Proceeding of the 11th World Congress on Intelligent Control and Automation
Shenyang, China, June 29 - July 4 2014

A Secure Distributed Consensus Scheme for Wireless Sensor Networks Against Data Falsification*

Shichao Mi[1,2], Hui Han[1], Shanying Zhu[2], Cailian Chen[2], Bo Yang[2], Xinping Guan[2]
1. The State Key Laboratory of Complex Electromagnetic Environment Effects on Electronics and Information System(CEMEE), Luoyang 471003, P. R. China
2. Department of Automation, Shanghai Jiao Tong University, and Key Laboratory of System Control and Information Processing, Ministry of Education of China, Shanghai 200240, P. R. China
mishichao@sjtu.edu.cn, cemee_hanhui@163.com, shyingzhu@gmail.com,{cailianchen, bo.yang, xpguan}@sjtu.edu.cn

***Abstract*— This paper focuses on the problem of secure distributed consensus to defend covert misbehavior in wireless sensor networks (WSNs). Distributed consensus is a promising method to improve the efficiency and precision of consensus results in WSNs, but it introduces new security issues that malicious nodes may manipulate false sensing data to degrade the sensing result of the whole network. A data falsification attack, i.e., the attacker injects random values into its neighboring nodes at each time-step of consensus process, is considered. This kind of attack cannot be defended against by most of existing detection mechanisms. We present a distributed detection mechanism with adaptive local threshold to isolate the abnormal nodes. A Weighted Averaging-based Consensus Scheme (WACS) is proposed to decrease the negative impact of the attack and make the network converge to a consensus value. It is proved that convergence property can be guaranteed by the relationship between weighted average of the noise and stochastic approximation. Simulation results are presented to show the effectiveness of the proposed secure scheme.**

***Index Terms*— Security, Data falsification, Weighted averaging, Distributed detection.**

I. Introduction

Wireless sensor networks (WSNs) are mostly distributed systems which are composed of large number of sensors deployed in harsh environments. Distributed computation in WSNs is thus a well-studied field with an extensive body of literature [1]-[4]. Many distributed algorithms have been proposed to facilitate the applications such as battlefield awareness, target localization [1], distributed detection and estimation[2][3] and target tracking [4] . In these algorithms, the nodes are assumed to cooperate obeying some specific protocols. However, there are several fundamental challenges of the distributed networks [5]. For example, the quantities of interest must be calculated by using only local information through sensor measurements or communication with neighboring nodes in the network. Another important challenge is that the distributed system has many vulnerable points for failures or attacks in the process of distributed exchange of information [6]. For example, if a sensor node is suffered from false data injection by malicious neighbor, it may cause sensing inaccuracy, transmission overhead increasing, network lifetime reduction, etc. So it is very important to design secure algorithms resilient to various forms of uncertainties.

A WSN exposes its protocols and the nodes to a lot of security threats, and many security problems should be investigated. There are inside and outside attackers in the network. An outside attacker is one who may intercept other nodes' states, inject false data, perform replay attack, or camouflage other honest nodes. While an inside attacker is a compromised sensor node, who has the knowledge of the keying material in the sensor node. An inside attacker can manipulate the compromised node's sensing state or the measurement. It sometimes causes more severely negative effects. Reaching consensus resiliently in the presence of misbehaving nodes has been studied in distributed computing and communication networks [7][8]. Generally, outlier detection algorithms rely on attack detection threshold to classify honest nodes and attackers. In [7], a continuous-time variation of the Mean-Subsequence-Reduce algorithms is proposed to solve asymptotic consensus problem under the F-total malicious model. An adaptive deviation-tolerant secure scheme is proposed to mitigate the misbehavior of inside malicious nodes and be tolerant the large deviation introduced by honest nodes in [8]. Several strategies are designed to construct model-based fault detection system by the state estimate residual [9][10]. In [9], a distributed fault detection and isolation methodology is described relying on the decentralized Kalman state-estimation technique. Ref. [10] presents an intrusion detection scheme for linear consensus networks with misbehaving nodes based on unknown input observability. The scheme makes each node detect and isolate the misbehaving nodes using only the information flow adopted by standard consensus protocols, but it is constrained by the assumption that there is only one intruder among all the nodes in the consensus algorithm. Those detection algorithms may detect misbehavior nodes,

* The work was partially supported by State Key Laboratory of CEMEE under the grant CEMEE2014K0102A, by NSF of China with the grant nos. 61221003, 61273181, 61174127 and 61290322, by Doctoral Fund of Ministry of Education of China under the grant 20110073130005, and by Science and Technology Commission of Shanghai Municipal, China under the grant 13QA1401900.

978-1-4799-5825-2/14/$31.00 ©2014 IEEE

however, an attacker will make the network converge to a wrong value with a large deviation before it is detected. There emerges some research on the relationship between the topology of network and the number of faulty nodes to assure the consensus. For example, Ref. [11] provides worst-case bounds for the number of concurrent faulty or malicious nodes that can be detected and identified. It is proved in [11] that the consensus network needs to be $2k+1$ connected for k malicious nodes to be generically detectable and identifiable by every normal node. Ref. [5] demonstrates the connectivity and degree properties of robust digraphs. The robustness maintains after edge removal and it is described that how to compare the relative robustness of different digraphs. The detection algorithm above may fail when the network topology changes.

Although many algorithms have been proposed to defend the faulty or malicious nodes in the distributed network, the current detection algorithms either rely on an attack detection threshold to identify misbehavior or compute the 2-Norm of the state residual to check whether there exist bad nodes or not. Therefore, if the attackers are too covert to be detected, the current detection algorithms fail to protect the network. Ref. [12] presents attacks on information in transmission. The information may be altered, spoofed, replayed again or vanished in transmission. As wireless communication is vulnerable, any attacker can monitor the traffic flow and get into action to interrupt, intercept, modify or fabricate packets. Thus, wrong information is easily injected to the base stations or sinks. In [13], a novel form of attack called covert adaptive data injection attack is proposed according to the distributed algorithm's vulnerability. An unknown vulnerability of existing bad measurement detection algorithm is exposed by presenting and analyzing a new class of attacks, called false data injection attacks [14].

To defend against attacks which are covert and to decrease the negative effect of attacks before it is detected, we propose a secure distributed consensus scheme for WSNs in this paper. We consider data falsification attack, i.e., the attacker injects random values into its neighbors at each time-step. When the resulting error of the attack is a linear combination of the column vectors of the weight matrix, the attack cannot be detected by the existing detection mechanism [14]. To defend this kind of attack, we present a distributed detection mechanism with adaptive local threshold to detect abnormal nodes. Then we propose a Weighted Averaging-based Consensus Scheme (WACS) which aims to decrease the negative impact of the misbehaving nodes that can pass the detection mechanism and the consensus scheme can make the network converge to the average of all the nodes' initial states.

The rest paper is organized as follows. In Section II, we define the system model and present the attack model. Section III is concerned with the consensus algorithm. The simulation in Section IV validates the performance of the proposed algorithm. Finally, we conclude this paper in Section V.

II. System Model

Consider a connected WSN containing n nodes $\mathcal{I} = \{1, 2, 3, ..., n\}$. It can be described by an undirected graph $\mathcal{G} = (\mathcal{N}, \mathcal{E})$, where $\mathcal{N}$ represents the set of nodes $\mathcal{N} = \{n_i | i \in \mathcal{I}\}$ and $\mathcal{E} \in \mathcal{N} \times \mathcal{N}$ represents the set of edges. If two nodes are connected by an edge, they can exchange information with each other. The node j is a neighbor of node i if $(i, j) \in \mathcal{E}$ where $i \neq j$. Denote the neighbor set of node i by $\mathcal{N}_i = \{j | (j, i) \in \mathcal{E}\} \subset \mathcal{N}$. $|\mathcal{N}_i|$ represents the number of elements in $\mathcal{N}_i$. A path in $\mathcal{G}$ consists of a sequence of nodes $(n_1, n_2, ..., n_l)$, $l \geq 2$ satisfying $(n_m, n_{m+1}) \in \mathcal{E}$ for all $1 \leq m \leq l-1$. The graph $\mathcal{G}$ is connected if any two different nodes in $\mathcal{G}$ are connected by a path.

The Laplacian matrix of the undirected graph $\mathcal{G}$ is defined as $\mathcal{L} = (l_{ij})_{n \times n}$, where

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

Suppose that each node i has an initial value, $x_i(0)$. The goal for each node is to achieve a common value determined by the initial values by sharing information only with neighboring nodes in an iterative way. At each time step k, all nodes will update and exchange their values with their neighbors based on some strategy. The scheme of this paper can be shown by a discreted-time equation:

$$x_i(k+1) = w_{ii} x_i(k) + \sum_{j \in \mathcal{N}_i} w_{ij} x_j(k) \tag{2}$$

where the w_{ij}'s $(i \in \mathcal{N}, j \in \mathcal{N}_i)$ are a set of weights. It can be seen from (2) that each node updates its own state value to be a linear combination of its own state value and its neighbors' values. The values of all nodes at time-step k can be aggregated into the vector $\mathrm{x}(k) = [x_1(k)\ x_2(k)\ ...\ x_n(k)]^T$, and the update strategy can be denoted as

$$\mathrm{x}(k+1) = W\mathrm{x}(k) \tag{3}$$

where $k = 0, 1, 2, ...,$, and the (i, j)-th entry of W is the weight w_{ij} ($w_{ij} = 0$ if $j \notin \mathcal{N}_i$)

A. Attack Model

In this paper, we consider an inside attack named data falsification attack here. Data falsification attack may either manipulate a fake sensing data in the sensing stage or inject a forged state value at each iteration step in the data fusing stage, or the attack may happen in both the sensing stage and the data fusing stage. This attack can be very dangerous because it can cause long-term impact on the network. Only one attacker that transmits a constant value at each step can make the whole network asymptotically converge to a fabricated value [13].

In this paper, we assume that the network is not dominated by the faulty nodes and the communication link is reliable. It is also assumed that the network topology remains unchanged during the consensus process. Data falsification attacker injects random values into its neighborhood at each time-step as long as it can result in a wrong value. In the following, we show the attack model of data falsification.

Instead of applying the update equation (2), node h updates its value at each iteration as

$$x_h(k+1) = w_{hh}x_h(k) + \sum_{j\in\mathcal{N}_h} w_{hj}x_j(k) + e_h(k) \quad (4)$$

where $e_h(k)$ is an additive error at time-step k. Node h is said to be malicious or faulty if $e_h(k)$ is nonzero for at least one time step k. Then we can get the update algorithm with some malicious or faulty nodes in the network

$$\mathrm{x}(k+1) = W\mathrm{x}(k) + e(k) \quad (5)$$

The attacker can choose any nonzero vector as the attack vector. The traditional detection approach computes the 2-Norm of the estimation residual to classify honest nodes and attackers. However, as shown in [14], the malicious state can pass the detection if e is a linear combination of the column vectors of W, that is , $e = Wc$, where c is an arbitrary nonzero vector. This attack is very covert and can disrupt the consensus algorithm by converging to an arbitrary value or causing the network divergence in most cases. In this paper, we present a distributed detection mechanism with adaptive local threshold and propose a secure consensus algorithm that can make the network converge to a desired value. In this sense, the attack can be defended.

III. A Secure Scheme against Data Falsification

This section presents a distributed detection with adaptive local threshold which aims to detect the abnormal sensor nodes and a secure consensus scheme named WACS which is designed to decrease the negative impact of the misbehaving nodes.

A. Distributed Detection with Adaptive Local Threshold

The goal of this detection mechanism is to detect and eliminate the abnormal states of the nodes. According to the consensus algorithm, the maximum state of the network is decreasing, while the minimum state is increasing until reaching consensus. So the difference between the maximum and minimum states will shrink to zero. The main idea of the detection algorithm is to use localized threshold at each sensor node.

It is likely to mistakenly judge an honest node with a relatively large deviation guilty using an accurate threshold. To avoid mistaking the veracious nodes with large deviation, we enlarge the threshold and adapt the threshold with diminishing behavior of the state difference. We now detail the detection algorithm below.

Node n_i makes a measurement independently and transmits it to its neighbors at the starting time. Then at the first time-step the node calculates the threshold as follows which can allow all the nodes participate in the iteration.

$$\lambda_i(0) = \max_{j\in\mathcal{N}_i}\{x_i(0) - x_j(0)\} \quad (6)$$

At the following iteration step, in order to adapt the detection threshold according to the shrinking difference between the neighboring nodes, the estimates of the threshold value can be calculated below

$$\lambda_i(k+1) = \frac{\sum_{j\in\mathcal{N}_i} |x_j(k+1) - x_i(k+1)|}{\sum_{j\in\mathcal{N}_i} |x_j(k) - x_i(k)|}\lambda_i(k) \quad (7)$$

According to the consensus algorithm, the maximum state of the network is monotonically decreasing, while the minimum state is monotonically increasing. The difference between a node state and its neighbors states gradually diminish until reaching zero. So the threshold gradually decreases to zero. Once a node is regarded to be malicious, it will be eliminated.

The detection algorithm as well as the existing detection algorithms can detect obvious misbehaving nodes. However, if a attacker injects a positive error by the data falsification attack mentioned in Section II in each iteration step before it is detected, the whole network will converge to a wrong value with a large deviation. We design a secure consensus algorithm to solve this problem in the following.

B. Weighted Averaging-based Consensus Scheme

Data falsification attack is very hard to be detected, if $e(k) = Wc < \lambda(k)$, the detection mechanism can do nothing to defend against the attack. Moreover, this kind of attack can affect the network for a long time and cause very serious consequences. Fortunately, it is known that stochastic approximation algorithm can be applied to find true values or functions that cannot be obtained directly via noisy observations. Thus, it could be an effective method to deal with additive error. It is proved that the convergence of a stochastic approximation algorithm is equivalent to the convergence of the weighted average of the associated noise [15]. The method of weighted averaging is based on parameters' values. So we can set values of the weight of the neighbor nodes to reduce the negative impact of the malicious or faulty nodes. A secure consensus algorithm is proposed based on weighted averaging below.

We introduce some preliminaries on weighted averaging first. Let H be a real Hilbert space and let $L = H^N$ be the vector space which contains all sequences on H. The inner product on H is denoted by $\langle\cdot,\cdot\rangle$ and the corresponding norm is denoted by $||\cdot||$. Let $(x)_k$ represent the kth element of the sequence x, and $x \to P$ means that x converges to $P \in H$. The weighted averaging operator with respect to a positive

real sequence $a = \{a_k\}$ is the operator $\mathcal{A}_a : L \to L$ defined by

$$(\mathcal{A}_a x)_k = \begin{cases} a_1 x(1), & if\ k = 1 \\ (1 - a_k)(\mathcal{A}_a x)_{k-1} + a_k x(k), & otherwise \end{cases} \tag{8}$$

where $x = \{x(k)\} \in L$. If $x \in L$, we call that $\mathcal{A}_a x$ is the weighted average of x. The sequence a is defined as the averaging sequence of the corresponding weighted average. And we can see that the operator $\mathcal{A}_a$ is linear.

Lemma 1 [15]: Given a real sequence $a = \{a_k\}$ satisfying $a_1 = 1$ and $0 < a_k < 1$ for all $k \geq 2$; define real sequence $\{\beta_k\}$ and $\{\gamma_k\}$ by

$$\beta_k = \begin{cases} 1, & n = 1 \\ \prod_{m=2}^{k} \frac{1}{1-a_k}, & otherwise \end{cases} \tag{9}$$

$$\gamma_k = a_k \beta_k \tag{10}$$

Then the following conditions hold
1. $\beta_k = \sum_{m=1}^{k} \gamma_m$;
2. $(\mathcal{A}_a x)_k = (1/\beta_k) \sum_{m=1}^{k} \gamma_m x(m)$ for any $x = \{x(k)\} \in L$.

Suppose that x is a sequence of estimates of an unknown parameter x^*, after the application of the weighted averaging to the sequence, we can get that if x does not converge to x^* but sufficiently well-behaved, then a weighted average of x may converge to x^*.

And it is shown that the stochastic approximation algorithm can be represented by a weighted average of the noise sequence when it converges. We consider the problem of recursively estimating the zero of an unknown linear function $Ax - b$, $A : H \to H$ and $b \in H$, via the following stochastic approximation algorithm:

$$x(k+1) = x(k) - a_k A_k x(k) + a_k b(k) + a_k e(k) \tag{11}$$

where $x_1 \in H$ can be arbitrary; A_k and b_k are estimates of A and b, respectively; and $e(k)$ represents the noise sequence. The step size $\{a_k\}$ is a sequence of nonnegative real number, and $a_1 = 1$, $a_k < 1$ for $k \geq 2$, $a_k \to 0$ and $\sum_{k=1}^{\infty} a_k = \infty$. We assume that A_k and b_k satisfy the following assumptions:
(i). A is a bounded linear operator with $\inf\{Re\lambda : \lambda \in \sigma(A)\} > 0$, where $\sigma(A)$ represents the spectrum of A.
(ii). $\limsup_{k\to\infty}(1/\beta_k) \sum_{m=1}^{k} \gamma_m ||A_m|| < \infty$.
(iii). $||(1/\beta_k) \sum_{m=1}^{k} \gamma_m A_m - A|| \to 0$.

The above distributed detection mechanism can detect abnormal node states, but if the attack inject a positive error into the network at every iteration step, and the additive error is a linear combination of the weighted vector $e = Wc < \lambda(k)$, the whole network will converge to a wrong value with a large deviation with the standard consensus method [16].

$$x(k+1) = x(k) - \epsilon \mathcal{L} x(k) \tag{12}$$

where $0 < \epsilon < (\max_i |\mathcal{N}_i|)^{-1}$.

To decrease the effect of the attacker, we propose a weighted averaging-based consensus scheme (WACS). The algorithm can make the network converge to a desired value in presence of the misbehaving nodes. We elaborate the consensus scheme as follows.

First, similarly to ordinary distributed consensus algorithm, each node makes a state independently and transmits it to its neighbors. Second, after the detection algorithm, at each time-step k in the data fusion phase, each node obtains the states of its neighbors and updates its state using both of its neighbors' states and its own state by the algorithm as follows.

$$x_i(k+1) = x_i(k) + \epsilon(k) \sum_{j \in \mathcal{N}_i} (x_j(k) - x_i(k) + e_j(k)) \tag{13}$$

$$x(k+1) = x(k) - \epsilon(k)(\mathcal{L} x(k) - e(k)) \tag{14}$$

where $x_j(k)$ denotes the true value that node j computed in the update phase, $e_j(k)$ represents the additive error of node j. e may be a linear combination of the column vectors of $\mathcal{I} - \epsilon(k)\mathcal{L}$. If j is not a misbehaving node, $e_j(k) = 0$. $\epsilon(k)$ is an update parameter satisfying $\epsilon(1) = 1$, $\epsilon(k) < 1$ for $k \geq 2$, $\epsilon(k) \to 0$ and $\sum_{k=1}^{\infty} \epsilon(k) = \infty$. Because $\epsilon(k)$ is changeable at every time-step, so the weight of the neighbor nodes is adjustable. So the effect of errors can be decreased if $\epsilon(k)$ is chosen properly. The convergence can be assured by adjusting $\epsilon(k)$. Now we prove the convergence of WACS.

According to Theorem 1, if the parameters of the secure consensus algorithm satisfy the Assumptions (i)-(iii), we can get the convergence of the weighted average of x(k) despite the existence of misbehaving nodes. It will be shown in the following theorem.

Theorem 1: x(k) converges to $(1/n)\sum_i x_i(0)$ if and only if $\mathcal{A}_a e$ converges to 0.

Proof: According to the attack model, we can represent the update algorithm (14) as

$$\mathrm{x}(k+1) = \mathrm{x}(k) - \epsilon(k)\mathcal{L}\mathrm{x}(k) + \epsilon(k)e(k) \tag{15}$$

which can be rewritten as

$$\mathrm{x}(k+1) = \mathrm{x}(k) - \epsilon(k)\mathcal{I}\mathrm{x}(k) + \epsilon(k)(\mathcal{I} - \mathcal{L})\mathrm{x}(k) + \epsilon(k)e(k) \tag{16}$$

where $\mathcal{I}_{n\times n}$ is a identity matrix. We have the following assertions:
(1). $\sigma(\mathcal{I}) = 1$, then $\inf\{Re\lambda : \lambda \in \sigma(\mathcal{I})\} > 0$.
(2). $||\mathcal{I}_{n\times n}|| = 1$, then

$$\begin{aligned} & \limsup_{k\to\infty}(1/\beta_k) \sum_{m=1}^{k} \gamma_m ||\mathcal{I}|| \\ = & \limsup_{k\to\infty}(1/\beta_k) \sum_{m=1}^{k} \gamma_m \times 1 \end{aligned}$$

$$= \limsup_{k\to\infty}(1/\sum_{m=1}^{k}\gamma_m)\sum_{m=1}^{k}\gamma_m$$
$$= 1 < \infty \tag{17}$$

(3).

$$||(1/\beta_k)\sum_{m=1}^{k}\gamma_m\mathcal{I}-\mathcal{I}||$$
$$= ||(1/\sum_{m=1}^{k}\gamma_k)\sum_{m=1}^{k}\gamma_m\mathcal{I}-\mathcal{I}||$$
$$= 0 \tag{18}$$

So the Assumptions (i)-(iii) are satisfied. Now we only need to prove that $\mathcal{A}_a e$ converges to 0.

According to the detection mechanism with adaptive local threshold, the threshold gradually converges to zero. To avoid being detected by the detection mechanism, the attack will diminish its additive error to adapt to the detection mechanism until to zero. So we can get that e converges to 0, and $\mathcal{A}_a e$ converges to 0. So $\mathrm{x}(k)$ converges to $(\mathcal{I}-\mathcal{L})\mathrm{x}(k)$ [15]. According to (15), we can get that

$$\mathbf{1}^T\mathrm{x}(k) = \mathbf{1}^T x(k-1) - \mathbf{1}^T\epsilon(k-1)\mathcal{L}\mathrm{x}(k-1) + \mathbf{1}^T\epsilon(k-1)e(k-1) \tag{19}$$

We all know that $\mathcal{L}\mathrm{x}(k)$ equals to zero, because zero is a eigenvalue of $\mathcal{L}$ and $\mathbf{1}$ is the corresponding eigenvector. So

$$\begin{aligned}&\mathbf{1}^T\mathrm{x}(k)\\ =\ &\mathbf{1}^T x(k-1) + \mathbf{1}^T\epsilon(k-1)e(k-1)\\ =\ &\cdots\\ =\ &\mathbf{1}^T x(0) + \mathbf{1}^T(\epsilon(0)e(0) + \epsilon(1)e(1)\\ &+\cdots+\epsilon(k-1)e(k-1))\end{aligned} \tag{20}$$

Because $\mathcal{A}_a e$ converges to 0, $\epsilon(0)e(0)+\epsilon(1)e(1)+\cdots+\epsilon(k-1)e(k-1)$ converges to zero. According to the consensus algorithm each node converges to a constant denoted by P, $x_i(k) = P$.

$$\mathbf{1}^T\mathrm{x}(k) = \mathbf{1}^T\mathrm{x}(0) \tag{21}$$

We can get that

$$nP = \mathbf{1}^T\mathrm{x}(0) \tag{22}$$

$$P = \frac{1}{n}\mathbf{1}^T\mathrm{x}(0) \tag{23}$$

So $\mathrm{x}(k)$ converges to $(1/n)\sum_i x_i(0)$. This proof is completed. ■

IV. Simulation Results

In this section, we present a numerical example to validate the performance of our algorithm by comparing with standard consensus algorithm. We consider the network is attacked by data falsification which is described in Section II, and then perform the normal distributed consensus algorithm and our secure scheme to the network after the distributed detection mechanism. We consider a sensor network shown in Fig.1 where 10 nodes are doing distributed estimating, in which the node set is $\mathcal{N} = \{1, 2, ...10\}$, and node $i \in \mathcal{N}$ has initial value $x_i(0)$. $\mathrm{x}(0) = [3\ 5\ 9\ 7\ 13\ 8\ 7\ 4\ 6\ 8]^T$. An attacker injects random false data into its neighborhood at each step-time. For simplicity, we choose the factor $\epsilon(1) = 1$,$\epsilon(k) = (1/k), k \geq 2$. We set the error vector, $e = (\mathcal{I} - \epsilon(k)\mathcal{L})c \times \lambda(k)$, $c = [2\ 1\ 3\ 1\ 0\ 1\ 0.5\ 2\ 0.3\ 1]$, $e_i = 0$ if $i \neq 6$, and we can know that $e < \lambda(k)$. So the faulty node cannot be detected. The network will converge to 7 if there is no attacker.

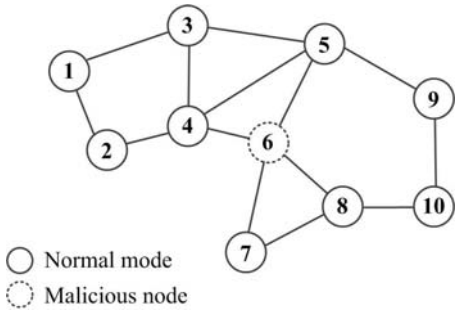

Fig. 1. A network with one attacker and 9 normal nodes.

First, we use a standard distributed consensus algorithm, we can get the simulation results in Fig.2. The result shows that the consensus reach a common value but the attacker drives the network to a wrong value, and the deviation is relatively large.

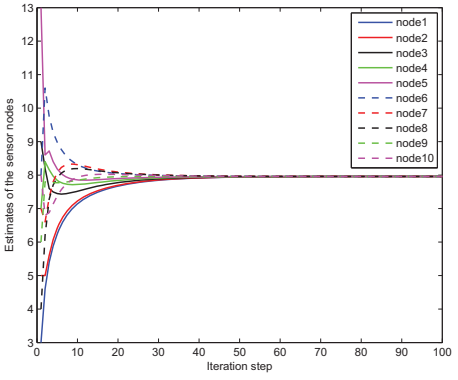

Fig. 2. The standard consensus scheme on the network.

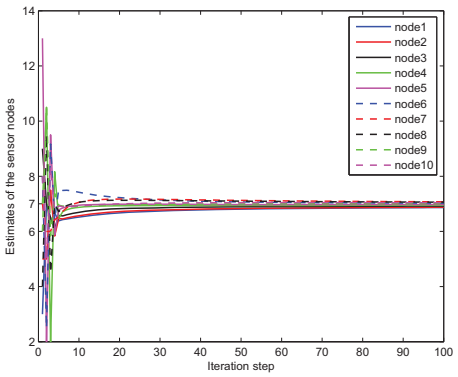

Fig. 3. A secure scheme with weighted averaging on the network.

Then we use WASC in the same circumstance. As shown in Fig.3, we can see that all the nodes' estimates converge to a common value, which is the average of the initial state, and even the attacker's state estimate converge to the value too. We can conclude that WACS has a quite well resistance against the data falsification attack.

Comparing the performance of the traditional consensus algorithm with WACS by the mean square error (MSE) and standard deviation (SD), we can see that the MSE and SD of WACS are not stable in the beginning iteration steps and gradually decreases in the following iteration steps. While the MSE and SD of the standard scheme are much larger. So WACS can make the consensus reach a more desired value. Because the additional error is a vector, if there are more than one attackers in the network, the secure scheme also works well.

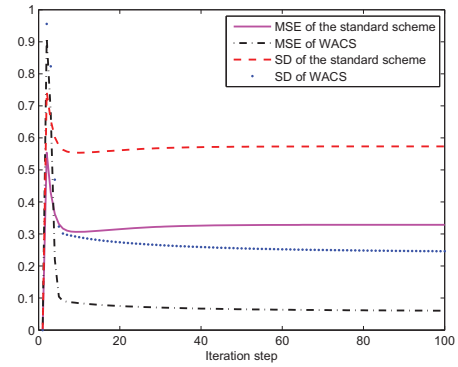

Fig. 4. Comparison of the MSE and SD for the standard and proposed scheme.

V. Conclusion and Future Work

In this paper, we study the problem of protection of the distributed consensus estimation in wireless sensor networks. We define the network as a network on an undirected graph, and then we present attacks that can disrupt the consensus algorithm or stealthily subvert the sensing results. A distributed detection mechanism with adaptive local threshold is presented, WACS is proposed to decrease the negative impact of the misbehaving nodes that can pass the detection mechanism. Simulation results illustrate the effectiveness of the proposed secure scheme.

References

[1] U. A. Khan, S. Kar and J. M. F. Moura, Distributed sensor localization in random environments using minimal number of anchor nodes, *IEEE Transactions on Signal Processing*, vol. 57, no. 5, pp. 2000-2016, 2009.

[2] S. Zhu, C. Chen and X. Guan, Consensus protocol for heterogeneous multi-agent systems: A Markov chain approach, *Chinese Physics B*, vol. 22, no. 1, pp. 018901-1-5, 2013.

[3] S. Zhu, C. Chen and X. Guan, Sensor deployment for distributed estimation in heterogeneous wireless sensor networks, *Ad Hoc & Sensor Wireless Networks*, vol. 16, no. 4, pp. 297-322, 2012.

[4] S. Zhu, C. Chen and X. Guan, Distributed optimal consensus filter for target tracking in heterogeneous sensor networks, *IEEE Transactions on Cybernetics*, vol. 43, no. 6, pp. 1963-1976, 2013.

[5] H. J. LeBlanc, H. Zhang, X. Koutsoukos and S. Sundaram, Resilient asymptotic consensus in robust networks, *IEEE Journal on Selected Areas in Communication*, vol. 31, no. 4, pp. 766-781, 2013.

[6] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, et al., Cyberphysical security of a smart grid infrastructure, *Proceedings of The IEEE*, vol. 100, no. 1, pp. 195-209, 2012.

[7] H. J. LeBlanc, X. Koutsoukos, Consensus in networked multi-agent systems with adversaries, in *Proceedings of the 14th International conference on Hybrid Systems: Computation and Control (HSCC'11)*, Chicago, USA, Apr. 12-14, 2011, pp. 281-290.

[8] S. Liu, H. Zhu, S. Li, X. Li, C. Chen, X. Guan, An adaptive deviation-tolerant secure scheme for distributed cooperative spectrum Sensing, in *Global Communications Conference (GLOBECOM'12)*, Anaheim, USA, Dec. 3-7, 2012, pp. 603-608.

[9] E. Franco, R. Olfati-Saber, T. Parisini and M. M. Polycarpou, Distributed fault diagnosis using sensor networks and consensus-based filters, in *45th IEEE Conference on Decision and Control*, San Diego, USA, Dec. 13-15, 2006, pp. 386-391.

[10] F. Pasqualetti, A. Bicchi, F. Bullo, Distributed intrusion detection for secure consensus computations, in *46th IEEE Conference on Decision and Control*, New Orleans, USA, Dec. 12-14, 2007, pp. 5594-5599.

[11] F. Pasqualetti, A. Bicchi, and F. Bullo, Consensus Computation in Unreliable Networks: A System Theoretic Approach, *IEEE Transactions on Automatic Control*, vol. 56, no. 12, pp. 90-104, 2012.

[12] A. K. Pathan, H. Lee, C. S. Hong, Security in wireless sensor networks: issues and challenges, in *the 8th International Conference Advanced Communication Technology (ICACT '06)*, Phoenix Park, UK, Feb. 20-22, 2006, pp. 1043-1048.

[13] Q. Yan, M. Li, T. Jiang, W. Lou, Y. Thomas Hou, Vulnerability and protection for distributed consensus-based spectrum sensing in cognitive radio networks, in *International Conference on Computer Communications(INFOCOM'12)*, Orlando, USA, Mar. 25-30, 2012, pp. 900-908.

[14] Y. Liu, P. Ning, M. Reiter, False data injection attacks against state estimation in electric power grids, *ACM Transactions on Information and System Security*, vol.14, no.1, pp. 21-32, 2011.

[15] I-J. Wang, Edwin K. P. Chong, Sanjeev R. Kulkarni, Weighted averaging and stochastic approximation, *Mathematics of Control, Signals and Systems*, vol. 10, no. 1, pp. 41-60, 1997.

[16] R. Olfati-Saber, J. A. Fax, and R. M. Murray, Consensus and cooperation in networked multi-agent system, *Proceedings of The IEEE*. vol. 95, no. 1, pp. 215-233, 2007.