sensors

MDPI

Article

Access Control Model Based on Time Synchronization Trust in Wireless Sensor Networks

Zhaobin Liu [1,*], Qiang Ma [2], Wenzhi Liu [1], Victor S. Sheng [3], Liang Zhang [1] and Gang Liu [1]

[1] School of Computer Engineering, Suzhou Vocational University, Suzhou 215104, China; lwzsz@126.com (W.L.); rainbow_zhli@163.com (L.Z.); liugang@jssvc.edu.cn (G.L.)

[2] School of Software, Tsinghua University, Beijing 100084, China; maq@greenorbs.com

[3] Department of Computer Science, University of Central Arkansas, Conway, AR 72035, USA; ssheng@uca.edu

* Correspondence: zbliusz@126.com; Tel.: +86-155-0615-5880

Received: 19 May 2018; Accepted: 27 June 2018; Published: 30 June 2018

Abstract: Internal reliability and external safety of Wireless Sensor Networks (WSN) data transmission have become increasingly outstanding issues with the wide applications of WSN. This paper proposes a new method for access control and mitigation of interfering noise in time synchronization environments. First, a formal definition is given regarding the impact interference noise has on the clock skew and clock offset of each node. The degree of node interference behavior is estimated dynamically from the perspective of time-stamp changes caused by the interference noise. Secondly, a general access control model is proposed to resist invasion of noise interference. A prediction model is constructed using the Bayesian method for calculating the reliability of neighbor node behavior in the proposed model. Interference noise, which attacks the time synchronization, is regarded as the key factor for probability estimation of the reliability. The result of the calculations determines whether it is necessary to initiate synchronization filtering. Finally, a division of trust levels with bilinear definition is employed to lower interference noise and improve the quality of interference detection. Experimental results show that this model has advantages in system overhead, energy consumption and testing errors, compared to its counterparts. When the disturbance intensity of a WSN increases, the proposed optimized algorithm converges faster with a lower network communication load.

Keywords: access control; time synchronization; wireless sensor networks; interference noise; reliability

1. Introduction

Internal reliability of WSN data transmission refers to random packet losses or error packets in a wireless link caused by topological changes, dynamic links, human disturbance or packet collisions [1,2], resulting in a failure to ensure the reliability and efficiency of data transmission. External safety means some safety threats like latent invasions and attacks, including safety threats and attacks caused by passive wiretapping, data tampering and retransmission, falsification of identity, denial of service, node capture and so on, which might affect the integrity, confidentiality, authentication and serviceability of data. Therefore, it is necessary to implement access control that can protect the network from outside interference. On the other hand, time synchronization is the precondition to realize network functions like cooperative awareness, communication, energy and access control management of nodes. For instance, the algorithms like malicious nodes perceiving, topology discovery and target tracing need nodes to mark time stamp on the awareness events and information data.

The fusion of time synchronization and accurate access control remains a challenging job due to some new characteristics of WSN such as large-scale remote deployment, application of low cost hardware facilities and limit on network energy supply. There are mainly three factors that interaction between time synchronization precision and access control.

First, clock drift exists in the current hardware clock, the frequency is easy to be affected by environment and interference noise (This includes internal and external interference) [3].

Second, synchronization method based on the reduction of the interference noise relies on access control to exchange the synchronization information, uncertain delay may occur in the process of sending and receipt information of access control.

Third, the access control is one of the key artifices which affect the accuracy of time synchronization. The timestamp change caused by interference noise selects different control strategies for the node resource access behavior.

Regarding internal reliability issue, Internal interference usually sends error time information to other nodes through compromised nodes to interfere with time synchronization, such as Delay Attack. A dynamic trust model based on multiple factors was proposed [4–7]. The model improves the reliability degree between WSN nodes and ensures the safety of node data transmission through a multi-angle reliability model which combines communication, data and energy. A hybrid trust computation scheme also was proposed, which first obtains a single trust value in a whole group [8] then, within each group, all sensor nodes calculate individual trust values for all group members and group heads aggregate these trust values and forward them to a base station. Following that, the base station periodically multicasts the current state of each group to all group heads. The information encryption access technology can guarantee the integrity and confidentiality of the information packet and can effectively resist external attacks but it cannot guarantee time accuracy [9]. The Fault Tolerant Time Synchronization Protocol (FTTSP) judges and detects the internal noise of the node based on the difference between the estimated value of the transmission time and the actual value by with fault-tolerance mechanism [10]. However, the above method does not correct the time rate, the synchronization accuracy is low, the synchronization error increases rapidly and there is no abnormality in the detection time rate and the abnormality of the time rate will affect the node time running, which will increase the time error between the nodes and eventually lead to time synchronization failure.

Regarding external safety issue, External interference usually causes time synchronization failures by tampering with the communication process between two trusted nodes, such as Masquerade Attack. The Accountable and Privacy-Enhanced Access Control in Wireless Sensor Networks (APAC) solution based on group signature provides protection privacy for access control in wireless sensor networks [11]. This solution divides users in a network into groups and users in different groups are given different access authorities. This limits the query behaviors of users. Query commands of users can only pass the verification of the node when they are set according to the access authority of the group to which they belong. Han [12] analyzed various applications of the reliability model and categorized the reliability models to defend against hostile attacks.

The reliability relationships between nodes are dynamic and uncertain in a complex WSN [13–15] however, which do not remain the same as the relationships that are recognized when the network is established [16]. Some entities which are reliable before might become unreliable for certain reasons as time passes. The hostile behaviors of unreliable entities might threaten the normal operations of a system if changes are ignored. Additionally, due to the importance of time synchronization in WSN data transmission, time synchronization access control has become a general approach to test whether a WSN experienced a hostile attack. In addition, the above model only allows one node to transmit a single data packet in one cycle. This results in a longer end-to-end transmission delay of the data packet. As the load increases, the data packet is likely to be accumulated in the node backlog. Node buffer overflows severely affect the performance of the network.

Currently, a Bayesian method is used to study WSN access control through defining time synchronization states of nodes and the spatial correlation between time synchronizations of different nodes [17]. A clustering algorithm was proposed for tracking targets [18]. A heterogeneous event access control method was proposed based on considering the heterogeneity in the access control of WSN [19]. Meanwhile, sensor node information also has a property of time correlation, which is used to conduct relevant research on realizing access control through taking advantage of characteristics of time and spatial information of nodes [20]. Among time synchronization correlations, different distances between nodes might have a different impact on the time synchronization. Normalized treatments on the distances between nodes are conducted to quantify the impact of distances, which further optimizes the algorithm of access control [21]. Affected by the topological location of nodes, perception similarity and time synchronization information reliability of different nodes might vary.

Taking the time correlation of WSN nodes and the shortage of WSN resources into consideration, adopting the principle of light weight, this paper puts forward a method to estimate the reliability degree between nodes based on a time synchronization access control model through analyzing the feasibility degree of disturbance noise and the time synchronization of nodes.

2. Clock Model

Given a topological structured undirected graph $G = (V, E)$, where $V = \{1, 2, \ldots, n\}$ are the nodes in the network G, and E are the communication links of all nodes, a neighbor set of node i can be defined as $N_i = \{j | (i, j) \in E, \forall j \in V\}$. Regarding node $i \in V$, $\deg(i) = |N_i|$, is the degree of node i. Hardware clock function [22,23] of each node is defined as follows:

$$H_i(t) = \alpha_i t + \beta_i,\ i \in V \tag{1}$$

where α_i is the hardware clock skew, representing clock speed and β_i is the hardware clock offset [24], $\forall i \neq j,\ \alpha_i \neq \alpha_j, \beta_i \neq \beta_j$. According to Formula (1), the relative logic clock relation equation of node i and j is defined as follows:

When there is no interference noise, the relation equation is defined as follows:

$$H_i(t) = a_{ij} H_i(t) + b_{ij} = a_{ij}\alpha_i t + a_{ij}\beta_i + b_{ij} \tag{2}$$

When there is interference noise, the relation equation is defined as follows:

$$H_i^+(t) = a_{ij} H_i(t) + b_{ij} + Q_i t = a_{ij}\alpha_i t + a_{ij}\beta_i + b_{ij} + Q_i t = \widetilde{x}_i t + \widetilde{y}_i + Q_i t \tag{3}$$

where $\widetilde{x}_i = a_{ij}\alpha_i$, $\widetilde{y}_i = a_{ij}\beta_i + b_{ij}$ and a_{ij} and b_{ij} respectively represent the relative clock skew and the relative clock offset of node i and j [25]; $\widetilde{x}_i$ and $\widetilde{y}_i$ represent the clock skew and offset of node i and j caused by internal disturbance noise, such as mutual communication delay [26], measurement deviation, clock vibration and internal covert attacks [27,28]. $Q_i(t) \in [\psi_1, \psi_2]$ defines external disturbance noise for node i from its neighbor nodes. It is a random delay from an external attack. $\left|H_i^+(t) - H_i(t)\right|$ is used to determine whether the node has received external interference and, if $\left|H_i^+(t) - H_i(t)\right| > 0$, it means this node is delayed or if $\left|H_i^+(t) - H_i(t)\right| \notin [\psi_1, \psi_2]$, this synchronization information is not trusted. When node i receives internal hidden interference, its current time $H_i^+(t)$ is not affected. However, $\widetilde{x}_i$ and $\widetilde{y}_i$ have deviated, for $\widetilde{x}_i^+ = \widetilde{x}_i + \xi, \widetilde{y}_i^+ = \widetilde{y}_i + \zeta$, the $\Delta\widetilde{x}_i = \left|\widetilde{x}_i^+ - \widetilde{x}_i\right|$ and $\Delta\widetilde{y}_i = \left|\widetilde{y}_i^+ - \widetilde{y}_i\right|$ are used as criteria to check whether the clock skew and offset of the node is normal. When $\left|\widetilde{x}_i^+ - \widetilde{x}_i\right| > 0$ and $\left|\widetilde{y}_i^+ - \widetilde{y}_i\right| > 0$, it means that time synchronization of this node is disturbed by the internal hidden interference and the synchronization information is not trusted.

3. Noise Detection

Assumption 1: Given a constant $\delta > 0$, if there exits an ε $(0 < \varepsilon \leq 1)$, for any $i \in V$, one can have:

$$P\{Q_i(t) \in [\psi - \delta, \psi + \delta] \forall \psi \in [\psi_1, \psi_2]\} \geq \varepsilon \tag{4}$$

Generally, disturbance noise is a random variation which obeys specific distribution, such as Gaussian distribution and index distribution [29], or distributions which have a fixed mean value and variance [30] for example. High accuracy and full-time synchronization can be realized in the sense of expectation for the above specific situation. However, the noise mode of disturbance noise might have different distributions in different times and have no fixed mean value or variance, which results in failure for an existing algorithm to realize synchronization. Moreover, the hostile behavior received by node i from its neighbor node might threaten the normal operation of a system [31].

Assumption 2: The domain of a random algorithm is $M \in \Theta$, which meets different interference $(\widetilde{x}_i, \xi)$ and $(\widetilde{y}_i, \zeta)$ for $A \subseteq Range(M)$ and all the data packets $C, C' \in \Theta$, with $\|C - C'\| \leq 1$:

$$P\{M(j) \in A\} \leq exp(\widetilde{x}_i + \widetilde{y}_i) \cdot P\{M(i) \in A\} + max(\xi, \zeta) \tag{5}$$

where M is an algorithm for time synchronization and access control, $\|C - C'\|_1$ is l_1 norm distance. When $\xi = 0 \wedge \zeta = 0$ is set up, M meets the difference interference of $(\widetilde{x}_i, \xi)$ and $(\widetilde{y}_i, \zeta)$ under the condition of $Q_i(t) \in [\psi_1, \psi_2]$, in which only one element's difference is between data packet C and C'. The authors refer to the two data packets whose difference is one element at most to the neighbor data packet. This can also be regarded as the disturbance protection level offered by the proposed algorithm. The smaller the parameter $(\widetilde{x}_i + \widetilde{y}_i)$, the higher the protection level is. When the parameter is zero, it can be regarded that the time synchronization algorithm has the same distribution on the two data packets with a single data difference for any input to query the output results. These results cannot reflect any useful information on the data packet. The larger the value of $(\widetilde{x}_i + \widetilde{y}_i)$, the more noise might be needed. This might lower the utility of data. Thus, the value needs to reach a certain balance between the disturbance protection level and the data utility.

When nodes are attacked by interference noise, the $\widetilde{x}_i$ and $\widetilde{y}_i$ values are unknown but according to the exchange of information between the nodes, one can get the estimated value of this moment, though this value can be out of the state at this moment.

The node i is taken as a reference node and the node j is a node to be synchronized. It needs to synchronize with the node i, shown in Figure 1. Assuming time synchronization information exchange happens N times, in the k^{st} information exchange, node i sends synchronization information of $t_{1,k}$ at the time of $t_{1,k}$ to node j, node j receives time synchronization information $[\widetilde{x}_i(t_{1,k})\ \widetilde{y}_i(t_{1,k})]^{t_{1,k}}$ at $t_{2,k}$ moment and responds with the time synchronization information data packet to node i at $t_{3,k}$ moment which includes $[\widetilde{x}_j(t_{2,k})\ \widetilde{y}_j(t_{2,k})]^{t_{2,k}}$ and $[\widetilde{x}_j(t_{3,k})\ \widetilde{y}_j(t_{3,k})]^{t_{3,k}}$ and, finally, node i receives the data packet at $t_{4,k}$ moment. Here $t_{1,k}$ and $t_{4,k}$ are the local time of node i, while $t_{2,k}$ and $t_{3,k}$ are the local time of node j. Following N rounds of exchanges completed, node i acquires a series of time synchronization information data packets $\left\{[\widetilde{x}_i(t_{1,k})\ \widetilde{y}_i(t_{1,k})]^{t_{1,k}}, [\widetilde{x}_j(t_{2,k})\ \widetilde{y}_j(t_{2,k})]^{t_{2,k}}, [\widetilde{x}_j(t_{3,k})\ \widetilde{y}_j(t_{3,k})]^{t_{3,k}}, [\widetilde{x}_i(t_{4,k})\ \widetilde{y}_i(t_{4,k})]^{t_{4,k}}\right\}_{k=1}^{N}$ with a time stamp $\{t_{1,k}, t_{2,k}, t_{3,k}, t_{4,k}\}_{k=1}^{N}$ caused by disturbance noise. A math model of the above process can be described mathematically as follows:

$$t_{2,k} = \widetilde{x}_i(t_{1,k} + \upsilon + \chi) + \widetilde{y}_i \tag{6}$$

$$t_{3,k} = \widetilde{x}_i(t_{4,k} - \upsilon - \chi) + \widetilde{y}_i \tag{7}$$

where mathematical symbol υ represents fixed delay of a node information exchange [32] and it can be considered that it is known during the synchronization period. χ represents the random delay of the mutual transmission between node i and node j, where χ obeys the Gaussian distribution of

Assumption 1 [33]. Thus, there are only two unknown numbers $\widetilde{x}_i$ and $\widetilde{y}_i$ in Formulas (6) and (7), which can be transformed as follows:

$$\begin{cases} \frac{t_{2,k}}{t_{1,k}+v+\chi} = \widetilde{x}_i + \frac{\widetilde{y}_i}{t_{1,k}+v+\chi} \\ \frac{t_{3,k}}{t_{4,k}-v-\chi} = \widetilde{x}_i + \frac{\widetilde{y}_i}{t_{4,k}-v-\chi} \end{cases} \tag{8}$$

One can further change the above formula into matrices as follows:

$$\begin{bmatrix} \frac{t_{2,k}}{t_{1,k}+v+\chi} \\ \frac{t_{3,k}}{t_{4,k}-v-\chi} \end{bmatrix} = \begin{bmatrix} 1 & \frac{1}{t_{1,k}+v+\chi} \\ 1 & \frac{1}{t_{4,k}-v-\chi} \end{bmatrix} \begin{bmatrix} \widetilde{x}_i \\ \widetilde{y}_i \end{bmatrix} \tag{9}$$

The established state equation of time synchronization is referred to as the state of the k^{st} moment and the state measurement value of the moment can be acquired through information exchanges between two nodes. Therefore, one can estimate the state of the system by a certain method and adjust the logical clock of node i to reach a synchronization between node i and j. However, this synchronization system is not stable due to the poor anti-interference ability and easy noise disruption.

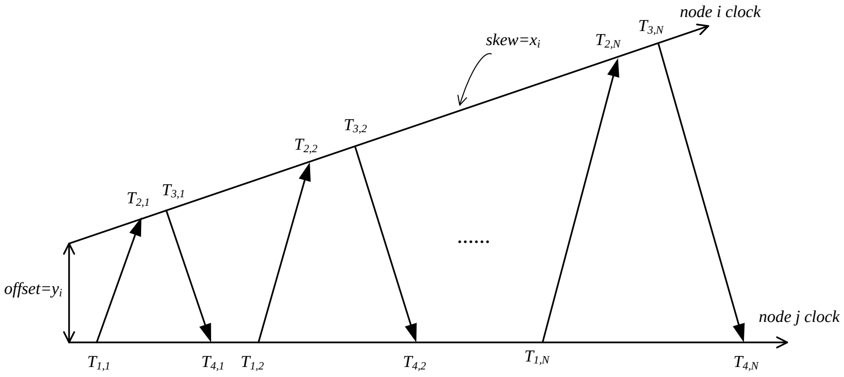


Figure 1. Two-way synchronous information exchange between two nodes.

The estimation of $Q_i(t)$ can be obtained by the Least Square Estimate [34], namely:

$$\hat{H}_i(t) = \hat{a}H_i(t) + \hat{b} \tag{10}$$

where k is the synchronization time:

$$\begin{cases} \hat{a} = \frac{(k-1)\sum_{m=1}^{k-1}\left[H_i(t_m)H_j(t_m)\right]-\sum_{m=1}^{k-1}H_i(t_m)\sum_{m=1}^{k-1}H_j(t_m)}{(k-1)\sum_{m=1}^{k-1}(H_i(t_m))^2-\left(\sum_{m=1}^{k-1}H_i(t_m)\right)^2} \\ \hat{b} = \frac{\sum_{m=1}^{k-1}H_j(t_m)}{k-1} - \hat{a}\frac{\sum_{m=1}^{k-1}H_i(t_m)}{k-1} \end{cases} \tag{11}$$

Let $\Delta H_i(t) = \left|H_i^+(t) - \hat{H}_i(t)\right|$ be established and draw $\Delta H_i(t) \approx Q_i(t)$. Only if $Q_i(t) \in [\psi_1, \psi_2]$ and $\widetilde{x}_i < \xi \wedge \widetilde{y}_i < \zeta$, is this synchronization information valid, otherwise it is discarded. When interference synchronization information of this node is continuously received, this node is deleted from the neighbor list and an alarm is issued. Only if $Q_i(t)$, can $\widetilde{x}_i$ and $\widetilde{y}_i$ be used as access control objects at the same time to avoid missed detection. Thus, it is necessary to find a solution for the above issues, which is why access control is needed to be introduced to the above-mentioned time synchronization model to reduce the impact from disturbance noise and to improve the reliability and the safety of data transmission through a certain control model to be described in the following section.

4. Access Control Model Based on Time Synchronization Trust

4.1. Time Synchronization Trust Relationship

Regarding the access control of sensor networks, time synchronization association refers to the perception information of node i which is, to some extent, associated to its neighbor nodes. The nearer the distance, the stronger the association and the more similar are the observed data. Therefore, it is very important whether the disturbance event test of the neighbor node is accurate. The association of sampling data between node i and its neighbor node $N_i = \{j|(i,j) \in E, \forall j \in V\}$ can be reflected by $\widetilde{x}_i$ and $\widetilde{y}_i$ parameters. The larger the parameter values, the more noise is in the disturbance event test of node i, caused by sampling data of the neighbor node and vice versa.

Based on the above thought, the safety and reliability of network node access can be improved by taking advantage of the feasibility of neighbor nodes, regarding $\widetilde{x}_i$ and $\widetilde{y}_i$ as a reliable approach to measure the environment of neighbor nodes. Concerning node i, the confidence weight value R_j of the perception information for the decision of neighbor node $N_i = \{j|(i,j) \in E, \forall j \in V\}$ is defined as follows [35]:

$$R_j = \frac{1/\left(\widetilde{x}_j + \widetilde{y}_j\right)}{\sum_{j \in N_i}^{deg(i)} 1/\left(\widetilde{x}_j + \widetilde{y}_j\right)} \tag{12}$$

where the weighted summation of all neighbor nodes is 1. The confidence weight value of node i for neighbor node N_i is synthesized as:

$$\Delta_{ij} = \sum_{j \in N_i}^{deg(i)} \left(e^{Q_j(t)} R_j\right) \tag{13}$$

which ensures the validity of access control under bounded noisy clock synchronization. During the process of the event test under the node access control, the confidence degree of a node is not only from reliable perception information of itself but, also, from judgement of the perception information for the external safety of its neighbor node. The subjective judgement whether Δ_{ij} of the node could offer accurate perception information for other nodes is largely subject to the final judgement whether there are events happening in all the neighbor nodes. When $t \to \infty$, it can realize the disturbance event test and efficiently eliminate the effects from bad nodes.

4.2. Access Control Model

Improve the subjective probability model by utilizing Assumption 2—the conditional probability by which node i is judged to be in convergence according to perception information of the neighbor nodes.

$$P\left\{\lim_{k \to \infty} \left(\widetilde{x}_i(k) - \widetilde{x}_j(k)\right) = 0\right\} = 1,\ P\left\{\lim_{k \to \infty} \left(\widetilde{y}_i(k) - \widetilde{y}_j(k)\right) = 0\right\} = 1 \tag{14}$$

This is also the node error tolerant model of access control. k is the iteration cycle of node i. Combined with formula (14), on the basis of the error tolerant model of node perception reliability based on time synchronization, suppose the node error rate is ϑ, the number of neighbor nodes with no disturbance events is γ, the probability of nodes in which disturbance events might occur is $\varsigma = (|N_i - \gamma|)/N_i$. The data of γ nodes in the neighbor node is w, which is consistent with node i. The subjective reliability probability of node i for its neighbor node $j \in N_i$ can be acquired through a Bayesian method [36]:

$$P_i(k) = P_i\{\Delta\widetilde{x}_i(k), \Delta\widetilde{y}_i(k), E_i(w,\gamma)\} = \frac{(1-\vartheta)\gamma\Delta_{ij}}{(1-\vartheta)\gamma\Delta_{ij} + \vartheta\left(|N_i| - \gamma\Delta_{ij}\right)} \tag{15}$$

Evidently, there exists $0 \leq P_i(k) \leq 1$ which is a kind of reliability degree test. As a result, the conformance vector of k iteration time synchronization acquired from the neighbor node $N_i = \{j|(i,j) \in E, \forall j \in V\}$ of node i is:

$$P(k) = \left[P_1(k), P_2(k), \ldots, P_{deg(i)}(k)\right] \tag{16}$$

Regarding node i, the behavior reliability of itself can be represented by a time series measured by itself. Regarding the periodic readout of the node as a sequence in chronological order, this readout sequence is virtually a sample value of node behavior process. Considering the limited calculation and storage capacity of the sensor, only the sample values in a certain period are kept. To improve the degree of reliability, taking the mean value $\breve{P}_i$ of the comprehensive time synchronization conformance estimation can be defined as follows:

$$\breve{P}_i(k) = \frac{1}{k}\sum_{j=1}^{deg(i)} P_j(k) \tag{17}$$

where the fluctuation of the sequence is little, that means the disturbance noise from its neighbor node N_i to node i is little and reliability is high. Therefore, the reliability of node i can be defined intuitively as the expectation and the variance of the time synchronization conformance estimate as follows:

$$E[P_i(k)] = \eta,\ \rho_i^2(k) = \frac{1}{k}\sum_{i=1}^{k}\left[\breve{P}_i(k) - P_i(k)\right]^2 \tag{18}$$

Formula (18) can be used to calculate the reliability property value of a node behavior. Using the reliability calculation, the sensor node which has a higher reliability degree should be the nodes with higher time synchronization conformance and higher reliability, for example a larger $P_i(k)$ value and a smaller $\rho_i^2(k)$ value. Regarding node i, a larger $P_i(k)$ value does not mean that the $\rho_i^2(k)$ value is large or small and vice versa. Thus, mapping $f\left[\breve{P}_i(k), \rho_i^2(k)\right]$ is introduced to ensure the node behavior reliability degree has a positive correlation with $\breve{P}_i(k)$ and a negative correlation with $\rho_i^2(k)$. The node behavior reliability degree is defined by bilinearity:

$$U_i(k) = f\left[\breve{P}_i(k), \rho_i^2(k)\right] = [1 - \varepsilon\rho_i(k)]\breve{P}_i(k) \tag{19}$$

Thus, the reliability degrees of node i for neighbor node j can be lined up according to $U_i(k)$ value and then graded by different thresholds $\phi \in [\phi_1, \phi_2]$.

4.3. Algorithm Design

The detailed steps of the authors' algorithm, as showed shown in Figure 2, Consistency Estimates of Access Control Model based on Time Synchronization (CEACM-TS), are as follows:

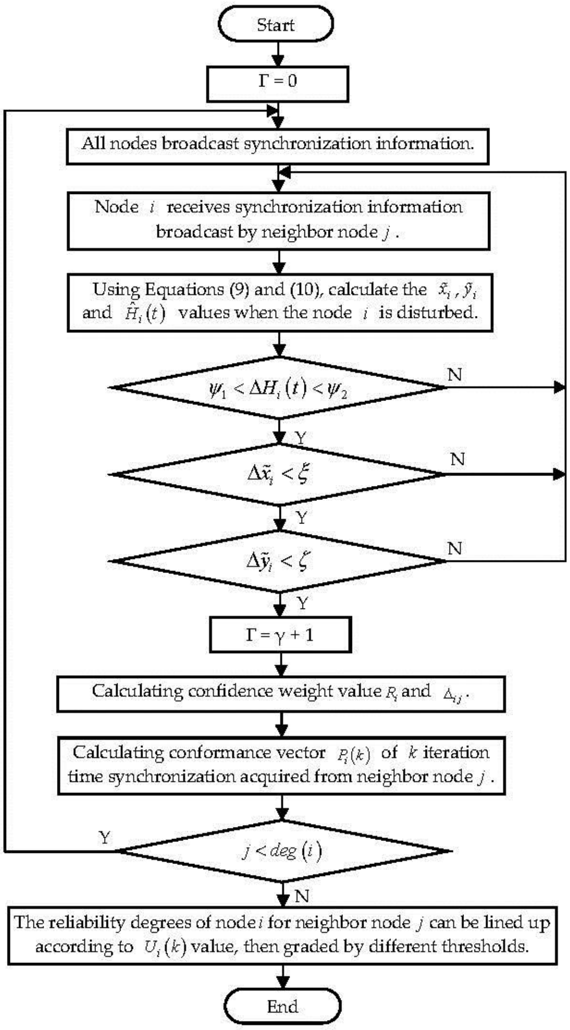

Start
Γ = 0
All nodes broadcast synchronization information.
Node i receives synchronization information broadcast by neighbor node j.
Using Equations (9) and (10), calculate the $\tilde{x}_i$, $\tilde{y}_i$ and $\hat{H}_i(t)$ values when the node i is disturbed.
$\psi_1 < \Delta H_i(t) < \psi_2$
N
Y
$\Delta\tilde{x}_i < \xi$
N
Y
$\Delta\tilde{y}_i < \zeta$
N
Y
$\Gamma = \gamma + 1$
Calculating confidence weight value R_i and Δ_{ij}.
Calculating conformance vector $P_i(k)$ of k iteration time synchronization acquired from neighbor node j.
Y
$j < deg(i)$
N
The reliability degrees of node i for neighbor node j can be lined up according to $U_i(k)$ value, then graded by different thresholds.
End

Figure 2. The basic steps of CEACM-TS.

Step 1: Number of neighbor nodes with no disturbance events is γ, the initial value of γ is 0.

Step 2: The node broadcasts the synchronization information and receives the synchronization information sent by its neighbor nodes.

Step 3: Node i receives synchronization information broadcast by neighbor node j. The node calculates the clock skew and clock offset caused by the interference noise received by the hidden attack inside the node according to Formula (9), respectively. The estimation of $Q_i(t)$ can be obtained by Least Square Estimate, namely $Q_i(t) \approx \Delta H_i(t) = \left|H_i^+(t) - \hat{H}_i(t)\right|$.

Step 4: Only if $Q_i(t) \in [\psi_1, \psi_2]$ and $\widetilde{x}_i < \xi \wedge \widetilde{y}_i < \zeta$ is this synchronization information valid, otherwise it is discarded. $Q_i(t)$, $\widetilde{x}_i$ and $\widetilde{y}_i$ can be used as access control objects at the same time to avoid missed detection.

Step 5: Establish the weight-value synthesis of reliability Δ_{ij} by calculating the trusted weight-value R_j of each node using Formulas (12) and (13) in Section 4.1.

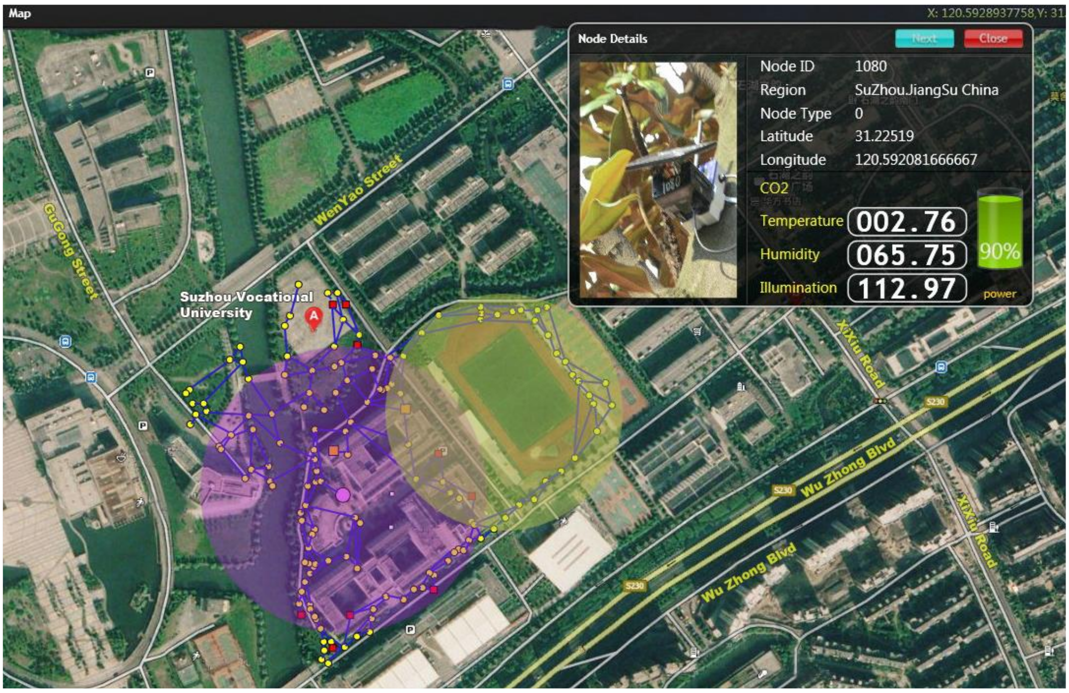
Step 6: Calculate the k iteration time synchronization conformance vector of node i for the neighbor node N_i, $P(k) = \left[P_1(k), P_2(k), \ldots, P_{deg(i)}(k)\right]$.

Step 7: Calculate the estimated mean value $\breve{P}_i$ of comprehensive time synchronization conformance according to Formula (17).

Step 8: Estimate the control ability of node i for the access transmission of its neighbor node according to its behavior reliability degree (Formula (19)) as mentioned in Section 4.2.

5. Performance Analysis and Experimental Results

This paper evaluates the access performance of the model for event test, taking the wireless sensor network of 200 nodes distributed in the 500 m × 400 m campus of Suzhou Vocational University (shown in Figure 3) as an example. The average communication radius of the node is 10 m. The broadcast period is set to 1 s, the error of the crystal oscillator is generally between 10 ppm and 100 ppm, there is an error of 10 microseconds to 100 microseconds per broadcast period. The he hardware clock skew is randomly selected within the [0.9999,1.0000] interval and the hardware clock offset is randomly selected in the [0,0.0002] interval. The schemes have been evaluated through a real outdoor campus consisting of 150 TelosB motes which run CTP protocol, where CTP is a data collection protocol that dynamically selects the best route to the sink according to a hybrid link estimation algorithm [37]. The operating system is based on TinyOS 2.1.2. The red nodes indicate malicious node in Figure 3. The evaluation will compare three schemes: CEACM-TS, APAC [9] and GTMS (Group based trust management scheme) [8], to show that CEACM-TS is a practical design for the tradeoff between keeping out of the interference and transmitting concurrently, comparing their advantages and disadvantages in terms of random packet losses, error packets, data tampering and retransmission, falsification of identity, denial of service, node capture resetting as well as system cost, energy consumption evaluation and error rate of access control test under the condition of simulative human disturbances and attacks. This topology structure is composed of two backbone networks which contains the cluster head node and sensor nodes. The cluster head node and sensor nodes constitute the multicast tree supported by the backbone network. The cluster head can perform topology control, access control, routing and monitoring the time synchronization state of sensor nodes. Cluster head node stores multicast routing state information, which can minimize routing complexity during link failure. The sensor nodes take part in CEACM-TS algorithm supported by backbone network, saves energy consumption of WSN and improves the performance of the whole network.



Node ID 1080
Region SuZhou.JiangSu China
Node Type 0
Latitude 31.22519
Longitude 120.592081666667
Temperature 002.76
Humidity 065.75
Illumination 112.97

Figure 3. A prototype network for event detection.

During the testing process, the authors set a fixed delay of node information exchange at $\upsilon = 0.01$ s, random delay $\chi = 0.013$ s, the number of nodes with no disturbance events occurring in their neighbor node $\gamma = 170$ and the error probability rate of links of any two nodes $\vartheta = 0.02$. As shown in Figure 1, thresholds of two different disturbance areas were set as $\psi \in [0.05, 0.1]$ and $\psi \in [0.2, 0.5]$.

5.1. System Cost

This test took the network area with a threshold of $\psi \in [0.2, 0.5]$, shown in Figure 4, as an example. There were two disturbance factors which caused failure in synchronization. The first was a data jam and missing caused by data tampering and retransmission in node 13. The data packet forwarded by node 13 had to be forwarded from node 15 by a detour. Second, a routing loop (solid line) was formed by nodes capturing resetting in the neighbor nodes of node 25. Thereafter, the authors performed CEACM-TS, APAC and GTMS, respectively, in the network and the network test with collection tree protocol. Test results showed that the tree structure of node 13 and node 25 changed. Both CEACM-TS and APAC broke the routing loop and transmitted data packets through broadcasting RBS protocol packages. When the network topological changed, its neighbor area changed automatically. As the number of neighbors increased, the synchronization and cluster between the depth of topological structures, as well as signal intensity clock drift and clock delay, became more and more close, therefore, the number of the time synchronization proofs required from relevant nodes also increased.

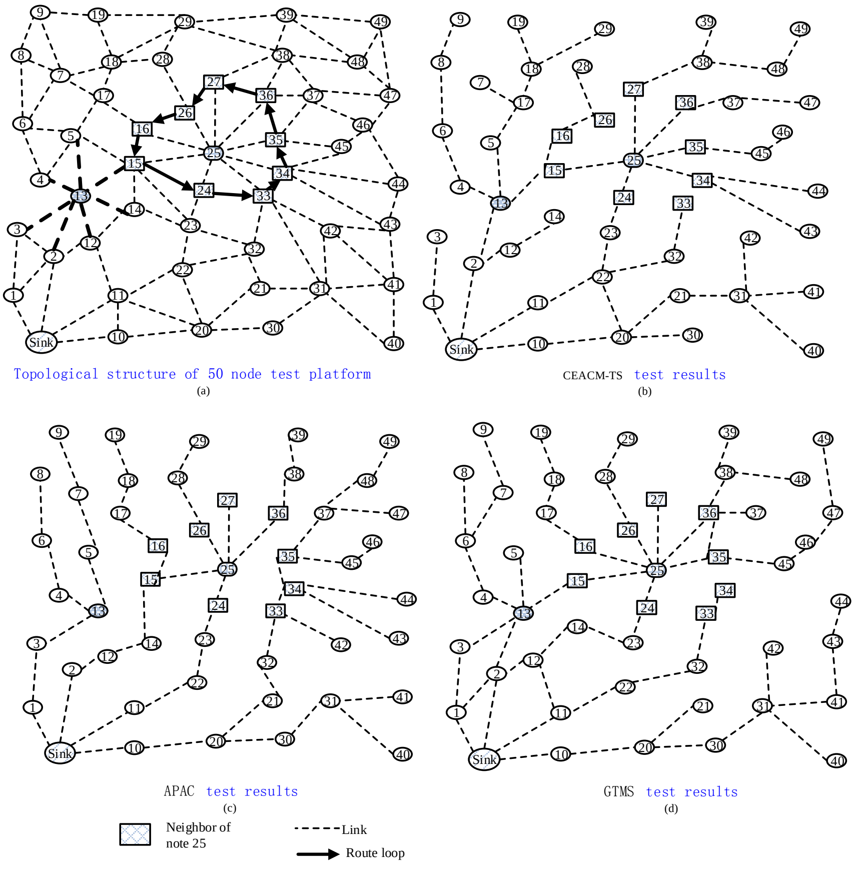


Figure 4. The topological structure of test platform with 50 nodes. (a) Topological structure of 50 node test platform; (b) CEACM-TS test results; (3) APAC test results; (d) GTMS test results.

Figure 4a shows the topology of 50 nodes in our experiments, including some probe traces. The protocol for this network is the CTP, for the analysis of impact with different access control approaches. In this work, we implement three algorithms for access control the network. Figure 4b,c,d describes three convergence tree structures. The process of sampling evidences is used to assign a local time synchronization trust to each node in evidence collection, while establishing convergence tree mainly includes broadcasting and receiving interference noise. Figure 4b shows the probability of a network with a depth less than 3, 4, 5 and 6, formed by CEACM-TS, was respectively 10%, 19%, 29% and 33%. Figure 4c shows the probability of a network with a depth less than 3, 4, 5 and 6 formed by APAC was respectively 8%, 15%, 24% and 27%, Figure 4d shows the corresponding result for GTMS was 25%, 20%, 6% and 6%, respectively. CEACM-TS also greatly reduced the maintenance cost of the time synchronization tree, clock drift and clock delay calculation, compared to APAC and GTMS.

Figure 5 demonstrates that the three algorithms had similar throughput capacities which increased as the intensity of disturbance noise rose. When the increment of disturbance noise intensity reached a certain threshold, the node gradually became unable to evacuate the caching queue of itself and the throughput capacities of CEACM-TS and APAC decreased. However, when the disturbance intensity was lower than 0.27, the throughput capacities of CEACM-TS and APAC remained increasing with the increment of load strength. The throughput capacity of CEACM-TS was much higher than that of APAC. Both CEACM-TS and APAC performed much better than GTMS in terms of throughput ability. Figure 5 shows that, with further increment of disturbance intensity, the throughput capacity of APAC decreased quickly. When the load intensity was higher than 0.36, the throughput of CEACM-TS was nearly 40 percent at its best performance, which still performed better than GTMS and APAC.

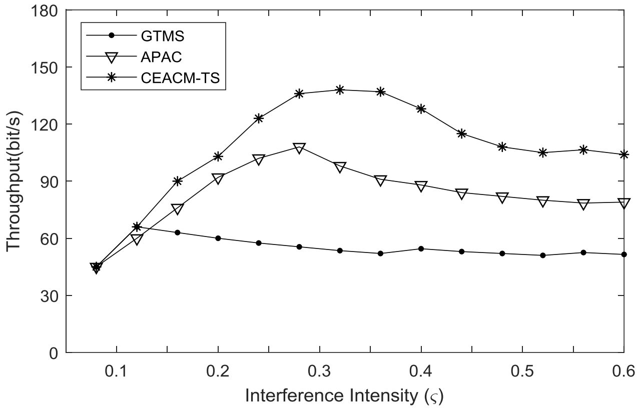


Figure 5. Throughput curve versus Interference intensity.

5.2. Energy Consumption Evaluation

The average energy consumption is defined as the ratio of the total energy cost over the total number of nodes. Figure 6 shows the relation between the average energy consumption and the load intensity. Since the number of data packets sent out by each source node was fixed in this experiment, when the load intensity was low, the network needed more operation cycles to finish the transmission of all data packets. When there was no data packet needing to be transmitted, the idle interception caused energy consumption. The operation cycle was where idle interception occurs. When the increment of load intensity decreased the work efficiency increased, so the average energy consumption generally decreased, as shown in Figure 6.

Figure 6 shows that the energy consumption of CEACM-TS was lowest among the three algorithms (CEACM-TS, APAC and GTMS). Between APAC and GTMS, APAC performed much better. This is because APAC enabled a data packet to realize multiple hop transmissions in a single cycle, thus, the data packet could be transmitted faster, shortening the working period for transmission of all data packets and saving energy. Due to adopting neighbor invitations and bilinear computer mechanisms, CEACM-TS made full use of sample values in a certain period, which realized swift and even transmission of the caching data packets to the gathering node. When the load intensity was higher than 0.36, CEACM-TS saved energy by 58% and 37% respectively, compared to GTMS and APAC.

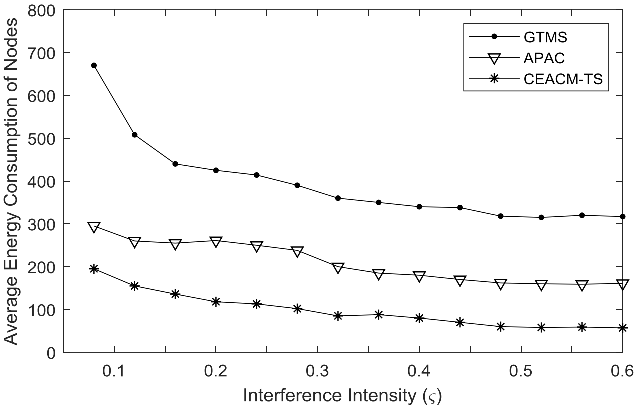


Figure 6. Energy consumption of different interference intensities.

5.3. *Error Rate of Access Control Detection*

Figure 7a shows that CEACM-TS was always superior to APAC and GTMS. It had the lowest error rate under different malfunction product rates of node disturbance event $\varsigma\vartheta$. When the malfunction product rate of node disturbance event $\varsigma\vartheta$ was 30%, APAC and GTMS respectively had 38% and 47% disturbance nodes which were not detected, while CEACM-TS only had approximately 15%. Figure 7b shows the probability of conformance estimation error in WSN, with the increment of node disturbance malfunction product rate and the conformance estimates errors of all three algorithms. However, the conformance estimate errors of CEACM-TS was much less than APAC and GTMS. The authors also show the average error correction probability in Figure 7c which demonstrates that, when the node disturbance malfunction product rate was 25%, the error correction probability of APAC and GTMS reached around 62% and 48% respectively, while CEACM-TS reached about 81%, which is significantly higher than that of APAC and GTMS. (Note that the higher percentage is preferred).

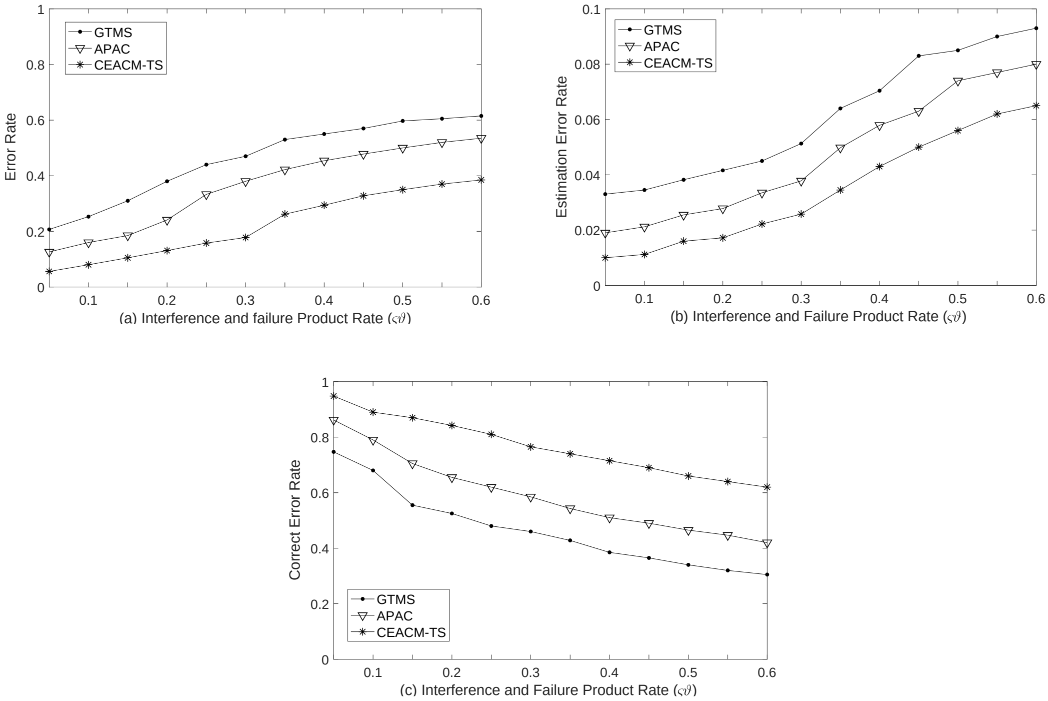


Figure 7. Error rate of access control detection: (**a**) Error rate; (**b**) Estimation error rate; (**c**) Correct error rate.

Differing from the above analysis is that the introduction of behavior reliability can improve the quality of disturbance event test and lower the effects from disturbance noise, which results in the improvement of reliability and the safety of data transmission. However, due to the impacts on the error tolerance detection from neighbor node disturbance, it is necessary to consider both factors of the node reliability and the number of disturbance neighbor nodes. It can be seen from the above analysis that the introduction of node bilinear behavior reliability can improve the safety of data transmission.

6. Conclusions

To improve the safety and fairness in the access control of WSN and, in consideration of the limitations of WSN resources, this paper proposed a WSN access control model CEACM-TS, based on time synchronization with the adoption of a light weight principle and a thought regarding testing time synchronization disturbance noise of the neighbor nodes as the reliability evaluation factor. This distributed access control model realizes reliable access control through two factors: one is the time synchronization similarity between sensor nodes and local sampling of neighbor nodes and the other is the conformity of random statistical characteristics for disturbance behaviors. An algorithm of adaptive weighted data fusion of neighborhood time synchronization is proposed, adaptive optimal weighted value is produced based on measurement interference noise variance estimated and constructed a judgment evidence, the sensor data is adaptive, fast, reasonable grouping weighted, a robust and exact results can be achieved. The method is a simple, practical algorithm and greatly reduces the redundancy of data within the network, saving a lot of storage resources and network bandwidth. This model can efficiently solve the problems faced by internal reliability and the external safety of data transmission due to its characteristics in distribution, low complexity, strong extendibility and robustness. Since the model has a strong extendibility, it still can work when the network scale changes. Furthermore, the model only requires time synchronization communication between nodes and neighbor nodes to reach the overall target. This avoids energy consumption caused by multi-hop communication and reduces the demand for storage space. Current test results showed the applications of the model in WSN mainly included sensor fusion and filtration, time synchronization, target location and tracing, sensor scheduling and more, which improved the ability of nodes in controlling neighbor access transmission and virtually reduced illegal access between neighbor nodes.

Author Contributions: Z.L. and Q.M. conceived and designed the experiments; L.Z. and G.L. performed the experiments; V.S.S. and W.L. analyzed the data and contributed analysis tools; Z.L. offered advice and modified the paper; V.S.S. offered advice and modified the paper; Z.L. wrote the paper.

Funding: This research was funded by the National Natural Science Foundation of China (61672372, 61472211), the Outstanding Science-technology Innovation Team Program of Colleges and Universities in Jiangsu.

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

References

1. Alrashed, E.A.; Karaata, M.H.; Hamdan, A.; Albahar, B. An adaptive stabilizing imposter detection scheme for distributed mobile wireless sensor networks. *Ad Hoc Netw.* **2017**, *65*, 1–12. [CrossRef]
2. Jesus, G.; Casimiro, G.; Oliveira, A. A Survey on Data Quality for Dependable Monitoring in Wireless Sensor Networks. *Sensors* **2017**, *17*, 2010. [CrossRef] [PubMed]
3. Cui1, J.; Zhang, Y.; Cai1, Z.; Liu, A.; Li, Y. Securing Display Path for Security-Sensitive Applications on Mobile Devices. *Comput. Mater. Contin.* **2018**, *55*, 17–35.
4. Pirzada, A.A.; McDonald, C. Establishing trust in pure ad-hoe networks. *Wirel. Pers. Commun.* **2006**, *37*, 139–168. [CrossRef]
5. Ahmed, M.R.; Huang, X.; Cui, H. A Novel Evidential Evaluation for Internal Attacks with Dempster-Shafer Theory in WSN. In Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Melbourne, Australia, 16–18 July 2013; Volume 52, pp. 688–693.

6. Ishmanov, F.; Kim, S.W.; Nam, S.Y. A Robust Trust Establishment Scheme for Wireless Sensor Networks. *Sensors* **2015**, *15*, 7040–7061. [CrossRef] [PubMed]
7. Ma, Q.; Zhang, S.; Zhu, T.; Liu, K.; Zhang, L.; He, W.; Liu, Y. PLP: Protecting Location Privacy Against Correlation Analyze Attack in Crowdsensing. *IEEE Trans. Mob. Comput.* **2017**, *16*, 2588–2598. [CrossRef]
8. Shaikh, R.A.; Jameel, H.; D'Auriol, B.J.; Lee, H.; Lee, S.; Song, Y. Group based trust management scheme for clustered wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.* **2009**, *20*, 1698–1712. [CrossRef]
9. Gao, M.; Feng, D.; Chu, J. Analysis of delay attacks based on game theory in time synchronization protocols. *Int. Conf. Commun. Technol.* **2014**, *51*, 987–996.
10. Ma, D.; Li, X.; Sun, Q.; Xie, X.; Simos, T. Fault tolerant synchronization of chaotic systems with time delay based on the double event-triggered sampled control. *Appl. Math. Comput.* **2018**, *333*, 20–31. [CrossRef]
11. Wei, J.; Yang, G.; Mu, Y. Comments on "Accountable and Privacy-Enhanced Access Control in Wireless Sensor Networks". *IEEE Trans. Wirel. Commun.* **2016**, *15*, 3097–3099. [CrossRef]
12. Han, G.; Jiang, J.; Shu, L.; Niu, J.; Chao, H.C. Management and applications of trust in wireless sensor networks. *J. Comput. Syst. Sci.* **2014**, *80*, 602–617. [CrossRef]
13. Verma, V.K. Pheromone and Path Length Factor-Based Trustworthiness Estimations in Heterogeneous Wireless Sensor Networks. *IEEE Sens. J.* **2016**, *17*, 215–220. [CrossRef]
14. Geetha, V.; Chandrasekaran, K. A distributed trust based secure communication framework for wireless sensor network. *Wirel. Sens. Netw.* **2014**, *6*, 173–183.
15. Reddy, V.B.; Venkataraman, S.; Negi, A. Communication and Data Trust for Wireless Sensor Networks Using D-S Theory. *IEEE Sens. J.* **2017**, *17*, 3921–3929. [CrossRef]
16. Jiang, J.; Han, G.; Wang, F.; Shu, L.; Guizani, M. An efficient distributed trust model for wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.* **2015**, *26*, 1228–1237. [CrossRef]
17. Nguyen, T.L.T.; Septier, F.; Rajaona, H.; Peters, G.W.; Nevat, I. A Bayesian Perspective on Multiple Source Localization in Wireless Sensor Networks. *IEEE Trans. Signal Process.* **2016**, *64*, 1684–1699. [CrossRef]
18. Souza, É.L.; Pazzi, R.W.; Nakamura, E.F. A prediction-based clustering algorithm for tracking targets in quantized areas for wireless sensor networks. *Wirel. Netw.* **2015**, *21*, 2263–2278.
19. Sandhya, M.K.; Murugan, K.; Devaraj, P. Selection of aggregator nodes and elimination of false data in wireless sensor networks. *Wirel. Netw.* **2015**, *21*, 1327–1341. [CrossRef]
20. Araghizadeh, M.A.; Teymoori, P.; Yazdani, N.; Safari, S. An efficient medium access control protocol for WSN-UAV. *Ad Hoc Netw.* **2016**, *52*, 146–159. [CrossRef]
21. Calafate, C.T.; Lino, C.; Diazramirez, A.; Cano, J.C.; Manzoni, P. An Integral Model for Target Tracking Based on the Use of a WSN. *Sensors* **2013**, *13*, 7250–7278. [CrossRef] [PubMed]
22. Li, Z.; Duan, Z.; Chen, G.; Huang, L. Consensus of multiagent systems and synchronization of complex networks: A unified viewpoint. *IEEE Trans. Circuits Syst. I Regul. Papers* **2010**, *57*, 213–224.
23. Wang, Z.; Zeng, P.; Zhou, M.; Li, D.; Wang, J. Cluster-Based Maximum Consensus Time Synchronization for Industrial Wireless Sensor Networks. *Sensors* **2017**, *17*, 141. [CrossRef] [PubMed]
24. He, J.; Li, H.; Chen, J.; Cheng, R. Study of consensus-based time synchronization in wireless sensor network. *ISA Trans.* **2014**, *53*, 347–357. [CrossRef] [PubMed]
25. Leng, M.; Wu, Y.C. A fast clock synchronization algorithm for wireless sensor networks. *Automatica* **2018**, *92*, 133–142.
26. Shrestha, D.; Pang, Z.; Dzung, D. Precise Clock Synchronization in High Performance Wireless Communication for Time Sensitive Networking. *IEEE Access* **2018**, *6*, 8944–8953. [CrossRef]
27. Benzaïd, C.; Bagaa, M.; Younis, M. Efficient Clock Synchronization for Clustered Wireless Sensor Networks. *Ad Hoc Netw.* **2017**, *56*, 13–27. [CrossRef]
28. Cheng, J.; Xu, R.; Tang, X.; Sheng, S.S.; Cai1, C. An Abnormal Network Flow Feature Sequence Prediction Approach for DDoS Attacks Detection in Big Data Environment. *Comput. Mater. Contin.* **2018**, *55*, 95–119.
29. Wang, H.; Shao, L.; Li, M.; Wang, P. Estimation of Frequency Offset for Time Synchronization with Immediate Clock Adjustment in Multihop Wireless Sensor Networks. *IEEE Int. Things J.* **2017**, *6*, 2239–2247. [CrossRef]
30. Li, J.; Li, S.; Zhao, F.; Du, R. Co-Channel Interference Modeling in Cognitive Wireless Networks. *IEEE Trans. Commun.* **2014**, *62*, 3114–3128. [CrossRef]
31. Serra, R.; Nabi, M. Wireless coexistence and interference test method for low-power wireless sensor networks. *Sci. Meas. Technol.* **2015**, *9*, 563–569. [CrossRef]

32. Noh, K.; Chaudhari, Q.M.; Serpedin, E.; Suter, B.W. Novel clock phase offset and skew estimation using two-way timing message exchanges for wireless sensor networks. *IEEE Trans. Commun.* **2007**, *55*, 766–777. [CrossRef]
33. Wang, D.; Xie, B.; Agrawal, D.P. Coverage and Lifetime Optimization of Wireless Sensor Networks with Gaussian Distribution. *IEEE Trans. Mob. Comput.* **2008**, *7*, 1444–1458. [CrossRef]
34. Shahid, A.; Choi, J.H.; Rana, A.H.S.; Kim, H.S. Least Squares Neural Network-Based Wireless E-Nose System Using an SnO_2 Sensor Array. *Sensors* **2018**, *18*, 1446. [CrossRef] [PubMed]
35. Wang, J.; Liu, B. Online Fault-Tolerant Dynamic Event Region Detection in Sensor Networks via Trust Model. *Wirel. Commun. Netw. Conf.* **2017**, *3*. [CrossRef]
36. Yang, S.; Adeel, U.; Tahir, Y.; Mccann, J. Practical Opportunistic Data Collection in Wireless Sensor Networks with Mobile Sinks. *IEEE Trans. Mob. Comput.* **2017**, *16*, 1420–1433. [CrossRef]
37. Gnawali, O.; Fonseca, R.; Jamieson, K.; Moss, D.; Levis, P. Collection tree protocol. In Proceedings of the 7th ACM Conference on Embedded Network, Sensor System, Berkeley, CA, USA, 4–6 November 2009; pp. 1–14.