This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSIPN.2018.2790361, IEEE Transactions on Signal and Information Processing over Networks



# A Novel Data Fusion Algorithm to Combat False Data Injection Attacks in Networked Radar Systems

Chaoqun Yang, *Student Member, IEEE,* Li Feng, Heng Zhang, *Member, IEEE,*
Shibo He, *Member, IEEE,* Zhiguo Shi, *Senior Member, IEEE*

***Abstract*—Networked radar systems are vulnerable to different types of attacks, including electronic countermeasure (ECM) jamming and false data injection (FDI) attack. Substantial research has concentrated on ECM jamming, which interferes with radar echoes between a radar and targets. However, FDI attack in which an attacker somehow replaces or modifies radars' measurements, has rarely been considered. FDI attack is much stealthier than ECM jamming, making detection more difficult. In this paper, we take the first attempt to investigate the FDI attack's effects on a networked radar system. Further, we propose a novel data fusion algorithm to combat this attack. The proposed algorithm can dramatically reduce the attack's adverse effects, since it creatively introduces data's confidence factors into data fusion and adaptively decreases the fusion weights of the injected data. Numerical results verify the effectiveness of the proposed algorithm.**

***Index Terms*—Covariance intersection, cyber physical system, data fusion, false data injection attack, networked radar system.**

## I. Introduction

In a networked radar system (NRS) [1], a number of radars, which are deployed appropriately in different geographic positions, are connected to a fusion center for detecting and tracking targets jointly, as shown in Fig. 1. Such an NRS can increase the accuracy of detecting and tracking targets significantly [2]. Therefore, it has wide applications including air traffic control [3] [4], military surveillance [5] [6], autonomous vehicles [7] [8], etc.

Unfortunately, the NRS is vulnerable to cyber attacks [9], because the wired or wireless networks connecting radars and the fusion center can be maliciously compromised. Since networked radar systems are usually deployed in civil and military infrastructures, cyber attacks potentially lead to great threats to national security and economy. Reuters ever reported a famous example [10]. In June 2014, 13 planes flying over Europe suddenly disappeared from radar screens and the whole process lasted for 25 minutes. Many governments suspected that the air traffic control systems had been hijacked.

The security issues of networked radar systems have received increasing attention recently. Most existing works have concerned how to combat electronic countermeasure (ECM) jamming that interferes with radar echoes between a radar and targets [11] [12]. However, few works have considered cyber attacks that potentially threaten to communication networks between radars and the fusion center. Cyber attacks can be easily launched when partial communication networks or radars are intruded or hijacked in an NRS. Compared with other cyber attacks, false data injection (FDI) attack is more difficult to be detected because the attacker can design injected data deliberately to avoid the intrusion detection [13]. Through modifying the measurements of attacked radars, FDI attack may deteriorate the estimation accuracy of the NRS. On the other hand, although FDI attack in cyber physical systems has been well studied [13], results in cyber physical systems can not be applied to networked radar systems directly. This is because most existing works about FDI attack do not consider data fusion which makes networked radar systems different from other cyber physical systems [1].

Motivated by this, firstly, we focus on studying the FDI attack's effects on an NRS. Specifically, we investigate the fusion estimation of an NRS when the FDI attack is launched, and we seek the relationship between the fusion estimation degradation of the NRS and time-invariant attack strength. In this way, we reveal that the FDI attack can dramatically

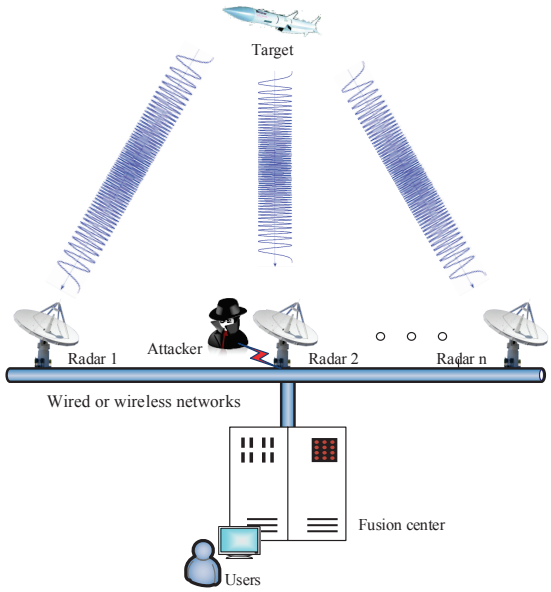



Fig. 1. A networked radar system under false data injection attack

C. Yang, S. He and Z. Shi are with the Faculty of Information Technology, Zhejiang University, Hangzhou, China. L. Feng is with the Faculty of Information Technology, Macau University of Science and Technology, Macau, China. H. Zhang is with Huaihai Institute of Technology, Lianyungang, China. (*Corresponding author: Zhiguo Shi*.)

This work is partially supported by Macao Science and Technology Development Fund under Grant 005/2016/A1, NSFC under Grant 61772467, 61503147, 61503337, U1401253, Zhejiang Provincial Natural Science Foundation of China under Grant LR16F010002, Y16F030011, and the National Nature Science Foundation of Jiangsu Province under Grant BK20171264.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSIPN.2018.2790361, IEEE Transactions on Signal and Information Processing over Networks



deteriorate the fusion estimation of the NRS when the attack strength is time-invariant. Roughly speaking, the reasons can be described as follows. Firstly, data fusion algorithms such as covariance intersection (CI) algorithm in the NRS assign fusion weights to different radars only depending on their estimate covariances. Secondly, the estimate covariances of the attacked radars have deviated from the actual estimate covariances when the attack is launched. Therefore, the data fusion algorithms based on unreasonable estimate covariances can not work efficiently.

To combat FDI attack for the NRS, we propose a novel data fusion algorithm named confident covariance intersection (CCI), where confidence factor is introduced to weight the estimate confidences of all radars. Different from the existing data fusion algorithms, the CCI algorithm assigns fusion weights relying on the estimate covariances and confidence factors simultaneously. Hence, the CCI algorithm can adaptively decrease the fusion weights of the injected data.

The contributions of this paper are summarized as follows:

- We reveal the relationship between the fusion estimation degradation of the NRS and time-invariant attack strength, and we prove that the FDI attack can dramatically deteriorate the fusion estimation of the NRS. To the best of our knowledge, this is the first work on studying the FDI attack in networked radar systems.
- We propose a CCI algorithm to combat the FDI attack. By integrating confidence factor into CI algorithm, the CCI algorithm can dramatically reduce the attack's adverse effects, and can be viewed as the generalization of the CI algorithm.

The rest of the paper is organized as follows. Section II reviews the related work. Section III presents the system model including target dynamic, an NRS and the FDI attack. Section IV analyzes the FDI attack's effects on the NRS. Section V describes the proposed algorithm, and analyzes its ability to combat the attack. Section VI presents numerical simulations. Finally, Section VII concludes the paper.

*Notations:* $\mathbb{R}^n$ stands for the set of $n\times 1$ vectors. $\mathbb{Z}^+$ denotes the set of positive integers. $\mathcal{N}(a,b)$ represents the Gaussian distribution with mean $a$ and covariance $b$. $X^T$ denotes the transpose of matrix $X$. $\mathrm{Tr(X)}$ denotes the trace of matrix $X$. $\rho(X)$ is the spectral radius of matrix $X$. For a variable $z$ and a set $A$, the following characteristic function indicates the subordinate relationship between them:

$$\chi_A(z) = \begin{cases} 0, & z \in A, \\ 1, & \text{otherwise.} \end{cases} \tag{1}$$

## II. Related Work

There are many researches on networked radar systems from different perspectives. For example, Gong *et al*. [14] [15] studied the coverage problem for bistatic networked radar systems to maximize intrusion detection. Bosse *et al*. [16] [17] considered the direct target location problem in an active NRS. Shi *et al*. [18] investigated the resource management problem for a distributed NRS. Deligiannis *et al*. [19] considered a power allocation problem for networked radar systems from the view of noncooperative game theory.

Although the security problems of networked radar systems have received increasing attention, among them, most current researches concentrated on ECM jamming, since it is a main threat to radars [11] [20]. For instance, Coluccia *et al*. [11] proposed a series of detection strategies based on adaptive beamformer orthogonal rejection technique to detect ECM signals from the received signals of an NRS. Zhao *et al*. [12] addressed a signal fusion-based algorithm to distinguish ECM jamming from radar targets. Wang *et al*. [21] proposed a coherent cancelling based suppression algorithm to suppress the false targets created by ECM jamming in an NRS.

Compared with ECM jamming, cyber attacks, which can be launched to the communication networks, are also important parts that can not be ignored for an NRS. Actually, cyber attacks have brought tremendous risks to communication networks in different systems. For example, communication networks which are vulnerable to cyber attacks in smart gird might lead to unreliable operations and extra expenditure [22] [23]. Distributed denial of service attack could disrupt service in Internet of Things by creating network congestion [24] [25] [26].

The reliability of an NRS depends on the reliability of communication networks in the NRS. However, few works have considered the vulnerability of NRS' communication networks to cyber attacks. A remarkable work is presented in [9], in which the authors proposed a chaos based communication algorithm to prevent the communication links in Indonesian maritime networked radar systems from potential cyber attacks.

On the other hand, FDI attack in cyber physical systems has been well studied. Extensive defense strategies have been proposed to combat FDI attack in different cyber physical systems. For example, Li *et al*. [13] proposed an online algorithm to detect the FDI attack in a smart grid. Illiano *et al*. [27] addressed a detection strategy of malicious data injections in wireless sensor networks. To combact the FDI attack in advanced metering infrastructure, Liu *et al*. [28] proposed a new collaborative intrusion detection mechanism. Using sparse optimization, Liu *et al*. [29] presented a detection approach for power grid . Yang *et al*. [30] proposed an en-route filtering scheme to filte false injected data for cyber physcial networked systmes. However, results in these works can not be applied directly into networked radar systems. To the best of our knowledge, there is rare work on studying the FDI attack in an NRS. Therefore, in this paper, we consider the FDI attack in an NRS.

Several remarkable studies on CI based algorithms can be found in the literatures [31] [32] [33] and [34]. Julier *et al*. [31] [32] proposed CI and split CI algorithms for the first time. Li *et al*. [33] provided the theoretical derivation of the split CI algorithm. Deng *et al*. [34] addressed a fast and recursive two-sensor CI algorithm. However, these CI based algorithms might fail to effectively achieve fusion estimation when cyber attacks eixst. Different from the existing CI based algorithms, the proposed CCI algorithm is the generalization of CI algorithm, with the novel function of combating the FDI

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSIPN.2018.2790361, IEEE Transactions on Signal and Information Processing over Networks



attack.

## III. System Model

In this section, we introduce the system model, including target dynamic, an NRS and the FDI attack.

### A. Target Dynamic

Consider a point target whose dynamic is given by

$$x_{k+1} = Fx_k + w_k, \tag{2}$$

where $x_k \in \mathbb{R}^n$ with $n \in \mathbb{Z}^+$, $x_k$ is the target state vector which usually consists of position and velocity of the target at time $k$, $F$ is the transition matrix, and $w_k$ is the motion noise, which follows $\mathcal{N}(0, Q)$. In (2), $F$ characterizes target dynamic with different kinematic models. For example, assume that $\Delta t$ is the sample period and

$$x_k = [\xi_{k,1} \quad \xi_{k,2} \quad \dot{\xi}_{k,1} \quad \dot{\xi}_{k,2} \quad \ddot{\xi}_{k,1} \quad \ddot{\xi}_{k,2}]^T,$$

where $(\xi_{k,1}, \xi_{k,2})$, $(\dot{\xi}_{k,1}, \dot{\xi}_{k,2})$, and $(\ddot{\xi}_{k,1}, \ddot{\xi}_{k,2})$ denote the position, velocity and acceleration of the target, respectively. Then

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

characterizes the target dynamic with constant velocity, while

$$F = \begin{bmatrix} 1 & 0 & \Delta t & 0 & \frac{(\Delta t)^2}{2} & 0 \\ 0 & 1 & 0 & \Delta t & 0 & \frac{(\Delta t)^2}{2} \\ 0 & 0 & 1 & 0 & \Delta t & 0 \\ 0 & 0 & 0 & 1 & 0 & \Delta t \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

characterizes the target dynamic with constant acceleration.

### B. Networked Radar System

To track the target described in (2), an NRS consisting of a data fusion center and $N$ radars equipped with Kalman filters is deployed in this region (Fig. 1). The $i$th radar measurement equation can be written as

$$y_{k,i} = Hx_k + v_{k,i}, i = 1, \cdots, N, \tag{3}$$

where $y_{k,i} \in \mathbb{R}^m$ with $m \in \mathbb{Z}^+$, $H$ is the measurement matrix, and $v_{k,i}$ are the measurement noises which are *i.i.d.* Gaussian distributed with 0 mean and covariance $R_i$.

The local state estimate $\hat{x}_{k,i}$ is calculated by the Kalman filter in the $i$th radar after $y_{k,i}$ is obtained. The Kalman filter is described as follows:

$$\hat{x}_{k+1|k,i} = F\hat{x}_{k,i}, \tag{4}$$

$$P_{k+1|k,i} = FP_{k,i}F^T + Q, \tag{5}$$

$$K_{k,i} = P_{k|k-1,i}H^T(HP_{k|k-1,i}H^T + R_i)^{-1}, \tag{6}$$

$$\hat{x}_{k,i} = \hat{x}_{k|k-1,i} + K_{k,i}(y_{k,i} - H\hat{x}_{k|k-1,i}), \tag{7}$$

$$P_{k,i} = P_{k|k-1,i} - K_{k,i}HP_{k|k-1,i}, \tag{8}$$

where $\hat{x}_{k+1|k,i}$ and $P_{k+1|k,i}$ denote the priori minimum mean squared error (MMSE) estimate of the state and the corresponding covariance, respectively, $\hat{x}_{k,i}$ and $P_{k,i}$ are the posteriori MMSE estimate of the state and the corresponding error covariance, respectively, and $K_{k,i}$ is the optimal gain at time $k$. We assume that $(F, H)$ is observable and $(F, \sqrt{Q})$ is controllable [35]. Under this assumption, estimation covariance matrix will converge to a steady state after a few steps, that is $P_{k,i} = \overline{P}_i$, $K_{k,i} = \overline{K}_i$ [36] [37].

In the NRS, each radar only has information about its local estimate, and the cross-correlation of different radar's local estimates is unknown [38]. Since CI algorithm can obtain a consistent fusion estimate when the local estimates of different radars are under unknown correlation [39], it is often used in the fusion center. In CI algorithm, local state estimate and the corresponding covariance of $i$th radar, i.e., $\hat{x}_{k,i}$, and $P_{k,i}$, are reported to the fusion center. CI algorithm uses a convex combination of the local estimates and the corresponding covariances, with the following form [34]:

$$\hat{x}_k = P_k \sum_{i=1}^{N} \omega_i P_{k,i}^{-1} \hat{x}_{k,i}, \tag{9}$$

$$P_k^{-1} = \sum_{i=1}^{N} \omega_i P_{k,i}^{-1}, \tag{10}$$

where $\omega_1, \cdots, \omega_N$ are fusion weights, and their sum is equal to one. The fusion weights are determined by minimizing the trace or determinant of $P_k$. With combination of the stable Kalman filter, (9) and (10), it is easy to prove that $P_k$ and $\omega_1, \cdots, \omega_N$ will also reach the steady-state values in a few steps [34].

**Remark 1.** *Under the assumption of unknown correlation of different radars' local estimates, (9) and (10) aim to yield a pessimistic fused estimate by combining the local estimates of different radars. Their effectiveness has been guaranteed since the fusion consistency of CI algorithm has been theoretically proved in [31]. Since the complexity to evaluate each inverse matrix equations (9) and (10) scales with cubic power with respect to the size of $\hat{x}_{k,i}$, then one can find that the computational complexity of (9) and (10) are $\mathcal{O}(Nn^3)$.*

### C. False Data Injection Attack

Assume that a malicious third party wants to deteriorate the target estimation by injecting false data into one attacked radar's measurements [40]. After invading the communication link of the attacked radar in the NRS, the attack is launched

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSIPN.2018.2790361, IEEE Transactions on Signal and Information Processing over Networks



TABLE I
PARAMETERS NOTATIONS

| Notation | Description |
|---|---|
| $\hat{x}_{k,i}$, $\overline{P}_i$ | local state estimate and the corresponding stable covariance of the $i$th radar in healthy system |
| $\hat{x}^a_{k,i}$, $\overline{P}^a_i$ | local state estimate and the corresponding stable covariance of the $i$th radar in attacked system |
| $\hat{x}_k$, $\overline{P}$ | fusion state estimate and the corresponding stable covariance of healthy system |
| $\hat{x}^a_k$, $\overline{P}^a$ | fusion state estimate and the corresponding stable covariance of attacked system |
| $\overline{K}_i$ | stable gain of the $i$th radar in healthy system |
| $\overline{K}^a_i$ | stable gain of the $i$th radar in attacked system |
| $\omega_i$ | stable fusion weight of the $i$th radar in healthy system |
| $\omega^a_i$ | stable fusion weight of the $i$th radar in attacked system |

from time $t$. As a result, the measurements about the target are compromised for the attacked radar. Without loss of generality, we assume that the $v$th radar is attacked by the malicious third party. The measurement equation of the $v$th radar under FDI attack at time $k(k > t)$ can be described as

$$y^a_{k,v} = y_{k,v} + \Delta y_k, \tag{11}$$

where $\Delta y_k$ is the data injected by the attacker.

It is worth mentioning that, the objectives of this paper are twofold: The first is to find the relationship between the FDI attack and the fusion estimation of the NRS; the second is to propose a novel data fusion algorithm to ensure the fusion estimation when the FDI attack is launched.

## IV. Analysis for NRS Under FDI Attack

To investigate the attack's effects on the NRS, we construct two parallel systems, namely, attacked system and healthy system. The former represents the actual NRS in which the attacked radar has been under the FDI attack from time $t$, while the latter stands for the virtual NRS which operates independently and concurrently in the absence of the attack. Notice that the latter system is only constructed for ease of theoretical analysis, and all analysis in this section is based on the premise that the statistics of all radars' noise are perfectly known. The notations of parameters in the two systems are defined in Table I.

We further introduce three metrics to evaluate the attack's effects on the NRS:

(1) Attack strength, $\Delta y_k$, which is the data injected by the attacker;

(2) Local estimation degradation, $\Delta x_{k,v} = \hat{x}^a_{k,v} - \hat{x}_{k,v}$, which is the difference between the local estimate of the attacked radar in the attacked system and in the healthy system;

(3) Fusion estimation degradation, $\Delta x_k = \hat{x}^a_k - \hat{x}_k$, which is the difference between the fusion estimate of the attacked system and the healthy system.

The following two lemmas denote the FDI attack's effects on the attacked radar's local estimate.

**Lemma 1.** *Consider the NRS (2)-(10) in presence of an FDI attacker. Suppose that the local Kalman filter (4)-(8) has reached a steady state. If the $v$th radar is under FDI attack with arbitrary attack strength $\Delta y_k$, we have*

$$\overline{K}^a_v = \overline{K}_v, \tag{12}$$
$$\overline{P}^a_v = \overline{P}_v, \tag{13}$$
$$\Delta x_{k,v} = M_v \Delta x_{k-1,v} + \overline{K}_v \Delta y_k, \tag{14}$$

*where $M_v = (I - \overline{K}_v H)F$.*

*Proof.* From (5), (6) and (8), the evolutions of Kalman gain and priori/posteriori MMSE estimate covariance only depend on the system parameters $F$, $H$, $Q$ and $R$, and are irrelevant to the local state estimate $\hat{x}_{k,i}$ and local measurement $y_{k,i}$. When the local Kalman filter has reached a steady state, (12) and (13) hold true. On the other hand, from (4) and (6), for the $v$th radar in the healthy and attacked systems, we have

$$\begin{aligned} \hat{x}^a_{k,v} &= \hat{x}^a_{k|k-1} + \overline{K}^a_v (y^a_{k,v} - H\hat{x}^a_{k|k-1,v}), \\ \hat{x}_{k,v} &= \hat{x}_{k|k-1} + \overline{K}_v (y_{k,v} - H\hat{x}_{k|k-1,v}), \end{aligned}$$

and it follows that

$$\begin{aligned} \Delta x_{k,v} &= \hat{x}^a_{k,v} - \hat{x}_{k,v} \\ &= (I - \overline{K}_v H)F(\hat{x}^a_{k-1,v} - \hat{x}_{k-1,v}) + \overline{K}_v \Delta y_k \\ &= M_v \Delta x_{k-1,v} + \overline{K}_v \Delta y_k. \end{aligned}$$

□

**Remark 2.** *On the premise that the statistics of all radars' noise are perfectly known, we can find that the attack strength $\Delta y_k$ cannot impact the calculation of estimation gain $K_v$ and the associated error covariance $P_v$. For example, if the FDI attacker injects random data to the measurements, it cannot change the estimation gain and associated error covariance.*

**Lemma 2.** *If $\rho(M_v) < 1$ and the attack strength is time-invariant, i.e., $\Delta y_k = \Delta y$, then $\Delta x_{k,v}$ converges to $-(M_v - I)^{-1}\overline{K}_v \Delta y$, with respect to $k$.*

*Proof.* Since FDI attack is launched from time $t$, we obtain $\Delta x_{t-1,v} = 0$. From Lemma 1, we also derive

$$\begin{aligned} \Delta x_{k,v} &= M_v \Delta x_{k-1,v} + \overline{K}_v \Delta y \\ &= M_v (M_v \Delta x_{k-2,v} + \overline{K}_v \Delta y) + \overline{K}_v \Delta y \\ &= M_v^2 \Delta x_{k-2,v} + M_v \overline{K}_v \Delta y + \overline{K}_v \Delta y \\ &= M_v^{k-t+1} \Delta x_{t-1,v} + \sum_{j=0}^{k-t} M_v^j \overline{K}_v \Delta y \\ &= (\sum_{j=0}^{k-t} M_v^j) \overline{K}_v \Delta y \\ &= -(M_v - I)^{-1}(I - M^{k-t+1}) \overline{K}_v \Delta y. \end{aligned}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSIPN.2018.2790361, IEEE Transactions on Signal and Information Processing over Networks



Under the assumption that $\rho(M_v) < 1$, $(M^{k-t+1})$ converges to zero, then $\Delta x_{k,v}$ converges to $-(M_v - I)^{-1}\overline{K}_v\Delta y$. □

Based on the above two lemmas, we investigate the attack's effects on the NRS.

**Lemma 3.** *Comparing the parameters of the attacked system and the healthy system, we have $\omega_i^a = \omega_i$ and $\overline{P}^a = \overline{P}$, where $i = 1, \cdots, N$.*

*Proof.* From Lemma 1, since the attack has no effect on the estimate covariance of the attacked radar, the objective function of CI algorithm is not influenced by the attack. Therefore, Lemma 3 can be directly obtained from Lemma 1 and CI algorithm. □

**Remark 3.** *Lemma 3 tells us that the FDI attack can not affect the fusion weights. However, according to Lemma 2, if the $v$th radar is under the attack, its local estimate will be deteriorated. Thus, it is unreasonable to assign the attacked radar's fusion weight as before. In fact, this is the main reason why the attack can cause the significant effects on the NRS. The following theorem will quantitatively analyze the attack's effects on the NRS.*

**Theorem 1.** *If $\rho(M_v) < 1$ and $\Delta y_k = \Delta y$, then $\Delta x_k$ converges to $-\omega_v\overline{P}\overline{P}_v^{-1}(M_v - I)^{-1}\overline{K}_v\Delta y$.*

*Proof.* According to (9), we have,

$$\hat{x}_k = \overline{P}\sum_{i=1}^{N}\omega_i\overline{P}_i^{-1}\hat{x}_{k,i}, \tag{15}$$

$$\hat{x}_k^a = \overline{P}^a\left[\omega_v^a[\overline{P}_v^a]^{-1}\hat{x}_{k,v} + \sum_{i=1,i\neq v}^{N}\omega_i^a[\overline{P}^a]^{-1}\hat{x}_{k,i}\right]. \tag{16}$$

From Lemma 3, we have

$$\Delta x_k = \hat{x}_k^a - \hat{x}_k = \omega_v\overline{P}\overline{P}_v^{-1}\Delta x_{k,v}.$$

As

$$\lim_{k\to\infty}\Delta x_{k,v} = -(M_v - I)^{-1}\overline{K}_v\Delta y,$$

leading to

$$\lim_{k\to\infty}\Delta x_k = -\omega_v\overline{P}\overline{P}_v^{-1}(M_v - I)^{-1}\overline{K}_v\Delta y.$$

□

**Remark 4.** *From Theorem 1, we can see that the fusion estimation degradation $\Delta x_k$ is approximately linear with respect to the attack strength $\Delta y$. It means that the attack with larger strength will cause more severe fusion estimation degradation. Hence, it is necessary to take actions to reduce the attack's effects on the NRS. The following corollary generalizes Theorem 1 to the case in which the number of the attacked radar is more than one.*

**Corollary 1.** *Suppose the number of attacked radar is $V$ with $1 < V < N$, and the attack strengths of these attacked radars are all time-invariant. Without loss of generality, we assume that radar $1, 2, \cdots, V$ are under FDI attacks with attack strengths $\Delta y_1, \Delta y_2, \cdots, \Delta y_V$. Then $\Delta x_k$ converges to $-\overline{P}\sum_{i=1}^{V}\omega_i[\overline{P}]_i^{-1}(M_i - I)^{-1}\overline{K}_i\Delta y_i$.*

*Proof.* From (15) and (16), we can derive

$$\hat{x}_k^a = \overline{P}^a\left[\sum_{i=1}^{V}\omega_i^a[\overline{P}_i^a]^{-1}\hat{x}_{k,i}^a + \sum_{i=V+1}^{N}\omega_i^a[\overline{P}_i]^{-1}\hat{x}_{k,i}\right],$$

$$\hat{x}_k = \overline{P}\left[\sum_{i=1}^{V}\omega_i[\overline{P}_i]^{-1}\hat{x}_{k,i} + \sum_{i=V+1}^{N}\omega_i[\overline{P}_i]^{-1}\hat{x}_{k,i}\right].$$

According to Lemma 1 and Lemma 3, $\overline{P}^a = \overline{P}$, and for $i = 1, \cdots, N$, $\omega_i^a = \omega_i$, $\overline{P}_i^a = \overline{P}_i$. Then we obtain

$$\Delta x_k = \overline{P}\sum_{i=1}^{V}\omega_i[\overline{P}_i]^{-1}\Delta x_{k,i}.$$

For the attacked radars, since their attack strengths are all time-invariant, $\Delta x_{k,i}$ converges to $(M_i - I)^{-1}\overline{K}_i\Delta y_i$, satisfying Lemma 2. Hence, $\Delta x_k$ converges to $-\overline{P}\sum_{i=1}^{V}\omega_i[\overline{P}]_i^{-1}(M_i - I)^{-1}\overline{K}_i\Delta y_i$. □

## V. Confident Covariance Intersection Algorithm

In this section, we present a novel data fusion algorithm named CCI, which can be regarded as the generalization of CI algorithm. Then we analyze the fusion estimation consistency of the proposed algorithm. We further investigate the fusion estimation of the CCI algorithm when the NRS is under the FDI attack.

### A. Algorithm Description

The CCI algorithm includes two procedures, the procedure of calculating confidence factor and the procedure of calculating fusion weights.

*1) The procedure of calculating confidence factor:* Before introducing the definition of confidence factor, we define the following parameters: $u_{k,i}$, $\alpha_{k,i}$, $z_{k,i}$ and $\eta_i$. Thereinto, $u_{k,i}$ is described as

$$u_{k,i} = y_{k,i} - H\hat{x}_{k|k-1,i}, \tag{17}$$

which is the residue of the $i$th radar. Then, we define $\alpha_{k,i}$ as

$$\alpha_{k,i} = u_{k,i}^T\Phi_i^{-1}u_{k,i}, \tag{18}$$

where $\Phi_i = H\overline{P}_i^{-1}H^T + R_i$. For the characteristic function defined in (1), let

$$z_{k,i} = \frac{1}{T}\sum_{j=k-T+1}^{k}\alpha_{j,i}, \tag{19}$$

and $A = [0, \eta_i]$, where $T$ is the window size. $\eta_i$ is defined as the confidence scalar of the $i$th radar. Then, we have

$$\chi_A(z_{k,i}) = \begin{cases} 0, & z_{k,i} \in [0, \eta_i], \\ 1, & \text{otherwise.} \end{cases} \tag{20}$$

Now we introduce a new variable, i.e., confidence factor, which weights the confidence of the $i$th radar's local estimate. Specifically, we define the following two types of suggested confidence factors:

$$\text{Type 1}: g_{k,i} = 1 - \chi_A(z_{k,i}), \tag{21}$$

$$\text{Type 2}: g_{k,i} = exp\{-(z_{k,i} - \eta_i)\chi_A(z_{k,i})\}. \tag{22}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSIPN.2018.2790361, IEEE Transactions on Signal and Information Processing over Networks



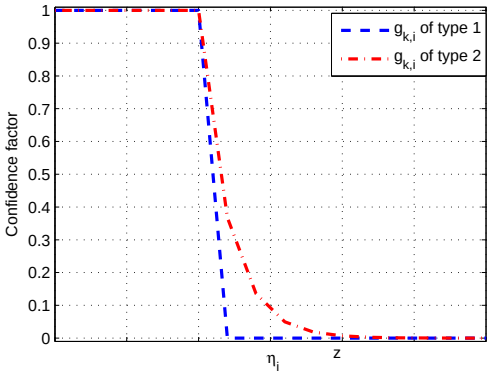



Fig. 2. The sketch of confidence factors

If the local estimate is confident, i.e., $z_{k,i} \in [0, \eta_i]$, these types of confidence factors are both equal to one; Otherwise, the confidence factor of type 1 becomes zero as a punishment, while that of type 2 decreases to zero exponentially. Fig. 2 shows the variation of these confidence factors with respect to $z_{k,i}$.

**Algorithm 1** The CCI Algorithm

1: **Input:** $\{y_{k,i}\}_{i=1}^N$
2: **Procedure 1:** Kalman filters in each radar
3: **for** $i = 1, \cdots, N$ **do**
4: Solve local estimates $\hat{x}_{k,i}$ and corresponding local covariance $P_{k,i}$ by (4)-(8)
5: Solve the residue of the $i$th radar, $u_{k,i}$, by (17)
6: Solve the confidence factor of the $i$th radar, $g_{k,i}$, by (18)-(22)
7: **end for**
8: **Procedure 2:** CCI fusion in the fusion center
9: Assign fusion weights $\{\omega_i\}_{i=1}^N$ by (25)
10: Solve fusion estimate $\hat{x}_k$ by (23)
11: Solve fusion estimate covariance $P_k$ by (24)
12: **Output:** $\hat{x}_k, P_k, \{\omega_i\}_{i=1}^N$

*2) The procedure of calculating fusion weights:* After obtaining the confidence factor, local estimate and corresponding estimate error of each radar, the fusion center calculates fusion weights as follows:

$$\hat{x}_k = P_k \sum_{i=1}^{N} \omega_i P_{k,i}^{-1} \hat{x}_{k,i}, \tag{23}$$

$$P_k^{-1} = \sum_{i=1}^{N} \omega_i P_{k,i}^{-1}, \tag{24}$$

where $\omega_i$ is the optimal solution of the following constrained optimization problem:

$$\begin{aligned} \min_{\omega_i, i=1,\cdots,N} \ & \mathrm{Tr}\left[\sum_{i=1}^{N} \omega_i g_{k,i} P_{k,i}^{-1}\right]^{-1}, \\ \text{s.t.} \ & \sum_{i=1}^{N} \omega_i = 1, \\ & \omega_i \geq 0. \end{aligned} \tag{25}$$

**Remark 5.** *Since each inverse matrix in the cost function scales with cubic power with respect to $n$, one can find the computational complexity to solve the problem in (25) is $\mathcal{O}(Nn^3)$, and the total computational complexity of the procedure of calculating fusion weight is $\mathcal{O}(Nn^3)$. If all local estimates from all radars are confident, i.e., $g_{k,i} = 1$, for $i = 1, \cdots, N$, the proposed algorithm is simplified to CI algorithm, Therefore, the CCI algorithm can be viewed as the generalization of CI algorithm. Finally, the pseudocode of the proposed CCI algorithm is shown in Algorithm 1.*

**Remark 6.** *The rationale of the proposed CCI algorithm is that the statistical features of the attacked radar will be changed after the FDI attack happens (The statistical features will be analyzed in the third subsection.). In order to eliminate the effect of the FDI attack on the NRS by utilizing the statistical features of the attacked radar, first, we define confidence factor, which depends on the statistical feature of each radar's measurement, to weight the confidence of the each radar's local estimate. Then we introduce confidence factor into CI algorithm. After that, to obtain the optimized fusion weight, different performance criteria of $\tilde{P}_k$, such as minimizing the trace or the determinant of $\tilde{P}_k$ can be used, where*

$$\tilde{P}_k = \left[\sum_{i=1}^{N} \omega_i g_{k,i} P_{k,i}^{-1}\right]^{-1}.$$

### B. Fusion Estimation Consistency of CCI Algorithm

According to [33], for any estimate, if its corresponding covariance is no smaller than its actual covariance, the estimate is consistent. For example, given an estimate $\{\hat{x}, P\}$, where $\hat{x}$ represents the state estimate, and $P$ is the corresponding covariance. $x_k$ is the state of the target, then the actual covariance of $\hat{x}$ is

$$P^* = E[(\hat{x} - x)(\hat{x} - x)^T].$$

$\hat{x}$ is a consistent estimate only if [39]

$$P - P^* \succeq 0. \tag{26}$$

For any CI based algorithm, the fusion estimation consistency is always expected to be guaranteed since it establishes the confidence of the fusion estimate. In [31], the authors proved that CI algorithm can yield a consistent fusion estimate. Here we prove that the proposed CCI algorithm can still guarantee the property of consistence. In other words, the proposed CCI algorithm can also achieve a confident fusion estimate.

**Theorem 2.** *Given two consistent local estimates of different radars, the correlation between them is unknown. Then for any choice of $\omega$ in the interval $[0, 1]$, the fusion estimate calculated by CCI algorithm described in (17)-(25) is consistent.*

*Proof.* See the Appendix. □

Here we give an example to illustrate Theorem 2.

**Example:** Suppose the local estimate covariances of two radars are

$$P_1 = \begin{bmatrix} 0.25 & -0.25 \\ -0.25 & 1.25 \end{bmatrix},$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSIPN.2018.2790361, IEEE Transactions on Signal and Information Processing over Networks



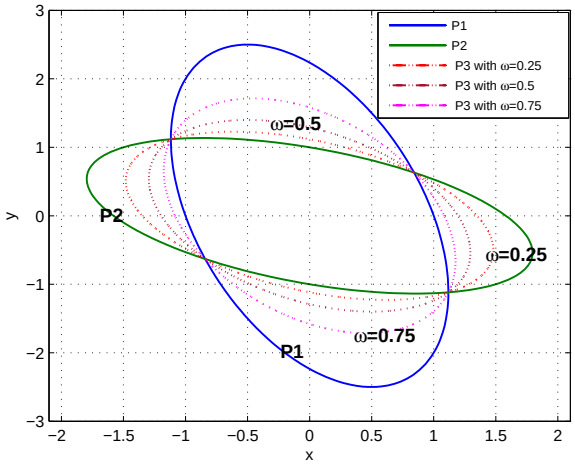



Fig. 3. The comparison of $P_1$, $P_2$ and $P_3$ with different fusion weights

and

$$P_2 = \begin{bmatrix} 0.625 & -0.25 \\ -0.25 & 0.125 \end{bmatrix},$$

respectively.

The covariance ellipse of $P_1$, $P_2$ and fusion estimate covariance $P_3$ calculated by CCI algorithm with different fusion weights are depicted in Fig. 3. It can be seen that the covariance ellipse of $P_3$ always contains the intersection region of $P_1$ and $P_2$ for any $\omega$. That explains the geometric meaning of the fusion estimation consistency.

### C. Analysis for CCI Algorithm Under FDI Attack

Now we analyze the fusion estimation of the NRS with CCI algorithm when the FDI attack is launched.

**Lemma 4.** *For the system model defined in (2)-(11), with the absence of the FDI attack, the residue $u_{k,i}$ is an i.i.d. Gaussian distribution with zero mean and covariance $\Phi_i$, $\alpha_{k,i}$ is a $\chi^2$ distribution with $m$ degrees of freedom.*

*Proof.* A direct result of the Theorem 1 in [41]. □

**Lemma 5.** *For the attacked radar in the attacked system, when the FDI attack happens, define $u^a_{k,v} = y^a_{k,v} - H\hat{x}^a_{k|k-1,v}$. If $\rho(M_v) < 1$ and $\Delta y_k = \Delta y$, then $u^a_{k,v}$ is a Gaussian distribution with covariance $\Phi_v$ and a time-variable mean. Especially, when $k \to \infty$, $u^a_{k,v}$ is a Gaussian distribution with covariance $\Phi_v$ and mean $\Psi_v$, where $\Psi_v = L_v\Delta y = (HF(M_v - I)^{-1}\overline{K}_v + I)\Delta y$.*

*Proof.* Thanks to $\hat{x}^a_{k-1,v} = \hat{x}_{k-1,v} + \Delta y$, it follows that

$$y^a_{k,v} - HF\hat{x}^a_{k-1,v} = y_{k,v} - HF\hat{x}_{k-1,v} - HF\Delta x_{k-1,v} + \Delta y,$$

i.e.,

$$\begin{aligned} u^a_{k,v} &= u_{k,v} - HF\Delta x_{k-1,v} + \Delta y, \\ &= u_{k,v} + [HF(M_v - I)^{-1}(I - M^{k-t+1})\overline{K}_v + I]\Delta y. \end{aligned}$$

The rightmost item in the above equation is time-variable, leading to a time-variable mean of the distribution of $u^a_{k,v}$. However, when $k \to \infty$, from Lemma 2, the rightmost item converges to a constant value,

$$u^a_{k,v} = u_{k,v} + L_v\Delta y,$$

where $L_v = (HF(M_v - I)^{-1}\overline{K}_v + I)$. Since $u_{k,v}$ is a Gaussian distribution with zero mean and covariance $\Phi_v$, one can see that Lemma 5 is true. □

**Lemma 6.** *If $\rho(M_v) < 1$ and $\Delta y_k = \Delta y$, let $\alpha^a_{k,i} = [u^a_{k,i}]^T[\Phi^a_i]^{-1}u^a_{k,i}$, then $\alpha^a_{k,i}$ is a $\chi^2$ distribution with a time-variant mean. Especially, when $k \to \infty$, $\alpha^a_{k,v}$ is a $\chi^2$ distribution with mean $tr(\Phi_v^{-1}\Psi_v\Psi_v^T) + m$.*

*Proof.* Since $u^a_{k,v}$ is still a Gaussian distribution, then $\alpha^a_{k,i}$ is still a $\chi^2$ distribution. By Lemma 5,

$$E[\lim_{k\to\infty} u^a_{k,v}[u^a_{k,v}]^T] = \Psi_v\Psi_v^T + \Phi_v.$$

When $k \to \infty$, we have

$$\begin{aligned} \lim_{k\to\infty} E[\alpha^a_{k,v}] &= \lim_{k\to\infty} E\left[tr(u^a_{k,v}\Phi_v^{-1}[u^a_{k,v}]^T)\right], \\ &= \lim_{k\to\infty} E\left[tr(\Phi_v^{-1}[u^a_{k,v}]^T u^a_{k,v})\right], \\ &= tr\left(E\left[\Phi_v^{-1}\lim_{k\to\infty}[u^a_{k,v}]^T u^a_{k,v}\right]\right), \\ &= tr\Big(\Phi_v^{-1}(\Psi_v\Psi_v^T + \Phi_v)\Big), \\ &= tr\big(\Phi_v^{-1}\Psi_v\Psi_v^T\big) + m. \end{aligned}$$

Therefore, when $k \to \infty$, $\alpha^a_{k,i}$ is a $\chi^2$ distribution with mean $tr(\Phi_v^{-1}\Psi_v\Psi_v^T) + m$. □

**Remark 7.** *Lemma 5 and Lemma 6 show that $E[\alpha^a_{k,v}]$ depends on the attack strength. Lemma 4 and Lemma 6 reveal that the margin between $E[\alpha_{k,v}]$ and $E[\alpha^a_{k,v}]$ converges to $tr(\Phi_v^{-1}\Psi_v\Psi_v^T)$ when $k \to \infty$. Inspired by this, we investigate the statistical features of $\alpha_{k,i}$, i.e., $z_{k,i}$ calculated by (19), and set an appropriate threshold $\eta_i$ as the confidence scalar of $i$th radar. Specifically, when confidence level (for example, 90%, 95%, and 99%) is given, the lower/upper confidence bounds of the threshold can be calculated.*

**Theorem 3.** *If $\rho(M_v) < 1$ and $\Delta y_k = \Delta y$, let $L_1$ denote the confidence level that $z_{k,i} > \eta_i$ in the healthy system, $L_2$ denote the confidence level that $z^a_{k,i} > \eta_i$ in the attacked system, then the lower and upper confidence bounds of the threshold $\eta_i$ in (20) can be calculated by (27) and (28), respectively.*

$$\frac{1}{T}\frac{\gamma(Tm/2, \eta_i/2)}{\Gamma(Tm/2)} \geq 1 - L_1, \quad (27)$$

$$\frac{1}{T}\frac{\gamma(T(tr(\Phi_v^{-1}\Psi_v\Psi_v^T) + m)/2, \eta_i/2)}{\Gamma(T(tr(\Phi_v^{-1}\Psi_v\Psi_v^T) + m)/2)} \leq 1 - L_2, \quad (28)$$

*where $z^a_{k,i} = \frac{1}{T}\sum_{j=k-T+1}^{k}\alpha^a_{j,i}$, $\gamma(\cdot,\cdot)$ is the lower incomplete Gamma function and $\Gamma(\cdot)$ is the Gamma function.*

*Proof.* For the healthy system, $\alpha_{k,i} \sim \chi^2(m)$ , then $z_{k,i} \sim \chi^2(Tm)/T$, and its cumulative distribution function is

$$F(z_{k,i}; Tm) = \frac{1}{T}\frac{\gamma(Tm/2, z_{k,i}/2)}{\Gamma(Tm/2)}.$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSIPN.2018.2790361, IEEE Transactions on Signal and Information Processing over Networks



The lower bound of $\eta_i$ is calculated by

$$Pr(0 \le z_{k,i} \le \eta_i) \ge 1 - L_1,$$

i.e.,

$$\frac{1}{T}\frac{\gamma(Tm/2, \eta_i/2)}{\Gamma(Tm/2)} \ge 1 - L_1.$$

For the attacked system, consider the case where $k \to \infty$, from Lemma 6, $\alpha_{k,i} \sim \chi^2(tr(\Phi_v^{-1}\Psi_v\Psi_v^T) + m)$, then $z^a_{k,i} \sim \chi^2(T(tr(\Phi_v^{-1}\Psi_v\Psi_v^T)+m))/T$, and its cumulative distribution function is

$$F(z^a_{k,i}; T(tr(\Phi_v^{-1}\Psi_v\Psi_v^T)+m)) = \frac{1}{T}\frac{\gamma(\frac{T(tr(\Phi_v^{-1}\Psi_v\Psi_v^T)+m)}{2}, \frac{z^a_{k,i}}{2})}{\Gamma(\frac{T(tr(\Phi_v^{-1}\Psi_v\Psi_v^T)+m)}{2})}.$$

The upper bound of $\eta_i$ can be calculated by

$$Pr(0 \le z^a_{k,i} \le \eta_i) \le 1 - L_2,$$

i.e.,

$$\frac{1}{T}\frac{\gamma(T(tr(\Phi_v^{-1}\Psi_v\Psi_v^T)+m)/2, \eta_i/2)}{\Gamma(T(tr(\Phi_v^{-1}\Psi_v\Psi_v^T)+m)/2)} \le 1 - L_2.$$

□

**Remark 8.** *Consider a special case in which $z_{k,v} > \eta_v$ for the confidence factor of type 1 and $z_{k,v} \gg \eta_v$ for the confidence factor of type 1. From (21) and (22), the confidence factors of both types are zero for the attacked radar, while for other radars, the confidence factors of both types are one. By solving the constrained optimization problem (25), the attacked radar's fusion weight is equal to zero. In other words, although the NRS is not aware of the attack, the local estimate from the attacked radar has been denied by the CCI algorithm, Hence, the fusion estimation degradation of the NRS has no relationship with the attack strength in this case.*

## VI. Numerical Simulations

In this section, we provide extensive simulation results to illustrate our analytical findings.

Consider an NRS consisting of a data fusion center and two radars with the capability of keeping surveillance of a 2D region. A target scenario where the target starts its motion at (-400m, 400m) point with the velocity vector [1 0] m/s is created. The target's dynamic model follows (2) with $Q = 0$, and the transition matrix

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

where $\Delta t = 1$ is the sample period. Its state $x_k$ consists of position and velocity.

The measurement matrix and measurement noise covariance matrix of the two radars are

$$H_1 = H_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix},$$

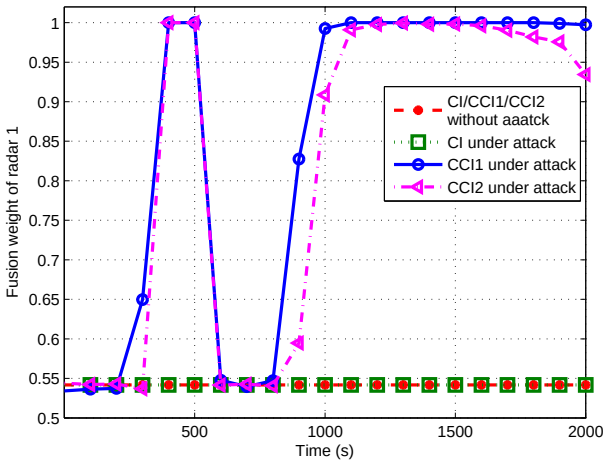



Fig. 4. Fusion weight of radar 1 in NRS with CI and CCI algorithms. (CCI1: the CCI algorithm with type 1 confidence factor. CCI2: the CCI algorithm with type 2 confidence factor.)

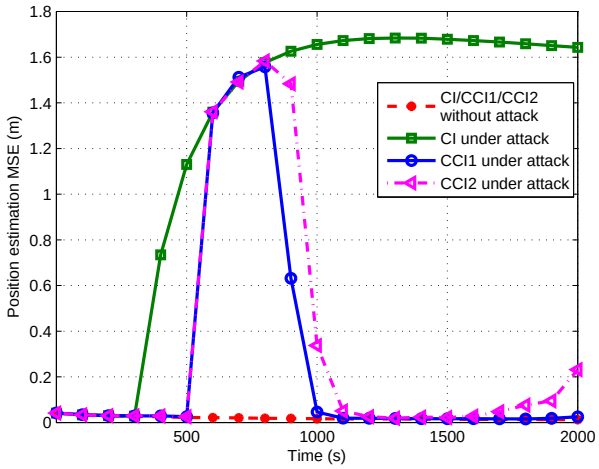



Fig. 5. Position estimation MSE of NRS with CI and CCI algorithms.

$$R_1 = \begin{bmatrix} 0.2 & 0 \\ 0 & 0.7 \end{bmatrix},$$

$$R_2 = \begin{bmatrix} 0.5 & 0 \\ 0 & 0.3 \end{bmatrix},$$

respectively.

The simulation time is set as 2000s. We assume that the 2nd radar keeps suffering the FDI attack from 300s to 2000s. As a consequence, for $k \ge 300$, its measurement $y_{k,2}$ is compromised to $y^a_{k,2}$. Let $\Delta y = [5 \quad 0]^T$. For the CCI algorithm, let the window size $T = 100$ and $\eta_i = 2.8$ that satisfies Theorem 3.

500 times Monte Carlo simulations are performed, and the results are shown in Fig. 4-7. Therein, Fig. 4 shows the 1st radar's fusion weight in the NRS with CI and CCI algorithms. As mentioned before, the CCI algorithm is simplified to CI algorithm when the attack is absent. Therefore, the CI and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSIPN.2018.2790361, IEEE Transactions on Signal and Information Processing over Networks



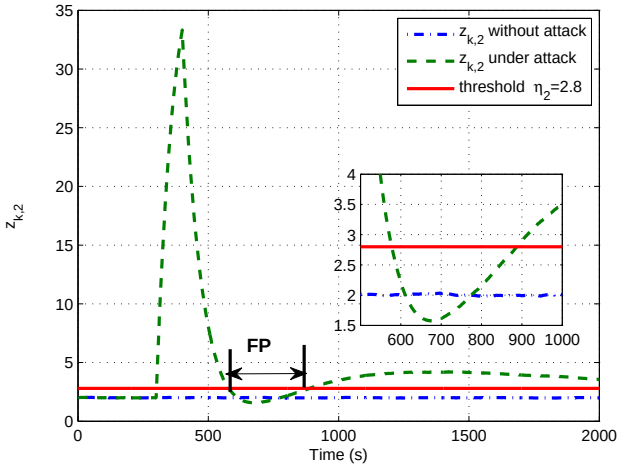



Fig. 6. $z_{k,2}$ with different conditions (under attack and without attack).

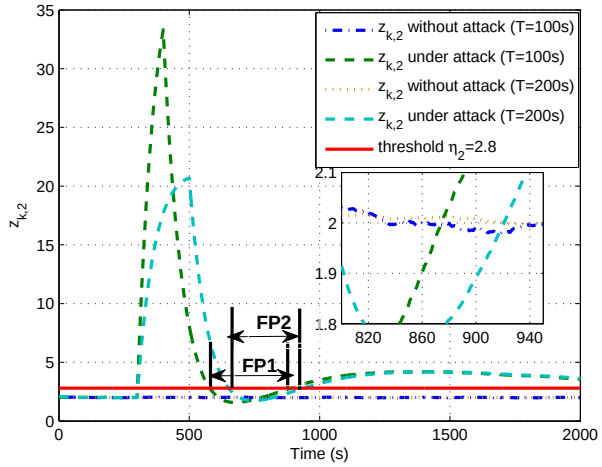



Fig. 7. False period time when different window sizes $T$ are set.

CCI algorithm with two kinds of confidence factor share the same curve when the attack is absent. Comparing the curve with hollow rectangle and that with solid circle, we can find that CI algorithm does not change the 1st radar's fusion weight even the 2nd radar has been under attack. This is the reason why this NRS is vulnerable to the attack. However, from the curve with hollow circle and that with hollow triangle, we can find the 1st radar's fusion weight in the NRS with CCI algorithm increases to 1 in most time after the attack begins. It means that the NRS has declined the polluted local estimate of the 2nd radar.

Fig. 5 presents the mean squared error (MSE) of the target's position estimation. we can see that this attack causes a significant deviation in position estimation of the NRS with CI algorithm. The deviation between the curve with rectangle and that with solid circle, will converge to a stable value, which can be calculated by Theorem 1. The NRS with CCI algorithm has a better estimation when suffering from the attack, since its estimation MSE becomes much smaller than that of the

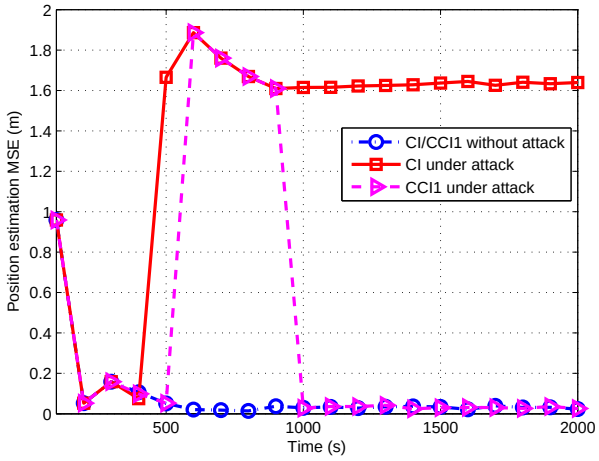



Fig. 8. Position estimation MSE of NRS (consisting of three radars) with CI and CCI algorithms.

NRS with CI algorithm.

From Fig. 4 and Fig. 5, we can also find that the performance of CCI algorithm degrades to that of CI algorithm during the false period from about 600-900s. Fig. 6 shows the reason for the false period. From Fig. 6, we can see that $z_{k,2}$ under the attack is smaller than the threshold $\eta_2 = 2.8$ in the false period (FP), which renders that the fusion center takes the estimate of the attacked radar (2nd radar) as confident value. The phenomenon of false period appears because Theorem 3 are derived on the condition that $k \to \infty$. On the other hand, Fig. 6 also verifies Lemma 5, Lemma 6 and Theorem 3. As shown in Fig. 6, $z_k$ and $z_k^a$ converge to $m = 2$ and $m + tr(\Phi_2^{-1}\Psi_2\Psi_2^T)$, respectively.

**Discussion.** Obviously, a shorter false period time will lead to a better estimation performance. There are two possible approaches to shorten false period time. The first is to extend the window size $T$. In Fig. 7, we compare the duration of false period when two different window sizes are set. We can find FP2<FP1, where FP1 is the false period time when T=100s, and FP2 is the false period time when T=200s. Another approach is to set an adaptive threshold $\eta_2$, which is our future work.

Next, we added one more healthy radar in the NRS, whose measurement matrix $H_3 = H_1$ and measurement noise covariance matrix is

$$R_3 = \begin{bmatrix} 0.1 & 0 \\ 0 & 0.8 \end{bmatrix}.$$

The results is presented in Fig. 8. As we can, similar results about the fusion estimation estimation degradation and false period time are obtained.

## VII. Conclusion

In this paper, we have studied the security issues of NRS. Specifically, we have investigated the effects of FDI attacks on an NRS, and proposed a novel data fusion algorithm to combat FDI attacks. The estimation performance of the proposed algorithm has been demonstrated by extensive numerical

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSIPN.2018.2790361, IEEE Transactions on Signal and Information Processing over Networks



results when an FDI attacker is present. The numerical results also reveal the remaining challenge, that is, how to further shorten the false period time. Therefore, in our future work, we will focus on achieving a better performance by choosing an adaptive threshold for shortening the false period time. Although the proposed algorithm is addressed to solve the security issues of networked radar systems, it could potentially be applied to other cyber physical system, such as smart grid and Internet of things.

## VIII. APPENDIX

**The proof of Theorem 2**.

*Proof.* Suppose the target state is $x_k$. The two local estimates with unknown correlation and the corresponding covariances are $\{\hat{x}_{k,1}, P_{k,1}\}$ and $\{\hat{x}_{k,2}, P_{k,2}\}$, respectively. We define the following variables:

$$\begin{aligned} \tilde{x}_{k,1} &= \hat{x}_{k,1} - x_k, \tilde{x}_{k,2} = \hat{x}_{k,2} - x_k, \\ P^*_{k,1} &= E[\tilde{x}_{k,1}\tilde{x}^T_{k,1}], P^*_{k,2} = E[\tilde{x}_{k,2}\tilde{x}^T_{k,2}], \\ P^*_{k,12} &= E[\tilde{x}_{k,1}\tilde{x}^T_{k,2}], P^*_{k,21} = E[\tilde{x}_{k,2}\tilde{x}^T_{k,1}], \end{aligned}$$

where $P^*_{k,1}, P^*_{k,2}, P^*_{k,12}, P^*_{k,21}$ are unknown. Now that the two local estimates are consistent, if follows that

$$P_{k,1} - P^*_{k,1} \succeq 0, \quad (29)$$

$$P_{k,2} - P^*_{k,2} \succeq 0. \quad (30)$$

Let $\{\hat{x}_k, P_k\}$ be the fusion estimate and the corresponding covariance calculated by CCI algorithm, and

$$\tilde{x}_k = \hat{x}_k - x_k, P^*_k = E[\tilde{x}_k\tilde{x}^T_k].$$

From (23) and (24), if follows that

$$\hat{x}_k = P_k\left(\omega P^{-1}_{k,1}\tilde{x}_{k,1} + (1-\omega)P^{-1}_{k,2}\tilde{x}_{k,2}\right), \quad (31)$$

$$P^{-1}_k = \omega P^{-1}_{k,1} + (1-\omega)P^{-1}_{k,2}. \quad (32)$$

Then, the proof of Theorem 2 can be represented as the proof of the following inequality

$$P_k - P^*_k \succeq 0. \quad (33)$$

From (32), it follows that

$$x_k = P_k(\omega P^{-1}_{k,1}x_k + (1-\omega)P^{-1}_{k,2}x_k). \quad (34)$$

According to (31) and (34), we obtain

$$\tilde{x}_k = P_k[\omega P^{-1}_{k,1}\tilde{x}_{k,1} + (1-\omega)P^{-1}_{k,2}\tilde{x}_{k,2}].$$

Hence, we have

$$\begin{aligned} P^*_k &= E[\tilde{x}_k\tilde{x}^T_k] = P_k\Big[\omega^2 P^{-1}_{k,1}P^*_{k,1}P^{-1}_{k,1} \\ &+ \omega(1-\omega)[P^{-1}_{k,1}P^*_{k,12}P^{-1}_{k,2} + P^{-1}_{k,2}P^*_{k,21}P^{-1}_{k,1}] \\ &+ (1-\omega)^2 P^{-1}_{k,2}P^*_{k,2}P^{-1}_{k,2}\Big]P_k. \end{aligned}$$

Augmenting the equation above into (33), equivalently, the proof of (33) reduces to the proof of the following inequality

$$\begin{aligned} P^{-1}_k - \omega^2 P^{-1}_{k,1}P^*_{k,1}P^{-1}_{k,1} - \omega(1-\omega)[P^{-1}_{k,1}P^*_{k,12}P^{-1}_{k,2} &+ \\ P^{-1}_{k,2}P^*_{k,21}P^{-1}_{k,1}] - (1-\omega)^2 P^{-1}_{k,2}P^*_{k,2}P^{-1}_{k,2} &\succeq 0. \end{aligned}$$

According to (29) (30) and (31), it follows that

$$P^{-1}_k \succeq \omega P^{-1}_{k,1}P^*_{k,1}P^{-1}_{k,1} + (1-\omega)P^{-1}_{k,2}P^*_{k,2}P^{-1}_{k,2}.$$

By utilizing the above two inequalities, the proof of (33) is equivalent to the proof of the following inequality

$$\begin{aligned} \omega(1-\omega)[P^{-1}_{k,1}P^*_{k,1}P^{-1}_{k,1} - P^{-1}_{k,1}P^*_{k,12}P^{-1}_{k,2} &- \\ P^{-1}_{k,2}P^*_{k,21}P^{-1}_{k,1} + P^{-1}_{k,2}P^*_{k,2}P^{-1}_{k,2}] &\succeq 0. \end{aligned}$$

i.e.,

$$\omega(1-\omega)E[(P^{-1}_{k,1}\tilde{x}_{k,1} - P^{-1}_{k,2}\tilde{x}_{k,2})(P^{-1}_{k,1}\tilde{x}_{k,1} - P^{-1}_{k,2}\tilde{x}_{k,2})^T] \succeq 0. \quad (35)$$

Since (35) holds true for any $\omega$ in the interval $[0, 1]$, the fusion estimate calculated by CCI algorithm described in (17)-(25) is consistent. This is the end of proof. □

## REFERENCES


[1] G. Zheng and Y. Zheng, "Radar netting technology and its development," in *Proceedings of IEEE/CIE International Radar Conference*, Chengdu, China, Oct. 2011, pp. 933–937.

[2] M. Wei, "Passive wireless local area network radar network using compressive sensing technique," *IET Radar, Sonar and Navigation*, vol. 9, no. 1, pp. 84–91, Feb. 2014.

[3] H. Wang, J. Johnson, C. Baker, L. Ye, and C. Zhang, "On spectrum sharing between communications and air traffic control radar systems," in *Proceedings of IEEE Radar Conference*, Washington DC, USA, May 2015, pp. 1545–1550.

[4] Z. Shi, C. Zhou, Y. Gu, N. A. Goodman, and F. Qu, "Source etimation using coprime array: A sparse reconstruction perspective," *IEEE Sensors Journal*, vol. 17, no. 3, pp. 755–765, Dec. 2017.

[5] G. Vivone and P. Braca, "Joint probabilistic data association tracker for extended target tracking applied to x-band marine radar data," *IEEE Journal of Oceanic Engineering*, vol. 41, no. 4, pp. 1007–1019, Mar. 2015.

[6] F. Meyer, O. Hlinka, H. Wymeersch, E. Riegler, and F. Hlawatsch, "Distributed localization and tracking of mobile networks including noncooperative objects," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 2, no. 1, pp. 57–71, Mar. 2016.

[7] X. Wang, L. Xu, H. Sun, and J. Xin, "On-road vehicle detection and tracking using mmw radar and monovision fusion," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 7, pp. 2075–2084, Apr. 2016.

[8] A. Mohammadi and K. Plataniotis, "Distributed widely linear multiple-model adaptive estimation," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 1, no. 3, pp. 164–179, Sept. 2015.

[9] N. Lestriandoko, H. Juhana, and R. Munir, "Security system for surveillance radar network communication using chaos algorithm," in *Proceedings of IEEE International Conference on Telecommunication Systems Services and Applications*, Kuta, Indonesia, Oct. 2014, pp. 1–6.

[10] T. Melville, "13 aircraft mysteriously disappear from radars in heart of europe," https://www.rt.com/news/165636-aircraft-disappear-radfars-austria/.

[11] A. Coluccia and G. Ricci, "Abort-like detection strategies to combat possible deceptive ECM signals in a network of radars," *IEEE Transactions on Signal Processing*, vol. 63, no. 11, pp. 2904–2914, June 2015.

[12] S. Zhao, L. Zhang, Y. Zhou, and N. Liu, "Signal fusion-based algorithms to discriminate between radar targets and deception jamming in distributed multiple-radar architectures," *IEEE Sensors Journal*, vol. 15, no. 11, pp. 6697–6706, Nov. 2015.

[13] S. Li, Y. Yılmaz, and X. Wang, "Quickest detection of false data injection attack in wide-area smart grids," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 2725–2735, Nov. 2015.

[14] X. Gong, J. Zhang, D. Cochran, and K. Xing, "Barrier coverage in bistatic radar sensor networks: Cassini oval sensing and optimal placement," in *Proceedings of the ACM international Symposium on Mobile Ad Hoc Networking And Computing*, Bangalore, India, July 2013, pp. 49–58.

[15] X. Gong, J. Zhang, D. Cochran, and K. Xing, "Optimal placement for barrier coverage in bistatic radar sensor networks," *IEEE/ACM Transactions on Networking*, vol. 24, no. 1, pp. 259–271, Feb. 2016.

[16] J. Bosse, O. Krasnov, and A. Yarovoy, "Direct target localization and deghosting in active radar network," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 51, no. 4, pp. 3139–3150, Oct. 2015.

[17] B. Jonathan, K. Oleg, and A. Yarovoy, "Direct target localization with an active radar network," *Signal Processing*, vol. 125, pp. 21–35, Aug. 2016.

[18] C. Shi, J. Zhou, and F. Wang, "LPI based resource management for target tracking in distributed radar network," in *Proceedings of IEEE Radar Conference*, Philadelphia, PA, USAMay 2016, pp. 1–5.

[19] A. Deligiannis, G. Rossetti, A Panoui, S. Lambotharan, and J. Chambers, "Power allocation game between a radar network and multiple jammers," in *Proceedings of IEEE Radar Conference*, Philadelphia, PA, USA, May 2016, pp. 6–10.

[20] C. Zhou, Y. Gu, S. He, and Z. Shi, "A robust and efficient algorithm for coprime array adaptive beamforming," *IEEE Transactions on Vehicular Technology*, DOI: 10.1109/TVT.2017.2704610.

[21] B. Wang, G. Cui, S. Zhang, and D. Ran, "Deceptive jamming suppression based on coherent cancelling in multistatic radar system," in *Proceedings of IEEE Radar Conference*, Philadelphia, PA, USA, May 2016, pp. 71–75.

[22] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 4, pp. 998–1010, Fourth Quarter, 2012.

[23] H. Zhang, Y. Qi, J. Wu, L. Fu, and L. He, "DoS attack energy management against remote state estimation," *IEEE Transactions on Control of Network Systems*, DOI: 10.1109/TCNS.2016.2614099.

[24] C. Zhang and R. Green, "Communication security in internet of thing: preventive measure and avoid DDoS attack over iot network," in *Proceedings of ACM Symposium on Communications and Networking*, San Diego, CA, USA, Apr. 2015, pp. 8–15.

[25] H. Zhang, Y. Qi, H. Zhou, J. Zhang, and J. Sun, "Testing and defending methods against DoS attack in state estimation," *Asian Journal of Control*, vol. 19, no. 4, pp. 1295–1305, July 2017.

[26] C. Zhou, Y. Gu, Y. D. Zhang, Z. Shi, T. Jin, and X. Wu, "Compressive sensing based coprime array direction-of-arrival estimation," *IET Communications*, vol. 11, no. 11, pp. 1719–1724, Aug. 2017.

[27] V. Illiano and E. Lupu, "Detecting malicious data injections in event detection wireless sensor networks," *IEEE Transactions on Network and Service Management*, vol. 12, no. 3, pp. 496–510, 2015.

[28] X. Liu, P. Zhu, Y. Zhang, and K. Chen, "A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2345–2443, Sept. 2015.

[29] L. Liu, M. Esmalifalak, Q. Ding, V. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 612–621, Mar. 2014.

[30] X. Yang, J. Lin, W. Yu, P. Moulema, X. Fu, and W. Zhao, "A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems," *IEEE Transactions on Computers*, vol. 64, no. 1, pp. 4–18, Jan. 2015.

[31] S. Julier and J. Uhlmann, "A non-divergent estimation algorithm in the presence of unknown correlations," in *Proceedings of IEEE American Control Conference*, Albuquerque, NM, USA, June 1997, pp. 2369–2373.

[32] S. Julier and J. Uhlmann, *Handbook of Data Fusion*, CRC Press, 2001.

[33] H. Li, F. Nashashibi, and M Yang, "Split covariance intersection filter: Theory and its application to vehicle localization," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 4, pp. 1860–1871, Dec. 2013.

[34] Z. Deng, P. Zhang, W. Qi, J. Liu, and Y. Gao, "Sequential covariance intersection fusion Kalman filter," *Information Sciences*, vol. 189, pp. 293–309, Apr. 2012.

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

[36] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *Proceedings of IEEE Conference on Decision and Control*, Atlanta, GA, USA, Dec.2010, pp. 5967–5972.

[37] D. Shi, R. Elliott, and T. Chen, "Event-based state estimation of discrete-state hidden markov models," *Automatica*, vol. 65, pp. 12–26, Mar. 2016.

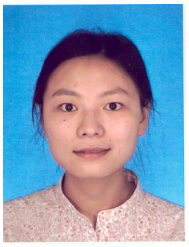
[38] J. Hu, L. Xie, and C. Zhang, "Diffusion Kalman filtering based on covariance intersection," *IEEE Transactions on Signal Processing*, vol. 60, no. 2, pp. 891–902, Feb. 2012.

[39] L. Chen, P. Arambel, and R. Mehra, "Estimation under unknown correlation: covariance intersection revisited," *IEEE Transactions on Automatic Control*, vol. 47, no. 11, pp. 1879–1882, Nov. 2002.

[40] G. Icriverzi and V. Cristea, "A security model for system track radar data," *CPB Scientific Bulletin, Series C: Electrical Engineering*, vol. 74, no. 3, pp. 4–14, Mar. 2012.

[41] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proceedings of Allerton Conference on Communication, Control, and Computing*, Monticello, IL, USA, Oct. 2009, pp. 911–918.


**Chaoqun Yang** received his B.Sc. degree in marine technology from Xiamen University, Xiamen, China, in 2015. He is currently pursuing the Ph.D. degree with the Department of Information Science and Electronic Engineering, Zhejiang University, Hangzhou, China. His current research interests include radar network, multi-target tracking and array signal processing.



**Li Feng** received the M.S. degree in operation research from Department of Mathematics, the University of Hong Kong, Hong Kong in 2007, and the Ph.D. degree from Faculty of Information Technology (FIT), Macau University of Science and Technology (MUST), Macao in 2013. Now she is an assistant professor in FIT, MUST. Her research interests include wireless and mobile networks, power saving, SDN, and performance analysis.

**Heng Zhang** received the Ph.D. degree in control science and engineering from Zhejiang University in 2015. He is currently an associate professor at the School of Science, Huaihai Institute of Technology, Lianyungang, Jiangsu, China. He is also a research fellow at Western Sydney University. His research interests include security and privacy in cyber-physical systems, control and optimization theory. He is an editor board member of several academic journals, including IET Wireless Sensor Systems, EURASIP Journal on Wireless Communications and Networking, KSII Transactions on Internet and Information Systems, etc. He also serves as a guest editor of Journal of The Franklin Institute, Peer-to-Peer Networking and Applications. He is also an active reviewer of IEEE TAC, IEEE TCNS, IEEE TIFS, and IEEE TWC, etc.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSIPN.2018.2790361, IEEE Transactions on Signal and Information Processing over Networks



**Shibo He** (M'13) is currently a professor with Zhejiang University. He was an Associate Research Scientist from March 2014 to May 2014, and a post-doctoral scholar from May 2012 to February 2014, with Arizona State University, Tempe, AZ, USA. He received the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2012. From Nov. 2010 to Nov. 2011, he was a visiting scholar with the University of Waterloo, Waterloo, ON, Canada. His research interests include wireless sensor networks, crowdsensing and big data analysis, etc. Dr. He serves on the editorial board of IEEE Transactions on Vehicular Technology, Springer Peer-to-Peer Networking and Application and KSII transactions on Internet and Information Systems, and is a guest editor of Elsevier Computer Communications and Hindawi International Journal of Distributed Sensor Networks. He served as Symposium Co-chiar for IEEE ICC 2017, Finance & Registration chair for ACM MobiHoc 2015, TPC Co-chair for IEEE ScalCom 2014, TPC Vice Co-chair for ANT 2013-2014, Track Co-chair for the Pervasive Algorithms, Protocols, and Networks of EUSPN 2013, Web Co-Chair for IEEE MASS 2013, and Publicity Co-chair of IEEE WiSARN 2010 and FCN 2014.

**Zhiguo Shi** (M10-SM15) received the B.S. and Ph.D. degrees in electronic engineering from Zhejiang University, Hangzhou, China, in 2001 and 2006, respectively. Since 2006, he has been a Faculty Member with the Department of Information and Electronic Engineering, Zhejiang University, where he is currently a Full Professor. From 2011 to 2013, he visited the Broadband Communications Research Group, University of Waterloo, Waterloo, ON, Canada. His current research interests include signal and data processing, and smart grid communication and network. Prof. Shi serves as an Editor for the IEEE Network, KSII Transactions on Internet and Information Systems, and IET Communications. He was a recipient of the Best Paper Award from the IEEE Wireless Communications and Networking Conference 2013, Shanghai, China, the IEEE/CIC International Conference on Communications in China 2013, Xian, China, and the IEEE Wireless Communications and Signal Processing 2012, Huangshan, China, and the Scientific and Technological Award of Zhejiang Province, China, in 2012.