

## Research Article

# Abnormal Event Detection in Wireless Sensor Networks Based on Multiattribute Correlation

**Mengdi Wang, Anrong Xue, and Huanhuan Xia**

*School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China*

Correspondence should be addressed to Anrong Xue; [xuear@ujs.edu.cn](mailto:xuear@ujs.edu.cn)

Received 10 February 2017; Accepted 27 March 2017; Published 6 April 2017

Academic Editor: Mengxing Huang

Copyright © 2017 Mengdi Wang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abnormal event detection is one of the vital tasks in wireless sensor networks. However, the faults of nodes and the poor deployment environment have brought great challenges to abnormal event detection. In a typical event detection technique, spatiotemporal correlations are collected to detect an event, which is susceptible to noises and errors. To improve the quality of detection results, we propose a novel approach for abnormal event detection in wireless sensor networks. This approach considers not only spatiotemporal correlations but also the correlations among observed attributes. A dependency model of observed attributes is constructed based on Bayesian network. In this model, the dependency structure of observed attributes is obtained by structure learning, and the conditional probability table of each node is calculated by parameter learning. We propose a new concept named attribute correlation confidence to evaluate the fitting degree between the sensor reading and the abnormal event pattern. On the basis of time correlation detection and space correlation detection, the abnormal events are identified. Experimental results show that the proposed algorithm can reduce the impact of interference factors and the rate of the false alarm effectively; it can also improve the accuracy of event detection.

## 1. Introduction

Abnormal event detection is one of the main problems in wireless sensor networks [1]. In wireless sensor networks, abnormal events are usually complex, because an event usually involves multiple observed attributes, and it is difficult to describe an abnormal event pattern [2]. Existing anomaly detection algorithms detect an abnormal event by comparing a single attribute threshold [3, 4] or by considering the spatiotemporal correlations of sensor readings [2, 5–8]. However, some important information may be hidden in the correlations among different attributes [9].

In [3], an adaptive distributed event detection method is proposed, which dynamically adjusts the decision threshold based on the trust value of the sensor nodes and uses the moving average filter to tolerate the transient faults of the sensor nodes. Although this method is fault-tolerant, it is still possible to misjudge the event nodes into faulty nodes. Particularly when the event range is large, the accuracy of detection will decrease significantly. Besides, this method computes a trust value for each sensor node, so it can only

be applied to univariate applications. Paper [5] models the event region based on Dynamic Markov Random Field. This method can effectively capture the dynamic changes of local area; since the method needs to exchange information of space-time neighbor constantly, the detection efficiency is low. Besides, the detection of the events lacks a global perspective, which may lead to misjudgment of abnormal events. Paper [6] proposed an event detection scheme based on spatiotemporal correlations. In this method, the sensor nodes are divided into multiple working groups; the time correlation of the sensor data is used to eliminate low frequency errors. Different working groups cooperate to determine whether the anomalies represent an event. However, this method only constructs the model based on the single sensing attribute and does not consider the relations between the multisensory attribute and the abnormal event.

The attributes of the sensor readings usually contain time information, sensor topology information, and other attributes directly sensed by the sensor (e.g., temperature, humidity, and light intensity). When abnormal events occur in the network, events often show temporal correlation,

spatial correlation, and attributes correlation [9]. In most cases, event detection methods that take the spatiotemporal correlation of the data into account are susceptible to both sensor failures and external environmental noises. For observed attributes, a simple threshold comparison is insufficient to determine whether an abnormal event occurs. For instance, in an indoor fire monitoring application, the increase of the temperature and smoke concentration may be caused by cooking, rather than a fire accident.

In order to improve the accuracy of abnormal event detection in wireless sensor networks with multiple attributes and reduce the influence of environmental noises and sensor failures on the event detection results, this paper proposes a new method called Abnormal Event Detection based on Multiattribute Correlation (MACAED). First, considering that Bayesian network can effectively represent the dependencies among variables, a Bayesian network is used to establish the dependency model of observed attributes. In this model, the dependency structure of abnormal events is obtained by structure learning. Each node learns the parameters to get a conditional probability table. Then, the attribute correlation confidence is introduced to judge whether the attribute correlation mode of the point is an abnormal mode. Based on the sliding window model, the degree of temporal correlation was calculated; the spatial similarity was calculated by using the neighbor node information. Finally, the anomaly events were detected by three kinds of attribute correlation.

## 2. Attribute Dependency Model

In wireless sensor networks, abnormal events usually show the following three characteristics:

- (1) For a single sensor node, the anomaly event will continue for a period of time once the event occurs; the adjacent time of the data shows a certain degree of similarity [7]. In addition, abnormal events will inevitably affect the physical environment of network monitoring, and the sensor data will change accordingly, showing a special mode.
- (2) For a number of sensor nodes, sensor nodes in the event region will exhibit spatial similarity when abnormal events occur [10]; in other words, the readings of adjacent nodes exhibit similar patterns.
- (3) When the abnormal events occur in the monitoring area, the sensed attributes of the sensor readings show a certain degree of relevance, and this correlation appears as probability relations [9].

According to the three kinds of characteristics of abnormal events in wireless sensor networks and the experience that Bayesian network can effectively represent the probability relationship among attributes, we construct the attribute dependency model. The attribute correlation confidence is proposed to measure the degree of similarity between the measured points and the anomalies in observed attribute probability model.

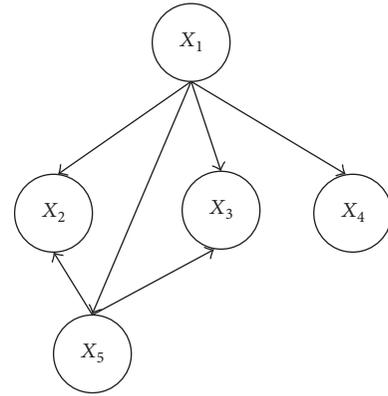


FIGURE 1: An example of attribute dependency model.

**2.1. Bayesian Network.** Bayesian network is a product of probability theory and graph theory. It is a directed acyclic graph with probabilistic annotations, which can represent the probability dependencies among random variables. It has a solid mathematical foundation [11]. On the one hand, the Bayesian network can reveal the structure of the problem intuitively by using graph theory. On the other hand, the Bayesian network can utilize the structure of the problem according to the principle of probability theory, which reduces the computational complexity of reasoning. In view of this, this paper establishes a dependency model of observed attributes based on the Bayesian network; each attribute is represented by a unique node, and the probabilistic dependencies are represented by arcs between nodes.

**2.2. Formal Description.** The attribute dependency model is represented by a triplet  $B = (D, G, \theta)$ , where  $D$  is the sample dataset that contains observed attributes,  $D = \{d_1, d_2, \dots, d_m\}$ ;  $G$  denotes a directed acyclic graph, which qualitatively describes the dependencies among attributes,  $G = (X, U)$ , where  $X$  is a set of nodes representing observed attributes, corresponding to the elements in  $D$ , and  $U$  is the directed edge set representing the dependencies among the attributes;  $\theta$  is the set of conditional probability distributions for each node, which quantitatively describes the dependencies among attributes,  $\theta = \{P(X_i | \pi(X_i))\}$ , where  $X_i$  is the  $i$ th node in  $G$  and  $\pi(X_i)$  is the set of parent nodes of node  $X_i$ . Figure 1 is an example of an attribute dependency model.

**2.3. Structure Learning.** For WSNs with large number of variables and implicit dependencies among variables, it is difficult to obtain a reasonable network structure relying on a priori information and expert knowledge, and the probability is subjective, so we learn the Bayesian network structure from training samples. This paper utilizes a strategy of scoring and searching. Specifically, we use a scoring function to evaluate the matching degree between a specific network structure and the training sample and select the appropriate search strategy to search the network structure with the highest scoring value.

Given a sample dataset  $D(d_1, d_2, \dots, d_m)$ , let Bayesian network  $G$  take all the variables in the node set  $X(X_1, X_2, \dots, X_m)$  as nodes, and instantiate all the variables of  $X$  using the attribute value  $d_i$  in the sample dataset. The variable  $X_i$  has  $r_i$  possible values  $(x_{i1}, x_{i2}, \dots, x_{ir_i})$ . Let the parent variable set of  $X_i$  be  $\Pi_i$ ,  $w_{ij}$  denotes the  $j$ th instantiation value of the parent node  $\Pi_i$  with respect to  $D$ , and  $N_{ijk}$  denotes the number of instances in which the value  $X_{ik}$  of the variable  $X_i$  is taken and is instantiated into  $w_{ij}$  by  $\Pi_i$ ,  $N_{ij} = \sum_{k=1}^{r_i} N_{ijk}$ . The Bayesian scoring criterion is used to compute the likelihood ratios of the two Bayesian network structures  $G_1$  and  $G_2$ . Since  $p(G_1 | D)/p(G_2 | D) = p(G_1, D)/p(G_2, D)$ , we only need to compare the joint probability  $p(G_1, D)$  and  $p(G_2, D)$ . This can be calculated by using the formula [12]

$$\begin{aligned} p(G, D) &= p(G) p(D | G) \\ &= p(G) \cdot \prod_{i=1}^n \prod_{j=1}^{q_i} \frac{(r_i - 1)!}{(N_{ij} + r_i - 1)!} \cdot \prod_{k=1}^{r_i} N_{ijk}!, \end{aligned} \quad (1)$$

where  $p(G)$  is the prior probability and the arrangement order of  $\Pi_i$  is  $(1, \dots, q_i)$ . Maximizing the joint probability  $p(G, D)$  in (1)

$$\begin{aligned} \max_G \{p(G, D)\} \\ = p(G) \prod_{i=1}^n \max_{\Pi_i} \left[ \prod_{j=1}^{q_i} \frac{(r_i - 1)!}{(N_{ij} + r_i - 1)!} \prod_{k=1}^{r_i} N_{ijk}! \right]. \end{aligned} \quad (2)$$

It can be seen that, for each variable  $X_i$ , it is only necessary to maximize

$$\max_{\Pi_i} \{g(i, \Pi_i)\} = \max_{\Pi_i} \left[ \prod_{j=1}^{q_i} \frac{(r_i - 1)!}{(N_{ij} + r_i - 1)!} \prod_{k=1}^{r_i} N_{ijk}! \right]. \quad (3)$$

In the initial stage of constructing the network structure, it is assumed that each node has no parent node. The nodes which meet the posterior probability maximization formula are recursively added to the parent set of nodes. When  $p(G, D)$  is no longer increased, stop adding to the parent node set; then the network structure  $G'$  is obtained. For the current sample dataset  $D$ ,  $G'$  is the optimal network structure under the Bayesian scoring standard.

**2.4. Parameter Learning.** According to the trained network structure, the parameter of each node in the network is learned to get the corresponding conditional probability table. The conditional probability table contains the probability relations among the variables. Using the maximum likelihood estimation method, suppose  $(x_1, x_2, \dots, x_n)$  is a set of possible values of random variable set  $(X_1, X_2, \dots, X_n)$ , and the probability of  $(X_1, X_2, \dots, X_n)$  falling in the neighborhood of  $(x_1, x_2, \dots, x_n)$  ( $n$ -dimensional cubes with side length  $dx_1, dx_2, \dots, dx_n$ , resp.) is approximated as  $\prod_{i=1}^n f(x_i; \theta) dx_i$ , where  $\prod_{i=1}^n f(x_i; \theta)$  is the joint probability density of  $(X_1, X_2, \dots, X_n)$ ,  $\theta$  is the structural parameters, and  $\theta \in \Theta$ . The maximum likelihood estimation value  $\hat{\theta}$  of  $\theta$

is calculated through  $\max_{\theta \in \Theta} L(x_1, \dots, x_n; \theta)$ . The conditional probability table for each node is obtained from the sample data and prior knowledge.

**2.5. Attribute Correlation Confidence.** Attribute correlation confidence is a concept we proposed to measure the fitting degree between the sensor reading and the abnormal event pattern. It is equal to the ratio of the joint probability distribution between the measured point and the abnormal point. Let  $(y_1, y_2, \dots, y_n)$  be the sensor reading at the current time. For an abnormal event  $E_i$ , the joint probability of all node variables  $P(X_1, X_2, \dots, X_n | E_i)$  is calculated according to the Bayesian network structure and the conditional probability table. Since in Bayesian network, not every node has an arc to the all the rest nodes, the conditional probability only depends on the direct parent node. In other words, given the values of parent variables, the probability of nondescendant node is conditionally independent of the parent node. So the calculation of joint probability  $P(X_1, X_2, \dots, X_n | E_i)$  can be simplified by using the chain rule [11],

$$p(x) = \prod_{i=1}^n p(x_i | x_{pa(i)}) \quad (4)$$

in which  $x_{pa(i)}$  represents the parent node of  $x_i$ .

After calculating  $P(X_1, X_2, \dots, X_n | E_i)$ , we can get the probability pattern of the reading in an event. According to the formula,

$$\alpha = \max_{i \in I} \frac{P(X_1 = y_1, \dots, X_n = y_n)}{P(X_1 = x_1, \dots, X_n = x_n | E_i)}, \quad (5)$$

the attribute correlation confidence  $\alpha$  of the tested point is calculated. The higher the probability, the more the possibility for the anomaly to represent an abnormal event.

### 3. Abnormal Event Detection Algorithm Based on Multiattribute Correlation

In this paper, we propose a detection algorithm based on multiattribute correlation, which is divided into three phases: attribute correlation pattern decision, temporal similarity detection, and spatial similarity detection.

**3.1. Description of Abnormal Event.** For an abnormal event, define event information  $Info = \{Tm, Loc, Attr, Parm, E_i\}$ , where  $Tm$  is the time of occurrence of abnormal events,  $Loc$  is the location of abnormal events, and  $Attr$  is the attribute set that an event involves.  $Parm$  is the parameter set, which includes temporal similarity threshold  $\varepsilon$ , spatial similarity threshold  $\delta$ , and attribute correlation confidence threshold  $\varphi$ . For different application environments, the values of each item in  $Parm$  can be adjusted to achieve the best detection result adaptively.  $E_i$  represents the event type,  $i = 0$  means no abnormal events occurred,  $i > 0$  means that abnormal events occurred, and the higher the value  $i$  is, the more severity the abnormal event has.

**3.2. Temporal Similarity Detection.** The data sampling frequency of most wireless sensor networks is relatively high and data change range at the adjacent time is relatively small, so the sensor data is time-correlated. Combining with sliding window model and the attribute dependency model obtained, candidate anomalies that may represent abnormal events are detected.

Let  $s$  be the size of the sliding window, and for each data sequence  $t_i$  within the window, calculate the similarity between  $t_i$  and the current time series  $t$

$$q(t_i, t) = \frac{1}{\left(1 + \sqrt{\sum_{k=1}^m (x_k^{t_i} - x_k^t)^2}\right)}. \quad (6)$$

Considering that the data sequence that is closest to the current time is most correlated, the average similarity between the current time data and the data in the window is calculated by the weighted summation method

$$\overline{q}(t) = \frac{\sum_{i=1}^{ws} w_i q(t_i, t)}{s}, \quad (7)$$

where the weight is  $w_i = 1/(t - t_i)$ . If the average similarity is smaller than the threshold  $\varepsilon$  and the confidence degree of the attribute correlation is greater than or equal to the threshold  $\varphi$ , it means that not only does the data sequence of the current time significantly deviate from the historical data, but also the relationship among the attributes is in accordance with the probability relation when the abnormal event occurs, which needs a further spatial correlation detection. In other cases, it will be filtered as a noise.

**3.3. Spatial Similarity Detection.** The similarity between the candidate anomaly and the neighbor node's data sequence is calculated. If the candidate anomaly and the neighbor node's data sequence satisfy certain similarity degree, it indicates that the abnormal event occurs in the region where the candidate anomaly is located and needs to be uploaded to the sink node.

The similarity between the candidate anomaly and the neighbor node sequence is calculated according to the following formula:

$$q(x_t, y_t) = \frac{1}{\left(1 + \sqrt{\sum_{k=1}^m (x_k^t - y_k^t)^2}\right)}. \quad (8)$$

If the spatial similarity  $q(x_t, y_t)$  is greater than or equal to the threshold  $\delta$ , it indicates that both nodes have detected an abnormal event at the same time and mark the candidate anomaly nodes and their neighbor nodes as abnormal event nodes. On the contrary, it indicates that no neighbor nodes detect abnormal information at this time, and the candidate anomaly belongs to noise data, which is also filtered out.

**3.4. Description of MACAED Algorithm.** Based on the calculation of attribute correlation confidence and the detection of

temporal and spatial correlation of sensor data, an abnormal event detection algorithm based on multiattribute correlation is proposed. The pseudocode of the algorithm is shown in Algorithm 1.

In the pseudocode of Algorithm 1, rows (2)~(3) train the Bayesian network through the scoring-searching method and choose the network structure  $M$  with the highest score as the observed attribute dependency model, rows (4)~(26) detect abnormal events in real time, where rows (9)~(10) proceed parameter learning for each sensor in order to update the probability distribution in attribute dependency model, rows (10)~(14) compute the attribute correlation confidence of observed attributes, row (15) calculates the average similarity between the current time readings and the readings within the window, row (18) calculates the average similarity between the current node and the adjacent node readings, and rows (17)~(24) determine whether the current reading represents abnormal events readings.

**3.5. Time Complexity Analysis.** Let  $n$  be the number of observed attributes, which corresponds to the number of nodes in Bayesian network;  $m$  is the number of instances, that is, the number of readings;  $r$  is the number of possible values for each observed attribute;  $N$  is the number of nodes in WSN;  $s$  is the size of sliding window. For the structure learning part, the time complexity is  $O(mn^4r)$  [12]. For abnormal event detection part, it contains two layers: outer layer loops  $O(m - s - 1)$  times and inner loops  $O(N)$  times. The parameter learning consists of a cycle of  $O(n)$  times. The time correlation detection consists of a cycle of  $O(s)$  times. The spatial correlation detection consists of a cycle of  $O(N)$  times. The total time complexity of the algorithm is  $O(mn^4r) + O(m - s - 1)O(N)O(n + s + N)$ . Since, for most wireless sensor networks, the value of  $n$  is small (less than 10) and sliding window  $s$  and the number of possible values of each attribute  $r$  are relatively small (in this experiment,  $s = 10$ ;  $r = 9$ ), the influence of these values on the total time complexity can be ignored, so the total time complexity can be simplified to  $O(m) + O(mN^2) = O(mN^2)$ .

## 4. Experimental Results and Analysis

**4.1. Datasets.** We test the performance of the MACAED algorithm by means of conducting simulation experiments on Matlab 2014a. The experiments are run on a PC with an Intel Core i3-2120 @3.30 GHZ Cpu, 4 GB memory, and Windows 7 operating system. For the instance of detecting fire event, the performance tests are based on the processed data of Intel Lab Data [13] from Intel Berkeley Lab. Except for the real data field, we insert the fire events and interference events data field into the dataset manually.

The experiment dataset contains the records of 54 sensors deployed in the IBRL lab during the time span from February 28th to April 5th in 2004. The MicaDot sensors collect temperature, humidity, light intensity, and voltage value every 31 seconds. Sensor node deployment is shown in Figure 2.

```

Input. WSN data set  $D$ 
Output. Abnormal event Information  $Info$ 
(1) standardize  $D$  into values between 0 and 1
(2) divide  $D$  into  $K$  subsets, choose the first set to learn Bayesian network
(3) choose the network with highest score as attribute
    dependency model  $M$ 
(4) for  $t = s + 1$  to  $epoch/epoch$  is incremental tick
(5)   if  $t \% period = 0 // period$  is parameter update period
(6)      $flag = true; // flag$  represents update parameter or not
(7)   end
(8)   for  $id = 1$  to  $N // id$  is the id of WSN,  $N$  is the number of sensors
(9)     learn parameter for each sensor node
(10)    if  $dataPointer[id] < group\_length$ 
        //prevent the  $id$  exceed the length of group
(11)      if  $groupData\_time[id] < t$ 
          //prevent a break caused by data loss
(12)        compute  $\alpha$  from  $M$ 
(13)      end
(14)    end
(15)    compute  $q(t_i, t)$ 
(16)    if  $q(t_i, t) < \epsilon$  &&  $\alpha \geq \varphi$ 
(17)      compute  $q(x_i, y_i)$ ;
(18)      if  $q(x_i, y_i) \geq \delta$ 
(19)        report  $Info$  to sink node;
(20)      else
(21)        filter as noise;
(22)      end
(23)    end
(24)  end
(25)   $flag = false$ ;
(26) end

```

ALGORITHM 1: Abnormal event detection algorithm based on multiattribute correlation.

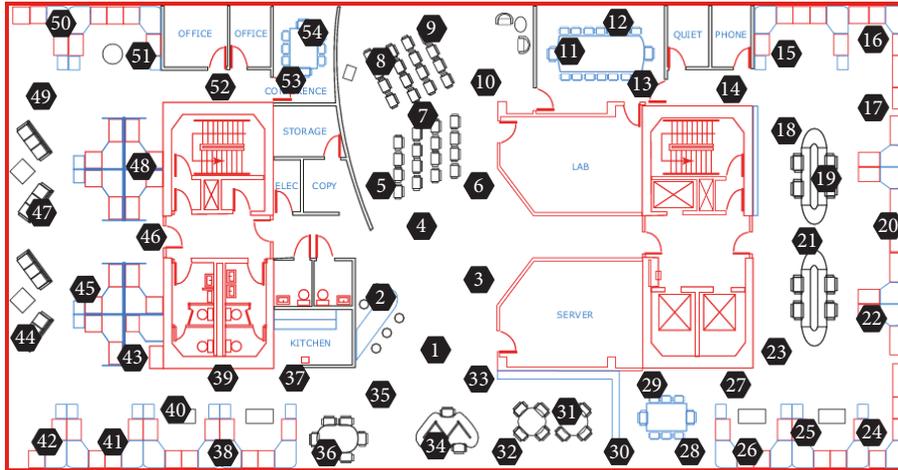


FIGURE 2: Location of sensor nodes deployed in IBRL lab.

4.2. *Data Preprocessing.* In our experiment, we choose the records within 24 hours in February 28th as our test data; we preprocess the raw data as follows:

- (1) Since the unit of measurement attributes directly sensed by each sensor is different and the changing range of different attributes is wide, so the raw data

needs to be standardized and mapped to  $[0, 1]$ ; in this way, the relative distance can be calculated.

- (2) Since the change of each attribute value is continuous and periodic, in order to facilitate the calculation, the experimental datasets are discretized, and the values of each attribute are divided into 10 intervals.

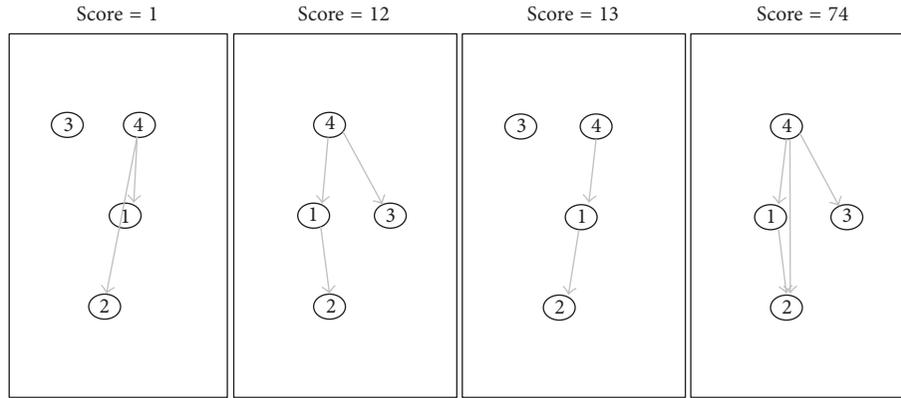


FIGURE 3: Network structure under Bayesian scoring criterion.

- (3) For some parts of the raw IBRL datasets have missing values and the failure nodes (both node 5 and node 15 have no records; node 28 only has 3 attribute records), the NaN is used in this experiment to fill the missing values, and these values will be discussed in different situations, not for computation.
- (4) In order to verify the performance of our algorithm on detecting abnormal events, abnormal readings that represent abnormal events are added in the dataset. In addition, the readings of the abnormal events with the interference are added (e.g., opening heater in the room will make the temperature rise).

**4.3. Experimental Parameters.** Temperature  $T$ , humidity  $H$ , light intensity  $L$ , and voltage  $V$  are numbered with 1, 2, 3, 4. In order to obtain relatively stable Bayesian network structure, we set the maximum number of parent nodes in structure learning  $max\_fan\_in = 2$ , learning step length  $step = 10$ , and the number of instances  $ncases = 1000$ . The optimal parameter learning cycle  $period = 600$ . Bayesian networks with four different scores are showed in Figure 3; the higher the score is, the more stable the network structure is. Thus, we choose the structure whose score = 74 as an attribute dependency model in this experiment.

In this method, the sliding window size has a direct impact on the detection results. The precision, the recall, and the  $F1$ -measure of anomaly detection under different sliding window sizes are experimented. The experimental results are shown in Figure 4.

From Figure 4, we can find that the recall decreases with the increase of the sliding window width; however, the overall change is not obvious. But the precision declines relatively faster, leading to the quick decrease of  $F1$  value. This is because, with the increase of window width, the historical data increases, and the calculated average value declines ceaselessly, which means that the possibility of becoming candidate anomalies is higher. Considering that the sliding window width is small and the amount of uploaded data is small, so we set the sliding window size  $s = 10$ ; in this way, we will make full use of historical data.

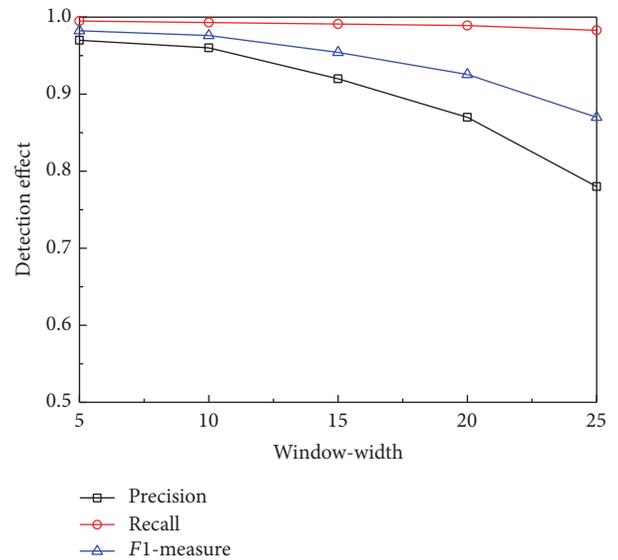


FIGURE 4: Influence of sliding window size on the test results.

There are different requirements for the threshold settings when the environment of wireless sensor networks differs. We change the value of three different thresholds and test the accuracy of the anomalies under the change of single threshold; the results are shown in Figure 5.

From Figure 5 it can be concluded that it gets the highest detection accuracy when temporal similarity threshold  $\epsilon = 0.1$ , spatial similarity threshold  $\delta = 0.2$ , and attribute correlation confidence threshold  $\varphi = 0.5$ .

**4.4. Contrast Experiment.** In the contrast experiment, we still use the IBRL dataset, in which the number of sensor nodes is 54, and the deployment of nodes is shown in Figure 2. We use  $(T, H, L, V)$  to represent four different attributes: temperature, humidity, light intensity, and voltage. Since there are no interference factors in the dataset, we add some false abnormal events artificially, which are shown in Table 1.

The contrast algorithms include the Adaptive Fault-Tolerant Event Detection (AFTED) algorithm proposed in

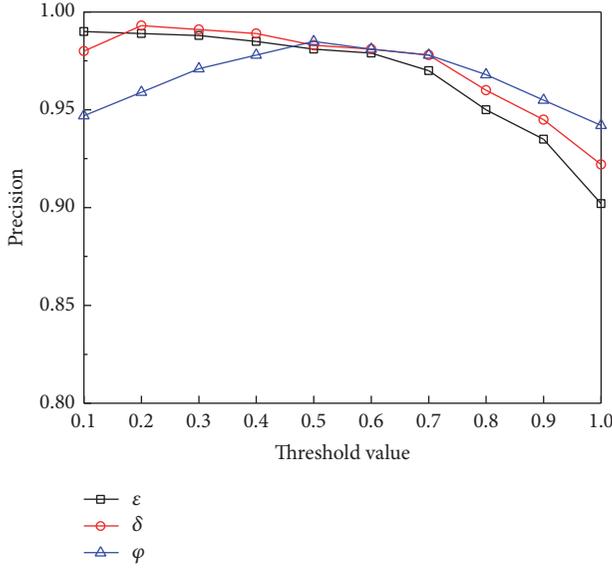


FIGURE 5: Influence of the three thresholds on the test results.

TABLE 1: False abnormal events.

Number	Event name	Attributes	Id of nodes
1	Cooking	$T, H, L, V$	2, 37
2	Air-condition	$T, H, V$	5, 17, 24, 36, 44
3	Heater	$T, V$	11, 12, 13
4	Bath heater	$T, L, V$	53, 54
5	Humidifier	$H$	27, 28, 29, 30

[3], the Online Dynamic Event Region Detection (ODERD) algorithm proposed in [5], the Real-Time Event Detection Approach based on Temporal-Spatial Correlations (TSCRED) presented in [6], and the Spatiotemporal Correlation based Fault-Tolerant Event Detection (STFTED) scheme proposed in [8]. And we compare the detection accuracy, false alarm rate, and detection time of abnormal events.

In the proposed algorithm, we use the same parameter settings as the previous experiments. In AFTED algorithm, we set the window size for tolerating transient faults  $M_{\text{AFTED}} = 4$ , and the threshold for filtering transient faults  $\delta_{\text{AFTED}} = 0.75$ , which have been verified to be the most appropriate in their experiment. In ODERD algorithm, since we only focus on the static abnormal event detection, the parameters controlling the shift and deformation of event regions are set to 0 s. To compare these algorithms in an equivalent level, we set the sliding window size of TSCRED and STFTED to 10, which is the same as the proposed algorithm. Besides, all of the sensor nodes have the same communication range  $R = 4$ . And each event region is assumed to be a circle with radius  $l = 2R$ .

The results of the proposed algorithm compared with the other four algorithms in detection accuracy are shown in Figure 6. It can be seen from Figure 6 that when the node failure rate goes from 0.05 to 0.3, the detection accuracies of the five algorithms are similar, reaching 0.96 or more; this is because most of the noise is filtered out in the time correlation

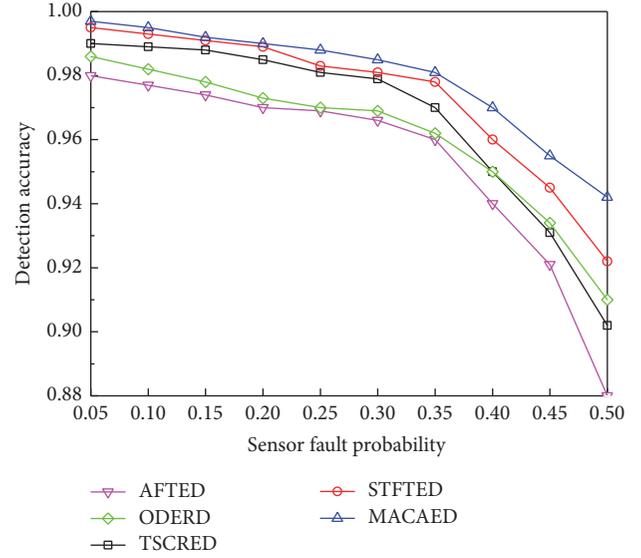


FIGURE 6: Detection accuracy of five algorithms.

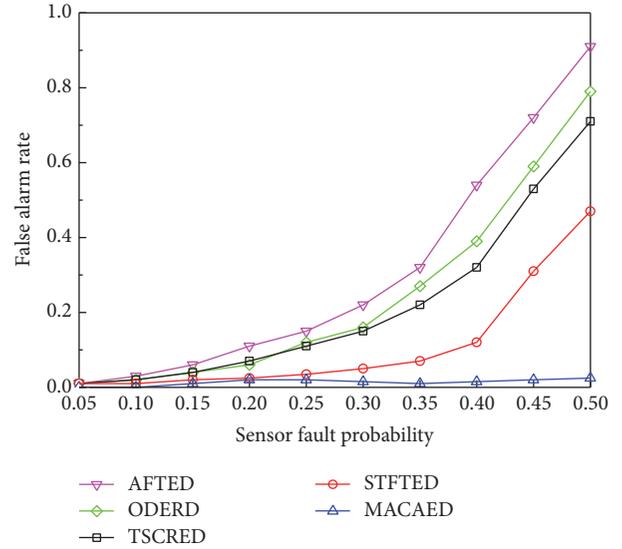


FIGURE 7: False alarm rate of five algorithms.

detection phase. When the node failure rate is greater than 0.3, the detection accuracies of the five algorithms decrease significantly, but the MACAED algorithm is significantly better than the other four algorithms. The reason is that all the five algorithms have the spatial correlation detection stage. With the increase of the failure rate, the faulty nodes are easily affected by the neighbor nodes which have not detected the abnormal events, and they are converted into the normal state, therefore misjudging that no abnormal events occurred.

As for the false alarm rate, these compared results are shown in Figure 7. It can be seen that MACAED has a significantly lower false alarm rate than the other four algorithms as the node failure rate increases. This is due to the fact that MACAED fully considers the impact of attribute correlations on abnormal event detection. By calculating the attribute

TABLE 2: Running time of five algorithms.

Algorithms	Time(s)
AFTED	8.381
ODERD	7.647
TSCRED	7.435
STFTED	10.917
MACAED	12.546

correlation confidence, the fitting degree between the data records and the abnormal event attribute dependency model can be determined, so the abnormal event and interference factor can be distinguished effectively.

The running time of the five algorithms is shown in Table 2.

It can be seen from Table 2 that the MACAED algorithm consumes the longest time. The reason is that the MACAED algorithm needs to train the network structure at the beginning. This process takes about 5 s on average. If the trained network structure is saved as the known result, the detection phase needs  $12.546 - 5 = 7.546$  s, which is very close to TSCRED algorithm and ODERD algorithm.

## 5. Conclusion

In this paper, we present a new approach to detect abnormal events in wireless sensor networks. We construct a dependency model of observed attributes based on Bayesian network and propose a new method to measure the dependency of the attributes. Combining with the temporal correlation detection based on sliding window and the spatial correlation detection based on neighbor node information, the influence of noise and interference event factors on event detection results is effectively reduced. Experimental results show that the algorithm proposed in this paper can effectively eliminate the influence of interference events. It not only reduces the false alarm rate of abnormal events but also improves the accuracy of event detection compared with the other four algorithms.

## Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

## Acknowledgments

This work is sponsored by Innovative Fund Project of Science and Technology Enterprises of Jiangsu Province in China no. BC2014212.

## References

- [1] Y. Zhang, N. Meratnia, and P. Havinga, "Outlier detection techniques for wireless sensor networks: a survey," *IEEE Communications Surveys and Tutorials*, vol. 12, no. 2, pp. 159–170, 2010.
- [2] A. De Paola, S. Gaglio, G. L. Re, F. Milazzo, and M. Ortolani, "Adaptive distributed outlier detection for WSNs," *IEEE Transactions on Cybernetics*, vol. 45, no. 5, pp. 888–899, 2015.
- [3] S.-J. Yim and Y.-H. Choi, "An adaptive fault-tolerant event detection scheme for wireless sensor networks," *Sensors*, vol. 10, no. 3, pp. 2332–2347, 2010.
- [4] Y. Wang, D. Wang, F. Chen, and W. Fang, "Efficient event detection using self-learning threshold for wireless sensor networks," *Wireless Networks*, vol. 21, no. 6, pp. 1783–1799, 2014.
- [5] T. Wu and Q. Cheng, "Online dynamic event region detection using distributed sensor networks," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 50, no. 1, pp. 393–405, 2014.
- [6] F. Li and Z. Feng, "An efficient real-time event detection approach based on temporal-spatial correlations in wireless sensor networks," in *Proceedings of the International Conference on Computer Science and Network Technology (ICCSNT '11)*, pp. 1245–1249, December 2011.
- [7] J. Yin, D. H. Hu, and Q. Yang, "Spatio-temporal event detection using dynamic conditional random fields," in *Proceedings of the 21st International Joint Conference on Artificial Intelligence (IJCAI '09)*, pp. 1321–1326, IEEE, Pasadena, Calif, USA, July 2009.
- [8] K. Liu, Y. Zhuang, Z. Wang, and J. Ma, "Spatiotemporal correlation based fault-tolerant event detection in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 643570, 2015.
- [9] C. Luo, J.-G. Lou, Q. Lin et al., "Correlating events with time series for incident diagnosis," in *Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '14)*, pp. 1583–1592, August 2014.
- [10] K.-Z. Liu, Y. Zhuang, S.-L. Zhou, and S.-J. Liu, "Event detection method based on belief model for wireless sensor networks," *Journal of Beijing University of Posts and Telecommunications*, vol. 38, no. 1, pp. 61–66, 2015.
- [11] D. Heckerman, "Bayesian networks for data mining," *Data Mining and Knowledge Discovery*, vol. 1, no. 1, pp. 79–119, 1997.
- [12] G. F. Cooper and E. Herskovits, "A Bayesian method for the induction of probabilistic networks from data," *Machine Learning*, vol. 9, no. 4, pp. 309–347, 1992.
- [13] IBRL, "Intel Lab Data[EB/OL]," 2004 <http://db.lcs.mit.edu/labdata/labdata.html>.



**Hindawi**

Submit your manuscripts at  
<https://www.hindawi.com>

