

## Research Article

# Traceability and Management Method of Supply Chain Information Based on Wireless Sensor Network

Chao Liu <sup>1</sup> and Tengfei Ma <sup>2,3</sup>

<sup>1</sup>Faculty of Management and Economics, Kunming University of Science and Technology, Kunming, 650093 Yunnan, China

<sup>2</sup>School of Marxism, Yunnan University, Kunming, 650500 Yunnan, China

<sup>3</sup>Development Planning Division, Yunnan Business Vocational College, Kunming, 651701 Yunnan, China

Correspondence should be addressed to Tengfei Ma; [better@ynu.edu.cn](mailto:better@ynu.edu.cn)

Received 27 July 2021; Revised 8 September 2021; Accepted 13 September 2021; Published 16 October 2021

Academic Editor: Zhihan Lv

Copyright © 2021 Chao Liu and Tengfei Ma. 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.

Wireless sensor network is an emerging technology with broad application prospects and will play an increasingly important role in many aspects of people's production practices. This article is aimed at conducting research on supply chain information traceability and management methods from the perspective of wireless sensor networks. This paper uses simulation methods and comparative experiment methods. From the perspective of Spanner algorithm research, the wireless sensor network technology is researched, the explanation and simplification of Spanner algorithm in supply chain information traceability are designed, and the parameters are optimized while the algorithm is optimized. Performance analysis introduced the research on supply chain disturbance management and conducted the reliability analysis of the supply chain trust scale. The experimental results show that among the three dimensions of supply chain information sharing, the reliability coefficients of the two dimensions of information sharing content and information sharing quality are 0.803 and 0.825, respectively, which are both greater than 0.8, indicating that the reliability is very good. Cronbach's coefficient in the information sharing level dimension is equal to 0.665, which is in an acceptable range, the CITC value of this dimension is all higher than 0.4, and the value of the deleted item is lower than 0.665, so all the items of the information sharing level will also be retained. The research of supply chain information traceability and management methods based on wireless sensor network is well completed.

## 1. Introduction

Wireless sensor networks (WSNs) rely on many randomly distributed smart micronodes. These nodes have the characteristics of low power consumption and high flexibility. The nodes work together to complete their processing and processing of data collected during user transmissions. Its tip is a sensor that can perceive and inspect the outside world. The sensors in the WSN communicate wirelessly, so the network settings are flexible, the location of the device can be changed at any time, and it can also be connected to the Internet in a wired or wireless manner [1], a multihop self-organizing network formed by wireless communication. Due to its strong perception, self-organization function, and wireless sensor, it has a wide range of application scenarios and has been successfully integrated into many application

fields such as industrial use, intelligent medical care, and environmental monitoring. Wireless sensor networks create new breakthroughs in social distancing and animal tracking research. The use of EFR32 Flex Gecko SoC-based Wireless Sensor Network equipment for social distancing and animal tracking research is the first to apply IoT technology in this field. Innovative nature observation technology allows simultaneous direct proximity sensing, high-resolution tracking, and remote data download so that their team can collect more data and observations about wild bats. Wireless sensor networks open the door to new areas of scientific knowledge such as the spread of infectious diseases, wildlife resources, foraging strategies, and physiology. In 2040, 10 billion devices will be interconnected through the Internet of Things technology, of which wireless sensor networks are an indispensable part. In recent years, with the

continuous popularization and promotion of the practical application of the Internet of Things worldwide, the wireless sensor network as the basis of the perception of the Internet of Things has achieved unprecedented rapid development [2]. At the same time, in-depth research on wireless sensor networks has been conducted in developed countries such as the United States and Europe. Among them, the United States has injected a large amount of research reserve funds through various methods such as the US Institute of Natural Sciences and the Department of Defense, for example, the COUGAR project of Cornell University and TinyD of Berkeley University in the United States. However, due to the late start of research in our country from abroad, only Harbin Institute of Technology, Heilongjiang University, Zhejiang University, and many other research universities have invested funds for research. In terms of technology development, the key to research around WSNs is the continuous deepening of time synchronization, topology control, positioning technology, MAC protocol, data compression, and network security.

Generally speaking, wireless sensor networks are built in barren areas. Due to the inherent resource constraints of sensor nodes, huge transmission consumption, large-area nodes, and high-density (up to hundreds of nodes) distribution, the “instability” external environment often reads wrong data, fails to transmit, and even comes from malicious element. Wireless sensor network nodes that monitor environmental information in real time can accurately measure environmental parameters and perform reliable transmission, which fully embodies the advantages of digitization, intelligence, and wirelessness between sensors [3]. It is precisely because of the above factors that her perception of data highlights problems such as errors, loss, and abnormalities. Therefore, wireless sensor networks have unreliable characteristics. Not only that, the uncertainty of network attacks makes the security of wireless sensor networks even more worrying. Therefore, there is an urgent need to study the security of wireless sensor networks and more in-depth research on security technologies based on traditional security technology systems to protect the security of wireless sensor networks [4]. In the field of wireless sensor network research, the aspect of security risks which became the main research is direction.

For the key randomization and management scheme, Ren et al. proposed a random key management scheme using the results of random graph theory, which was later regarded as the basic scheme. But their research did not propose an improved algorithm with different shared keys between different nodes [5]. As time goes by, there are fewer and fewer normal working nodes in the sensor network. In order to ensure the normal operation of the network, new nodes must be added in due course. Aiming at the sensor network, an efficient key establishment scheme is proposed. This scheme constructs  $n$  mutually independent subkey pools, and there are associated keys between two adjacent subkey pools. The sensor node deployed for the  $j$ th time only selects the key from the  $j$ th subkey pool. Theoretical analysis and simulation results show that compared with the scheme using a fixed key pool, the survivability of the

scheme is significantly improved. Shaikh et al. proposed an area-based key management for wireless sensor networks based on the E-G scheme and divided the target area and key pool into corresponding small areas to improve the probability of key sharing between nodes. But their research did not solve the problem of wireless sensor network broadcast key distribution protocol based on secret sharing [6]. Rashid et al. proposed a Markov traffic prediction model to determine whether the network has intrusions based on the deviation between the prediction at a certain time and the actual traffic of sensor nodes detected by monitoring. The model does not depend on hardware, and each node can detect independently. But the biggest shortcoming of this model lies in the energy consumption of the nodes [7].

The innovations of this article are as follows. (1) In the methodological description of the research strategy, the whole process of Spanner’s algorithm is simplified, the target variables of Spanner’s algorithm are obtained, and the full text is academically explained. (2) The technical risks of wireless sensors were considered, and the ethical discussion and explanation of the article were carried out. (3) In the analysis part, the influence of trust relationship on the agility of the supply chain is added and a double explanation of the chart is carried out.

## 2. Method of Traceability and Management Method of Supply Chain Information Based on Wireless Sensor Network

*2.1. Definition and Classification of Wireless Sensor Networks.* The wireless sensor network is a multihop self-organizing wireless network without infrastructure composed of a large number of small-sized, energy-limited, and low-cost sensor nodes deployed in the monitoring area [8]. In its operation process, sensor nodes collect information data and perform simple processing and then send the data to the base station [9, 10], and finally, the base station will send the data to the information center after fusion [11]. However, the communication capability of the sensor is very limited. The collected data is not directly sent to the base station [12], but the routing algorithm selects the relay node to transmit to the base station in the form of store and forward [13], as shown in Figure 1.

The wireless network information process diagram is shown in Figure 2.

The standard definition of a sensor is a device that can collect specified measured data and convert it into an identifiable useful signal according to a specific rule. It is generally composed of two parts: a sensitive element and a conversion element [14, 15]. The sensor node is mainly composed of three basic components: one is a sensing component that can convert physical quantities, chemical quantities, or biomass into electrical signals and perform digital processing to obtain data from the physical environment; an information processing component [16], various components on the scheduling equipment coordinate work and data temporary storage; the other is a wireless communication component, which is used to send and receive messages [17]. The

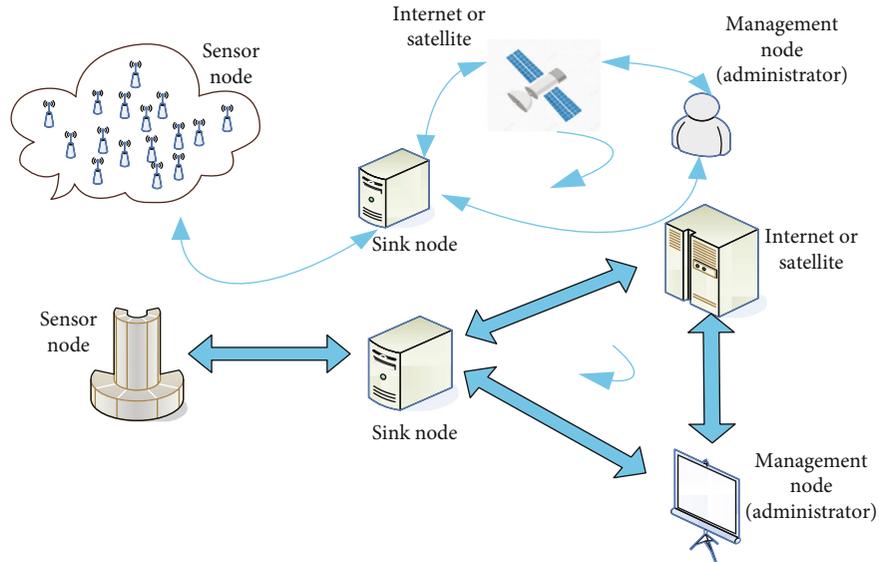


FIGURE 1: Wireless sensor network structure.

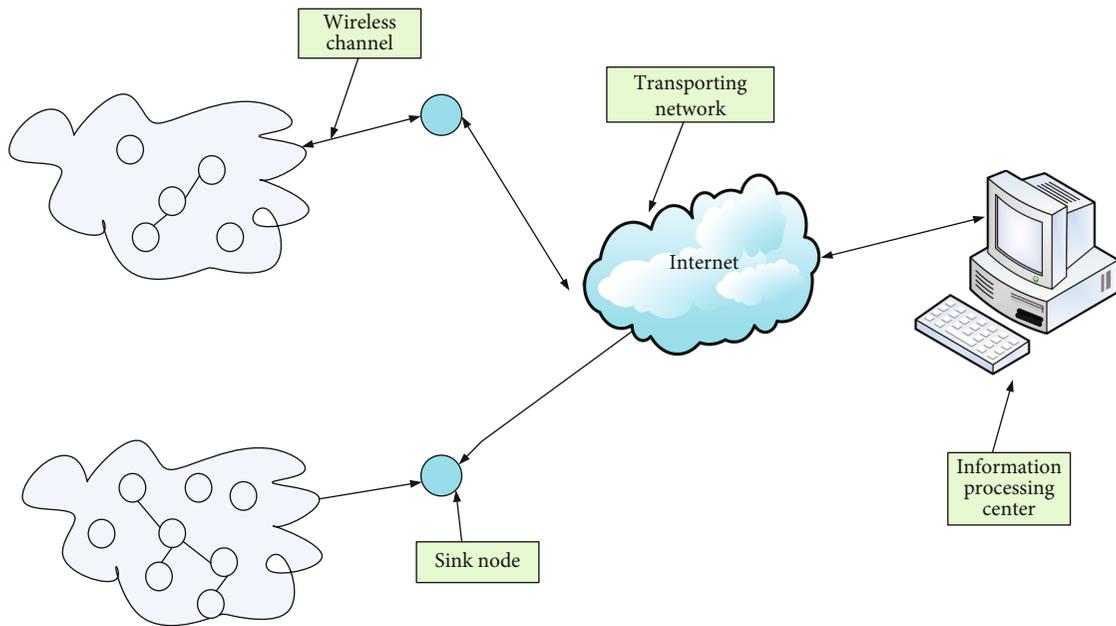


FIGURE 2: Wireless network information process diagram.

acceleration sensor includes a silicon diaphragm, an upper cover, and a lower cover. The diaphragm is located between the upper cover and the lower cover and is bonded together; one-dimensional or two-dimensional nanomaterials, gold electrodes, and leads are distributed on the diaphragm, and adopt pressure welding process to lead wires; industrial field vibration sensor, mainly piezoelectric acceleration sensor. Its working principle is mainly conducive to the piezoelectric effect of the piezoelectric sensitive element to obtain the amount of charge or voltage that is proportional to the vibration or pressure. Industrial scenes typically use an IEPE-type acceleration sensor and a piezoelectric acceleration sensor with a built-in IC circuit. The sensor outputs a

voltage signal proportional to the amount of vibration. In addition, there must be an energy source that provides sensors to perform monitoring tasks. Optional modules include a positioning module used to detect its own location and a mobile module used to change the position of the sensor to improve the accuracy of the perception data [18], as shown in Figure 3.

2.2. *Impact of Trust Relationship on the Agility of the Supply Chain.* Quick response strategy is an important idea in supply chain management. It is based on the goal of meeting customer needs [19]. The key point is to respond quickly to changes in customer needs, and to meet consumer needs

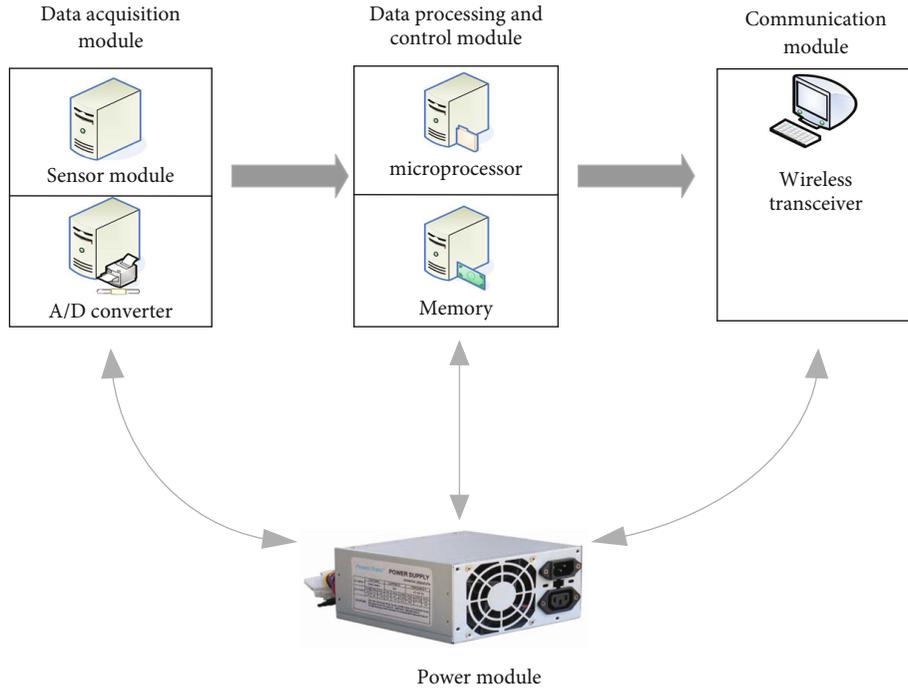


FIGURE 3: Functional structure of the sensor.

with the shortest delivery lead time becomes its essence. The role of supply chain trust relationship in improving the agility of supply chain is mainly reflected in the improvement of ability trust and good faith trust in the rapid response ability of the supply chain and the improvement of customer satisfaction [20, 21]. Trust is a very complex social, economic, and psychological phenomenon. People have discussed trust from many angles such as psychology, sociology, and economics. For example, Shabell believes that “mutual trust is the firm belief of all parties in cooperation that no one party will use the other party’s weaknesses to gain benefits.” Some people think that trust is belief and dependence. For example, Witz believes that trust is the belief of an organization and its needs will be satisfied by the behavior of another partner in the future. Merman believes that trust is dependent on the willingness of trusted trading partners. Arrow pointed out that trust is the lubricant of economic exchanges, and many economic backwardness in the world can ultimately be attributed to a lack of trust. Hesse pointed out that trust is a necessary public virtue in many economic transactions. But Meyer, Dawei, and Scolman believe that “mutual trust means that although one party has the ability to monitor or control the other party, it is willing to give up this ability and believe that the other party will consciously do things that are beneficial to it.”

Supply chain trust can improve the rapid response capability and customer satisfaction of the supply chain through capability trust, thereby improving the agility of the supply chain which can increase by nearly 10% [22]. First, competence trust can enable partners to strictly abide by contract terms and effectively coordinate the inevitable conflicts between supply chain members. The members will develop toward a common goal, which saves time cost and response

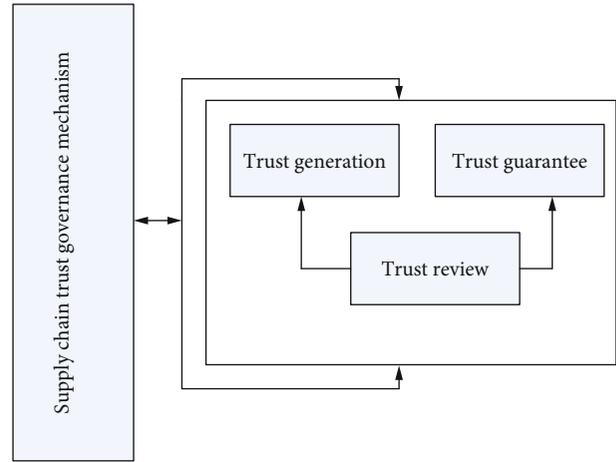


FIGURE 4: Schematic diagram of supply chain structure.

time in the supply chain. In short, the agility of the supply chain is enhanced; the transactions between supply chain enterprises have common standards and specifications, the development of competence trust can prompt partners to comply with requirements, the coordination workload is greatly reduced, and the supply chain can make rapid changes to the environment [23]. Second, the existence of competence trust can prompt enterprises to immediately organize the distribution and production of raw materials after receiving orders and then immediately deliver the finished products to wholesalers and retailers and finally to consumers, so as to satisfy customers. In the demand for product production efficiency, the existence of competence trust can greatly reduce the cost of the production process, consumers can buy more high-quality, inexpensive, and

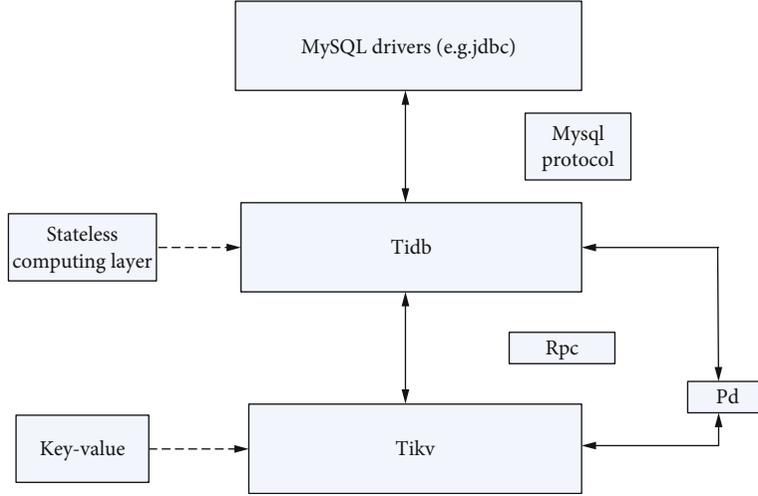


FIGURE 5: Spanner algorithm flowchart.

value-for-money products and services, and their satisfaction will naturally increase significantly [24, 25].

In addition to competence trust, good faith trust can also improve the agility of the supply chain by improving the rapid response capability of the supply chain and customer satisfaction [26]. First of all, good faith trust can go beyond the flexibility of the contract. Partners can give each other an understanding and commitment beyond the contract, and they can negotiate new contract terms when emergencies occur, so as to reduce the number of emergencies. The mutual excuses from time to time [27] make the handling of emergencies more efficient and agile; good faith means flexibility beyond the contract, partners are always ready to help each other in emergency situations, willing to ignore accidental defects, this can promote mutual integration between enterprises, and the rapid response capability of the supply chain is enhanced. Secondly, companies in the supply chain may have speculative behavior for their own interests. The speculative behavior of a single company will have an adverse impact on the entire supply chain. Good faith can effectively eliminate speculative behavior and the uncertainty of partner behavior. Greatly reduced, all companies in the supply chain as a whole can better deal with future uncertainties. The logic diagram of supply chain trust is shown in Figure 4.

**2.3. Introduction to Spanner Algorithm.** There are many technologies involved in wireless sensor network research. Among these technologies, there are network topology control, routing algorithms, flow control, link scheduling, and other technologies. The Spanner algorithm is introduced and summarized here.

The protocol interference model is based on the vulnerability circle capture model and defines a condition for successful communication on a given link. Given a link (or a node), judge whether it is interfered by other links (or nodes) that are transmitting at the same time and what is the degree of interference. The most accurate standard for judging the existence of interference and the degree of inter-

```

1. E := ∅
2. Do if D_G(u, v) > td(u, v)
3. Then add E(u, v) to E
4. End
5. Return G(V, E)
    
```

 ALGORITHM 1: Greedy Spanner original  $(V, t)$  algorithm.

ference is the actual measurement: when possible interference sources send data at the same time and while keeping silent at the same time, measure the throughput rate of the target link (node), respectively; compare the two; if they are the same, then there is no interference; otherwise, there is interference. The ratio of the two is a measure of the degree of interference. The flowchart of the Spanner algorithm is shown in Figure 5.

As shown in the formula,

$$\left| X_k - X_{R(i)} \right| > (1 + \Delta) \left| X_i - X_{R(i)} \right|. \quad (1)$$

According to the definition of the physical interference model, if the SINR at point  $X$  is equal to or greater than a given threshold,  $u$  is a parameter,  $v$  is the speed node,  $x$  and  $y$  correspond to the position of the node, and the others represent various fixed parameters when we run various algorithms, which is

$$\frac{P_i / \left( \left| X_i - X_{R(i)} \right|^n \right)}{\sigma^2 + \sum_{k \in N, k \neq i} \left( P_k / \left( \left| X_k - X_{R(i)} \right|^n \right) \right)} \geq \beta. \quad (2)$$

Define the distance support ratio:

$$\cos t(u, v) = \sum d(x, y). \quad (3)$$

```

1.Input :  $V$  and  $t > 1$ 
2.Output :  $t$ -spanner  $G(V, E)$ 
3.Set  $K :=$  the smaller integer such that  $T = 1/(\cos \theta - \sin \theta)$ 
4. $\theta = 2\pi/k$ 
5. $E := \emptyset$ 
6.For each point  $p \in V$  do
7. $C_1, \dots, C_k :=$  nonoverlapping cones with angle  $\theta$ 
8.With apex at  $P$ 
9.For each cone  $C_i$  do
10.Connect  $P$  to the closest point in  $C_i$ 
11.End
12.End
13.Return  $G(V, E)$ 

```

ALGORITHM 2: Graph algorithm.

Define energy support ratio:

$$\cos t(u, v) = \sum d(x, y)^\alpha. \quad (4)$$

Define the hop support ratio:

$$\cos t(u, v) = \sum d(x, y)^0. \quad (5)$$

Introduce the nature of strong support graphs. When  $H$  is called the additive  $c$ -support graph of  $G$  and  $C$  is called the additive support ratio, it satisfies

$$\cos t_H(u, v) \leq \cos t_G(u, v) + c. \quad (6)$$

When  $H$  is called the  $(c, d)$  support diagram of  $G$ , it satisfies

$$\cos t_H(u, v) \leq c \cdot \cos t_G(u, v) + d. \quad (7)$$

The steps of the Algorithm 1 are as follows.

Let  $p$  be any node on the plane and give a definition

$$C_p : C + p := \{x + p; x \in C\}. \quad (8)$$

The same definition

$$l_{c,p} = l_c + p. \quad (9)$$

The Algorithm 2 of node set  $S$  is as follows.

Use  $q$  and  $q'$  to represent any two nodes in set  $B$ ; then, the following conditions are true.

$$\begin{aligned} |pp'| &\leq \left(\frac{2}{s}\right) |pq|, \\ |p'q'| &\leq \left(\frac{1+4}{s}\right) |pq|. \end{aligned} \quad (10)$$

After the simultaneous equations are used, triangle inequalities can be used to obtain

$$\begin{aligned} |p'q'| &\leq |p'p| + |pq| + |qq'| \\ &\leq \left(\frac{2}{s}\right) |pq| + |pq| + \left(\frac{2}{s}\right) |pq| \\ &\leq \left(\frac{1+4}{s}\right) |pq|. \end{aligned} \quad (11)$$

Finally, by deleting some unnecessary algorithms, plus some more advanced and not cumbersome methods, the code to simplify the WSPD Algorithm 3 is as follows.

The algorithm is simplified, and the experiment is ready to begin.

### 3. Supply Chain Information Traceability and Management Experiment and Analysis Based on Wireless Sensor Network

*3.1. Preinvestigation Analysis Methods and Analysis Results.* Reliability means that the results measured by different items in the scale at different time points are consistent and unbiased. It is a stability indicator. In academic research, the Cronbach  $\alpha$  coefficient is the most commonly used to measure sample reliability. The closer the coefficient value is to 1, the higher the internal consistency reliability. For a scale with ideal reliability, the subscale coefficient should be greater than 0.7, and it is acceptable if it is between 0.6 and 0.7; the reliability factor of the total scale is preferably greater than 0.8, and it is still acceptable if it is between 0.7 and 0.8. If the scale is above 0.9, the reliability of the scale is very good; if the Cronbach coefficient of the subscale is lower than 0.6 or the reliability coefficient of the total scale is lower than 0.8, the items that do not meet the requirements should be deleted or the scale should be revised. In addition to the Cronbach coefficient meeting the requirements, the total correlation coefficient of the corrected item should also be greater than 0.4; otherwise, the item should be deleted until the item meets the requirements of the reliability coefficient and the CITC coefficient. Table 1 is the reliability analysis of the supply chain trust scale.

Table 2 is the overall variable reliability analysis of supply chain trust.

```

1.Input:  $V$  and  $T > 1$ 
2.Output:  $t$  - spanner $G(V, E)$ 
3.Set  $w :=$  WSPD of  $V$  w.r.t.  $s := 4(t+1)/(t-1)$ 
4.Set  $E = \emptyset$ ;
5.For each  $(A_i, B_i) \in W$  do
6.Select an arbitrary node  $U \in A_i$  and a node  $V \in B_i$ 
7.Add edge  $(U, V)$  to  $E$ 
8.End
9.Return  $G(v, E)$ 

```

ALGORITHM 3: WSPD algorithm.

TABLE 1: Reliability analysis of various dimensions of supply chain trust.

Latent variable	Item number	CITC	Deleted	Coefficient of each dimension
Competence trust	CT1	0.604	0.802	0.829
	CT2	0.617	0.798	
	CT3	0.616	0.798	
	CT4	0.610	0.801	
	CT5	0.688	0.777	
Good faith	GT1	0.461	0.695	0.728
	GT2	0.523	0.669	
	GT3	0.414	0.711	
	GT4	0.473	0.688	
	GT5	0.585	0.643	

TABLE 2: Analysis on the reliability of supply chain trust's overall variables.

Latent variable	Item number	CITC	Deleted	Coefficient of each dimension
Supply chain trust	CT1	0.528	0.821	0.836
	CT2	0.569	0.818	
	CT3	0.619	0.813	
	CT4	0.586	0.815	
	CT5	0.591	0.815	
	GT1	0.468	0.829	
	GT2	0.553	0.819	
	GT3	0.387	0.836	
	GT4	0.474	0.826	
	GT5	0.547	0.819	

Using SPSS 24.0 to analyze the reliability of the two dimensions of supply chain trust, the results are shown in the table. The Cronbach  $\alpha$  coefficient values of capability trust and good faith trust are both greater than 0.7, indicating that the reliability is relatively ideal; at the same time, the CITC value is greater than 0.4. In addition, the Cronbach alpha value of the deleted item in the ability trust is not greater than 0.829, and the Cronbach alpha value of the deleted item in the good faith trust is not greater than 0.728, so all items are retained.

Table 3 is the reliability analysis of various dimensions of supply chain information sharing.

Table 4 is the reliability analysis of the overall variables of supply chain information sharing.

Among the three dimensions of supply chain information sharing, the reliability coefficients of the two dimensions of information sharing content and information sharing quality are 0.803 and 0.825, respectively, which are both greater than 0.8, indicating that the reliability is very good. At the same time, the CITC value of both dimensions is above 0.4, and the deleted  $\alpha$  value of the item does not exceed 0.803 and 0.825; therefore, all the items in these two dimensions are retained; the Cronbach coefficient in the information sharing level dimension is equal to 0.665, which is in an acceptable range and this dimension. The CITC values of all are higher than 0.4, and the alpha values of the deleted items are all lower than 0.665, so all the items at the information sharing level will also be retained.

Table 5 is the reliability analysis of supply chain agility.

Table 6 is the KMO value and Bartlett sphere test. Before performing factor analysis on variables, you need to use KMO values to test whether the data is suitable for factor analysis. The value range is from 0 to 1. The closer the value is to 1, the more common factors between variables, and the more suitable for factor analysis.

Exploratory factor analysis of the supply chain trust scale: after the software extracts two common factors, the total variance explained by the software reaches 54.343% > 50%. The rotation component matrix of the trust degree of the supply chain is shown in Table 7.

**3.2. Descriptive Statistical Analysis of Variables.** The descriptive statistical analysis of the variables in this study mainly focuses on the dimensions of supply chain trust, the dimensions of information sharing, and the agility of the supply chain. The distribution of each variable and its dimensions is analyzed by understanding the mean and standard deviation of each variable and its dimensions. The results of descriptive statistical analysis of variables are shown in Figure 6.

The rotation component matrix of the supply chain information sharing scale is shown in Figure 7.

The regression analysis of supply chain information sharing and its dimensions on supply chain agility is shown in Figure 8.

**3.3. Node Failure Types of WSN.** In this paper, MATLAB R2016a is used as the simulation platform. The experiment uses 20 WSN nodes to monitor the ambient temperature and humidity in a certain area. This experiment is carried out in an empty yard. The experimental equipment is selected as the JN5139-Z01-M02 sensor node based on JN5139 chip from Jennic, UK. The node is equipped with temperature and humidity sensor SHT10, power supply module, Zigbee wireless communication module, and low-power MCU. The device follows the IEEE 802.15.4 protocol and is a standardized platform for Zigbee. At the same time, the platform is accompanied by a serial port debugging tool for use. The experimental structure is shown in Figure 9.

TABLE 3: Reliability of supply chain information sharing in all dimensions.

Latent variable	Item number	CITC	Deleted	Coefficient of each dimension
Information sharing level	ISS1	0.409	0.654	0.665
	ISS2	0.610	0.379	
	ISS3	0.422	0.641	
Information sharing content	ISC1	0.551	0.777	0.803
	ISC2	0.529	0.780	
	ISC3	0.629	0.757	
	ISC4	0.554	0.775	
	ISC5	0.606	0.762	
	ISC6	0.504	0.785	
Information sharing quality	ISQ1	0.587	0.800	0.825
	ISQ2	0.640	0.785	
	ISQ3	0.633	0.788	
	ISQ4	0.632	0.787	
	ISQ5	0.615	0.792	

TABLE 4: Supply chain information sharing overall variable reliability.

Latent variable	Item number	CITC	Deleted	Coefficient of each dimension
Supply chain information sharing	ISS1	0.630	0.887	0.896
	ISS2	0.587	0.889	
	ISS3	0.521	0.892	
	ISC1	0.582	0.890	
	ISC2	0.529	0.892	
	ISC3	0.586	0.889	
	ISC4	0.584	0.889	
	ISC5	0.651	0.886	
	ISC6	0.598	0.888	
	ISQ1	0.524	0.891	
	ISQ2	0.610	0.888	
	ISQ3	0.602	0.889	
	ISQ4	0.648	0.887	
	ISQ5	0.575	0.890	

TABLE 5: Supply chain agility reliability.

Latent variable	Item number	CITC	Deleted	Coefficient of each dimension
Supply chain agility	AS1	0.683	0.854	0.875
	AS2	0.662	0.857	
	AS3	0.62	0.861	
	AS4	0.636	0.859	
	AS5	0.560	0.868	
	AS6	0.706	0.852	
	AS7	0.590	0.864	
	AS8	0.623	0.860	

During the experiment, 20 nodes were selected to collect experimental data. Due to the particularity of the experiment, some artificial faults were set up for some nodes. Four normal nodes, 4 nodes lacking power supply, 4 temperature

and humidity sensor module failure nodes, 4 processor module failure nodes, and 4 communication module failure nodes are included. The 20 fault sample information decision table collected is shown in Table 8. Cronbach's coefficient (Cronbach's  $\alpha$ ) is a statistic that refers to the average of the half-reliability coefficients obtained by all possible item division methods of the scale and is the most commonly used reliability measurement method. It was first named by American educator Lee Cronbach in 1951, where  $K$  is the number of samples,  $\sigma^2 X$  is the variance of the total sample, and  $\sigma^2 Y_i$  is the variance of the currently observed sample.

Since the failure of WSN is always accompanied by the appearance of multiple signs, the article analyzes based on experience and some mechanisms and finally selects the following characteristic parameters related to the failure to construct the fault information table: issue multiple query commands whether the tested node responds; whether the

TABLE 6: KMO and Bartlett test results.

Scale	KMO	Approximate chi-square	Df	Sig
Supply chain trust	0.828	329.404	45	0.000
Supply chain information sharing	0.847	663.350	91	0.000
Supply chain agility	0.870	329.286	28	0.000

TABLE 7: Rotating component matrix of supply chain trust scale.

Supply chain trust	Ingredient	
	1	2
CT1	0.781	0.093
CT2	0.732	0.207
CT3	0.714	0.290
CT4	0.686	0.269
CT5	0.787	0.180
GT1	0.238	0.600
GT2	0.326	0.621
GT3	0.048	0.682
GT4	0.189	0.658
GT5	0.192	0.751

tested node regularly returns signals; whether the tested node can correctly execute the command sent by the sink node; whether the temperature and humidity values returned by the tested node are far from the normal value; whether the temperature and humidity values returned by the tested node are always 0; whether the tested node can correctly transmit other node information; whether the tested node has temperature and humidity return values; and change the transmission frequency and issue the inquiry command again, whether the tested node responds.

The reduced WSN node failure sample decision table is shown in Table 9.

According to the reduced fault sample decision table and the above classification algorithm, MATLAB is used to simulate the fault diagnosis of WSN. The real experiment was completed in our experimental scene yard, and the simulation experiment was performed in a virtual scene. The artificially added noise can make the experiment obtain more data. If the experiment obtains more data, the reliability will be improved and increase. Since WSNs are generally used in complex environments, shortwave channels are susceptible to interference from meteorological conditions and changes in ionospheric state. At the same time, some factors such as noise will cause a certain deviation in the data obtained by the node. A certain amount of noise is added in the simulation process to make the data reliability 80%. Five randomly selected test samples affected by noise are shown in Figure 10.

Table 10 shows the actual diagnosis results.

When only the rough set is used to diagnose the fault of WSN, the diagnosis results of two of the five test samples are different from the actual fault of the sample, and the correct rate is only 60%. It can be seen that the generalization ability

and fault tolerance ability of rough set are relatively weak, it is more sensitive to noise, and it is prone to misjudgment. Therefore, this paper will adopt the method of least squares support vector machine combined with rough set theory to diagnose the fault of WSN and improve the generalization ability and fault tolerance of the diagnosis system. The columns of Tables 8 and 9 represent 20 WSN nodes, and the rows represent different faults. Table 10 shows the experimental results completed on their basis.

Real-time data collection and management of the Internet of Things is shown in Figure 11.

The detection accuracy rates of SVM, PCA+SVM, AE+SVM, and SAE+SVM are listed. In the experiment, the trial and error method is used to determine the number of nodes in each output layer, and at the same time, set the initial value of the hidden layer node number to 35; through the application of different classification algorithms, SVM is only suitable for tasks with small batches of samples and cannot accommodate tasks with millions or even hundreds of millions of samples. The difference is that the application of PCA+SVM is to add PCA to our experiment; the purpose is to help us. You can see how this algorithm is strengthened in SVM in this experiment and how much is strengthened and gradually decrease to 10 according to the step size 5 to preliminarily judge the detection accuracy of a certain area, as shown in Figure 12.

The comparison of F1 after AE and SAE compression is shown in Figure 13.

## 4. Discussion of the Method

*4.1. Research Content of Supply Chain Disturbance Management.* Supply chain disruption management studies the disturbance problem in the supply chain field. The frequency of disturbance factors will increase with the trend of complex supply chain network structure. Disturbances in a certain link of the supply chain will spread along the network. In the "Internet +" era, this influence will be within the scope of the global supply chain network. Dissemination is a new challenge to supply chain management research.

Supply chain disturbance management mainly studies system disturbances caused by uncertain factors such as equipment failure, interruption of raw material supply, surge in scarce resource prices, and drastic changes in demand. Numerous and complex disturbance factors have caused the actual operating status of the supply chain network to deviate from the established state and even risk that the original plan needs to be terminated. In view of this, effective measures should be taken immediately after the disturbance factor occurs to reduce or eliminate the negative impact of the disturbance event on the system. The goal of disturbance

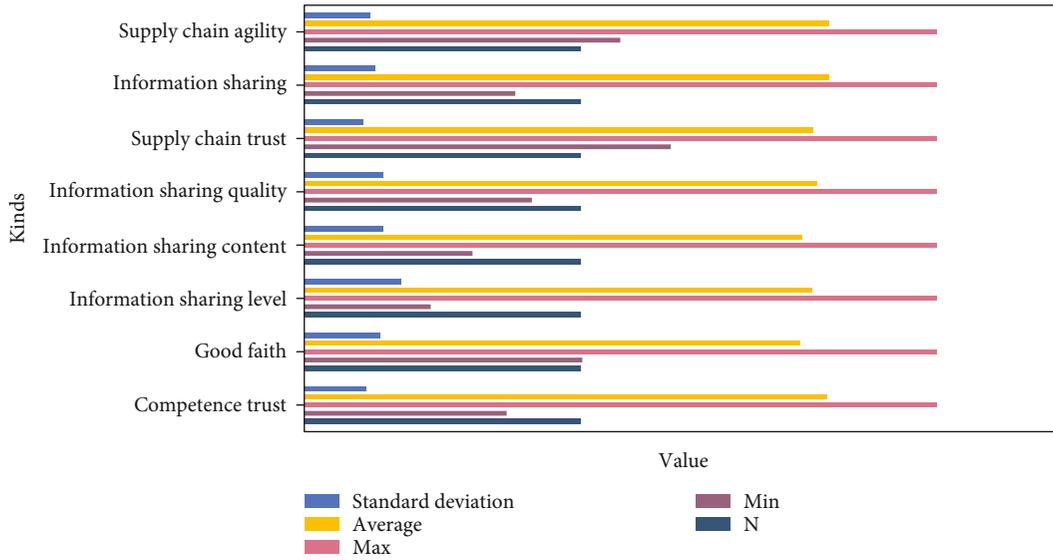


FIGURE 6: Descriptive statistical analysis results of variables.

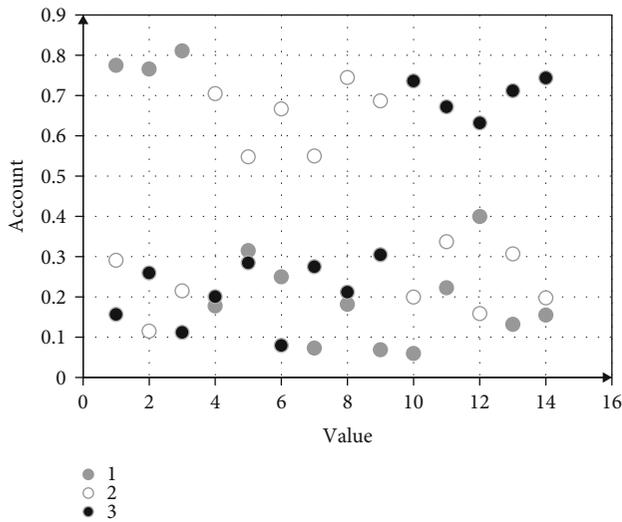


FIGURE 7: Rotating component matrix of supply chain information sharing scale.

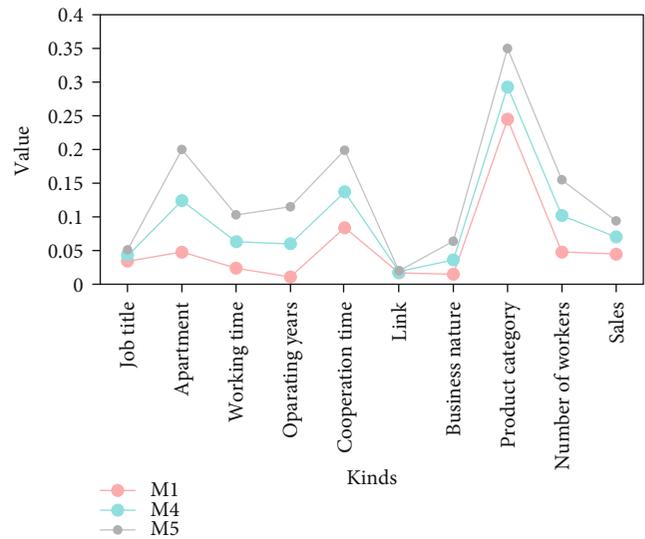


FIGURE 8: Supply chain information sharing and regression analysis of its dimensions on supply chain agility.

management is to minimize losses through various measures so that the supply chain system continues to operate smoothly. There are numerous successful cases of disturbance management. For example, in the field of electronic communication, Philips’s smart chip factory caught fire in the early years, which caused Nokia and Ericsson downstream of the supplier to suffer the same disturbance, but the two took different measures. The disturbance response strategy of Nokia has greatly increased the market share of Nokia, while Ericsson lost 1.68 billion U.S. dollars. In the field of disturbance management, scholars at home and abroad have established a large number of adaptive disturbance factor models based on the characteristics of disturbance events. Specifically, they can be divided into two categories, network graph models and mathematical models.

The advantage of the network graph model is that it is clear at a glance and has good intuition and comprehensibility. The main disadvantage is that the model has fewer parameters, which is very troublesome to solve and is not suitable for studying complex problems. The mathematical model can overcome the above shortcomings of the network graph model, so it has a very wide range of applications.

4.2. Sources of Cost Disturbance. The cost of a supply chain network node enterprise (cost) refers to the sum of various costs incurred in the process of providing products and services to consumers. Supply chain costs have evolved from the early distribution costs. With the process of global economic integration, the business volume involved in the supply chain has continued to increase, and the concept of



FIGURE 9: Experimental structure.

TABLE 8: WSN node failure sample decision table.

Sample U	Attribute type								Type F
	M1	M2	M3	M4	M5	M6	M7	M8	
X1	1	1	1	1	1	1	1	1	D1
X2	0	1	0	1	0	0	1	1	D1
X3	1	1	1	1	1	1	1	1	D1
X4	0	1	0	1	0	0	1	1	D1
X5	0	0	0	0	0	0	0	0	D2
X6	0	0	0	0	0	0	0	0	D2
X7	0	0	0	0	0	0	0	0	D2
X8	0	0	0	0	0	0	0	0	D2
X9	1	1	1	0	0	1	1	1	D3
X10	1	1	1	0	0	1	1	1	D3
X11	1	1	1	1	0	1	1	1	D3
X12	1	1	1	1	0	1	1	1	D3
X13	1	1	0	1	1	1	1	1	D4
X14	1	1	0	1	1	1	1	1	D4
X15	1	1	0	1	1	1	1	1	D4
X16	1	1	0	1	1	1	1	1	D4
X17	0	1	0	1	0	0	0	0	D5
X18	0	1	0	1	1	0	1	0	D5
X19	0	1	0	1	0	0	0	0	D5
X20	0	1	0	1	1	0	1	0	D5

supply chain costs has gradually matured. Supply chain cost is a very important source of supply chain disturbance factors, scholars have experienced a long time to understand it, and the research on supply chain cost has also developed in the direction of multipolarization. Regarding the composition of supply chain costs, researchers have expressed their opinions. The cost management of most node enterprises only stays at the internal cost including direct cost and indirect cost. Due to the complexity and interrelationship of the supply chain network, the total cost of the supply chain should also include the transaction costs of finished product transactions and information exchanges between various node enterprises. Therefore, based on previous studies, supply chain costs should include the following three aspects: (1) direct costs, (2) indirect costs, and (3) transaction costs.

Uncertainty in the supply chain will cause demand disturbances. In actual operations, factors such as the rapid

TABLE 9: Simplified WSN node failure sample decision table.

Sample U	Attribute type				Type F
	M3	M4	M5	M8	
X1	1	1	1	1	D1
X2	0	1	0	1	D1
X3	1	1	1	1	D1
X4	0	1	0	1	D1
X5	0	0	0	0	D2
X6	0	0	0	0	D2
X7	0	0	0	0	D2
X8	0	0	0	0	D2
X9	1	0	0	1	D3
X10	1	0	0	1	D3
X11	1	1	0	1	D3
X12	1	1	0	1	D3
X13	0	1	1	1	D4
X14	0	1	1	1	D4
X15	0	1	1	1	D4
X16	0	1	1	1	D4
X17	0	1	0	0	D5
X18	0	1	1	0	D5
X19	0	1	0	0	D5
X20	0	1	1	0	D5

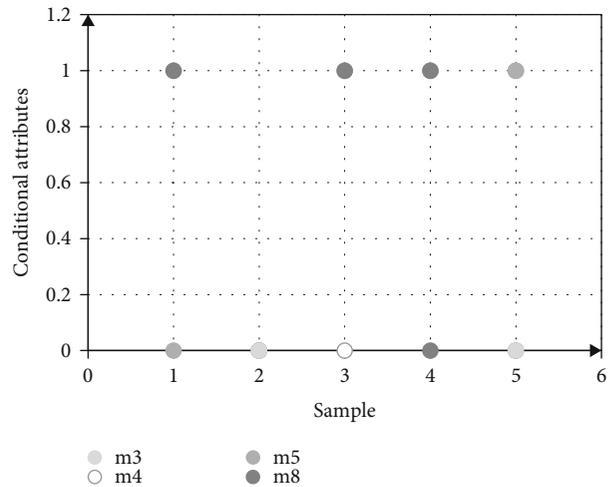


FIGURE 10: Test samples affected by noise.

changes in the market environment and the internal innovative technologies of node enterprises will affect market demand to a certain extent. Chen Ting [23] pointed out in the research that the demand disturbance factors refer to the frequency of their occurrence, and the specific impact on demand and the timeliness and urgency of calming disturbances can be divided into frequent demand disturbances and sudden demand disturbances.

New and traditional disturbance factors together constitute a typical frequent demand disturbance factor, among which traditional demand fluctuation factors include commodity price and quality, seasonal products, and the

TABLE 10: Comparison of fault diagnosis results.

Failure sample	Diagnostic result	Sample actual failure
1	D3 (sensor module failure)	D1 (no failure)
2	D2 (power module failure)	D2 (power module failure)
3	Unknown fault	D3 (sensor module failure)
4	D4 (handle module failure)	D4 (handle module failure)
5	D5 (wireless communication module failure)	D5 (wireless communication module failure)

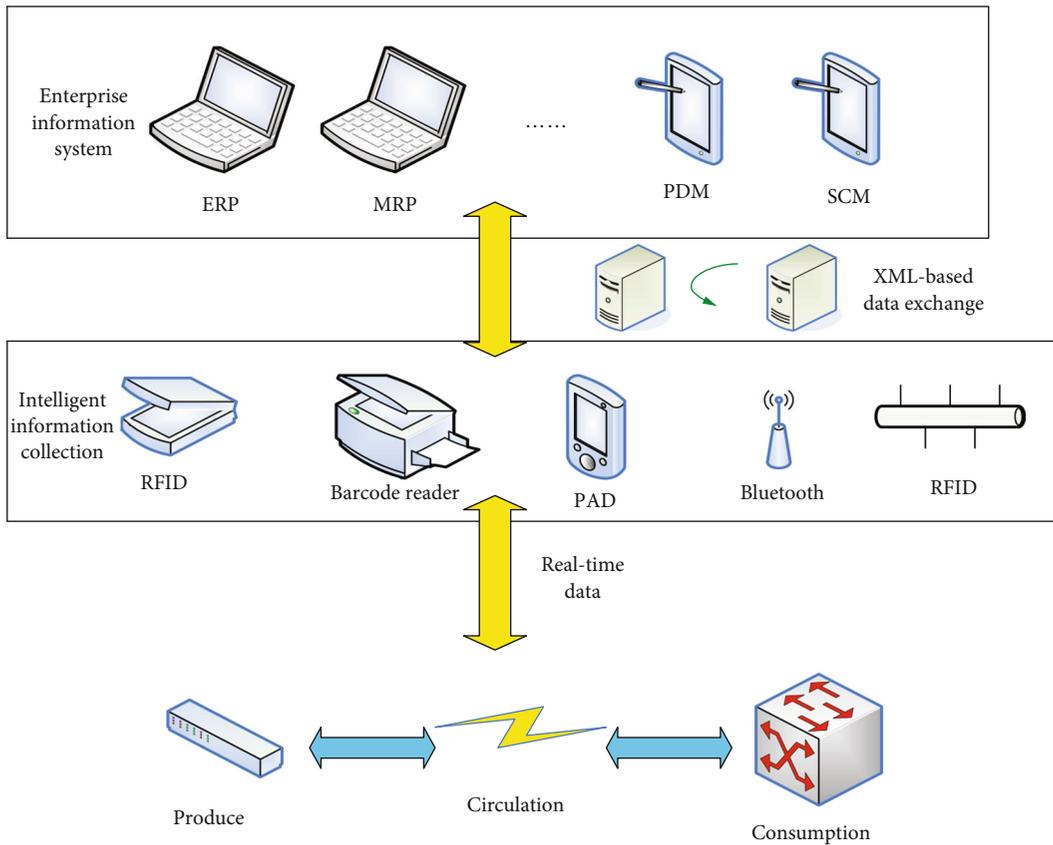


FIGURE 11: Real-time data collection and management of the Internet of Things.

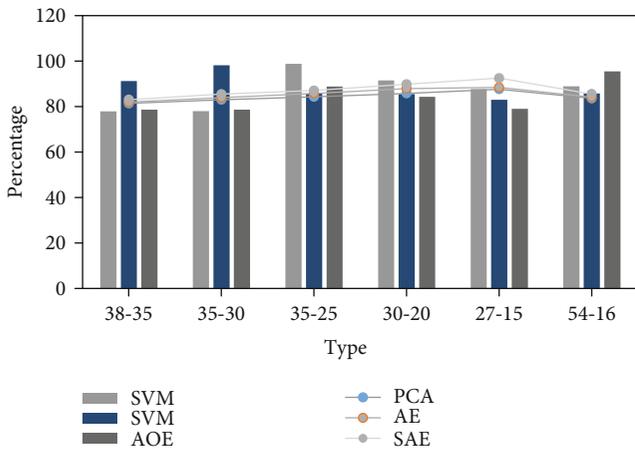


FIGURE 12: Comparison of accuracy of different classification methods.

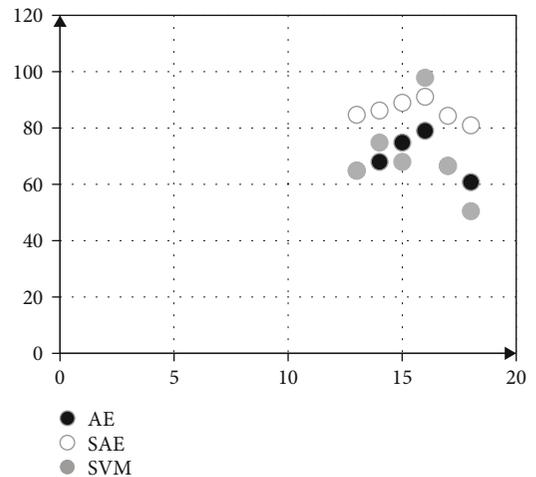


FIGURE 13: AE and SAE compressed F1 comparison (%).

correlation between commodity demand, such as mutual substitutes and complementary products. Corresponding to the traditional demand disturbance factors, the new demand disturbance factors are determined by the characteristics of consumers in the “Internet +” era. The vastly different psychological needs between consumers have led to increasingly prominent individual requirements for goods and services. Many new standards and requirements have been added in the process of selecting goods and receiving services, such as safe, fast, and thoughtful supply requirements, green health, low-carbon environmental protection requirements, and differentiated needs of ordinary goods to meet the psychological changes of different consumers. Sudden demand disturbances refer to demand fluctuations caused by emergencies, such as large-scale infectious diseases, earthquakes and other unexpected events, and financial crises.

*4.3. RFID Technology.* In the application of wireless network, the reader sends a radio frequency signal of a specific frequency through the transmitting antenna. When the electronic tag enters the effective working area, an induced current is generated, thereby obtaining energy to be activated so that the electronic tag transmits its own coded information through the built-in antenna. The receiving antenna of the reader receives the modulated signal sent from the tag and transmits it to the signal processing module of the reader via the modulator of the antenna. After demodulation and decoding, the effective information is transmitted to the background host system for relevant processing. Logic operations identify the identity of the tag, make corresponding processing and control for different settings, and finally send a signal to control the reader to complete different read and write operations. RFID technology is called radio frequency identification technology in Chinese, and it is a noncontact identification technology. It uses radio frequency signals to automatically identify targets and obtain relevant data. The identification does not require human intervention. It can work in various environments and has been widely used in the field of food traceability. RFID systems generally include data processing systems, tags (tag or transponder) and readers (interrogator or reader). Tags are generally composed of modulators, antennas, encoders, and storage units. The readers are mainly composed of antenna control units and radio frequency transceiver modules. The control modules usually include decoding and error correction circuits, amplifiers, clock circuits, microprocessors, and power supplies. The working principle of RFID is when the tag enters the magnetic field, when the reader receives a special frequency signal, the tag will send out the product information in the chip through the energy obtained by the induction current, the reader reads the information, and after being decoded, it is sent to the computer information processing system for relevant data processing.

Compared with barcode technology, RFID has its unique functions. RFID tags can store a large amount of data and can read multiple tags at a time, and the reading distance can be extended to several meters or tens of meters and is not affected by harsh environments such as rain, oil stains, and dust. Based on various advantages, RFID has been

widely used since its appearance. It has been used in logistics management, ID cards, passes, baggage sorting, all-in-one cards, electronic toll collection, access control systems, livestock or wild animal identification, electronic medical records, and other fields. RFID has also been widely used in food traceability systems.

## 5. Conclusions

The experimental results show that the research of supply chain information traceability and management method based on wireless sensor network proposed in this paper has better statistical effect and more comprehensive statistics than traditional supply chain information traceability management methods. The article adds a description of the research content of supply chain disturbance management, the source of cost disturbances, and RFID technology. In terms of simplification and explanation of the algorithm, the Spanner algorithm is simplified to make the information traceability and fusion rate of this article better. This paper uses simulation method and comparative experiment method to carry out the reliability analysis of the supply chain trust scale. First, formulate IoT strategic planning, industrial policies, and related laws and regulations to define and plan the content of all aspects of the IoT industry from the national strategic planning level. The overall strategy for the development of the Internet of Things in my country is to drive industrial development with technological innovation, keep up with the pace of the development of the international Internet of Things industry and technology, and strengthen the research on cutting-edge technologies of the Internet of Things. Analyze the advantages and disadvantages of the development of my country's Internet of Things industry; clarify the status, role, and relationship of upstream and downstream enterprises in the Internet of Things industry; and promote the construction of infrastructure and the formulation of subsequent supporting policies. The development of the Internet of Things is ultimately to be applied to all aspects of life, and a sound legal system not only provides a good order for the development of the Internet of Things but also provides a guarantee for the development of the Internet of Things. Second, establish independent standards for the Internet of Things as soon as possible to improve my country's right to speak in the field of international Internet of Things. In the two information revolutions of computers and the Internet, it is precisely because of China's weak right to speak in the formulation of international standards that it has led to passivity. In the information revolution of the Internet of Things, we must learn lessons and establish independent standards for the Internet of Things as soon as possible. Coordinate and integrate the strength of relevant domestic standards organizations, speed up the formulation and improvement of various IoT technical standards in line with my country's national conditions, and build an open-architecture IoT standard system. It is necessary to advance and be compatible with international standards, but also to maintain its core competitiveness, develop core technologies, open up the international market, and infiltrate China's own standards

into the development of the Internet of Things in other countries. Actively participate in the work of international standard proposals, strive to lead the formulation of international standards for the Internet of Things, in order to grasp the initiative of industrial development, and enhance my country's international competitiveness and voice in the field of Internet of Things. The experimental results show that among the three dimensions of supply chain information sharing, the reliability coefficients of the two dimensions of information sharing content and information sharing quality are 0.803 and 0.825, respectively, which are both greater than 0.8, indicating that the reliability is very good. The shortcomings of this article are as follows. (1) The amount of data collected in the sample is relatively limited. In future research, the experimental sample can be expanded to obtain the credibility of the research results. (2) The Spanner algorithm designed in this paper does not have separate control variables in the process of simplifying the algorithm. Although the actual experimental results did not have an impact, the reliability of the algorithm should be more rigorously studied in future research.

### Data Availability

No data were used to support this study.

### Conflicts of Interest

There are no potential competing interests in our paper.

### Authors' Contributions

All authors have seen the manuscript and approved to submit to your journal.

### References

- [1] Z. Cai and Z. He, "Trading private range counting over Big IoT data," in *The 39th IEEE International Conference on Distributed Computing Systems (ICDCS 2019)*, 2019.
- [2] M. Jahanbakht, W. Xiang, L. Hanzo, and M. R. Azghadi, "Internet of Underwater Things and big marine data analytics – a comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 904–956, 2021.
- [3] Y. Sun, H. Song, A. J. Jara, and R. Bie, "Internet of things and big data analytics for smart and connected communities," in *IEEE Access*, vol. 4, pp. 766–773, 2016.
- [4] X. Zheng and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial IoTs," *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 38, no. 5, pp. 968–979, 2020.
- [5] J. Ren, Y. Zhang, K. Zhang, A. Liu, J. Chen, and X. S. Shen, "Lifetime and energy hole evolution analysis in data-gathering wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 2, pp. 788–800, 2016.
- [6] F. K. Shaikh and S. Zeadally, "Energy harvesting in wireless sensor networks: a comprehensive review," *Renewable and Sustainable Energy Reviews*, vol. 55, no. 3, pp. 1041–1054, 2016.
- [7] B. Rashid and M. H. Rehmani, "Applications of wireless sensor networks for urban areas: a survey," *Journal of Network & Computer Applications*, vol. 60, no. 2, pp. 192–219, 2016.
- [8] N. Kapileswar and H. Gerhard, "A survey on urban traffic management system using wireless sensor networks," *Sensors*, vol. 16, no. 2, pp. 157–178, 2016.
- [9] H. Jawad, R. Nordin, S. Gharghan, A. Jawad, and M. Ismail, "Energy-efficient wireless sensor networks for precision agriculture: a review," *Sensors*, vol. 17, no. 8, pp. 1781–1792, 2017.
- [10] J. Luo, J. Hu, and R. L. Di Wu, "Opportunistic routing algorithm for relay node selection in wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 1, pp. 112–121, 2015.
- [11] C. Benzaid, K. Lounis, A. Al-Nemrat, N. Badache, and M. Alazab, "Fast authentication in wireless sensor networks," *Future Generation Computer Systems*, vol. 55, no. 2, pp. 362–375, 2016.
- [12] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An efficient distributed trust model for wireless sensor networks," *IEEE Transactions on Parallel & Distributed Systems*, vol. 26, no. 5, pp. 1228–1237, 2015.
- [13] I. Cardei and M. Cardei, "Energy-efficient connected coverage in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8449–8462, 2016.
- [14] R. Amin and G. P. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," *Ad Hoc Networks*, vol. 36, no. 1, pp. 58–80, 2016.
- [15] H. Zhang, H. Xing, J. Cheng, A. Nallanathan, and V. C. M. Leung, "Secure resource allocation for OFDMA two-way relay wireless sensor networks without and with cooperative jamming," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 5, pp. 1714–1725, 2016.
- [16] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, "A survey on software-defined wireless sensor networks: challenges and design requirements," *IEEE Access*, vol. 5, no. 9, pp. 1872–1899, 2017.
- [17] M. Dong, K. Ota, and A. Liu, "RMER: reliable and energy-efficient data collection for large-scale wireless sensor networks," *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 511–519, 2016.
- [18] L. Guo, Y. Li, and Z. Cai, "Minimum-latency aggregation scheduling in wireless sensor network," *Journal of Combinatorial Optimization*, vol. 31, no. 1, pp. 279–310, 2016.
- [19] K. D. Wowak, C. W. Craighead, and D. J. Ketchen, "Tracing bad products in supply chains: the roles of temporality, supply chain permeation, and product information ambiguity," *Journal of Business Logistics*, vol. 37, no. 2, pp. 132–151, 2016.
- [20] T. Djabatna and A. Ginantaka, "Traceability of information routing based on fuzzy associative memory modelling in fisheries supply chain," *International Journal of Fuzzy Systems*, vol. 22, no. 2, pp. 373–416, 2019.
- [21] R. Vikaliana, R. Rasi, and I. N. Pujawan, "Traceability system on mangosteen supply chain management using blockchain technology: a model design," *Studies of Applied Economics*, vol. 39, no. 4, pp. 99–101, 2021.
- [22] K. Yang, D. Forte, and M. M. Tehranipoor, "CDTA," *ACM Transactions on Design Automation of Electronic Systems*, vol. 22, no. 3, pp. 1–31, 2017.
- [23] C. Y. Liu and C. Y. Lee, "Multiple supply chain adoption under uncertainty," *International Journal of Physical Distribution & Logistics Management*, vol. 49, no. 3, pp. 305–326, 2019.

- [24] Q. Lu and X. Xu, "Adaptable blockchain-based systems: a case study for product traceability," *IEEE Software*, vol. 34, no. 6, pp. 21–27, 2017.
- [25] M. L. Deng and P. Feng, "Research on a traceability scheme for a grain supply chain," *Journal of Sensors*, vol. 2021, Article ID 8860487, 9 pages, 2021.
- [26] Y. C. Liu, "Development and applications of mobile farming information system for food traceability in health management," *Applied Computing in Medicine & Health*, vol. 2, no. 8, pp. 244–268, 2016.
- [27] S. Al-Farsi, M. M. Rathore, and S. Bakiras, "Security of blockchain-based supply chain management systems: challenges and opportunities," *Applied Sciences*, vol. 11, no. 12, pp. 5585–5585, 2021.