_{u,h}>0$, thus, (29) is verified. This completes the proof. □

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[2] R. R. Brooks, P. Ramanathan, and A. M. Sayeed, "Distributed target classification and tracking in sensor networks," *Proc. IEEE*, vol. 91, no. 8, pp. 1163–1171, Aug. 2003.

[3] C. Huang, D. W. C. Ho, and J. Lu, "Partial-information-based distributed filtering in two-targets tracking sensor networks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 59, no. 4, pp. 820–832, Apr. 2012.

[4] D. Zhang, P. Shi, W.-A. Zhang, and L. Yu, "Energy-efficient distributed filtering in sensor networks: A unified switched system approach," *IEEE Trans. Cybern.*, to be published. [Online]. Available: http://dx.doi.org/10.1109/TCYB.2016.2553043.

[5] Y. Zhu, L. Zhang, and W. X. Zheng, "Distributed H_∞ filtering for a class of discrete-time Markov Jump Lur'e systems with redundant channels," *IEEE Trans. Ind. Electron.*, vol. 63, no. 3, pp. 1876–1885, Mar. 2016.

[6] X. Ge and Q.-L. Han, "Distributed event-triggered H_∞ filtering over sensor networks with communication delays," *Inf. Sci.*, vol. 291, pp. 128–142, Jan. 2015.

[7] D. Zhang, L. Yu, and W. A. Zhang, "Energy efficient distributed filtering for a class of nonlinear systems in sensor networks," *IEEE Sensors J.*, vol. 15, no. 5, pp. 3026–3036, May 2015.

[8] T. Bonaci, L. Bushnell, and R. Poovendran, "Node capture attacks in wireless sensor networks: A system theoretic approach," in *Proc. 49th IEEE Conf. Decision Control*, Atlanta, GA, USA, Dec. 2010, pp. 6765–6772.

[9] H. Chan and A. Perrig, "Security and privacy in sensor networks," *Computer*, vol. 36, no. 10, pp. 103–105, Oct. 2003.

[10] H. Li, L. Lai, and W. Zhang, "Communication requirement for reliable and secure state estimation and control in smart grid," *IEEE Smart Grid*, vol. 2, no. 3, pp. 476–486, Sep. 2011.

[11] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2005, pp. 49–63.

[12] P. Pradhan and P. Venkitasubramaniam, "Stealthy attacks in dynamical systems: Tradeoffs between utility and detectability with application in anonymous systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 4, pp. 779–792, Apr. 2017.

[13] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *Proc. 49th IEEE Conf. Decision Control*, Atlanta, GA, USA, Dec. 2010, pp. 5967–5972.

[14] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, "A game-theoretic approach to fake-acknowledgment attack on cyber-physical systems," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 3, no. 1, pp. 1–11, Mar. 2016. [Online]. Available: http://dx.doi.org/10.1109/TSIPN.2016.2611446

[15] R. Gentz, S. X. Wu, H.-T. Wai, A. Scaglione, and A. Leshem, "Data injection attacks in randomized gossiping," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 2, no. 4, pp. 523–538, Dec. 2016.

[16] 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.

[17] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal DoS attack scheduling in wireless networked control system," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 3, pp. 843–852, May 2016.

[18] Y. Yuan, H. Yuan, L. Guo, H. Yang, and S. Sun, "Resilient control of networked control system under DoS attacks: A unified game approach," *IEEE Trans. Ind. Informat.*, vol. 12, no. 5, pp. 1786–1794, Oct. 2016, [Online]. Available: http://dx.doi.org/10.1109/TII.2016.2542208

[19] A. Chan, X. Liu, G. Noubir, and B. Thapa, "Broadcast control channel jamming: Resilience and identification of traitors," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 2007, pp. 2496–2500.

[20] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, "Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach," *IEEE Trans. Autom. Control*, vol. 60, no. 10, pp. 2831–2836, Oct. 2015.

[21] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attack strategies and network defense policies in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 9, no. 8, pp. 1119–1133, Aug. 2010.

[22] R. Poisel, *Modern Communications Jamming Principles and Techniques*. Norwood, MA, USA: Artech House, 2011.

[23] J. He, P. Cheng, L. Shi, and J. Chen, "SATS: Secure average-consensus-based time synchronization in wireless sensor networks," *IEEE Trans. Signal Process.*, vol. 61, no. 24, pp. 6387–6400, Dec. 2013.

[24] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor Network Security: A Survey," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 2, pp. 52–73, 2nd Quart., 2009.

[25] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, Oct. 2002.

[26] A. Petitti, D. Di Paola, A. Rizzo, and G. Cicirelli, "Consensus-based distributed estimation for target tracking in heterogeneous sensor networks," in *Proc. 50th IEEE Conf. Decision Control Eur. Control Conf.*, Orlando, FL, USA, Dec. 2011, pp. 6648–6653.

[27] S. Zhu, C. Chen, W. Li, B. Yang, and X. Guan, "Distributed optimal consensus filter for target tracking in heterogeneous sensor networks," *IEEE Trans. Cybern.*, vol. 43, no. 6, pp. 1963–1976, Dec. 2013.

[28] J. Nilsson, "Real-time control systems with delays," Ph.D. dissertation, Lund Inst. Technol., Lund, Sweden, 1998.

[29] X. Ge, Q.-L. Han, and X. Jiang, "Distributed H_∞ filtering over sensor networks with heterogeneous Markovian coupling intercommunication delays," *IET Control Theory Appl.*, vol. 9, no. 1, pp. 82–90, Jan. 2015.

[30] L. Zhang, "H_∞ estimation for discrete-time piecewise homogeneous Markov jump linear system," *Automatica*, vol. 45, no. 11, pp. 2570–2576, Nov. 2009.

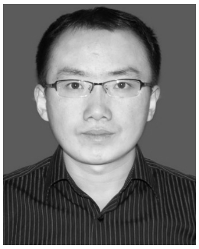
[31] G. Zhai, B. Hu, K. Yasuda, and A. N. Michel, "Qualitative analysis of discrete-time switched systems," in *Proc. Amer. Control Conf.*, Anchorage, AK, USA, May 2002, pp. 1880–1885.

[32] J. P. Hespanha and A. S. Morse, "Stability of switched systems with average dwell-time," in *Proc. 38th IEEE Conf. Decision Control*, Phoenix, AZ, USA, Dec. 1999, pp. 2655–2660.

[33] Q.-L. Han, "Absolute stability of time-delay systems with sector-bounded nonlinearity," *Automatica*, vol. 41, no. 12, pp. 2171–2176, Dec. 2005.

[34] E. Boukas and Z. Liu, "Robust H_∞ control of discrete-time Markovian jump linear systems with mode-dependent time-delays," *IEEE Trans. Autom. Control*, vol. 46, no. 12, pp. 1918–1924, Dec. 2001.

[35] R. W. Eustace, B. A. Woodyatt, G. L. Merrington, and T. A. Runacres, "Fault signatures obtained from fault implant tests on an F404 engine," *ASME Trans. J. Eng. Gas Turbines Power*, vol. 116, no. 1, pp. 178–183, Jan. 1994.



YANPENG GUAN received the B.Sc. degree in mathematics from Changchun Normal University, Changchun, China, in 2005, the M.Eng. degree in control theory and control engineering from Hangzhou Dianzi University, Hangzhou, China, in 2010, and the Ph.D. degree in computer engineering from Central Queensland University, Rockhampton, QLD, Australia, in 2014. He is currently a Lecturer with the Department of Automation, Shanxi University.

His research interests include networked control systems, cyber-physical systems, secure estimation, distributed control and estimation, and event-triggered control.

XIAOHUA GE received the B.Eng. degree in electronic and information engineering from Nanchang Hangkong University, Nanchang, China, in 2008, the M.Eng. degree in control theory and control engineering from Hangzhou Dianzi University, Hangzhou, China, in 2011, and the Ph.D. degree in computer engineering from Central Queensland University, Rockhampton, QLD, Australia, in 2014.

He was a Research Assistant with the Centre for Intelligent and Networked Systems, Central Queensland University, from 2011 to 2013. In 2014, he was a Research Fellow with the Centre for Intelligent and Networked Systems, Central Queensland University. From 2015 to 2016, he was a Research Fellow with the Griffith School of Engineering, Griffith University, Gold Coast, Australia. He is currently a Lecturer with the School of Software and Electrical Engineering, Swinburne University of Technology, Melbourne, Australia.

His current research interests include networked control and filtering, distributed networked control systems, multi-agent systems, and sensor networks.