sensors

MDPI

Article

A Secure Scheme for Distributed Consensus Estimation against Data Falsification in Heterogeneous Wireless Sensor Networks

Shichao Mi [1,2,*], Hui Han [1,†], Cailian Chen [2,†], Jian Yan [2,†] and Xinping Guan [2,†]

[1] Luoyang Electronic Equipment Test Center (LEETC), Luoyang 471003, China; cemee_hanhui@163.com
[2] Department of Automation, Shanghai Jiao Tong University, and Key Laboratory of System Control and Information Processing, Ministry of Education of China, Shanghai 200240, China; cailianchen@sjtu.edu.cn (C.C.); jyan@ysu.edu.cn (J.Y.); xpguan@sjtu.edu.cn (X.G.)
* Correspondence: mishichao@sjtu.edu.cn; Tel./Fax: +86-185-3885-2458
† These authors contributed equally to this work.

Academic Editor: Rongxing Lu
Received: 30 November 2015; Accepted: 12 February 2016; Published: 19 February 2016

Abstract: Heterogeneous wireless sensor networks (HWSNs) can achieve more tasks and prolong the network lifetime. However, they are vulnerable to attacks from the environment or malicious nodes. This paper is concerned with the issues of a consensus secure scheme in HWSNs consisting of two types of sensor nodes. Sensor nodes (SNs) have more computation power, while relay nodes (RNs) with low power can only transmit information for sensor nodes. To address the security issues of distributed estimation in HWSNs, we apply the heterogeneity of responsibilities between the two types of sensors and then propose a parameter adjusted-based consensus scheme (PACS) to mitigate the effect of the malicious node. Finally, the convergence property is proven to be guaranteed, and the simulation results validate the effectiveness and efficiency of PACS.

Keywords: security; relay nodes; data falsification; distributed estimation; heterogeneous wireless sensor networks

1. Introduction

With the features of being low cost, easy to deploy and the self-organization of sensor nodes, wireless sensor networks (WSNs) are widely used to estimate the physical parameters in hazardous and remote areas, such as military defense, intelligent transportation, industrial production, environment monitoring, smart homes, and so on [1–5]. In most applications, the environment may be complicated and needs different kinds of sensors. Therefore, it is wiser to use a combination of different sensors: numbers of cheap, low-end sensors and some expensive, high-quality sensors, making up the heterogeneous wireless sensor networks (HWSNs) [6–9].

In WSNs, it is often necessary for some or all of the nodes to calculate some functions with certain parameters. Additionally, distributed estimation is an effective tool to exchange information among sensor nodes in the network. It is a well-studied domain and has attracted much attention [10–16]. However, in most applications, the networks are deployed in a harsh environment or a hostile region. Due to the restrictions of the computation abilities, storage capacity and battery power of sensor nodes, they are unable to be loaded with firewall-like security tools [17]. There inevitably exists a security problem in distributed networks. For example, if a sensor is intruded in an HWSN, other kinds of sensors are affected, and this may cause network congestion, network lifetime reduction, sensing inaccuracy, *etc.* [18–20]. Therefore, the study of the security of distributed estimation in HWSNs is very important for addressing the issue of the growing malicious attack threat.

As we know, distributed estimation in the presence of malicious nodes has attracted considerable attention in homogeneous wireless sensor networks [21–23]. Generally, fault monitoring algorithms are based on a detection threshold or state estimate residuals to distinguish attackers from honest nodes. In an HWSN, with different types of sensors, data are integrated in different ways. Therefore, the detection algorithms in homogeneous wireless sensor networks are not suitable for HWSNs. Nevertheless, some security schemes have been proposed for HWSNs. Incorporating pairwise keys used for sensor nodes communicating with each other has been studied in [24]. Key management schemes for providing security operations in the HWSN have been considered [25]. Some researchers were concerned with mutual authentication frameworks [26]. These secure schemes based on authentication and key management cost much energy and storage capacity, while sensor nodes have the restrictions of computation abilities, storage capacity and battery power. The schemes were not practical for low-cost sensors. Some secure schemes based on a distributed consensus estimation algorithm have also been proposed for wireless sensor networks. A weighted averaging-based consensus scheme (WACS) [27] was proposed to mitigate the negative impact of malicious nodes for homogeneous wireless sensor networks. The scheme was based on weighted average parameters, which were prescribed as fixed values within a certain range, and the parameters affected the convergence speed or there was the effect of the weighted averaging-based consensus scheme (WACS). The results with the WACS finally converged to the average of the initial values of all sensor nodes. If the initial values were forged by attackers, the scheme could do nothing to protect the network from attackers injecting false data into the sensing stage. Considering the restrictions of the computation abilities, storage capacity, the battery power of sensor nodes and the security of the network, this paper focuses on security issues in HWSNs.

In this paper, we consider distributed estimation in the HWSNs consisting of two types of sensors: sensor nodes (SNs) and relay nodes (RNs). SNs have a good hardware architecture and are high quality, and they can sense the surrounding parameters and are responsible for data fusion. RNs are inexpensive and low end, and their main role is to relay the information for SNs. In the case the network is attacked by malicious nodes, we present a data falsification attack, that is malicious nodes manipulate false data in the network and damage the consensus of the whole system. Then, we propose a parameter adjusted-based consensus scheme (PACS) to decrease the negative effect of the data falsification attack. The main difference from the existing algorithm is that we explicitly consider the heterogeneity of responsibilities between the two types of sensors. With the network topology, we demonstrate the transformation of the distributed consensus method to overcome the challenges produced by the heterogeneity. Additionally, by adjusting the weights of sensor nodes, we illustrate how the PACS can decrease the effect of malicious nodes and avoid excluding the honest nodes with large deviations to participate in the distributed consensus. We evaluate the effectiveness and efficiency of the PACS.

The reminder of the paper is outlined as follows. The network model and the attack model are introduced in Section 2. In Section 3, we propose the secure scheme. Section 4 provides some simulations. The conclusion and future work are presented in Section 5.

2. System Model

2.1. Network Model

For the large-scale network, the long distance transmission costs much energy and may result in separate groups of sensors. A popular method is to deploy relay sensors for connecting the separate groups. Thus, the whole network can be connected. Here, we consider a connected HWSN with a combination of different sensors: sensor nodes (SNs) and relay nodes (RNs). The network contains N nodes, which consists of M numbers of SNs and $(N-M)$ numbers of RNs. $\mathcal{I}_S = \{1, 2, ..., M\}$ represents the set of SNs, and $\mathcal{I}_R = \{M+1, M+2, ..., N\}$ represents the set of RNs. Each SN can perceive the surrounding parameters, while RNs cannot sense the parameters, but can relay information for the

network. We use an undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ to describe the network. $\mathcal{V}$ denotes the set of nodes, and $\mathcal{V} = \mathcal{I}_S \cup \mathcal{I}_R$, where $\mathcal{I}_S$ represents the set of SNs and $\mathcal{I}_R$ represents the set of RNs; $\mathcal{E} \in \mathcal{V} \times \mathcal{V}$ denotes the set of edges referring to the communication links. If there exists an edge connecting two nodes, the two nodes can communicate with each other. If $(i, j) \in \mathcal{E}$ where $i \neq j$ (*i.e.*, node j can transfer information with node i), we call node j a neighbor of node i. $\mathcal{N}_i = \{j | (j, i) \in \mathcal{E}\} \subset \mathcal{V}$ represents the neighbor set of node i. The number of elements in $\mathcal{N}_i$ is denoted by $|\mathcal{N}_i|$.

Define the Laplacian matrix of $\mathcal{G}$ as $L = (l_{ij})_{N \times N}$, then:

$$l_{ij} = \begin{cases} -1, & \text{if } j \neq i, j \in \mathcal{N}_i \\ |\mathcal{N}_i|, & \text{if } j = i \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

Each node $i \in \mathcal{I}_S$ is supposed to begin with a private value $x_i(0)$ by sensing the environment. The aim for the network is to converge to a common value relying on $x_i(0)$ by the incorporation of each node. During the distributed consensus estimation, at each iteration step k, each sensor node updates and exchanges its values with neighbors according to a prescribed strategy, which can be modeled by a discrete-time equation, and each node i updates its estimation as follows:

$$x_i(k+1) = x_i(k) + \epsilon \sum_{j \in \mathcal{N}_i} a_{ij}(x_j(k) - x_i(k)), \text{ if } i \in \mathcal{I}_S \tag{2}$$

and:

$$x_i(k+1) = \sum_{j \in \mathcal{N}_i} \gamma_{ij} x_j(k), \text{ if } i \in \mathcal{I}_R \tag{3}$$

where:

$$0 < \epsilon < (\max_i |\mathcal{N}_i|)^{-1} = \frac{1}{\Delta} \tag{4}$$

$x_i(k)$ represents the state value of node i at time step k. Δ represents the maximum degree of the network, and a_{ij} denotes the amplitude of the signal received by sensor i from sensor j. γ_{ij} is the corresponding weight satisfying $\gamma_{ij} > 0$, and $\sum_{j \in \mathcal{N}_i} \gamma_{ij} = 1, \forall i \in \mathcal{I}_R$. We set the notation $\gamma_{ij} = 0$, for $j \notin \mathcal{N}_i$. For all $j \in \mathcal{N}_i$, we have that $\sum_{j=1}^{N} \gamma_{ij} = 1, \forall i \in \mathcal{I}_R$. It is clear that each node updates its estimates by the linear combination of its neighbors' state values and its own values.

To simplify the consensus scheme, we combine Equations (2) and (3) and get the consensus equation that only contains the SNs, but implies the state of RNs.

$$x_i(k+1) = x_i(k) + \epsilon \left[\sum_{j \in \mathcal{N}_i^S} a_{ij}(x_j(k) - x_i(k)) + \sum_{k \in \mathcal{N}_i^R} \sum_{j \in \mathcal{N}_k{}^S} a_{ik}\gamma_{kj}(x_j(k) - x_i(k)) \right] \tag{5}$$

$\mathcal{N}_i^S$ represents the sensor neighbor set of node i, while $\mathcal{N}_i^R$ represents the relay neighbor set of node i.

2.2. Attack Model

A familiar attack called data falsification is considered in this paper. A false state value may be manipulated in the sensing stage or in the state updating progress by a data falsification attacker. We can see that the data falsification attack is easy to implement if a sensor node has been captured. Moreover, due to noise in the environment, there is usually a large error when a sensor node perceives parameters. Therefore, it is hard to distinguish whether a sensor node is captured by data falsification or not. Since this kind of attack can effect the consensus process and cause long-term impacts, it can be destructive to the network. Three types of data falsification will be presented in the following [28].

Perception Data Falsification (PDF) Attack: This attack changes the value of $x_i(0), i \in \mathcal{I}_S$. An attacker aims to forge a false sensing data and to disseminate it to its neighbors. However, in the information

fusing phase, malicious nodes correctly update their estimates and send the estimated value to their neighbors. This kind of attack is easy to implement, but difficult to distinguish from honest nodes with a large deviation. To avoid mistaking honest nodes with a large deviation, the objective of our scheme in this paper is to decrease, but not to eliminate the attackers.

Iteration Data Falsification (IDF) Attack: False data are injected both in the sensing stage and at each iteration step by attackers. This type of attack can impact the consensus process; therefore, it can compromise the network for a long time.

Random Data Falsification (RDF) Attack: The attacker injects forged data or correctly executes a distributed estimation process in a random way. This type of attack is difficult to be detected because of its concealed feature.

In this paper, a distributed secure scheme based on parameter adjustment is presented to decrease the effect of the data falsification attack. We adjust the parameters in the distributed consensus algorithm (Equation (5) in Section 2.1). Abnormal nodes are distinguished from honest nodes via an adaptive local threshold. If a node is considered to be abnormal, the weight is reduced. In this way, we propose the PACS to decrease the effect of malicious nodes and to ensure the security of the network.

3. Secure Scheme

In this section, we propose a PACS for protecting the network from the data falsification attack. Then, its effectiveness is demonstrated by analyzing the algorithm.

3.1. Parameter Adjusted-Based Consensus Scheme

Detection algorithms are designed to assort abnormal nodes and honest nodes in the network. With the characteristics of the consensus algorithm, the state values of all of the nodes in the network converge to a common value, and the difference among all of the states is reduced to zero. Based on this characteristic, this paper presents a detection algorithm by comparing a localized threshold to the difference produced by each node state and its neighbors', and the threshold adaptively shrinks to zero.

We now elaborate the consensus secure scheme based on the detection algorithm below. In the first stage, the node $i \in \mathcal{I}_S$ makes a measurement independently and transfers the measurement value to its neighbors. Then, node i compares the state value to its neighbor's value. The set of nodes satisfying $|x_j(k) - x_i(k)| < \lambda_i(k)$ is denoted as $\mathcal{N}_i^T$, and the set of nodes satisfying $|x_j(k) - x_i(k)| \geq \lambda_i(k)$ is denoted as $\mathcal{N}_i^F$. $\alpha_i(k)$ and $\beta_i(k)$ represent the number of $\mathcal{N}_i^F$ and $\mathcal{N}_i^T$, respectively. If $\beta_i(k) + 1 \geq \alpha_i(k)$, the measurement of the node $i \in \mathcal{I}_S$ is correct, and its state update equation is demonstrated as follows.

$$x_i(k+1) = x_i(k) + \sigma(k) \left[\sum_{j \in \mathcal{N}_i^{ST}} a_{ij}(x_j(k) - x_i(k)) + \sum_{j \in \mathcal{N}_i^{SF}} \frac{a_{ij}}{a(k)}(x_j(k) - x_i(k)) \right.$$
$$\left. + \sum_{k \in \mathcal{N}_i^R} \sum_{j \in \mathcal{N}_k{}^{ST}} a_{ik}\gamma_{kj}(x_j(k) - x_i(k)) + \sum_{k \in \mathcal{N}_i^R} \sum_{j \in \mathcal{N}_k{}^{SF}} \frac{a_{ik}}{a(k)}\gamma_{kj}(x_j(k) - x_i(k)) \right] \tag{6}$$

$\sigma(k) > 0$ represents the weight. $\mathcal{N}_i^{ST}$ denotes the set of sensor nodes in $\mathcal{N}_i^T$, and $\mathcal{N}_i^{SF}$ denotes the set of sensor nodes in $\mathcal{N}_i^F$. $a(k)$ is a parameter that can affect the consistency coefficient. From the equation, we can see that if $a(k)$ becomes larger, the effect of the corresponding node becomes smaller. If a node is detected to be abnormal at the iteration step k, the corresponding coefficient $a(k)$ becomes larger, and finally, its influence can be reduced. Additionally, $a(k+1) = a \times a(k)$, where a is an integer whose value is larger than one. If a node stops injecting false data at the iteration step, the corresponding coefficient $a(k)$ decreases. If $a(k) > 1$, $a(k+1) = (1/a) \times a(k)$ at the iteration step until $a(k) = 1$. If $a(k) = 1$ and the node performs normally, $a(k)$ stays at one.

We define $P(k) = I - \sigma(k)L$. Then, we can get the compact form of Equation (6):

$$x(k+1) = P(k)x(k) \tag{7}$$

Meanwhile, if the nodes satisfy $\beta_i(k) + 1 < \alpha_i(k)$, the nodes are considered to be incorrect, and their update equation remain as Equation (5).

To determine the threshold $\lambda_i(k)$ of each node n_i, we give the equation as follows.

$$\lambda_i(k) = \frac{1}{|\mathcal{N}_i|} \sum_{j \in \mathcal{N}_i} \left| x_j(k) - \frac{x_i(k) + \sum_{j \in \mathcal{N}_i} x_j(k)}{|\mathcal{N}_i| + 1} \right| \tag{8}$$

Considering that malicious nodes inject false data with a large deviation from the sensing data of authentic nodes, we can detect the attacker by comparing the threshold with the difference between the neighbors' states and the state of node i. Furthermore, as the consensus is carried out, the localized threshold $\lambda_i(k)$ will decease to zero, and the attackers are given no tolerance.

The whole procedure of PACS is concluded in the following Algorithm 1.

Algorithm 1: Parameter Adjusted-Based Consensus Scheme (PACS).

Require: Graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, M SNs, $N - M$ RNs
Ensure: $x(k)$
set $k = 0$
for $i \in \mathcal{I}_S$ **do**
  set $a(k) = 1$, $a > 1$, $\alpha_i = 0$ and $\beta_i = 0$
  i makes the measurement and gets the initial $x_i(0)$, then transmits $x_i(0)$ to its neighbors.
end for
for the consensus is not reached **do**
  for $i \in \mathcal{I}_S$ **do**
    $\lambda_i(k) = \frac{1}{|\mathcal{N}_i|} \sum_{j \in \mathcal{N}_i} \left| x_j(k) - \frac{x_i(k) + \sum_{j \in \mathcal{N}_i} x_j(k)}{|\mathcal{N}_i| + 1} \right|$
    for $j \in \mathcal{N}_i$ **do**
      if $|x_i(k) - x_j(k)| > \lambda_i(k)$ **then**
        $\alpha_i = \alpha_i + 1$
        if $a(k) = 1$ **then**
          $a(k) = a$
        else
          $a(k) = a \times a(k)$
        end if
      else
        $\beta_i = \beta_i + 1$
        if $a(k) > 1$ **then**
          $a(k) = \frac{1}{a} a(k)$
        else
          $a(k) = 1$
        end if
      end if
    end for
    if $\beta_i + 1 > \alpha_i$ **then**
      $x_i(k)$ updates its state according to Equation (6) and transmits the state estimation to its neighbors.
      Update L_{ii} and ensure the sum of i-th row sum is 1.
    end if
  end for
  set $k = k + 1$
end for

3.2. Performance Analysis

In this section, we analyze the performance of the proposed PACS. We consider that node v_1 is an abnormal node injecting false data in the sensing stage. The neighbors of v_1 are denoted by $v_2, v_3, ..., v_{|\mathcal{N}_1|+1}$. Then, at the iteration step k, we can get the Laplacian matrix $L(k)$ as follows:

$$l_{ij} = \begin{cases} -\frac{a_{ij}}{a^k}, & \text{if } j \neq 1, i \in \mathcal{N}_1^S \\ -\frac{a_{ij}}{a^k}\gamma_{kj}, & \text{if } j \neq 1, i \in \mathcal{N}_1^R \\ l_{ij} - a_{ij} + \frac{a_{ij}}{a^k}, & \text{if } j = i \neq 1, j \in \mathcal{N}_1^S \\ l_{ij} - a_{ij}\gamma_{ij} + \frac{a_{ij}}{a^k}\gamma_{ij}, & \text{if } j = i \neq 1, j \in \mathcal{N}_1^R \\ l_{ij}, & \text{otherwise} \end{cases} \tag{9}$$

According to the proposed algorithm, if the state value is considered abnormal at each iteration k, the corresponding parameter of $x_1(k)$ decreases. Additionally, $P(k)$ is also changed. We suppose that the HWSN is not dominated by attackers.

Firstly, we illustrate that the network can reach convergence. Note that there are n eigenvalues of $L(k)$ at the first place. According to the Gershgorin circle theorem [29] and $\gamma_{ij} < 1$, we get the following inequations:

$$|\xi_m - |\mathcal{N}_j| + 1 - \frac{a_{ij}}{a^k}\gamma_{ij}| \leq |\mathcal{N}_j| - 1 + \frac{a_{ij}}{a^k}\gamma_{ij}, \forall j \in \mathcal{N}_1^R \tag{10}$$

$$|\xi_m - |\mathcal{N}_j| + 1 - \frac{a_{ij}}{a^k}| \leq |\mathcal{N}_j| - 1 + \frac{a_{ij}}{a^k}, \forall j \in \mathcal{N}_1^S \tag{11}$$

$$|\xi_m - |\mathcal{N}_j|| \leq |\mathcal{N}_j|, \forall j \notin \mathcal{N}_1 \tag{12}$$

where ξ_m $(1 \leq m \leq n)$ is an eigenvalue of $L(k)$ at the first place. Because of $0 < \sigma(k) < (\max_i \mathcal{N}_i)^{-1}$, we can get that $0 \leq \xi_m \leq 2(\max_i \mathcal{N}_i)^{-1}$. The eigenvalue of $P(k)$ is $\xi_m^* = 1 - \sigma(k)\xi_m$, so we can obtain that $-1 < \xi_m^* < 1$. Moreover, the network is connected, and $rank(\mathcal{G}) = n - 1$ [4]. Thus, L has only a single zero eigenvalue, and $P(k)$ has only one single eigenvalue, which is $\mathbf{1}$. The network can reach convergence.

With the consensus-based estimation, $x_1(k)$ finally converges to a normal range, and $P(k)$ keeps a common value P_0 when k is large enough. We assume $P(k)$ keeps a common value P_0 for $k = k_0$. Thus, we can get the result of the consensus.

$$x(k) = \lim_{k\to\infty} P_0^k \prod_{k=1}^{k_0-1} P(k)x(0) \tag{13}$$

Secondly, we prove the efficiency of the scheme by computing $\lim_{k\to\infty} P_0^k \prod_{k=1}^{k_0-1} P(k)$. A lemma is introduced as follows.

Lemma 1. *[13] Given a primitive nonnegative matrix P_0, if there exist eigenvectors u and w^T satisfying $P_0 u = u$ and $w^T P_0 = w^T$, then $\lim_{k\to\infty} P_0^k = \frac{uw^T}{w^T u}$ holds.*

If the graph $\mathcal{G}$ is a strongly connected component, we can get that P_0 is a primitive nonnegative matrix [13]. The eigenvectors $u = \mathbf{1}$ and $w^T = [1, a^k, ...a^k]$ satisfy the conditions in Lemma 1. Thus, we can obtain the following equation:

$$\lim_{k\to\infty} P_0^k = \frac{uw^T}{1 + a^k(N-1)} \tag{14}$$

According to the result of $\lim_{k\to\infty} P_0^k$, we can compute $x(k)$. For the convenience of discussion, a two-hop network is considered. A theorem is presented as below. Additionally, a row vector z_i^T is defined as follows:

$$z_i^T = \begin{cases} z_1, & \text{if } i = 1 \\ z_2, & \text{if } 1 < i \leq 1 + |\mathcal{N}_1| \\ z_3, & \text{if } 1 + |\mathcal{N}_1| < i \leq N \end{cases} \tag{15}$$

where $z_3 \geq z_2 \geq a^k z_1$. If a network has more hops, we can extend $z^T = [z_1, z_2, ..., z_2, z_3, ..., z_3, ..., z_n, ..., z_N]$ satisfying $z_N \geq ... \geq z_3 \geq z_2 \geq a^k z_1$, and a similar conclusion can be made. Define that $\mathcal{N}_i^G = \{j | j \neq 1 \text{ and } j \in \mathcal{N}_i / \mathcal{N}_1, \forall 1 < i \leq |\mathcal{N}_1| + 1\}$ and $\mathcal{N}_i^H = \{j | j \in \mathcal{N}_i \bigcap \mathcal{N}_1, \forall |\mathcal{N}_1| + 1 < i \leq N\}$. The numbers of the above set are denoted as $|\mathcal{N}_i^G|$ and $|\mathcal{N}_i^H|$, respectively. The element number of the two-hop node set in the neighboring set of one-hop nodes is constant. Meanwhile, the element number of the one-hop node set in the neighboring set of two-hop nodes is constant, too. Thus, we get $|\mathcal{N}_2^G| = |\mathcal{N}_i^G|$; $|\mathcal{N}_3^H| = |\mathcal{N}_i^H|$ is invariable. Additionally, the following theorem is drawn.

Theorem 1. *Given a row vector z^T satisfying $z_3 \geq z_2 \geq a^k z_1$ and $\psi^T = z^T P(k)$ satisfying:*

$$\psi_i^T = \begin{cases} \psi_1, & \text{if } i = 1 \\ \psi_2, & \text{if } 1 < i \leq 1 + |\mathcal{N}_1| \\ \psi_3, & \text{if } 1 + |\mathcal{N}_1| < i \leq N \end{cases} \tag{16}$$

then $\psi_3 \geq \psi_2 \geq a^k \psi_1$ and $\psi^T \mathbf{1} = z^T \mathbf{1}$ as long as $\sigma(k) \leq \frac{1}{|\mathcal{N}_2^G| + |\mathcal{N}_3^H|}$ and $\sigma(k) \leq \frac{1}{|\mathcal{N}_1| + 1}$.

Proof. Since $\psi^T = z^T P(k)$, for all $j \in \mathcal{N}_1^S$, we can get the following equation:

$$\psi_1 = z_1 - \sigma(k) a_{1j} z_1 |\mathcal{N}_1| + \frac{a_{1j}}{a^k} \sigma(k) |\mathcal{N}_1| z_2 \tag{17}$$

and:

$$\psi_j = \psi_2 = \sigma(k) z_1 + z_2 - \frac{a_{1j}}{a^k} \sigma(k) z_2 + \sigma(k) |\mathcal{N}_2^G| (z_3 - z_2), \forall j \in \mathcal{N}_i^G \tag{18}$$

$$\psi_j = \psi_3 = z_3 + \sigma(k) |\mathcal{N}_2^H| (z_2 - z_3), \forall j \in \mathcal{N}_i^H \tag{19}$$

From the above equations, we have that:

$$\psi^T \mathbf{1} = \psi_1 + |\mathcal{N}_1| \psi_2 + (N - 1 - |\mathcal{N}_1|) \psi_3 = z_1 + |\mathcal{N}_1| z_2 + (N - 1 - |\mathcal{N}_1|) z_3 = z^T \mathbf{1} \tag{20}$$

For all $j \in \mathcal{N}_1^R$, the corresponding equations similar to the above Equations (17)–(20) are holds. Since the matrix $P(k)$ eliminating the first column and the first row is a symmetric matrix, we get $|\mathcal{N}_1||\mathcal{N}_2^G| = (N - 1 - |\mathcal{N}_1|)|\mathcal{N}_3^H|$.

Then, we compare $a^k \psi_1$, ψ_2 and ψ_3; for all $j \in \mathcal{N}_1^S$.

$$\psi_2 - a^k \psi_1 = (z_2 - a^k z_1)[1 - \sigma(k)](\frac{a_{1j}}{a^k} + |\mathcal{N}_1|) + \sigma(k) |\mathcal{N}_2^G| (z_3 - z_2) \tag{21}$$

Since $\sigma(k) \leq \frac{1}{|\mathcal{N}_1| + 1}$, $\sigma(k) \leq \frac{1}{|\mathcal{N}_1| + a^{-k}}$. Additionally, $z_3 \geq z_2 \geq a^k z_1$, we can get that $\psi_2 - a^k \psi_1 \geq 0$.

$$\psi_3 - \psi_2 = (z_3 - z_2)[1 - \sigma(k)(|\mathcal{N}_3^H| - |\mathcal{N}_2^G|)] + \sigma(k)(\frac{a_{1j}}{a^k} z_2 - z_1) \tag{22}$$

Because of $\sigma(k) \leq \frac{1}{|\mathcal{N}_2^G| + |\mathcal{N}_3^H|}$ and $z_3 \geq z_2 \geq a^k z_1$, the inequation $\psi_3 - \psi_2 \geq 0$ holds. When $j \in \mathcal{N}_1^R$, the calculating process is similar; the inequations $\psi_2 - a^k \psi_1 \geq 0$ and $\psi_3 - \psi_2 \geq 0$ hold, too. □

Define that the network finally converged to $x(k)$.

$$x(k) = u\Gamma^T x(0) \tag{23}$$

where $u = [1, 1, ..., 1]^T$ and $\Gamma^T = \frac{w^T}{1+a^k(N-1)} \prod_{k=1}^{k_0-1} P(k) = [\Gamma_1, \Gamma_2, ..., \Gamma_N]$. Since $a > 1$, we derive that $\Gamma_N \geq ... \geq \Gamma_2 \geq a\Gamma_1$ and $\Gamma_1 + \Gamma_2 + ... + \Gamma_N = 1$. Thus, $\Gamma_1 \leq \frac{1}{N}$. Therefore, the weights of the misbehaving nodes can be reduced, but the misbehaving nodes are not eliminated by the proposed scheme. $\Gamma_2 \geq a\Gamma_1$; the effect of the misbehaving nodes becomes smaller when a becomes larger. Additionally, our scheme is especially efficient when the false nodes attack the network continuously.

4. Evaluation

This section presents numerical examples to illustrate the PACS algorithm. We validate the efficiency of PACS by comparing the consensus results without attackers and with data falsification attackers. The algorithm presented by Olfati-Saber [13] is called the Olfati algorithm here. The proposed PACS and the Olfati algorithm are compared in this section.

4.1. Experiments Setup

We get the experiment reports at an apartment in Shanghai Jiao Tong University (SJTU). We use nine USRPs (Universal Software Radio Peripherals) with a broadband antenna (70–1000 MHz) and a TVRX daughterboard (50–860-MHz receiver) to detect three channels of TV broadcasts and three relay nodes to transmit information. The nodes are deployed in a 10 m $\times$ 10 m area. Energy detection is adopted here because of its short sensing time and simplicity. Although the positions of some nodes are very close, there are big differences among the sensing reports. Table 1 shows the sensing reports of close node pairs; (5, 6) and (8, 9) could be quite different. These features illustrate that it is hard to distinguish the diversity of sensing reports caused by data falsification or not, and it is impractical to judge malicious nodes only by using a threshold. Therefore, we design a consensus secure scheme to overcome the diversity of sensing data and the unsafe factors in the network. The consensus algorithm can solve the problem of the sensing data diversity. Additionally, the adjusted parameters in the consensus algorithm can reduce the effect of uncertainties in the network.

Table 1. The sensing reports of sensor nodes (5, 6, 8, 9).

Region	662–670 MHZ	750–758 MHZ	798–806 MHZ
5	3.3626	8.4791	4.1553
6	6.5966	1.9973	8.2043
8	3.8923	4.2489	5.0492
9	2.8713	8.7158	3.9781

Throughout the numerical examples, the initial sensing value (*i.e.*, $x_i(0)$) is the average of 300 sensing reports for the band of 750–758 MHz. We set 10% as the initial link loss rate of each link, *i.e.*, $a_{ij} = 0.90$. Then, we use the off-line data analysis to validate the efficiency of the proposed scheme. Weights for RNs are set to be $\gamma_{ij} = a_{ij}/\Sigma_{j\in\mathcal{N}_i} a_{ij}, \forall i \in \mathcal{I}_R$. The algorithm is implemented with the decreasing weight sequence $\sigma(k) = 1/10, k \leq 20$ and $\sigma(k) = 1/(k-1), k > 20$, and $a = 5$.

4.2. Numerical Example 1

In this experiment, we select 12 sensors: nine SNs and three RNs; shown in Figure 1. Firstly, we illustrate the results with PACS. Figure 2a shows the result without attackers. The network converges to 4.9864. Then, we consider the network attacked by Node 4. The attacker executes the *PDF* attack and forges 16.5966 as the sensing value. Figure 2b shows the results, and the consensus value is 5.0013. Furthermore, Node 4 is set to broadcast the adjusting value with $x_4(k) = x_4(k) + \omega_4(k)$ where ω_4

is randomly selected in $[-0.5, 0.5]$ in the case of the *IDF* attack. The estimated value of the attacker may fluctuate in the data fusion process, but the network converge to 4.9543, as fast as in Figure 2c. Then we take the *RDF* attack into account; the attacker manipulates the sensing state value and adds Gaussian white noise to the states in each iteration step randomly. The result by PACS is demonstrated in Figure 2d. The network can converge to 5.0007 very quickly. We can see that the differences between the convergence value with attackers and without attackers are less than 0.1 (*i.e.*, the error is less than 2%). It is considered that the proposed scheme defends against the data falsification attack effectively.

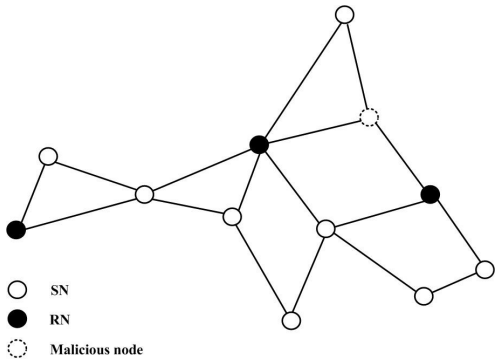
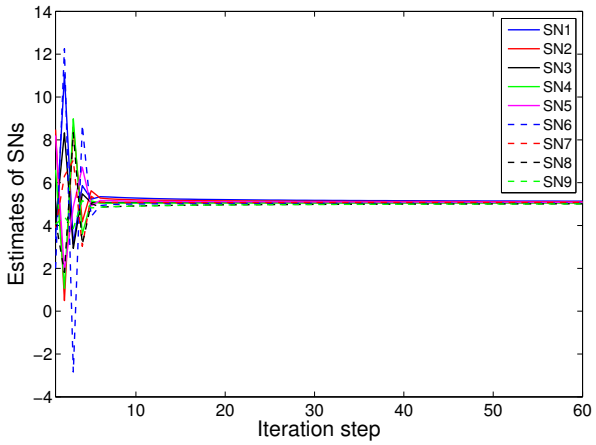


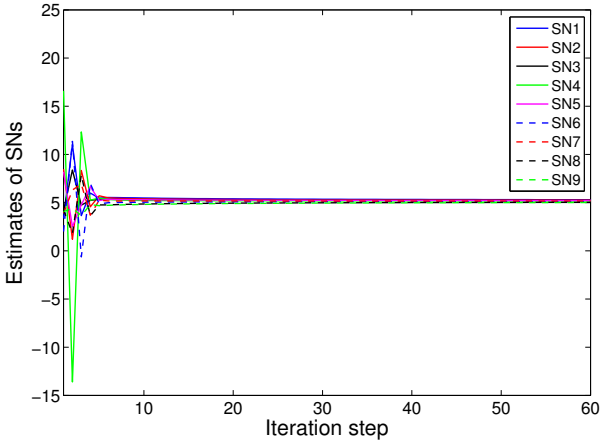
Figure 1. A network with eight honest sensor nodes, three relay nodes and one attacker.

Then, considering the same attack with the above simulation, we show the simulation results with the Olfati algorithm. Figure 3a shows the result without attackers. The consensus results under three different types of attackers are shown in Figure 3b–d, respectively. We can see that the attacks make the network converge to a wrong value or even destroy the convergence of the network.

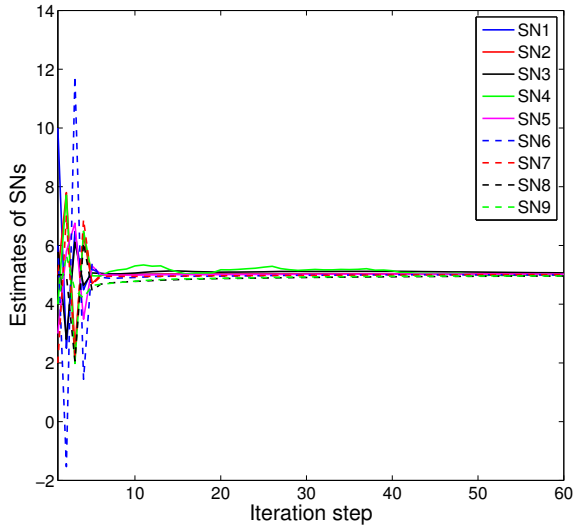


(a)

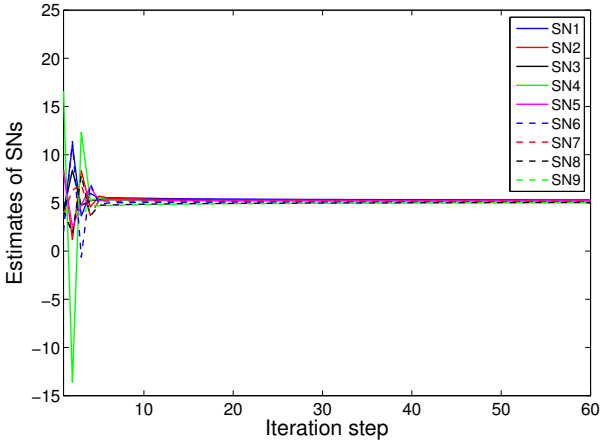
Figure 2. *Cont.*



(b)



(c)

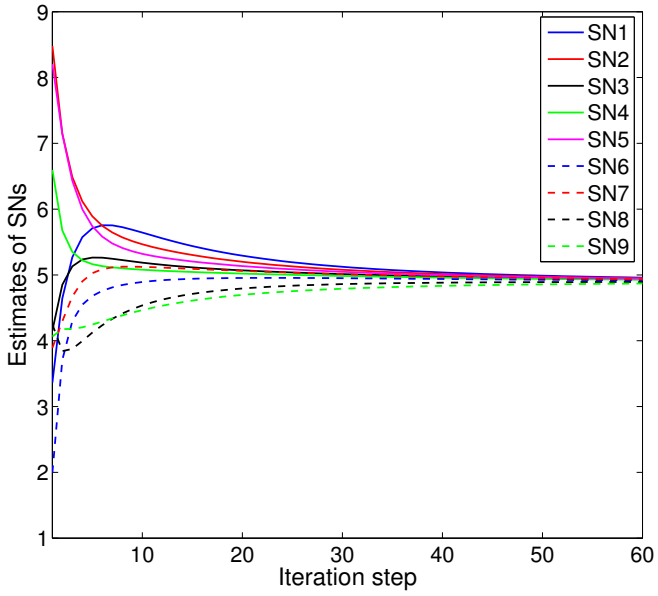


(d)

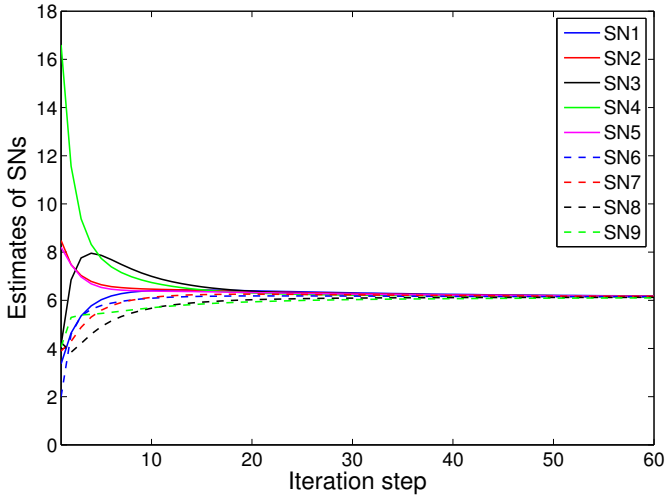
Figure 2. Convergence of parameter adjusted-based consensus (PACS): (**a**) without attackers; (**b**) with one *Perception Data Falsification (PDF)* attacker; (**c**) with one *Iteration Data Falsification (IDF)* attacker; (**d**) with one *Random Data Falsification (RDF)* attacker.

4.3. Numerical Example 2

We consider more sensors as in Figure 4. Firstly, the results of PACS are demonstrated. Figure 5a shows the results of the PACS algorithm on the network without attackers. The consensus result is 4.7543. Additionally, the convergence is quick, although there are more sensor nodes in the network. Then, we consider the case that there are three attackers executing three different attacks: the *SDF*, *ISF* and *RDF* attack, respectively. Figure 5b demonstrates that the value of $x_i(k)$ converges to 4.8561, and the difference between this value with the result without the attack is 0.1018 (*i.e.*, the error is less than 2.14%). We can see that the scheme has a quite good resistance against the variety of data falsification attacks that exists in the network simultaneously.

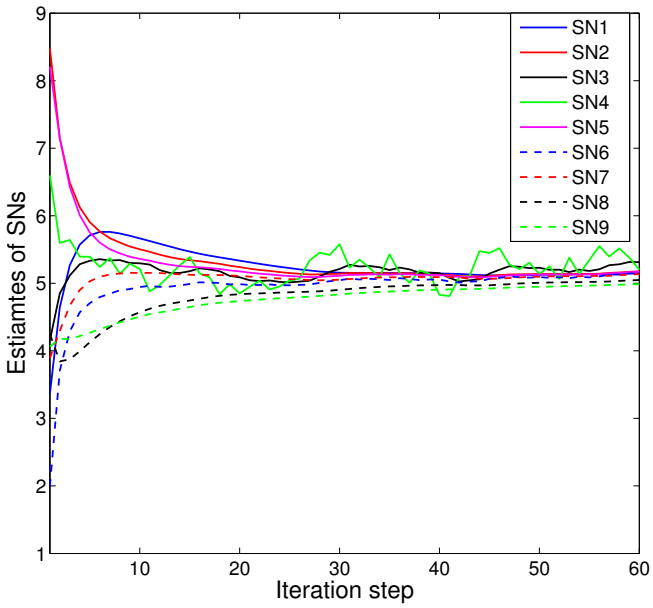


(a)

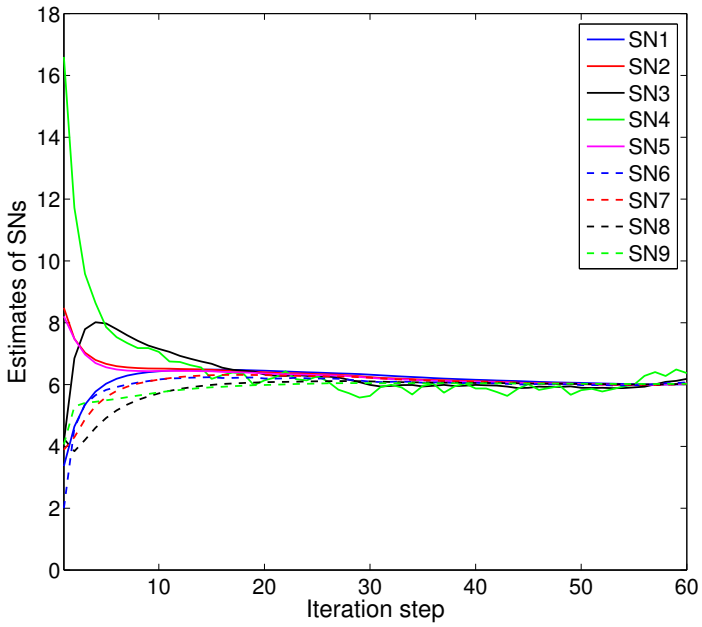


(b)

Figure 3. *Cont.*



(c)



(d)

Figure 3. Convergence of the Olfati algorithm: (**a**) without attackers; (**b**) with one *SDF* attacker; (**c**) with one *IDF* attacker; (**d**) with one *RDF* attacker.

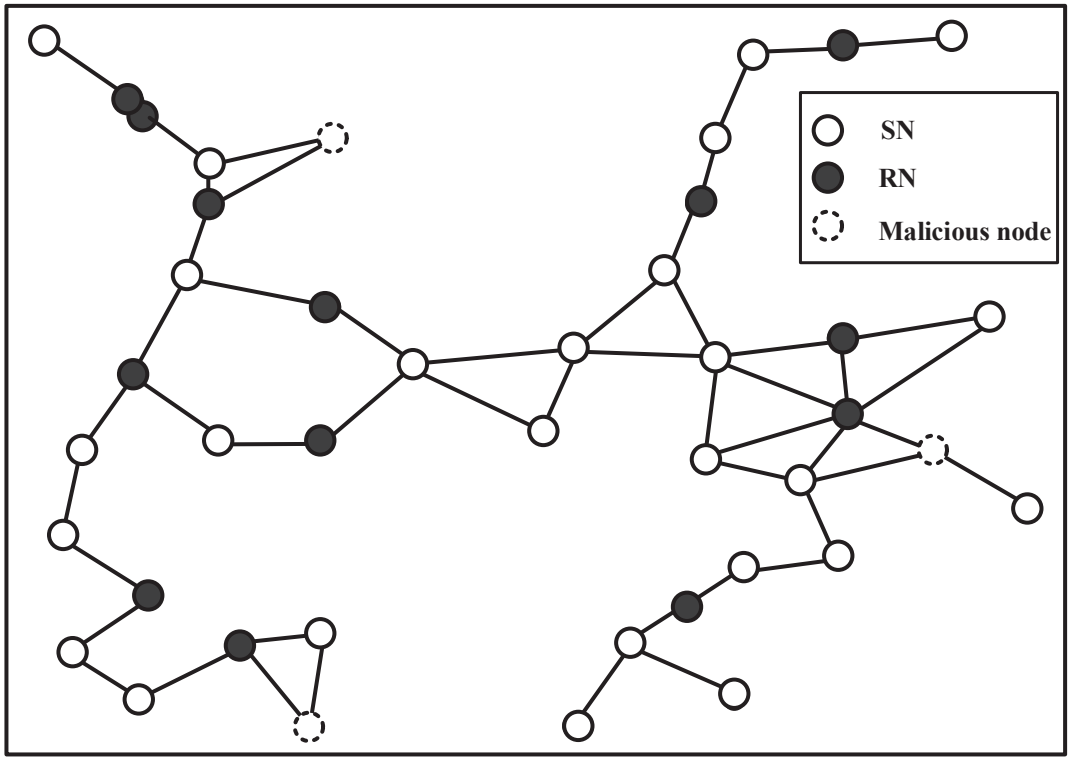
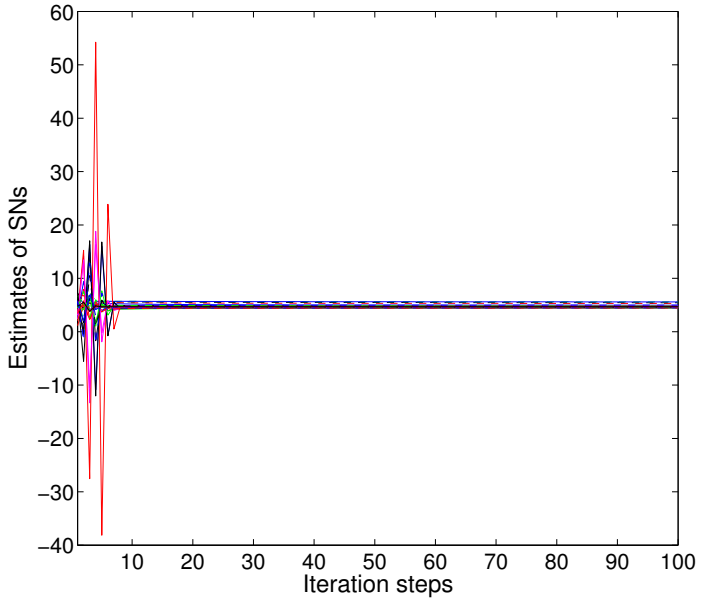
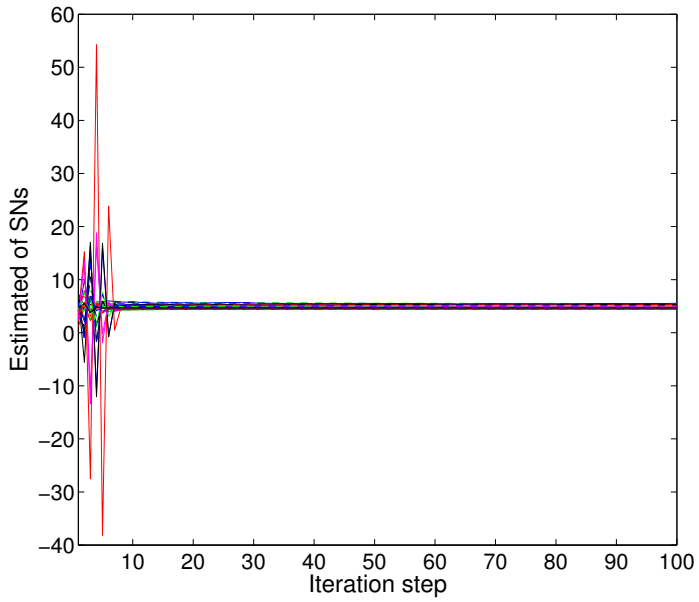


Figure 4. A network with 27 honest sensor nodes, 13 relay nodes and three attackers.



(a)

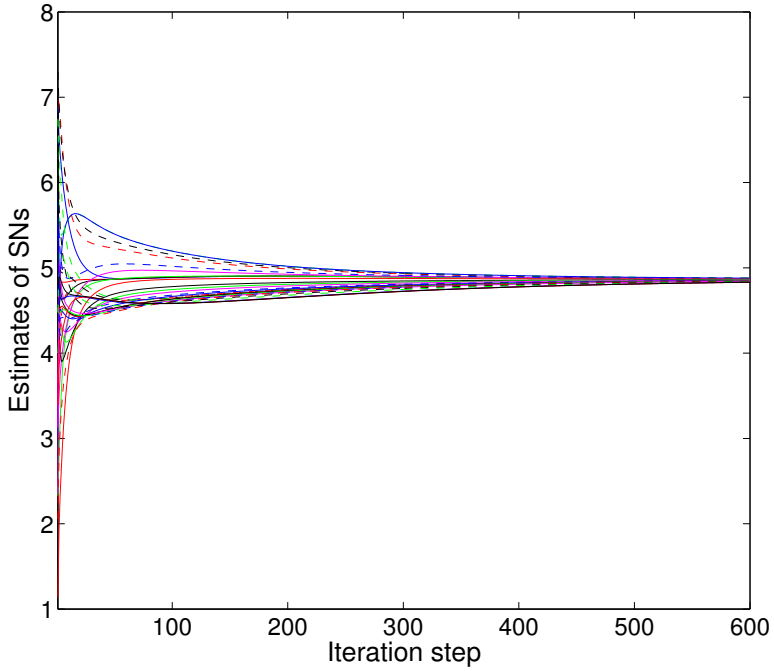
Figure 5. *Cont*.



(b)

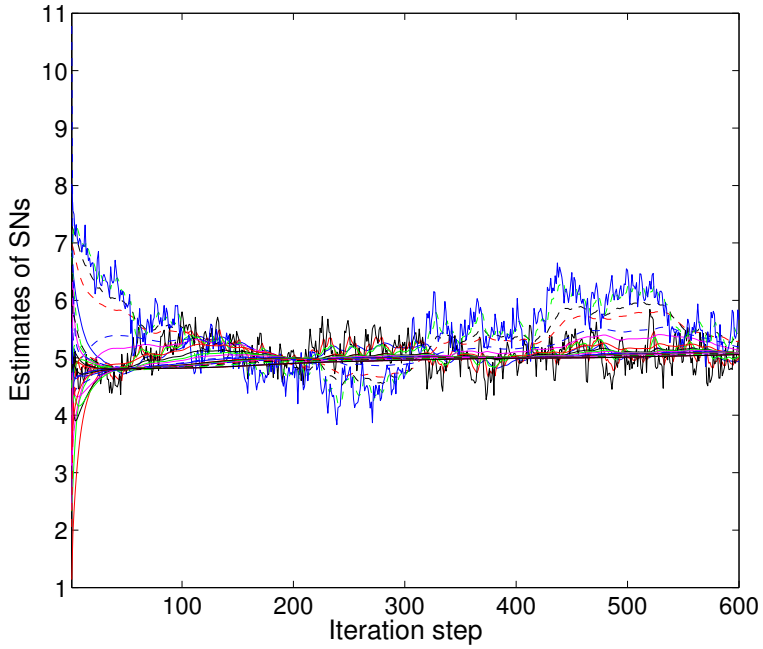
Figure 5. Convergence of PACS in numerical Example 2: (**a**) without attackers; (**b**) with three attackers.

Then, the results of Olfati algorithm on the network without attackers is shown in Figure 6a. The consensus speed is small, because the scale of the network is large. The consensus result is 4.7617. The same attackers are considered to execute the same types of attacks as the above. The results of the Olfati algorithm are shown as Figure 6b; the network cannot reach a consensus obviously.



(**a**)

Figure 6. *Cont.*



(**b**)

Figure 6. Convergence of Olfati in numerical example 2: (**a**) without attackers; (**b**) with three attackers.

5. Conclusions and Future Work

In this paper, we propose a secure scheme to reduce the destructive impact of the abnormal nodes in HWSNs. We utilize an undirected graph to represent the HWSNs and then introduce three different kinds of data falsification. A distributed detection algorithm with a local threshold is presented for classifying malicious nodes from honest ones. PACS is proposed to protect the network from the malicious nodes by decreasing their weights in the distributed estimation. The convergence property of PACS is proven to be guaranteed, and the simulation results illustrate the effectiveness and efficiency of the proposed scheme. We will study the issues of the attack under random graph topologies in heterogeneous wireless sensor networks in future work.

Acknowledgments: The work was partially supported by the State Key Laboratory of CEMEEunder Grant CEMEE2014K0102A, by the NSF of China with Grant Nos. 61221003, 61273181, 61503320 and 61290322, by Postdoctoral Science Foundation Funded Project under 2015M570235 and B2015003018 and by the Science and Technology Commission of Shanghai Municipal, China, under Grant 13QA1401900.

Author Contributions: All authors contributed to the research with their ideas, knowledge and discussion. After studying the literature, Shichao Mi proposed the idea and design of the secure scheme. Hui Han provided the network model and the attack model. Cailian Chen contributed to the analysis of the performance of the security scheme. Jing Yan and Xinping Guan contributed to the organization of the paper and performed critical revisions on an early version of the manuscript. All authors have contributed to the discussion of the proposed framework and have read and approved the final version of the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. Wireless sensor networks: A survey. *Comput. Netw.* **2002**, *38*, 393–422.
2. Yick, J.; Mukherjee, B.; Ghosal, D. Wireless sensor network survey. *Comput. Netw.* **2008**, *52*, 2292–2330.
3. Gao, T.; Massey, T.; Selavo, L.; Chen, B.; Lorincz, K.; Shnayder, V.; Hauenstein, L.; Dabiri, F.; Jeng, J.; Chanmugam, A.; *et al*. The advanced health and disaster aid network: A light-weight wireless medical system for triage. *IEEE Trans. Biomed. Circuits Syst.* **2007**, *1*, 203–216.

4. Li, Z.; Yu, F.R.; Huang, M. A distributed consensus-based cooperative spectrum-sensing scheme in cognitive radios. *IEEE Trans. Veh. Technol.* **2010**, *59*, 383–393.
5. Buratti, C.; Conti, A. ; Dardari, D.; Verdone, R. An overview on wireless sensor networks technology and evolution. *Sensors* **2009**, *9*, 6869–6896.
6. Xu, K.; Hassanein, H.; Takahara, G.; Wang, Q. Relay Node Deployment Strategies in Heterogeneous Wireless Sensor Networks. *IEEE Trans. Mob. Comput.* **2009**, *9*, 145–159.
7. Cheng, X.; Du, D.; Wang, L.; Xu, B. Relay sensor placement in wireless sensor networks. *Wirel. Netw.* **2008**, *14*, 347–355.
8. Zhu, S.; Chen, C.; Guan, X. Consensus protocol for heterogeneous multi-agent systems: A Markov chain approach. *Chin. Phys. B* **2013**, *22*, 018901:1–018901:5.
9. Zhu, S.; Chen, C.; Guan, X. Distributed optimal consensus filter for target tracking in heterogeneous sensor networks. *IEEE Trans. Cybern.* **2013**, *42*, 1963–1976.
10. Khan, U.A.; Kar, S.; Moura, J.M.F. Distributed sensor localization in random environments using minimal number of anchor nodes. *IEEE Trans. Signal Process.* **2009**, *57*, 2000–2016.
11. Wei, X.; Li, C; Zhou, L; Zhao, L. Distributed Density Estimation Based on a Mixture of Factor Analyzers in a Sensor Network. *Sensors* **2015**, *15*, 19047–19068.
12. Barbarossa, S.; Scutari, G. Decentralized maximum-likelihood estimation for sensor networks composed of nonlinearly coupled dynamical systems. *IEEE Trans. Signal Process.* **2007**, *55*, 3456–3470.
13. Olfati-Saber, R.; Fax, J.A.; Murray, R.M. Consensus and cooperation in networked multi-agent systems. *IEEE Proc.* **2007**, *95*, 215–233.
14. Olfati-Saber, R. Flocking for multi-agent dynamic system: Algorithms and theory. *IEEE Trans. Autom. Control* **2006**, *51*, 401–420.
15. Mi, S.; Zhu, S.; Chen, C.; Guan, X. TWGS: A Tree Decomposition Based Indoor Pursuit-Evasion Game for Robotic Networks. In Proceedings of the 13th IFAC Symposium on Large Scale Complex Systems: Theory and Applications, Shanghai, China, 7–10 July 2013; pp. 135–140.
16. Chen, C.; Zhu, S.; Guan, X.; Shen, X. *Wireless Sensor Networks: Distributed Consensus Estimation*; Springer: Berlin, Germany, 2014.
17. Wang, Y.; Attebury, G.; Ramamurthy, B. A Survey of Security Issues In Wireless Sensor Networks. *IEEE Commun. Surv. Tutor.* **2006**, *8*, 1–23.
18. Pathan, A.K.; Lee, H.; Hong, C.S. Security in wireless sensor networks: Issues and challenges. In Proceedings of the 8th International Conference Advanced Communication Technology (ICACT'06), Phoenix Park, UK, 20–22 February 2006; pp. 1043–1048.
19. Liu, Y.; Ning, P.; Reiter, M. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur.* **2011**, *14*, 21–32.
20. Yan, Q.; Li, M.; Jiang, T.; Lou, W.; Thomas Hou, Y. Vulnerability and protection for distributed consensus-based spectrum sensing in cognitive radio networks. In Proceedings of the International Conference on Computer Communications(INFOCOM'12), Orlando, FL, USA, 25–30 March 2012; pp. 900–908.
21. Mo, Y.; Kim, T.H.-J.; Brancik, K.; Dickinson, D.; Lee, H.; Perrig, A.; Sinopoli, B. Cyberphysical security of a smart grid infrastructure. *IEEE Proc.* **2012**, *100*, 195–209.
22. Pasqualetti, F.; Bicchi, A.; Bullo, F. Consensus computation in unreliable networks: A system theoretic approach. *IEEE Trans. Autom. Control* **2012**, *57*, 90–104.
23. LeBlanc, H.J.; Zhang, H.; Koutsoukos, X.; Sundaram, S. Resilient asymptotic consensus in robust networks. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 766–781.
24. Lu, K.; Qian, Y.; Guizani, M.; Chen, H.H. A framework for a distributed key management scheme in heterogeneous wireless sensor networks. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 639–647.
25. Du, X.; Xiao, Y.; Mohsen, G.; Chen, H. An effective key management scheme for heterogeneous sensor networks. *Ad Hoc Netw.* **2007**, *5*, 24–34.
26. Kumar, P.; Mika, Y.; Gurtoy, A.; Lee, S.-G.; Lee, H.-J. An Efficient and Adaptive Mutual Authentication Framework for Heterogeneous Wireless Sensor Network-Based Applications. *Sensors* **2014**, *14*, 2723–2755.
27. Mi, S.; Han, H.; Zhu, S.; Chen, C.; Yang, B.; Guan, X. A Secure Distributed Consensus Scheme for Wireless Sensor Networks Against Data Falsification. In Proceedings of the 11th World Congress on Intelligent Controland Automation (WCICA), Shenyang, China, 29 June–4 July 2014; pp. 3025–3030.

28. Liu, S.; Zhu, H.; Li, S.; Li, X.; Chen, C.; Guan, X. An adaptive deviation-tolerant secure scheme for distributed cooperative spectrum Sensing. In Proceedings of the Global Communications Conference (GLOBECOM'12), Anaheim, CA, USA, 3–7 December 2012; pp. 603–608.
29. Horn, R.A. ; Johnson, C.R. *Matrix Analysis*; Cambridge Univercity Press: Cambridge, UK, 1985.