Journal of Ambient Intelligence and Humanized Computing (2022) 13:1495–1503
https://doi.org/10.1007/s12652-020-02801-6

ORIGINAL RESEARCH

A secure and efficient privacy-preserving data aggregation algorithm

Hui Dou[1,2] · **Yuling Chen**[1,2] · **Yixian Yang**[1,3] · **Yangyang Long**[1,2]

Received: 18 May 2020 / Accepted: 5 December 2020 / Published online: 10 February 2021

Abstract
As a significant part of the Internet of things, wireless sensor networks (WSNs) is frequently implemented in our daily life. Data aggregation in WSNs can realize limited transmission and save energy. In the process of data aggregation, node data information is vulnerable to be eavesdropped and attacked. Therefore, it is of great significance to the research of data aggregation privacy protection in WSNs. We propose a secure and efficient privacy-preserving data aggregation algorithm (SECPDA) based on the original clustering privacy data aggregation algorithm. In this algorithm, we utilize SEP protocol to dynamically select cluster head nodes, introduce slicing idea for the private data slicing, and generate false information for interference. A comprehensive experimental evaluation is conducted to assess the data traffic and privacy protection performance. The results demonstrate that the proposed SECPDA algorithm can effectively reduce data traffic and further improve data privacy of nodes.

Keywords Wireless sensor network · Privacy protection · Data aggregation · Low energy consuming · CPDA

1 Introduction

Wireless sensor networks (WSNs) (IanF et al. 2016) consist of many low-power wireless sensor nodes with limited storage and computing power. These sensor nodes are used to sense and collect useful information in the network. Currently, WSNs are frequently applied in habitat monitoring (Smita and Mrinal 2019), intelligent space, medical systems (Muhammad et al. 2020), Smart Grid (He et al. 2017) and robotic exploration. In WSNs, sensor nodes are easily captured, physical tampering, denial of service and other attacks, which may lead to a series of challenges in foundational researches. In the data collection process, these sensor nodes may generate some redundant data, and the further data transmission will consume extra energy. Data aggregation (Sabrina et al. 2018), as the crucial technology in WSNs, is widely used to overcome the energy consumption issue. Aggregators can calculate and count the sum, average, minimum and maximum values from the child sensor nodes, and send the aggregated result to higher-level aggregator. Through redundancy process and information synthesis, the network traffic and energy consumption will be decreased. However, in the data aggregation process, when sensor nodes are communicating with each other, anyone with a relevant wireless receiver can detect and intercept messages between sensor nodes. The attacker may use illegal means to communicate with powerful workstations (Yang et al. 2020; Wang et al. 2020a, b, c, d). Illegal interactions and information theft can cause severe harm to the network, and even propel the entire network into a state of paralysis.

In recent years, the researches in data aggregation and privacy protection can be divided into three categories: hop by hop encryption, end-to-end encryption and non-encryption mechanism. He et al. (2007) proposed CPDA and SMART privacy protection algorithm in terms of hop by hop encryption mechanism, which utilize TAG tree model (Madden et al. 2002) to aggregate the data from sensor nodes. Yao and Wn (2008) proposed the DADPP algorithm to meet the needs of different privacy levels, and reach the privacy protection while obtaining accurate aggregation results. Yang et al. (2008) introduced SDAP algorithm, which utilize probability grouping technology to effectively verify the correctness of aggregated data. Feng et al. (2008)

✉ Yuling Chen
ylchen3@gzu.edu.cn

[1] State Key Laboratory of Public Big Data, Guizhou University, Guizhou, Guiyang, China

[2] School of Computer Science and Technology, Guizhou University, Guizhou, Guiyang, China

[3] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, China

utilized interference numbers to protect the privacy of and reduce the communication overhead of node data. He et al. (2009) proposed an iCPDA protocol to overcome the data integrity issue, which increases the data integrity protection and inherits the data privacy protection capability of the CDPA algorithm. Ozdemir and Yang (2008) proposed an IPHCDA protocol, which provides data privacy and integrity protection by employing homomorphic encryption algorithm based on elliptic curve encryption and MAC mechanism. Guo (2012) improved the CPDA scheme, and reduced the computational and communication costs. Based on iPDA and CPDA algorithms, Bista et al. (2012) proposed the DCIDA algorithm, which utilizes real part of complex number to protect data privacy and utilized the imaginary part to verify data integrity by introducing the concept of complex number. Guo and Ding (2014) proposed an ILC-CPDA algorithm to reduce data transmission by utilizing the LEACH protocol and simple aggregation methods. This algorithm can detect data integrity by adding homomorphic message authentication code. In recent years, some privacy protection schemes (Liu et al. 2020a, b; He et al. 2019) in WSNs have been proffered. Zhang et al. (2019) proposed an energy efficient and reliable in-network data aggregation scheme for WSNs. Man et al. (2017) proposed an energy-efficient cluster-based privacy data aggregation (E-CPDA), Fang et al. (2017) proposed a novel energy-efficient secure data aggregation scheme cluster-based private data aggregation (CSDA). These literatures have proffered the data aggregation protocol in smart grid (Afshin et al. 2019; Kong et al. 2020; Liu et al. 2018), Secure multi-party computation (Wang et al. 2020a, b, c, d) can also be applied to data aggregation in the future. These literatures have reduced traffic, but for higher privacy needs, it needs to be a further improvement.

In this work, we focus on the data traffic and privacy issues in CPDA, and proposed a secure and efficient data aggregation privacy protection algorithm (SECPDA). The SECPDA algorithm utilizes SEP protocol to select the cluster head node dynamically, and utilizes false message to enhance privacy protection capability. Experimental evaluations and performance analysis show that the proposed SECPDA algorithm has a lower data traffic, high security, privacy protection ability than other algorithms.

The contributions of our work in this article are shown as follow:

1. We adopt the SEP protocol to dynamically select cluster head nodes and merge them into the simple addition cluster to reduce the communication overhead of data, and propose a secure and efficient data aggregation privacy protection algorithm (SECPDA).
2. We adopt the method of data slicing and node false message to aggregate data for a further improvement the privacy needs in the communication process.

The rest of the paper is structured as follows: Sect. 2 describes the model and background, including sensor network model, encryption method and clustering method. Section 3 presents the SECPDA algorithm, including the formation of the cluster, aggregation process and the SECPDA algorithm flow. Section 4 describes the results of simulation and performance analysis, including the simulation of clustering process of sensor nodes, privacy performance analysis and data traffic analysis. Section 5 summarizes the paper and layout future research.

2 Model and background

2.1 Sensor network model

Generally, sensor nodes are divided into three categories: base station, cluster head node and sensor node (He et al. 2007). The sensor node uploads the data to the cluster head node, then the cluster head node aggregates the received data with its own data, finally uploads the aggregated results to the base station. The sensor network model is demonstrated in Fig. 1

2.2 Encryption method

The encryption method adopted by SECPDA is the same as that adopted by CPDA, which employs random key distribution scheme (Laurent and Virgil 2002). First, generate a key pool containing K keys, each of them has its own identity. Then each node randomly selects k keys from the key pool and stores them in the node. Each node broadcasts its own

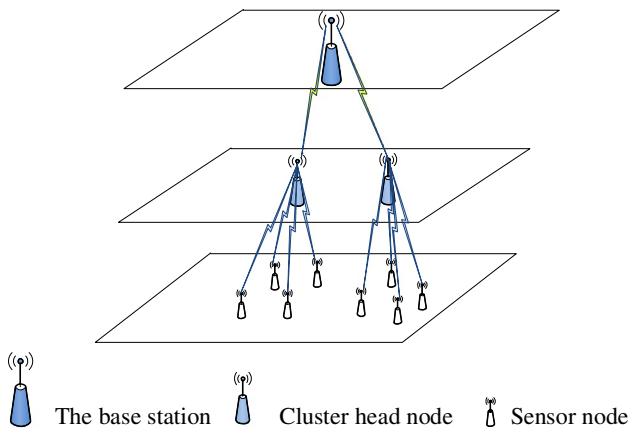

Fig. 1 Sensor network model

key, if the neighbor node has a public key with it, they will share a security link. Therefore, the probability of any two nodes sharing the security link is demonstrated in Formula (1):

$$P_{connect} = 1 - \frac{((K-k)!)^2}{(K-2k)!K!}. \tag{1}$$

If the public key is not found between two nodes, the intermediate node forms a secure link between the two nodes by means of multiple hop links. In this process, the probability that the shared key is eavesdropped by the attacker is demonstrated in Formula (2):

$$P_{overhear} = k/K. \tag{2}$$

Here, K is the total number of keys in the key pool, k represents the number of keys randomly selected for each node.

2.3 Clustering method

SEP protocol (Smaragdakis et al. 2004) is utilized to cluster in our proposed SECPDA algorithm. SEP protocol is an improved clustering protocol based on LEACH protocol (Heinzelman et al. 2000). In SEP protocol, owning to the different initial energy, these sensor nodes is divided into two categories: advanced nodes and normal nodes. In addition, different thresholds are set to make these advanced nodes to be more frequently selected as the cluster head nodes. Therefore, the build and transport process of the cluster is a cycle, and there exists a random proportion of advanced nodes. If the proportion of advanced nodes is a, the number of advanced nodes in the network with n nodes is na. Then, we can find that the number of normal nodes is $(1-a)n$. Respectively, if the initial energy of the advanced node is b times than the normal nodes' energy. Each node generates a random number r and the range of r is from 0 to 1. If the threshold $T(n)$ is greater than the random number r, the node is selected as the cluster head, and other nodes add the corresponding cluster according to the signal strength to complete the cluster construction. The probability of the advanced node and normal node being selected as cluster head is p_1, p_2, as demonstrated in Formulas (3) and (4):

$$p_1 = \frac{p}{1+ba}(1+b) \tag{3}$$

$$p_2 = \frac{p}{1+ba}. \tag{4}$$

Here, p represents the proportion of the heads in the clusters, and the thresholds for advanced nodes and normal nodes are demonstrated in Formulas (5) and (6):

$$T(n_1) = \begin{cases} \frac{p_1}{1-p_1\left[r \bmod \left(\frac{1}{p_1}\right)\right]} & \text{if } n \in G_1 \\ 0 & \text{otherwise} \end{cases} \tag{5}$$

$$T(n_2) = \begin{cases} \frac{p_2}{1-p_2\left[r \bmod \left(\frac{1}{p_2}\right)\right]} & \text{if } n \in G_2 \\ 0 & \text{otherwise} \end{cases}. \tag{6}$$

Here, r is the number of rounds, G_1, G_2 represents a set nodes that are not elected as cluster heads in the nearest round of these sensor nodes. In the transmission phrase, the node sends the collected data to the cluster head, which aggregates the data of all nodes, and then sends the aggregated result to the sink node. After a period of stabilization, the network proceeds to the next round of elections.

3 Secure and efficient privacy-preserving data aggregation algorithm SECPDA

The functionalities of these components are demonstrated in Table 1.

3.1 The formation of the cluster

We utilize SEP protocol to select the cluster head node. Suppose there are 1 base station node and 10 sensor nodes in the network. When the base station sends a data request, the node sends its address to the base station, base station

Table 1 Symbol description

Symbol	Definition
a, b, c	Private data of nodes A,B and C
a_i, b_i, c_i	Slice information corresponding to private data a, b and c
a_i', b_i', c_i'	False information corresponding to slice information a_i, b_i, c_i
K_{IJ}	Shared key between nodes I and J
$Enc(a_i, K_{IJ})$	Node I encrypts the slice information with a shared key and sends it to node J
$Enc(a_i', K_{IJ})$	Node I encrypts the false information with a shared key and sends it to node J
$Dnc(a_i, K_{IJ})$	Node J decrypts the received slice information with a shared key
$Dnc(a_i', K_{IJ})$	Node J decrypts the received false information with a shared key
F_I	Aggregation data values collected by node I

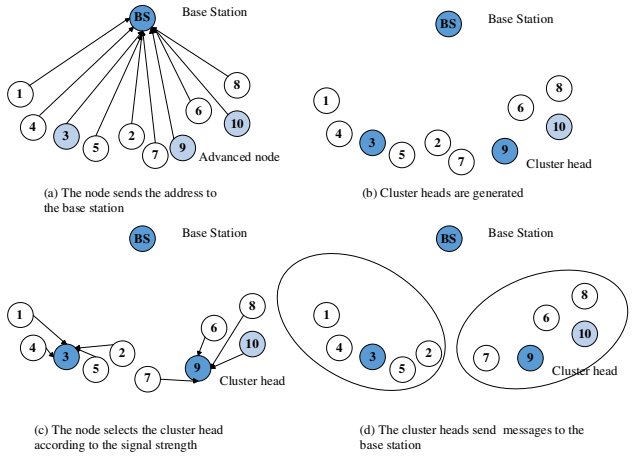

Fig. 2 The formation of the cluster

is node no. 1–10. We select the cluster head node according to the threshold of the advanced node and the ordinary node, other nodes decide which cluster to join based on the strength of the signal. The specific process is demonstrated in Fig. 2

3.2 Aggregation process

Suppose a cluster has three nodes A, B and C, where A is cluster head node. a, b and c respectively are the privacy data of each node. Here we will divide a into a_1, a_2 and a_3, that is $a = a_1 + a_2 + a_3$. The node a will generate false information while slicing, a_1 correspond to a_1', a_2 correspond to a_2', a_3 correspond to a_3', The information of privacy slice a_1 is retained by this node A.

Divide b into b_1, b_2 and b_3, that is $b = b_1 + b_2 + b_3$. The node b will generate false information while slicing, b_1 correspond to b_1', b_2 correspond to b_2', b_3 correspond to b_3', the node B send the information of privacy slice b_1 to the cluster head node A. send false information b_1', b_2' and b_3' to the cluster head node A. The process of node C is similar to that of node B.

Node A, B and C encrypt the privacy slice information and corresponding false information, then send them to other nodes randomly.

Where, the node A encrypts a_2 and a_2', then sends them to the node B, encrypts a_3 and a_3', then sends them to the node C. The process is demonstrated in Formula (7):

$$\begin{cases} Enc(a_2, K_{AB}), Enc(a_2', K_{AB}); \\ Enc(a_3, K_{AC}), Enc(a_3', K_{AC}); \end{cases}. \tag{7}$$

Similarly, the node B encrypts b_2 and b_2', then sends them to the node A, encrypts b_3 and b_3', then sends them to the node C. The process is demonstrated in Formula (8):

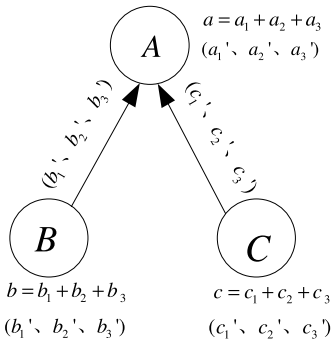

Fig. 3 Privacy data slicing

$$\begin{cases} Enc(b_2, K_{BA}), Enc(b_2', K_{BA}); \\ Enc(b_3, K_{BC}), Enc(b_3', K_{BC}); \end{cases}. \tag{8}$$

Similarly, the node C encrypts c_2 and c_2', then sends them to the node A, encrypts c_3 and c_3', then sends them to the node B. The process is demonstrated in Formula (9):

$$\begin{cases} Enc(c_2, K_{CA}), Enc(c_2', K_{CA}); \\ Enc(c_3, K_{CB}), Enc(c_2', K_{CB}); \end{cases}. \tag{9}$$

Now the node A, B and C decrypts the received data by utilizing the shared secret key, which can be calculated to F_A, F_B and F_C as demonstrated in Formulas (10)–(12):

$$\begin{cases} Dnc(b_2, K_{BA}), Dnc(b_2', K_{BA}); \\ Dnc(c_2, K_{CA}), Dnc(c_2', K_{CA}); \\ F_A = b_2 + b_2' + c_2 + c_2'; \end{cases} \tag{10}$$

$$\begin{cases} Dnc(a_2, K_{AB}), Dnc(a_2', K_{AB}); \\ Dnc(c_3, K_{CB}), Dnc(c_3', K_{CB}); \\ F_B = a_2 + a_2' + c_3 + c_3'; \end{cases} \tag{11}$$

$$\begin{cases} Dnc(a_3, K_{AC}), Dnc(a_3', K_{AC}); \\ Dnc(b_3, K_{BC}), Dnc(b_3', K_{BC}); \\ F_C = a_3 + a_3' + b_3 + b_3'; \end{cases}. \tag{12}$$

The node B and C send F_B and F_C to node A. Here, F_B mainly includes a_2, a_2', c_3, c_3', and similarly F_C includes a_3, a_3', b_3, b_3', F_A includes b_2, b_2', c_2, c_2'. In the initial stage, node B and C send their first slice data and all the false information to the cluster head node A, then A knows b_1, c_1, a_1', a_2', a_3', b_1', b_2', b_3', c_1', c_2', c_3' and knows a_1 (its first slice data). Finally, A gets the aggregation values of a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3, a_1', a_2', a_3', b_1', b_2', b_3', c_1', c_2' and c_3'. If we set S_1 to be the sum of a, b and c, the values of S_1 can be obtained without knowing b and c. Figures 3, 4 and 5 demonstrated the aggregation process of all nodes.

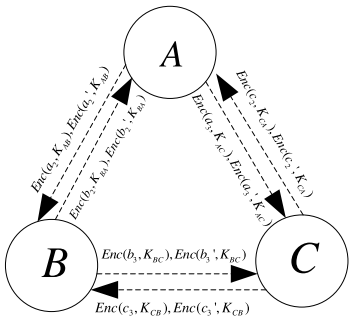

Fig. 4 Encrypts and sends

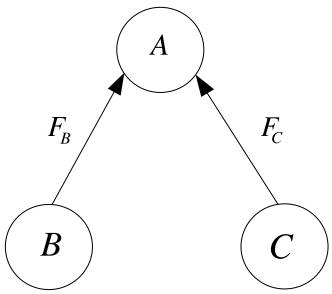

Fig. 5 Data aggregation

3.3 The SECPDA algorithm flow

In SECPDA algorithm, node clustering, node data information processing and data aggregation algorithm flow are as follows:

Algorithm 1: Node Clustering

Input: $a, b, p, r, T(n_1), T(n_2)$

Output: Clustering results

For each node

Each node determines whether it is an advanced node or a normal node based on $p_1 = \frac{p}{1+ba}(1+b)$ and $p_2 = \frac{p}{1+ba}$.

End for

For each node

The node determines the cluster-head node according to $T(n_1)$ and $T(n_2)$

if the nodes are cluster head nodes

The node is the cluster head node;

Broadcast the message as a cluster head;

Waiting for request message;

else

Wait for the cluster head to broadcast;

Select the appropriate cluster head as own cluster head, then send a request message to the cluster head;

end if

End for

Algorithm 2: Node data information processing

Input: Key, private data

Output: Slice information, false information

For each node in the WSN

Generate private data;

End for

For each cluster

For each node

Divide the private data of the node into p_{i1}, p_{i2} and p_{i3}, and generate false information p_{i2}', p_{i2}' and p_{i3}';

if the nodes are cluster head nodes

The section information p_{i1} of cluster head node and the false information for all slices were retained;

else

The node sends p_{i1}, p_{i1}', p_{i2}' and p_{i3}' to the cluster head node;

end if

End for

End for

For each cluster

For each node

Encrypt all slice information and corresponding false information $Enc(p_{ij}, K_{IJ}), Enc(p_{ij}', K_{IJ})$;

The node sends p_{i2}, p_{i3} slice information and the corresponding false information p_{i2}' and p_{i3}' randomly to other nodes in the cluster;

End for

End for

Algorithm 3: Data aggregation

Input: Key, slice information, false information

Output: The final data aggregation value

For each cluster

For each node

Decrypt the received encrypted slice information and false information $Dnc(p_{ij}, K_{IJ}), Dnc(p_{ij}', K_{IJ})$;

Calculate the node aggregation F_I;

End for

if non-cluster head node

Send F_I to the cluster head node;

else

Aggregate the data sent by the remaining nodes;

end if

End for

4 Simulation and performance analysis

In this work, we introduced a secure and efficient privacy-preserving data aggregation algorithm. To simulate the

clustering aggregation process of sensor nodes, we executed our algorithm on MATLAB. we suppose that 100 sensor nodes are deployed randomly in 100×100 area. The base station node is centrally located (50, 50). Set the proportion of the advanced nodes to be 0.1. Figure 6 demonstrates the random deployment of 100 sensor nodes in 100×100 area. Figure 7 demonstrates the result of cluster-head election. Figure 8 is the result of clustering by distance matrix. Figure 9 demonstrates the cluster heads gather the aggregation results to the base station.

4.1 Communication overhead

We analyze the communication overhead of CPDA, ILCCPDA and SECPDA algorithms respectively. In the CPDA algorithm, nodes within the cluster need to broadcast their own seeds within the cluster. Suppose a cluster has n nodes, So there are n nodes broadcasting the seeds, and each node needs to send encrypted data to other neighbor nodes, then each node sends $n-1$ data, finally, n sensor nodes will send their aggregation data to the cluster head node. In the ILCCPDA algorithm, n nodes send values to two nodes. The other nodes in the cluster will send the aggregation values to the cluster head node. In the SECPDA algorithm, each node randomly selects two nodes to send its own two privacy slicing information and corresponding false information respectively, then n nodes emit $4n$ data. Finally, n sensor nodes send the aggregation data to the cluster head node. We experimentally verified the analysis results. As can be seen from Fig. 10, in the whole network, SECPDA algorithm has less communication overhead than CPDA algorithm and is not significantly different from ILCCPDA algorithm. In SECPDA and ILCCPDA algorithms, both have private data slicing technology. With the increase of the number of clusters, the communication overhead of data is not very obvious, but the CPDA algorithm has been greatly increased.

The communication overhead in the whole network needs to consider the communication overhead formed by the network topology, the communication overhead in a cluster and the communication overhead between clusters. The Fig. 11 is a simulation of the communication overhead in the whole network. As can be seen from the Fig. 11, the communication overhead in the whole network of SECPDA algorithm and ILCCPDA algorithm is less than CPDA algorithm.

4.2 Privacy performance analysis

In CPDA algorithm, when the sensor nodes exchange messages within the same cluster, the privacy data will be leaked to the neighbor nodes. For a cluster of size m, the node sends $m-1$ encrypted messages to the other $m-1$ members of the cluster. The node can only be cracked if the attacker obtains the $m-1$ keys, Otherwise, private data cannot be exposed. The average

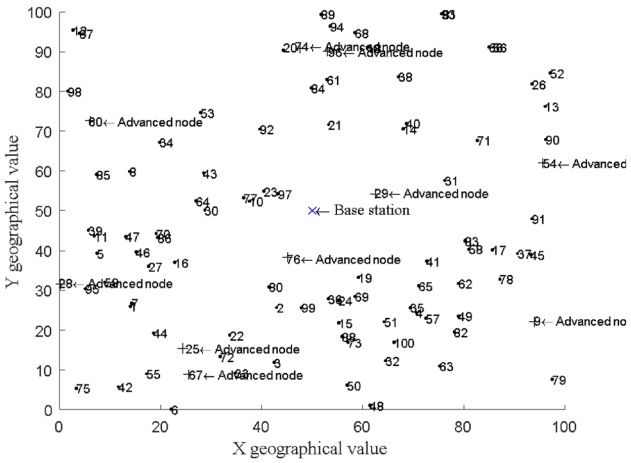

Fig. 6 Sensor node distribution

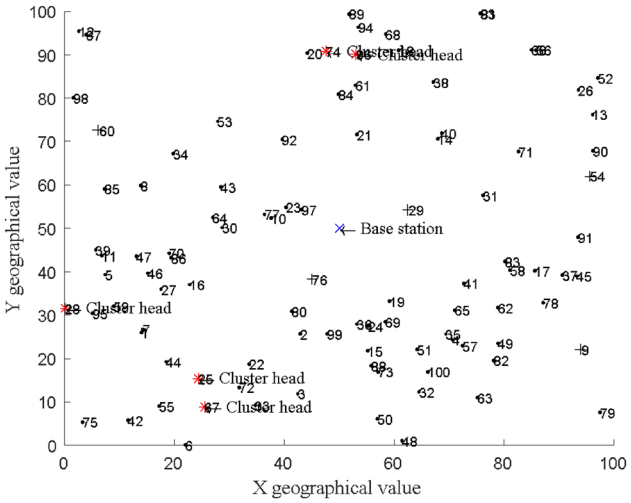

Fig. 7 Cluster head node election

probability of data of all nodes in the cluster being cracked can be obtained as demonstrated in Formula (13):

$$P_1(q) = \sum_{k=m_c}^{d_{\max}} P(m=k)\left(1-\left(1-q^{k-1}\right)^k\right). \tag{13}$$

Here, m_c is the minimum number of nodes in the cluster, and $d_{\max}$ is the maximum number of nodes in the cluster, and q is the probability that the node link is cracked.

In ILCCPDA algorithm, if an eavesdropper wants to steal data from node s, they must know the two slices of data from node s and the information from the neighbor node. Therefore, the eavesdropper must break the link between node s and the neighbor node that gets the slice information of node s, as well

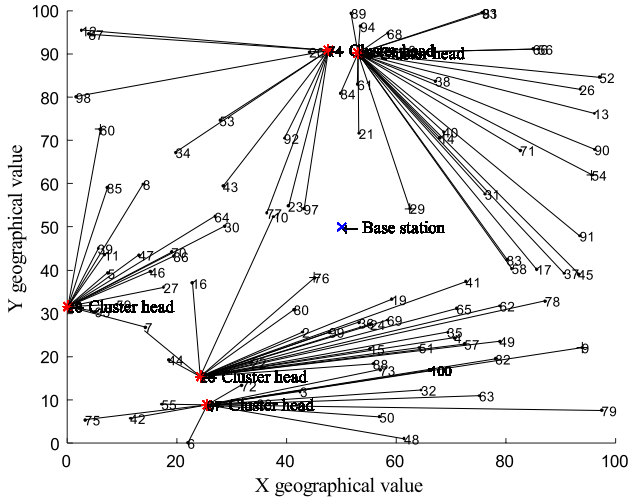

Fig. 8 Within the cluster aggregation

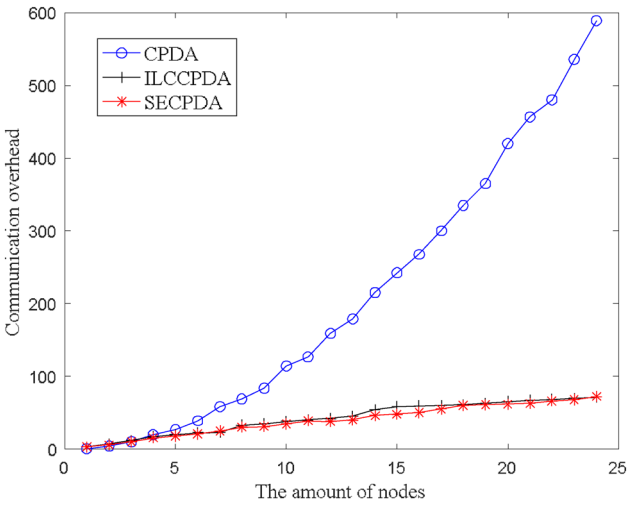

Fig. 10 Communication overhead comparison

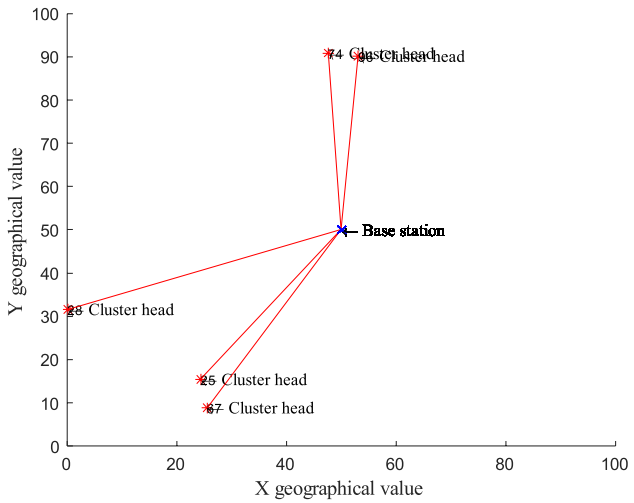

Fig. 9 Outside the cluster aggregation

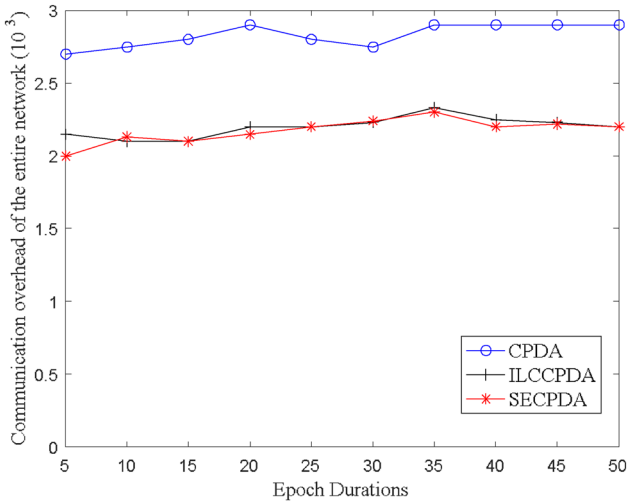

Fig. 11 Communication overhead of the entire network

as the link between the neighbor node and the cluster node. The average probability of data of all nodes in the cluster being cracked can be obtained as shown in Formula (14):

$$P_2(q) = q^2 \sum_{k=0}^{n-1} P(in = k) q^k. \tag{14}$$

Here, q^2 represents the probability of information being stolen from two neighboring nodes, and $\sum_{k=0}^{n-1} P(in = k) q^k$ represents the probability of all transmitted information being stolen.

In our proposed SECPDA algorithm, each node in the cluster randomly selects two neighbor nodes, then sends encrypted privacy slices and false information to the neighbor node. And, each node only sends two encrypted messages, and the number of encrypted messages received by each node is uncertain. The attacker needs to crack the slice information sent by the node and the information received by the node. Therefore, the average probability of data of all nodes in the cluster being cracked as demonstrated in Formula (15):

$$P_3(q) = C_2^1 q C_2^1 q \sum_{k=0}^{n-1} P(in = k) C_2^1 q^k. \tag{15}$$

Here, q is the probability that the node link is cracked. $C_2^1 q C_2^1 q$ is the probability of messages being cracked, $\sum_{k=0}^{n-1} P(in = k) C_2^1 q^k$ is the probability of the received message being cracked, C_2^1 stands for which of the hacked information is slice information or false message. $P(in = k)$

represents the probability that k nodes send information to node s. $P(in = k)$ is shown in Formula (16):

$$P(in = k) = C_{n-1}^{k}\left(\frac{1}{n-1}\right)^{k}\left(\frac{n-2}{n-1}\right)^{n-1-k}. \quad (16)$$

When the probability of node link being cracked takes different values, the comparison of the probability of private data being stolen from CPDA, ILCCPDA and SECPDA algorithm is shown in Fig. 12. In Fig. 12, the privacy protection capability of SECPDA algorithm is higher than that of CPDA algorithm and ILCCPDA algorithm.

Security proof The attack model is as follows.

We suppose that any adversary (Liu et al. 2020a, b; Wang et al. 2020a, b, c, d) wants to steal the private data of node A, the adversary needs to obtain all slice data (a1, a2 and a3) of private data a. Such an approach is harder to obtain the privacy data a than the unsliced private data. When this adversary attacks the privacy data, the attacker still can't get rid of the interference of false information. This is owning to the false information and slice privacy data are encrypted with this random key distribution scheme. Even if the data (sent by node A to other nodes) is intercepted by the adversary, the adversary also needs to ensure whether the eavesdropped data is a slice data of private data or a false data.

If any adversary wants to impersonate the node and exchange the slice data with some attacked nodes. Owing to the slice data is only a part of private data, the slice data does not make much sense, and the node also have false information to interfered, which increases the difficulty of being intercepted.

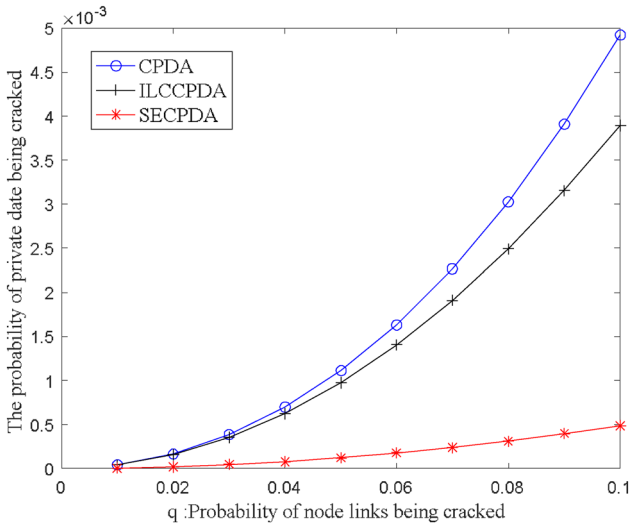

Fig. 12 Privacy comparison

We can utilize the probability formula to analyze the privacy protection capability. In Formula (15), when $q = 0.02$, $P_3(q)$ is about 0, which has a very low probability of being intercepted.

5 Conclusion

We propose a new data aggregation privacy protection algorithm called SECPDA, based on CPDA algorithm. Our algorithm adopts SEP protocol for cluster head elections and nodes aggregation. It greatly reduces communication overhead. The ability of privacy protection is improved by adding false information to interfere. After theoretical analysis and simulation experiments, the privacy performance of the SECPDA algorithm is better than CPDA algorithm and ILCCPDA algorithm, data traffic is also effectively reduced. For the future work, we are going to investigate how to ensure the integrity of data in the transmission process.

Funding Funding was provided by National Natural Science Foundation of China (Grant No. 61962009), Major Scientific and Technological Special Project of Guizhou Province (Grant No. 20183001), Open Funding of Guizhou Provincial Key Laboratory of Public Big Data (Grant No. 2018BDKFJJ005).

References

Afshin K, Maede AT, Ladani BT (2019) An efficient privacy-preserving data aggregation scheme in smart grid. In: 27th Iranian conference on electrical engineering (ICEE), pp 1967–1971

Bista R, Kim Y, Song MS, Chang JW (2012) Improving data confidentiality and integrity for data aggregation in wireless sensor networks. IEICE Trans Inf Syst 95:67–77

Fang W, Wen XZ, Xu J (2017) CSDA: a novel cluster-based secure data aggregation scheme for WSNs. Clust Comput 22:5233–5244

Feng TM, Wang C, Zhang WS et al (2008) Confidentiality protection for distributed sensor data aggregation. In: 27th conference on computer communications, pp 56–60

Guo H (2012) A modified scheme for privacy-preserving data aggregation in WSNs. In: 2nd international conference on consumer electronics, pp 790–794

Guo ZW, Ding XJ (2014) Low energy-consuming cluster-based algorithm to enforce integrity and preserve privacy in data

aggregation. In: 13th international symposium on distributed computing and applications to business, pp 152–156
He WB, Liu X, Hoang N, Klara N, Tarek A (2007) PDA: privacy-preserving data aggregation in wireless sensor networks. In: 26th IEEE international conference on computer communications, pp 2045–2053
He WB, Liu X, Nguyen H, Nahrstedt K (2009) A cluster-based protocol to enforce integrity and preserve privacy in data aggregation. In: 29th IEEE international conference on distributed computing systems workshops, pp 14–19
He DB, Neeraj K, Sherali Z, Alexey V, Laurence TY (2017) Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries. IEEE Trans Smart Grid 8(5):2411–2419
He J, Cai L, Cheng P, Pan J, Shi L (2019) Consensus-based data-privacy preserving data aggregation. IEEE Trans Autom Control 64(12):5222–5229
Heinzelman WR, Chandrakasan A, Balakrishnan H (2000) Energy-efficient communication protocol for wireless microsensor networks. In: 33rd annual Hawaii international conference on system sciences
IanF A, Weilian S, Yogesh S, Erdal C (2016) A survey on sensor networks. IEEE Commun Mag 40(8):102–114
Kong W, Shen J, Vijayakumar P, Cho Y, Chang V (2020) A practical group blind signature scheme for privacy protection in smart grid. J Parallel Distrib Comput 136:29–39
Laurent E, Virgil DG (2002) A key-management scheme for distributed sensor networks. In: 9th ACM conference on computer and communications security, pp 41–47
Liu Y, Guo W, Fan CI, Chang L, Cheng C (2018) A practical privacy-preserving data aggregation (3PDA) scheme for smart grid. IEEE Trans Ind Inf 15(3):1767–1774
Liu XZ, Yu XY, Zhu HJ, Yang GY, Wang YL, Yu XM (2020a) A game-theoretic approach of mixing different qualities of coins. Int J Intell Syst 35:1899–1911
Liu XW, Yu JG, Zhang XW, Zhang Q (2020b) Energy-efficient privacy-preserving data aggregation protocols based on slicing. EURASIP J Wirel Commun Netw 1:1–12
Madden S, Franklin MJ, Hellerstein JM, Hong W (2002) TAG: a tiny aggregation service for ad-hoc sensor networks. ACM SIGOPS Oper Syst Rev 36(1):131–146
Man DP, Wang CY, Yang W, Wang W, Xuan SC, Jin XP (2017) Energy-efficient cluster-based privacy data aggregation for wireless sensor networks. J Tsinghua Univ 57(2):213–219
Muhammad M, Romana T, Ali HS, Sandeep P (2020) A multi-sensor data fusion enabled ensemble approach for medical data from body sensor networks. Inf Fusion 53:155–164
Ozdemir S, Yang X (2008) Integrity protecting hierarchical concealed data aggregation for wireless sensor networks. Comput Netw 55(8):1735–1746
Sabrina B, Djallel EB, Azeddine B, Homero TC (2018) Big data challenges and data aggregation strategies in wireless sensor networks. IEEE Access 6:20558–20571
Smaragdakis G, Matta I, Bestavros A (2004) SEP: a stable election protocol for clustered heterogeneous wireless sensor networks. In: second international workshop on sensor and actor network protocols and applications (SANPA)
Smita D, Mrinal KD (2019) A survey on coverage problems in wireless sensor network based on monitored region. In: Advances in data and information sciences, pp 349–359
Wang YL, Yang GY, Li T, Li FY, Tian YL, Yu XM (2020a) Belief and fairness: a secure two-party protocol toward the view of entropy for IoT devices. J Netw Comput Appl 161:102641
Wang YL, Yang GY, Bracciali A, Leung HF, Tian HB, Ke L, Yu XM (2020b) Incentive compatible and anti-compounding of wealth in proof-of-stake. Inf Sci 530:85–94
Wang YL, Yang GY, Li T, Zhang LF, Yu XM (2020c) Optimal mixed block withholding attacks based on reinforcement learning. Int J Intell Syst 9:2032–2048
Wang YL, Bracciali A, Yang GY, Li T, Yu XM (2020d) Adversarial behaviours in mixing coins under incomplete information. Appl Soft Comput 96:106605
Yang Y, Wang XR, Zhu SC, Cao GH (2008) SDAP: a secure hop-by-hop data aggregation protocol for sensor networks. ACM Trans Inf Syst Secur 11(4):356–367
Yang GY, Wang YL, Wang ZJ, Tian YL, Li SZ (2020) IPBSM: An optimal bribery selfish mining in the presence of intelligent and pure attackers. Int J Intell Syst 35(11):1735–1748
Yao J, Wen G (2008) Protecting classification privacy data aggregation in wireless sensor networks. In: 4th international conference on wireless communications, pp 1–5
Zhang J, Hu P, Xie F, Long J, He A (2019) An energy efficient and reliable in-network data aggregation scheme for WSN. IEEE Access 6:71857–71870