Hindawi
Mobile Information Systems
Volume 2022, Article ID 3580607, 10 pages
https://doi.org/10.1155/2022/3580607

Research Article

Low-Energy Data Fusion Privacy Protection Algorithm for Three-Dimensional Wireless Sensor Network

Limin Feng[1,2,3] and Bo Liu[4]

[1]*School of Computer and Artificial Intelligence, Wuhan Textile University, Wuhan 430200, China*
[2]*Hubei Garment Information Engineering Technology Research Center, Wuhan 430200, China*
[3]*Hubei Engineering Research Center for Intelligent Textile and Garment, Wuhan 430200, China*
[4]*Network and Computing Center of Huazhong University of Science and Technology, Wuhan 430030, China*

Correspondence should be addressed to Limin Feng; 2006291@wtu.edu.cn

Received 1 January 2022; Revised 23 February 2022; Accepted 3 March 2022; Published 26 March 2022

Academic Editor: Ateeq Rehman

Wireless sensor networks are now widely used in a variety of fields. It has the advantages of being low cost, practical, and adaptable. Methods of data fusion can help to increase efficiency. However, in the process of information transmission, once some nodes are invaded, the privacy of data will be threatened. Therefore, the research on its data privacy protection technology is very important. Under the premise of ensuring data privacy, existing data fusion methods of this type complete data fusion by preventing other nodes from knowing the private data collected by sensor nodes. Research on the current hot issues of data fusion privacy protection improves the shortcomings of traditional data fusion privacy protection technology and proposes an improvement, innovation, and three-dimensional space-oriented wireless sensor network low-energy data fusion privacy algorithm LEC-CPDA. Through simulation experiments and theoretical analysis, it is concluded that the LEC-CPDA algorithm can significantly improve the protection of privacy and improve the accuracy of data fusion.

1. Introduction

At present, the Internet of Things (IoT) is very popular in many fields, and there has been in-depth research. Industrial monitoring, intelligent transportation, environmental monitoring, and other fields have tried IoT applications. Through the integration of sensor, embedded computing, distributed information processing, and communication technologies that based on a large number of nodes scattered in the environment, the wireless sensor network (WSN) performs real-time monitoring and perception, to collect useful, detailed, and accurate information, and the collected information can be used for analysis and processing. Therefore, through WSN, a large amount of detailed and reliable field information (such as national defense and military, environmental monitoring, traffic management, and medical health) can be obtained anytime and anywhere. In the transmission of information on the IoT, the protection of information privacy is of utmost importance. Especially when it comes to some sensor terminals in the country and the collected sensitive data information, these need to be protected more. Not only do the terminal and the collected data need to be encrypted and protected but also in the process of data processing. Typical applications in this area are behavior analysis based on data mining. Therefore, it is urgent to solve the problem of data privacy protection in the Internet of Things. Only, in this way, this technology is more maturely used in practice. Currently, with the deepening of research, there are many and various privacy protection data fusion methods that are proposed by researchers related to WSN. In the process of data fusion, not only the efficiency but also the privacy protection of fusion needs to be considered. In terms of privacy protection, some encryption techniques are used. Literature [1–3] gives an overview of security issues in WSN data fusion. Privacy protection and data fusion algorithms are divided into two types including nonencrypted and encrypted data fusion algorithms. Most of the early research focuses on nonencrypted data fusion algorithms, using data modification operations to hide the original data, but privacy protection is not ideal. End-to-end encryption and hop-by-hop encryption are two main methods of encryption-based privacy protection data fusion schemes. Among them, end-to-end refers to the establishment of a secure link between each node and the base station node. The private data of each node is encrypted and then sent upwards.

After the base station node obtains the encrypted packet, it extracts the real data through the key negotiated with each node. In this way, the intermediate node remains transparent during the entire communication process. However, this method generally cannot achieve data fusion. At the same time, the disadvantage of this type of method is that the nodes close to the base station have too frequent transmission operations, which makes them have excessive energy loss and low communication efficiency. The privacy protection scheme proposed in the literature [4, 5] solves these problems to a certain extent. They implement end-to-end fusion encryption by introducing homomorphic encryption technology so that data can be directly fused without decryption. Another hop-by-hop encryption method is that each node first decrypts the received merged data packet, then merges it with the original data, then encrypts it, and finally merges it upwards. The encryption and decryption processes are based on the abovementioned specific key distribution scheme. A data fusion algorithm based on hop-by-hop encryption is proposed in the literature [6–9]. This method has an intermediate decryption process in the fusion process. It can be seen that its privacy protection is weaker than the first method. Literature [10] addresses some shortcomings of the end-to-end method. For intrusion detection and privacy protection, literature [11] proposed a unified fusion algorithm. He et al. [7] proposed the privacy-preserving data aggregation privacy protection data fusion scheme by studying the additive fusion function sum. The scheme includes Cluster-Based Private Data Aggregation (CPDA) and Slice Mix Aggregate (SMART) algorithm. CPDA is based on the idea of algebraic operations and adopts the method of introducing noise for privacy protection; SMART uses the method of shuffling fragments for privacy protection. Although the topological structure of the two methods is not the same (CPDA is based on a cluster structure, while SMART is a tree topology), both of them use the TAG (tiny aggregation) [12] tree model to complete the data transfer task to the base station. By combining the data fusion method with data and node-to-node encryption and decryption method, the SMART prevents attacks from external intruders, ensures the accuracy of the data fusion results, and obtains private data for the internal trusted nodes and QS. It is computationally expensive for CPDA. Also, it is heavy of data communication for SMART data communication. Not only that, it is sensitive to data loss, and it takes a lot of time to get relatively good accuracy. A privacy protection method based on complex number domain data fusion under a tree topology was proposed [13].

Characteristics of the data fusion tree frame are used to compress the communication overhead that is used to reduce energy [14]. Based on query server and multilayer query, [15] proposed a privacy protection data fusion method. According to different security requirements, this method divides the query into different levels and establishes a hierarchical network model. Many improved methods for SMART such as energy-efficient and high-accuracy secure data aggregation (EEHA) [16] and energy-saving privacy-preserving data aggregation (ESPART) [8] have been proposed. By adding 5 types of optimization factors, a high-accuracy and privacy-preserving oriented data aggregation (P-SMART-CLPNT) [17] was proposed. It improved the accuracy of data fusion, reduced the data collision rate, and decreased the possibility of data loss due to collision. Compared with the SMART method, it has the characteristics of high fusion accuracy and low communication volume. Although the methods in [15–17] are optimized for the problem of large SMART communication volume, SMART communication volume is still large compared to the CPDA method. In 2008, Yao and Wen proposed a layered network-based privacy protection method (data aggregation different privacy-level protection (DADPP)) based on CPDA [18]. After the clustering process is over, DADPP divides the nodes in the cluster, logically in different groups to reduce the computational dimension, thereby reducing computational complexity and communication volume. Although this method reduces the number of fusion nodes in the cluster, it requires the participation of specific network nodes and does not propose a method for the general division of any node cluster. Guo proposed a simple improvement scheme based on CPDA, taking the clustering of three nodes as an example to perform asymmetric privacy data fusion, thereby reducing the computational dimension and the amount of communication [19]; but when there are a few nodes in the cluster, when the number is greater than 3, the article does not propose a general solution. In response to the above, to improve the large amount of calculation and communication problems that exist in the existing privacy protection data fusion methods, this paper proposes an intracluster privacy protection data fusion with low energy consumption method (LEC-CPDA), with a view to on the premise of ensuring data privacy, further reduce the amount of calculation and communication of network nodes.

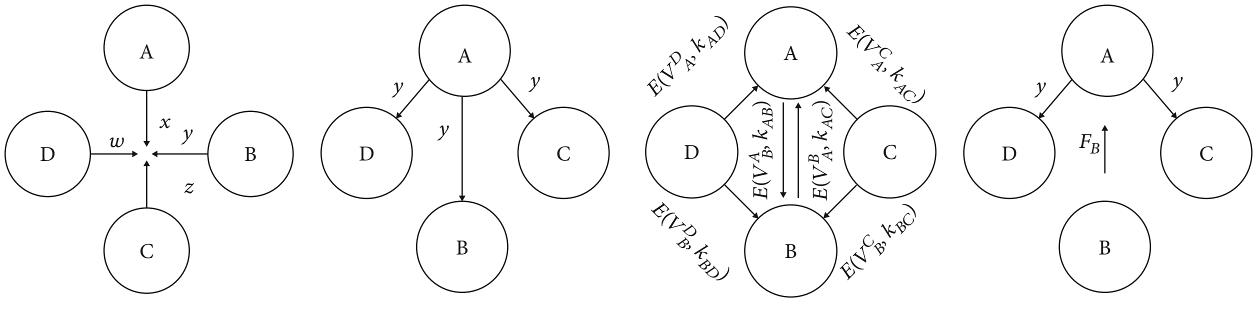
The rest of the paper is organized as Section 2 provides the proposed steps and algorithm of LEC-CPDA. Experimental analyses and results are explained in Section 3. The conclusion is given in Section 5.

2. Proposed LEC-CPDA: A Low-Energy Data Fusion Privacy Protection Algorithm

For a cluster, given n nodes (i.e., one cluster head and $n-1$ cluster members). If node $N_i (i = 1, 2, \cdots, n)$ collects data x_i at time t, the data fusion function is

$$f(t) = f(x_1(t), x_2(t), \cdots, x_i(t), \cdots, x_n(t)). \quad (1)$$

Among them, there can be lots of functions for fashioning (e.g., sum, average, median, minimum, maximum, and count). In this article, we mainly focus on the sum function which is defined as $y(t) = \sum_{i=1}^{n} x_i(t)$.



(a) (b) (c) (d)

Figure 1: Communication process diagram.

2.1. Steps

(1) *LEC-CPDA Clustering Stage*. By sending a Hello message, the query server (QS) can trigger a query. For a node, when the message is received, the node will be converted to the cluster head node and send a Hello message to neighboring nodes at the same time. For the remaining nodes that have been waiting, they will stop waiting and join the group unless the neighbor node sends a Hello message. Otherwise, as long as the cluster head sends them a JOIN message, they will immediately join the cluster

After the topological structure is formed, the key distribution of the nodes will be carried out. According to the principle of secure multiparty computing [20, 21], the security model of LEC-CPDA uses a semihonest model, and the key distribution mechanism is the same as that of CPDA, and both use a random key predistribution method [23]. In this way, the probability of the node key being cracked can be reduced as much as possible, and the data security protection is higher when the base station and the node are not trustworthy.

(2) *Fusion Stage within LEC-CPDA Cluster*. After the clustering is over, the nodes in the cluster begin to sense data and perform fusion operations. For the convenience of explanation of a cluster, we assume that it contains 4 nodes A, B, C, and D, respectively, broadcasting its seed value x, y, z, and w, where A is the cluster head that is generating an undisclosed random value r_A, r_B, r_C, r_D. For each fusion process, first node A randomly selects a node, and the remaining nodes calculate the seed value and random value and send them to the cluster head and the nodes according to the selection of the cluster head. The communication process can be shown in Figure 1. Among them, Figure 1(a) shows the propagation seed value of the nodes in the cluster, Figure 1(b) shows the seed value of the selected node propagation by the cluster head node, and Figure 1(c) is the information exchange process. Figure 1(d) is the collaborative node sending the calculation result to the cluster head

Assume that node A selects node B as the cooperative node. The calculation result of node A is

$$\begin{cases} V_A^A = a + r_A x, \\ V_B^A = a + r_A y. \end{cases} \tag{2}$$

Among them, a is the data obtained by node A.

The calculation result of node B:

$$\begin{aligned} V_A^B &= b + r_B x, \\ V_B^A &= a + r_B y. \end{aligned} \tag{3}$$

Among them, b is the data obtained by node B.

The calculation result of node C:

$$\begin{aligned} V_A^C &= c + r_C x, \\ V_B^C &= c + r_C y. \end{aligned} \tag{4}$$

Among them, c is the data obtained by node C.

The calculation result of node D :

$$\begin{aligned} V_A^C &= c + r_C x, \\ V_B^C &= c + r_C y. \end{aligned} \tag{5}$$

Among them, c is the data obtained by node C.

Node A receives messages from other nodes and generates intermediate value F_A after fusion processing

$$F_A = V_A^A + V_A^B + V_A^C + V_A^D = (a + b + c + d) + x(r_A + r_B + r_C + r_D). \tag{6}$$

The intermediate value F_B after node B fusion processing is

$$F_B = V_B^A + V_B^B + V_B^C + V_B^D = (a + b + c + d) + y(r_A + r_B + r_C + r_D). \tag{7}$$

Node B sends F_B to cluster head A, and cluster head A calculates the fusion result $a + b + c + d$ according to the formula $U = G^{-1} F$.

```
The LEC-CPDA topology is initialized to complete the process of node clustering
Set the message sending time interval $\Delta t$ for data fusion
If the current node belongs to a cluster
    Broadcast their respective seed values to nodes in the cluster
End if
The nodes are waiting
If a node receives the query request
    By randomly selecting a cooperative node, the cluster head node broadcasts its seed value
    The nodes in the cluster perform noise processing on the acquired data and send them to the cluster head and the cooperative node, respectively. At the same time, the cluster head node and the cooperative node also send the results of the noise processing to each other
    The cooperative node sends the calculated intermediate result to the cluster head, and the final cluster head calculates the fusion result
End if
The cluster head node establishes a TAG tree and transfers the fusion result to the base station by borrowing the TAG tree
The node resumes its waiting state
```

Algorithm 1: LEC-CPDA algorithm.

$$\mathbf{G} = \begin{bmatrix} 1 & \mathrm{x} \\ 1 & \mathrm{y} \end{bmatrix}, \mathbf{F} = [F_A, F_B]^T. \tag{8}$$

(3) *Fusion Stage between LEC-CPDA Clusters*. Similarly, compared with CPDA, the intercluster fusion process of LEC-CPDA used the TAG tree, i.e., the cluster head uploads the fusion value to the base station by the TAG tree

2.2. LEC-CPDA Algorithm Flow

3. Experimental Analyses and Results

We mainly analyze the performance of LEC-CPDA from three aspects: privacy protection, data communication volume, and accuracy. TAG [12], SMART [7], ESPART [8], and CPDA [7] are typical data fusion technology used in wireless sensor networks. We use it as the data privacy analysis, calculation, and communication of LEC-CPDA contrast items of quantity and fusion accuracy.

3.1. Data Privacy Analysis. Data privacy reflects the possibility of node private data that was being cracked. The scale of the cluster cannot grow indefinitely, and its distribution law can be expressed by equations (9)–(11). It can be seen from equations (9) to (11) that the distribution of cluster size is related to the parameters p_c and d_i.

$$p_i = (1 - p_c)\frac{1}{d_i p_c}, \tag{9}$$

$$p(|C_i| = k) = \begin{bmatrix} d_i \\ k-1 \end{bmatrix} p_i^{k-1} \bullet (1 - p_i)^{d_i - k + 1}, \tag{10}$$

$$p(|C_i| < m_c) = \sum_{k=1}^{m_c - 1} p(|C_i| = k) = \sum_{k=0}^{m_c - 2} \begin{bmatrix} d_i \\ k \end{bmatrix} p_i^{k} \bullet (1 - p_i)^{d_i - k}. \tag{11}$$

(i) C_i represents the cluster with node i as the head no

(ii) p_i is the probability that indicates the neighbor of i joins the cluster

(iii) k is the node number with C_i

(iv) $\mathrm{m_c}$ is the minimum number of nodes possible for a cluster C_i

(v) $p(|C_i| = k)$ represents the probability that the cluster C_i contains k nodes

(vi) $p(|C_i| < m_c)$ indicates the probability that the cluster size of C_i is less than the minimum cluster size m_c

(vii) d_i is the degree of an adjacent node of node; p_c is the probability of becoming a cluster head for a node

Not only the clustering results of the whole network parameters are affected by d_i and p_c affect but also the privacy of node data is affected by them. In CPDA, each member node in the cluster performs polynomial operations on its data and unsecured seeds and then encrypts it and transmits it to others. Each node transmits $m - 1$ piece of encrypted information to other in-cluster nodes when cluster size is m, and only when other in-cluster obtain these $m - 1$ encryption keys, the corresponding data of it is cracked. Thus, the average probability that the data of all nodes in the cluster will be cracked is

$$p_1(q) = \sum_{k=d_{\min}}^{d_{\max}} p(m = k) \bullet \left(1 - \left(1 - q^{k-1}\right)^{k}\right). \tag{12}$$

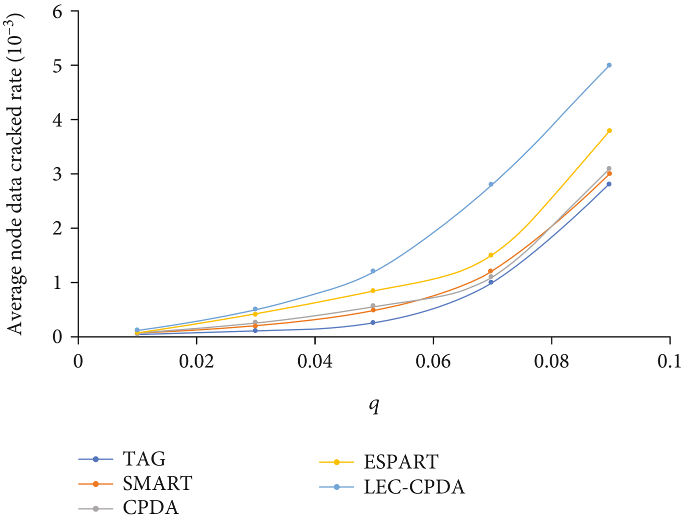


Figure 2: Privacy comparison ($p_c = 1/5$).

Here, $d_{\max}$ and $d_{\min}$, respectively, refer to maximum and minimum node number of the corresponding cluster.

If all $J-1$ out-degree and all in-degree links of the node in SMART are cracked, the real data of the node will be exposed

$$p_2(q) = q^{J-1} \sum_{k=0}^{d_{\max}} p(\text{in\_degree} = k) \bullet q^k. \tag{13}$$

The minimum node degree for the ESPART is $d_{\min}$. If the in-degree and out-degree links of the node are both cracked, the real data of the node will be exposed, so

$$p_3(q) = \sum_{k=d_{\min}}^{d_{\max}} p(m = k) \bullet q^k. \tag{14}$$

In the LEC-CPDA method, two encrypted messages are sent by each node to the cluster head and the node randomly designated by it. Therefore, before cracking the data of the source node, it is necessary to know the secret key for communicating with these two nodes. The average probability that the data of all nodes in the cluster in LEC-CPDA will be cracked is

$$p_4(q) = \sum_{k=d_{\min}}^{d_{\max}} p(m = k) \bullet \left(1 - \left(1 - \frac{q^2}{k}\right)^k\right). \tag{15}$$

Here, q is the probability of eavesdropping. Figure 2 shows the privacy comparison of the four methods under different q. We conclude that LEC-CPDA has the strongest degree of privacy, followed by the ESPART method. Privacy comparison ($p_c = 1/5$) is shown in Figure 2.

Figure 3 shows the privacy distribution of LEC-CPDA when p_c values are different. When the value of p_c increases, the scale of the formed cluster is smaller (the number of nodes $m \geq 3$), and the privacy of LEC-CPDA is greater. Therefore, the node data will be not easily cracked. Therefore, an appropriate value of p_c must be selected.

Figure 4 is a cluster scale distribution diagram obtained from cluster scale distribution (9)–(11).

When $p_c = 1/5$, the cluster size of the entire network is mostly concentrated in 3 ~ 7 nodes, and the proportion of clusters of a single node is small. Therefore, when the scale of the formed cluster is concentrated in 3 ~ 7 nodes, the mechanism proposed in this paper can ensure that the data exposure rate is in a low range, thereby ensuring the privacy of the data.

3.2. Calculation and Communication Volume Analysis. In this section, we will discuss calculation amount, intracluster fusion traffic, network-wide traffic, residual energy ratio, and fusion accuracy analysis in detail.

3.2.1. Calculation Amount. In the preparation phase of the ESPART algorithm, the same as TAG, the Hello signal is first sent out from QS. When each node receives the Hello signal for the first time, its parent node is selected as the Hello signal source node. Thus, to build a data fusion tree, it sends the signal; each node needs to transfer data upwards within the time slice in the upward data fusion stage. Simplify, we give each layer the same time slices. To avoid conflicts in the time slice, we randomly send them. The ESPART requires each node to record the number of its child nodes in the first step of the fusion stage. The preparation phase, compared with TAG, is the same for the data traffic of the first step generated by ESPART. Each node, respectively, sends 1 Hello signal and 1 fusion data. After fixing the tree structure and recording subnode numbers, the amount of data transmission between the subsequent nodes of the collusion communication phase can be reused. Therefore, in the experiments, the data communication volume generated in the preparation phase can be ignored.

Concerning ESPART and SMART algorithms, what is measured in the simulation process is the number of all data packets which are sent by all nodes of the network in the

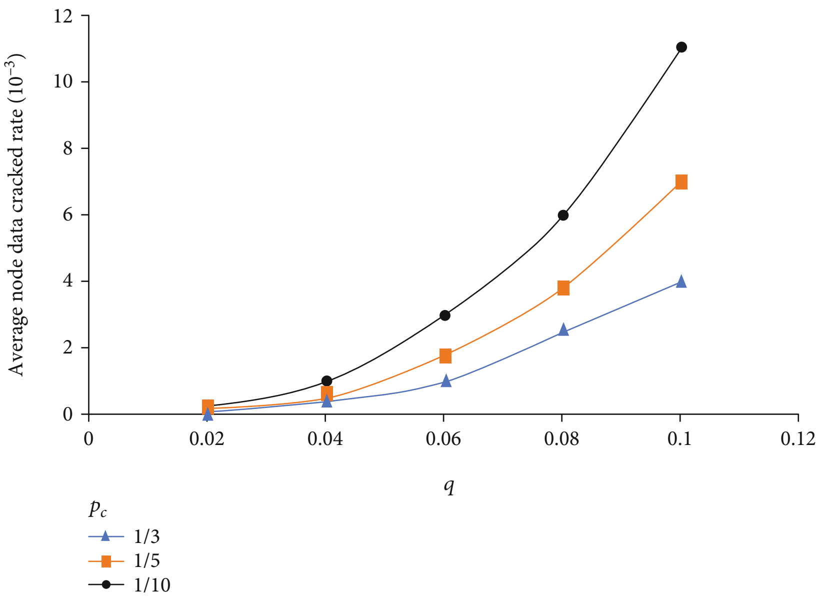


Figure 3: Comparison of LEC-CPDA privacy when p_c value is different.

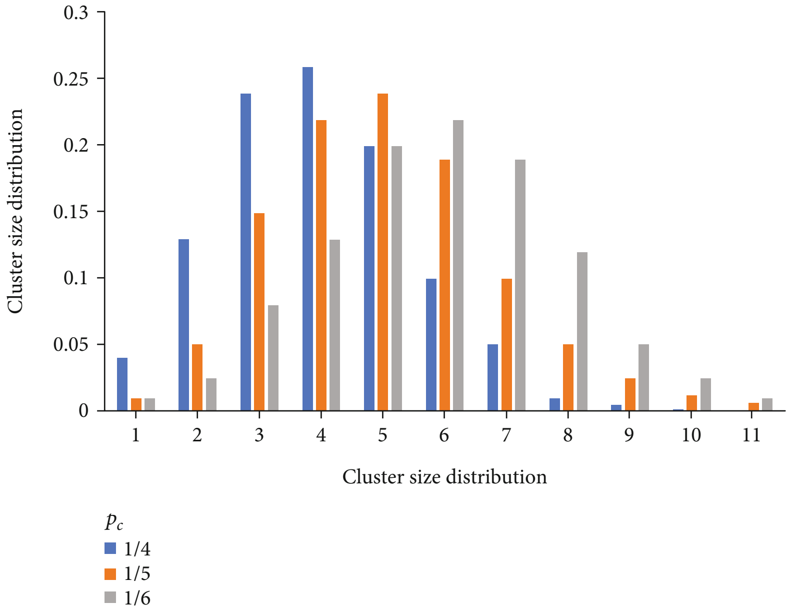


Figure 4: Cluster size distribution (node connection degree $d = 12$).

process of collusion. In terms of TAG, we measure the number of all data packets sent by all nodes in a single establishment and integration process.

For the CPDA algorithm and the LEC-CPDA algorithm, this paper divides the calculation amount present in the node into two cases:

(1) The calculation amount of the nodes in the cluster

(2) The calculation amount of the cluster head

The amount of calculation includes arithmetic operations, that is, noise interference processing, encryption, decryption operations, and data fusion operations. α, β, γ are used to represent arithmetic, encryption, and decryption operations, while fusion operation is represented by δ. Suppose 4 nodes A, B, C, and D are in a cluster. Among them, A is the cluster head node, and B, C, and D are nodes of the cluster.

In the CPDA mechanism, all nodes in the cluster will perform the following steps in the cluster fusion process: After each node collects data, use the public seed value of each node in the cluster and 3 private random values for noise processing. The operation, that is, converted into 4 third-degree polynomials. In the entire calculation process, the number of arithmetic operations is 39; each node encrypts the 3 noise interference values and sends them to

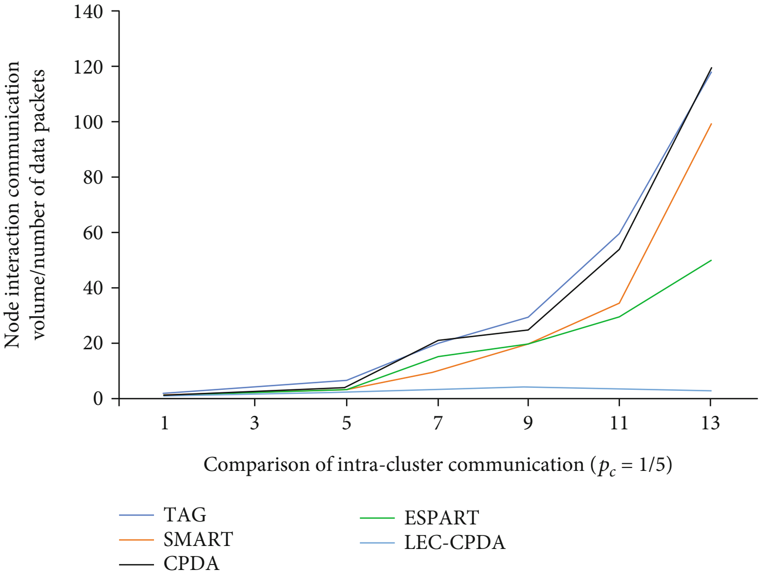


Figure 5: Comparison of intracluster communication ($p_c = 1/5$).

the other 3 nodes in the cluster, and the node will also receive 3 sent from the other 3 nodes. The third-degree polynomial, after decrypting the noise interference value with a shared key, performs a third-order arithmetic operation to combine 4 polynomials (the node itself retains a polynomial). Therefore, the calculation amount for a cluster size of 4 can be expressed as

$$Q_{\text{CPDA-node}} = 39\alpha + 3\beta + 3\gamma. \quad (16)$$

For the cluster head node, besides performing the operations of the nodes in the cluster, it also needs to consider the fusion operation. The calculation amount of the cluster head can be expressed as

$$Q_{\text{CPDA-cnode}} = 39\alpha + 3\beta + 3\gamma + \delta. \quad (17)$$

For the LEC-CPDA algorithm, all the nodes will perform the following steps in the process of fusion within the cluster: After each node collects data, use the node's public seed value and 3 private random values to perform noise interference operations, namely, converted into 4 second-degree polynomials. In the whole calculation process, the number of arithmetic operations is 4; each node sends 2 encrypted noise interference values to the cluster head and the cooperating node. At the same time, they receive the noise processing results sent by other nodes; after decrypting the noise value with the shared key, it performs 2 arithmetic operations to combine 2 polynomials. Therefore, the calculation amount for a cluster size of 4 can be expressed as

$$Q_{\text{LEC-CPDA-node}} = 4\alpha + 2\beta. \quad (18)$$

The calculation amount of the cooperative node can be expressed by

$$Q_{\text{LEC-CPDA-midnode}} = 4\alpha + \beta + 3\gamma. \quad (19)$$

For the cluster head node, besides performing the operations of the nodes in the cluster, it also needs to consider the fusion operation. The calculation amount of the cluster head can be expressed as

$$Q_{\text{LEC-CPDA-node}} = 4\alpha + \beta + 3\gamma + \delta. \quad (20)$$

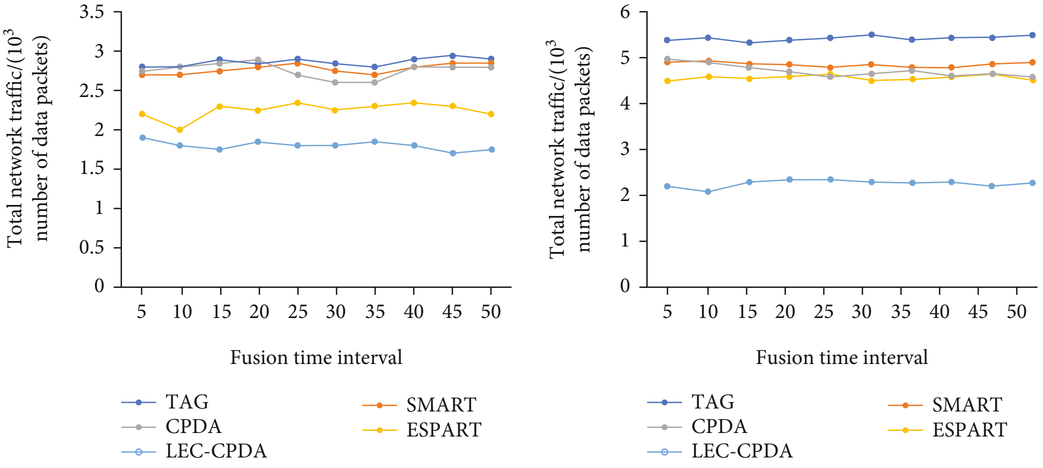
It can be seen that LEC-CPDA has a greater advantage over CPDA in terms of calculation.

3.2.2. Intracluster Fusion Traffic. Figure 5 shows the comparison of the average intracluster communication volume between LEC-CPDA and TAG, SMART, ESPART, and CPDA.

It can be seen from Figure 5 that the graphs of the other methods have roughly increased exponentially, and the TAG and CPDA methods have the fastest growth. Due to the uneven distribution of cluster size, the curve growth trend when the cluster size is $7-8$ is different from the previous growth trend of $3-7$. This is because the number of clusters with $7-8$ node size is different from the cluster number containing $3-7$ nodes. Similarly, the curve with the node number containing $10-11$ nodes has a breakpoint phenomenon. The traffic curve in LEC-CPDA is roughly linear. It can be seen that in the process of intracluster fusion, LEC-CPDA has a greater advantage in communication complexity, thereby reducing the amount of data communication.

3.2.3. Network-Wide Traffic. The aspects that need to be considered when calculating the communication volume in the entire network are the communication volume during the formation of the network topology, the communication volume merged within the cluster, and the communication volume merged between the clusters.

Given n nodes of the cluster, in the CPDA mechanism, firstly, cluster heads send a Hello message to neighboring nodes to form clusters. This process needs to transmit 1



(a)

(b)

Figure 6: Comparison of total communication volume ($p_c = 1/3$ and $p_c = 1/5$).

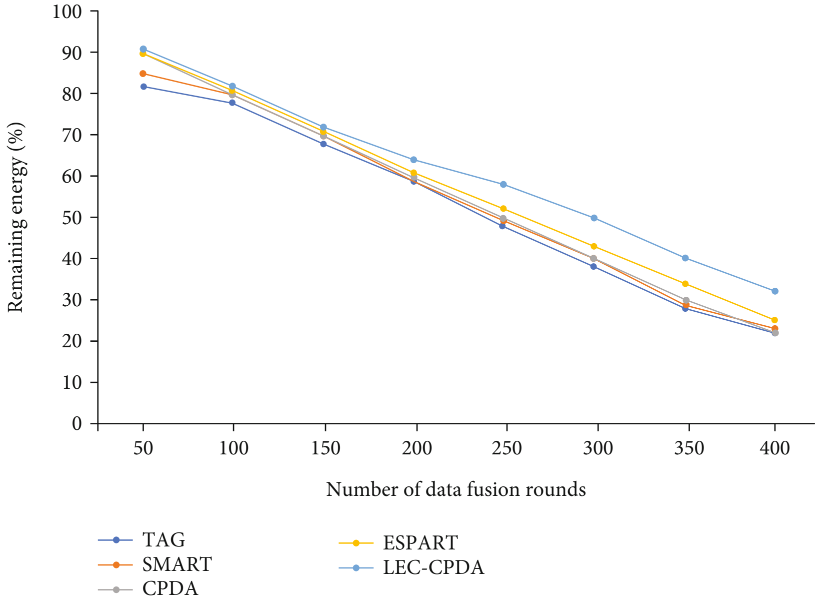


Figure 7: Residual energy ratio.

message; secondly, respective seed values of these nodes are broadcasted; then, perform intracluster fusion; finally, the upper cluster head receives the fusion result forwarded by cluster head. In the whole process, the cluster head sends and nodes in the cluster, respectively, send $n + 3$ and $n + 2$ messages; in the LEC-CPDA mechanism, the clustering stage is the same as CPDA, and one message needs to be transmitted. Secondly, respective seed values of the nodes in the cluster are broadcasted; again, perform the LEC-CPDA intracluster fusion; finally, the upper cluster head node receives the fusion result from the cluster head. Throughout the process, the cluster head, nodes of the cluster, and the collaboration node, respectively, sent 5 and 3 messages.

It can be seen from Figure 6 that LEC-CPDA has less overall network traffic than the other four methods. When $p_c = 1/3$, LEC-CPDA's overall network communication volume is 29% lower than CPDA; when $p_c = 1/5$, LEC-CPDA's overall network communication volume is about 54% lower than CPDA. In the entire network, given fixed node size, for the cluster size distribution and the parameter p_c, the larger the parameter p_c, the smaller the cluster size, and the smaller the p_c, the larger the cluster size. Due to the large cluster size, when p_c decreases, the data communication volume of LEC-CPDA does not change much, but the communication volume of CPDA increases significantly.

3.2.4. Residual Energy Ratio. This paper compares the remaining energy of the entire network after each round of fusion. Set the initial energy of each node as $E_0 = 150\,\text{J}$, the energy consumption of one calculation is $E_c = 220\,\text{nJ}$,

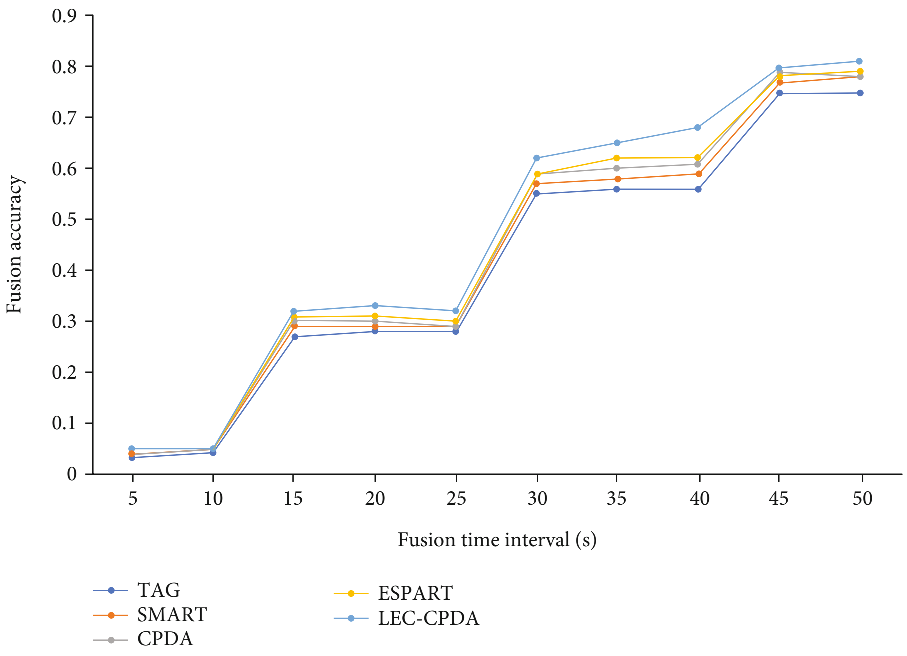


FIGURE 8: Accuracy comparison ($p_c = 1/5$).

the transmission energy consumption is $W_{tr} = 0.66\,\text{W}$, the receiving energy consumption is $W = 0.395\,\text{W}$, 400 fusion simulations are performed, and the remaining energy comparison can be seen in Figure 7. Figure 7 displays that the energy consumption of TAG is the fastest. This is due to a large amount of calculation and communication of TAG, which requires multiple calculations, sending and receiving data. In the network, communication and transmission are the node's main energy consumption, and the amount of communication and transmission of LEC-CPDA is less than that of CPDA. Therefore, after the same number of rounds of data fusion, the energy consumption of LEC-CPDA is significantly less than that of CPDA, which is more conducive to extending the life cycle of the network.

3.3. Fusion Accuracy Analysis. Given $p_c = 1/5$, in this experiment, to ensure that most nodes in the network are covered, we use 600 nodes which are distributed in the range of 400 m × 400 m. At the same time, we, respectively, set the transmission range and transmission rate of the nodes as 50 m and 1 Mb/s. In the same scenario, LEC-CPDA can guarantee the same fusion accuracy as other methods.

According to Figure 8, we can conclude that LEC-CPDA outperforms ESPART in terms of fusion accuracy. In the intracluster fusion of LEC-CPDA, for the cluster head node and the cooperating nodes, the nodes of the cluster only need to send two messages to them. Compared with other methods, the collision in the communication transmission process is reduced, and the fusion accuracy is improved. In addition, when the fusion time interval increases, the fusion accuracy increases. When the fusion time interval extends, the data packet which is sent by the node allows a longer time to reach the destination node, so it has a better fusion effect.

4. Conclusion

For the wireless sensor network to fuse data with low energy consumption while also ensuring data privacy, this paper improves the existing CPDA method and proposes a low-energy privacy protection mechanism LEC-CPDA. The results of experiments display the LEC-CPDA outperforms other methods in terms of calculation volume, communication volume consumption, and fusion accuracy. This article only analyzes the sum function, and analyzing the multitype fusion function is the next step. In addition, this article does not consider the verification of data integrity, and further research will be done in this area in the future.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This study was supported by the Hubei Education Science Planning Leading Group (Grant No. 2020GB025).

References

[1] A. Perrig, J. Stankovie, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[2] H. Alzaid, E. Foo, J. M. Nieto, and D. G. Park, “A taxonomy of secure data aggregation in wireless sensor networks,” *International Journal of Communication Networks and Distributed Systems*, vol. 8, no. 1/2, pp. 101–148, 2012.

[3] S. Ozdemir and Y. Xiao, “Secure data aggregation in wireless sensor networks: a comprehensive overview,” *Computer Networks*, vol. 53, no. 12, pp. 2022–2037, 2009.

[4] C. Castelluccia, E. Mykletun, and G. Tsudik, “Efficient aggregation of encrypted data in wireless sensor networks,” in *Proceedings of the 2nd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services*, pp. 109–117, San Diego, USA, 2005.

[5] E. Cristofaro, “A secure and privacy-protecting aggregation scheme for sensor networks,” in *Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, pp. 1–5, Espoo, Finland, 2007.

[6] Y. Yi, X. R. Wang, S. C. Zhu, and G. H. Cao, “SDAP: a secure hop-by-hop data aggregation protocol for sensor networks,” in *Proceedings of the ACM Transactions on Information and System Security*, vol. 11no. 4, pp. 1–43, New York, USA, 2008.

[7] W. B. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, “PDA: privacy-preserving data aggregation in wireless sensor networks,” in *Proceedings of the 26th IEEE International Conference on Computer Communications*, pp. 2045–2053, Anchorage, AK, 2007.

[8] G. Yang, A. Q. Wang, Z. Y. Chen, J. Xu, and H. Y. Wang, “An energy-saving privacy-preserving data aggregation algorithm,” *Chinese Journal of Computers*, vol. 34, no. 5, pp. 792–800, 2011.

[9] R. Bista, D. Kim, and J. Chang, “A new private data aggregation scheme for wireless sensor networks,” in *Proceedings of the 2010 IEEE 10th International Conference on Computer and Information Technology*, pp. 273–280, Bradford. West Yorkshire, UK, 2010.

[10] T. M. Feng, C. Wang, W. S. Zhang, and L. Ruan, “Confidentiality protection for distributed sensor data aggregation,” in *Proceedings of the 27th IEEE International Conference on Computer Communications*, pp. 56–60, Phoenix, USA, 2008.

[11] C. Wang, G. L. Wang, W. S. Zhang, and T. M. Feng, “Reconciling privacy preservation and intrusion detection in sensory data aggregation,” in *Proceedings of the 30th IEEE International Conference on Computer Communications*, pp. 336–340, Shanghai, China, 2011.

[12] S. Madden, M. Franklin, J. M. Hellerstein, W. Hong, and J. M. Hellerstein, “TAG: a tiny aggregation service for ad-hoc sensor networks,” in *Proceedings of the 5th Symposium on Operating Systems Design and Implementation*, vol. 36Supplement I, pp. 131–146, New York. USA, 2002.

[13] R. Bista and K. J. Jo, “A new approach to secure aggregation of private data in wireless sensor networks,” in *Proc 8th IEEE International Conference on Dependable Autonomic and Secure Computing*, pp. 394–399, IEEE Press, Chengdu, China, 2009.

[14] F. Wang, “Data merging method by protecting energy in wireless sensor networks,” *Journal of Networks*, vol. 9, no. 6, pp. 1558–1564, 2014.

[15] L. Li, Q. Qin, L. Hua, and L. Jian, “Data fusion algorithm of privacy protection based on QoS and multilayers hierarchically,” *International Journal of Distributed Sensor Networks*, vol. 9, no. 12, Article ID 926038, 2013.

[16] H. Li, K. Lin, and K. Li, “Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks,” *Computer Communications*, vol. 34, no. 4, pp. 591–597, 2011.

[17] G. Yang, S. Li, Z. Y. Chen, J. Xu, and Z. Yang, “High-accuracy and privacy-preserving oriented data aggregation algorithm in sensor networks,” *Chinese Journal of Computers*, vol. 36, no. 1, pp. 189–200, 2013.

[18] J. B. Yao and G. J. Wen, “Protecting classification privacy data aggregation in wireless sensor networks,” in *Proc 4th International Conference on Wireless Communication, Networking and Mobile Computing, WiCOM*, Dalian, China, 2008IEEE Press.

[19] H. Z. Guo, “A modified scheme for privacy-preserving data aggregation in WSNs,” in *Proc 2nd International Conference on Consumer Electronics. Communications and Networks (CECNet)*, pp. 790–794, IEEE Press, Yichang. China, 2012.

[20] A. Ukil and J. Sen, “Secure multiparty privacy preserving data aggregation by modular arithmetic,” in *Proc 1st International Conference on Parallel, Distributed, and Grid Computing*, pp. 329–334, IEEE Press, Solan, India, 2010.

[21] O. Goldreich, “Secure multi-party computation (working draft) version 1,” *Multimodal Output Generation*, 2002.