



Research and Improvement of Wireless Sensor Network Secure Data Aggregation Protocol Based on SMART

Jun Wang¹ · Yu Chen¹

Received: 16 October 2017 / Accepted: 26 December 2017
© Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract

The privacy-preserving of information is one of the most important problems to be solved in wireless sensor network (WSN). Privacy-preserving data aggregation is an effective way to protect security of data in WSNs. In order to deal with the problem of energy consumption of the SMART algorithm, we present a new dynamic slicing D-SMART algorithm which based on the importance degree of data. The proposed algorithm can decrease the communication overhead and energy consumption effectively while provide good performance in preserving privacy by the reasonable slicing based on the importance degree of the collected raw data. Simulation results show that the proposed D-SMART algorithm improve the aggregation accuracy, enhance the privacy-preserving, reduce the communication overhead to some extent, decrease the energy consumption of sensor node and prolong the network lifetime indirectly.

Keywords Component · Dynamic data slicing · Wireless sensor network · Data aggregation · Privacy-preserving · Communication overhead

1 Introduction

Wireless sensor networks (WSNs) is a multi-hop self-organizing network formed by a large number of wireless sensor nodes through wireless communication. A large number of sensor nodes are randomly deployed in different environments (for example, some bad environments that human can't stay for long time), which be used to sense and collect target information so that people can analyze and process it to make reasonable judgments. Nowadays, wireless sensor networks are applied in many areas, such as environmental monitoring, military field, intelligent transportation, logistics tracking, intelligent healthcare [1–3] and so on.

However, the sensor node has many disadvantages in the real world at the same time. For example, the sensor node energy is limited and can not add energy, when collecting information, data calculation and sending data, the sensor node will consume energy. The energy consumption of each

node will affect the lifetime of entire network. Paper [4, 5] shows that the amount of energy consumed by one Berkeley node executing 800 instructions is almost similar to the energy consumed to transmit 1bit data, therefore, the data traffic between nodes can not be too large in order to extend the life cycle of entire network; The nodes are deployed in an unattended environment and are easily captured by an adversary. The attacker can either steal confidential data directly or tamper the confidential data through faking the sensor node, and the collected data is easy to be detected and eavesdropped when the data are transmitting by wireless. Therefore, it is very important to invent an efficient privacy protection algorithm.

Nowadays, Wireless sensor nodes usually are deployed in military, medical and smart grid and other related applications to collect data, in such a highly confidential application, data leakage and tampering will result in an unpredictable loss. If we can't protect the data confidentiality, this will expose attackers with highly-sensitive privacy information such as operational environment information in battlefield surveillance applications and patient medical records in healthcare applications. The attacker will know lots of information, which would threaten our security and life.

Although many researchers have proposed a series of aggregation algorithms that can provide data information

✉ Jun Wang
Wj_software@hotmail.com

Yu Chen
1139068321@qq.com

¹ Computer Science and Technology, Shenyang University of Chemical Technology, Shenyang, China

security algorithms. That can protect the data confidentiality. But there are still some problems with the data confidentiality. After looking through many different data security aggregation algorithms. We presents a D-SMART data aggregation algorithm based on the SMART [3]. The improved D-SMART algorithm extends the network life cycle and enhances the privacy protection.

The rest of the paper is organized as follow: Section 2 presents some typical wireless sensor network security data aggregation algorithms. Section 3 introduces the SMART security data aggregation algorithm in detail. Section 4 states the proposed D-SMART algorithm in detail. Section 5 describes the simulation results, and the paper concluding remarks in Sect. 6.

2 Wireless Sensor Network Security Data Aggregation

Data aggregation technology is one of the key technologies of wireless sensor networks. It can remove redundant information in the network and reduce the amount of data transmission, thus effectively improve the energy and bandwidth efficiency of the whole network [6–8]. However, the computing power, storage capacity and energy supply of the wireless sensor nodes are very limited, and all the nodes form the network through wireless self-organization. Therefore, the wireless sensor network data aggregation process is vulnerable to various types of attacks. Through the research and analysis of the development of wireless sensor network security data protection technologies, we can see the potential of the security data protection technology in the future [9–11].

Some typical wireless sensor network security data aggregation algorithms were proposed such as the SMART algorithm, the CPDA algorithm, the ESPDA algorithm and so on.

- (a) The SMART algorithm is a secure data aggregation algorithm based on data slicing technology. The basic idea of the SMART algorithm is to slice the original data information collected by each sensor node in the monitoring target into a fixed number of data slices, and then send the data slices randomly to their own neighbor node, after all nodes have received the data slices and mixed them, the new mixed data will be sent to the aggregation node for data aggregation operation. In this way, when the network is attacked, the node data information is intercepted, the attacker only get several incomplete data slices and not complete the data information, effectively protect the privacy of monitoring data, but it would consume more energy.
- (b) In the Cluster-based Privacy Data Aggregation (CPDA), the sensor nodes hide the real data values by

adding random seeds and private random values to the original data. The cluster head node solves the exact summation aggregation result by algebraic properties of polynomials. However, it is performed by way of polynomial algebra, which not only requires a large amount of computation, but also needs to send information with each neighbouring nodes during aggregation process, resulting in huge energy consumption.

- (c) Cam and Ozdemir proposed a pattern-based clustered wireless sensor network security data aggregation protocol Energy-efficient and Secure Pattern-based Data aggregation (ESPDA), the idea is as follows: the nodes calculate data pattern code after collecting the original data (the original data are classified and identified by the pattern code, the original data with the same pattern code are similar and can be regarded as redundant data), and then nodes send data according to the pattern codes. If different sensor node sets have the same pattern Code, only need to send one of the encrypted original data to the cluster head node. So the whole original data aggregation process becomes the aggregation of pattern codes, the original data information can be hidden better. This approach achieves more efficient aggregation, but has the disadvantage of being resistant to external attacks and not defending against attacks from internal nodes [12–15].

3 The SMART Security Data Aggregation

Security data aggregation is the core of wireless sensor networks privacy and security [16–20]. The Slice-Mix-AggRegaTe (SMART) security data aggregation algorithm was proposed by He et al. [3]. This algorithm introduces data slice and mix technology into wireless sensor network security data aggregation issues in the study, provide better privacy protection for the data aggregation process. The security performance and practicality of the SMART algorithm are validated in the simulation experiment [21]. This data privacy protection mechanism is implemented by three phases: the Slice phase, the Mix stage, and the Aggregation phase. The workflow of the protection mechanism is listed as follows:

- (a) In the Slice phase, the sensor node slices the collected original data into J ($J \geq 3$) data slices, and J is a fixed value. In addition to retaining one of the original slices, the node randomly distributes the remaining $J - 1$ data slices to other neighbour nodes.
- (b) In the Mix phase, the nodes mix the received data slices with its own remaining original data slices into a new packet.

- (c) In the Aggregation phase, the nodes transmit the mixed data packets to the aggregation nodes. The aggregation nodes will aggregate the collected data and the received data from other nodes, then continue to transmit to the upper node until all the aggregation data arrives at the base station, and finally integrate and decrypt all the data slices at the base station to obtain the real data.

Although the SMART algorithm has a good data privacy protection performance, but there are still some other deficiencies that affect its practicality. First of all, sending a number of data slices will result in largely increasing the data traffic between nodes, which reduces the working life of nodes in the data slice phase. According to the privacy probability formula in the SMART algorithm, it can be seen that the privacy protection performance of the algorithm is proportional to the number of data slices J, which cause the network system to make compromise on network working life in order to obtain better network security performance. Secondly, with the increase of data transmission, the probability of occurrence of data transmission collision, delay, error will rise, and ultimately affect the accuracy of data aggregation results and data aggregation efficiency [22–24]. The proposed security data aggregation D-SMART algorithm is based on the optimization and improvement of SMART algorithm is a more secure and efficient data aggregation algorithm.

4 Improvements to the SMART Algorithm

In the SMART algorithm, the sensor node does not consider whether the perceived information is important or not, slice all the collected data into three slices, but sometimes some unimportant data also be sliced into 3 slices is unnecessary, just consuming excess energy; it is too less to be sliced into 3 slices for some very important data, reducing the data privacy protection performance so that easily reveal the important data.

4.1 The Basic Idea of the D-SMART Algorithm

In this case, we propose the D-SMART algorithm which base on dynamical slicing technology. The algorithm classify the perceived data into three different degree according to their importance, then dynamically slice data and then send the slices according to the importance degree of the perceived data. Unimportant data will be less sliced, important data will be more sliced, the ordinary degree data (2 slices), the important degree data (3 slices), the confidential degree data (4 slices). The algorithm improves the shortcomings of the SMART algorithm in terms of data transmission and data aggregation accuracy, optimizes the construction style of tree

aggregation network. It enhances the data privacy protection, reduce the communication cost and computing load of sensor nodes and prolong the network life.

4.2 The Standards of Dynamic Slicing

In this paper, the degree of deviation between the perceived variables by the sensor nodes and the magnitude of their mean values is used to determine the importance degree of the perceived data. Assuming that the sensor node senses x temperature values during T minutes, you can set:

$$\chi = \frac{x_1 + x_2 + \dots + x_n}{x}, \quad \sigma^2 = \frac{\sum (x_i - \chi)^2}{x - 1} \tag{4.1}$$

we use the degree of σ^2 decide the data slice number as follow:

$$\begin{cases} \text{Ordinary Data-2 slice, } & \sigma^2 < T_1 \\ \text{Important Data-3 slices, } & T_1 \leq \sigma^2 \leq T_2 \\ \text{Confidential Data-4 slices, } & \sigma^2 > T_2 \end{cases} \tag{4.2}$$

The T_1 and T_2 are given threshold.

4.3 The Implementation Steps of the D-SMART Algorithm

In this paper, the wireless sensor network is abstracted as the connected graph $G(V, E)$, where V denotes the sensor node set, $|V| = N$ denotes the number of sensor nodes, and E denotes the communication link of the sensor nodes [25].

In this chapter, all the nodes are classified into three types: Base Station (BS), Aggregator Node (AN) and Leaf Node (LN), where BS is located at the top of the tree-type aggregation network, the aggregator node and the leaf node are distributed at the bottom of the network, The leaf node is only responsible for collecting the data and passing it to the aggregator nodes. The aggregator nodes aggregate these data slices into a new packet and pass the new packet to the BS node. The BS node obtains the final data aggregation result. So we define the data aggregation function as follow [26, 27]:

$$y(t) = f(d_1(t) + d_2(t) + \dots + d_i(t)) \quad (i = 1, 2, \dots, N) \tag{4.3}$$

In the function, $d_i(t)$ represents the data collected by node i at time t (as is shown in Fig. 1). There are many typical data aggregation functions, such as count, average, max, min, etc. can be simplified to sum function, so we use the sum function:

$$y(t) = \sum_{i=1}^N d_i(t), \tag{4.4}$$

as the research object in this article.

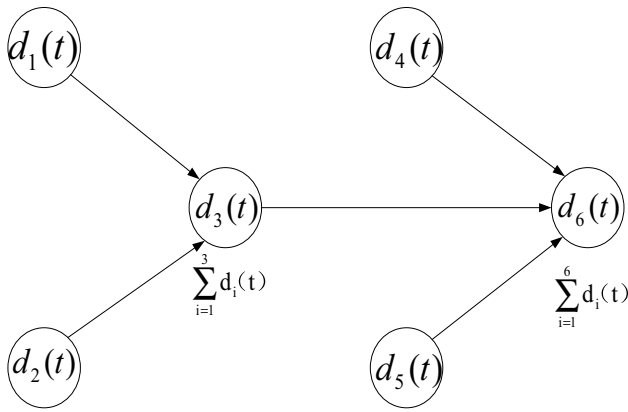


Fig. 1 Data aggregation sum function diagram

1. The phase of building the data aggregation tree

- (a) The BS node broadcasts the “hello” message to the nodes at network lower level to recruit the child nodes. After receiving the “hello” message, any nodes can send the “join_request” message to the sender to apply as its child node. If the node already has a parent node, it will not reply. If a node receives many “hello” messages at the same time, it will randomly select a sender to reply the “join_request” message to become the child node of the sender node. Then the sender acknowledges its node relationship after receiving the “join_accept message”.
- (b) The system given value P_a determines the probability that any node becomes the aggregator node in the network. Assuming that the total number of nodes is N in the network, so the number of aggregator nodes is $N * P_a$, the number of other $N*(1 - P_a)$ node are leaf nodes. The aggregator nodes continue to broadcast the “hello” message to the lower neighbor node to recruit the child nodes. When the recruiting behaviors are over in the network, the construction of the data aggregation tree is complete [28–30].

2. The data slicing phase

The sensor node dynamically slice the collected original data depending on the degree of σ^2 , encrypt these data slices through the shared keys, then send these data slices to their neighbor nodes. We can see from Fig. 2.

3. The data mixing phase

The sensor node decrypts the received data slices and mixes them with its previous retaining raw slice to generate

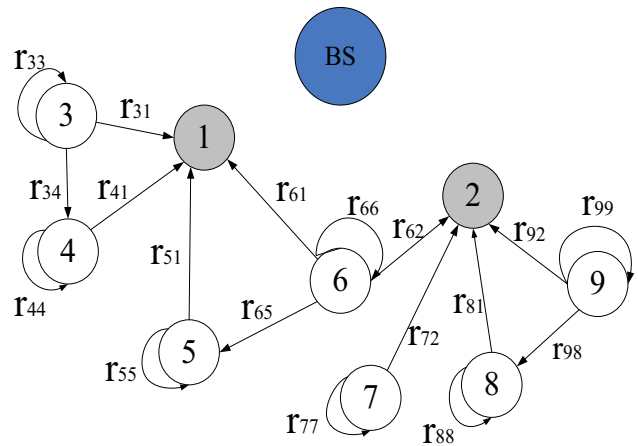


Fig. 2 Data slicing

a new packet. A_b is the new packet after the mixed calculation of node b , U_b is the nodes set which send slice to node b , r_{ab} represents the number of slice. The data slices mixed operation function is defined as:

$$A_b = \sum_{a \in U_b} r_{ab} \tag{4.5}$$

We can see from Fig. 3

4. The data aggregation phase

After the aggregator nodes accept all data slices sent by their child nodes. The aggregator nodes decrypt the slices and then perform the aggregation operation, after encrypting

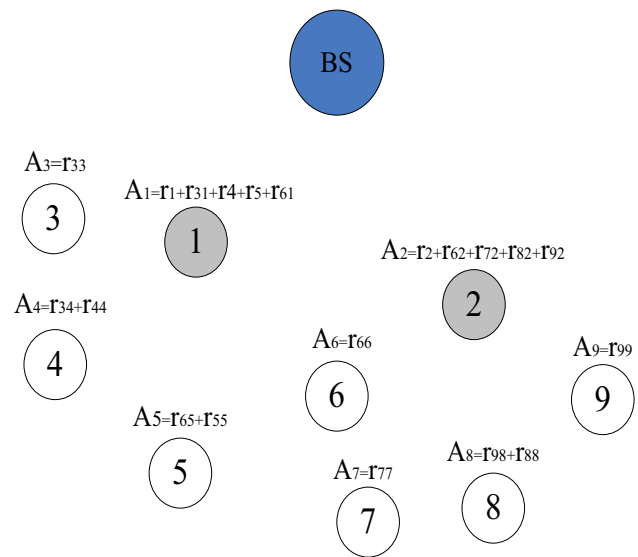


Fig. 3 Data mixing

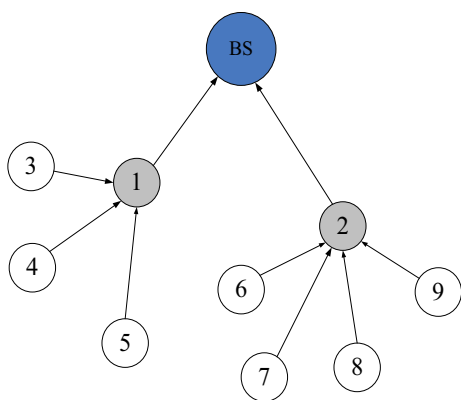


Fig. 4 Data aggregation

the aggregation result and pass it to the base station. When all the mixed data arrives at the base station, the base station decrypts these mixed data with the shared key and obtains the final data aggregation result. We can see from Fig. 4.

We can see the whole process of D-SMART algorithm process from Fig. 5.

We can see that after the construction of TAG tree, the sensor nodes start collect environment information in the preparing phase; Then, the sensor nodes evaluate the importance of information firstly, slice the data packet depending on the importance degree, mixing the slices into a new packet and aggregate the new packet.

5 Simulation Results and Analysis

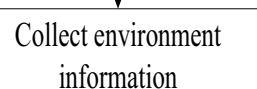
In this paper, we will use the embedded Simulator (SOS-SIM) in TinyOS as a simulation tool to simulate the network security performance of D-SMART algorithm, TAG algorithm and SMART algorithm respectively. The network environment is deployed as follows: 400 m * 400 m rectangular area, randomly distributing 600 sensor nodes at the region, the aggregator node ratio is set to $P_a = 0.1$, the background noise is -105 dBm, Gaussian white noise is 4 dB. Simulation experiments include: communication overhead, the data privacy protection performance and data aggregation accuracy.

5.1 The Performance of Privacy Protection

We define $P(q)$ as the probability of private data being decrypted and use it as a measure of privacy protection, where q is the probability that the link between nodes is decrypted.

In the SMART algorithm, the attacker must break all the $J - 1$ out-degree links and all the in-degree links, then he is

Preparing phase:



Privacy-preserving:

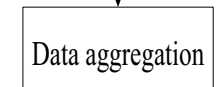
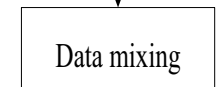
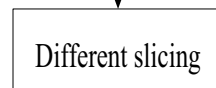
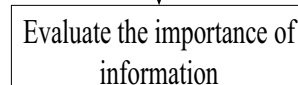


Fig. 5 D-SMART algorithm flow chart

able to completely break its privacy. Correspondingly, $P(q)$ can be defined as:

$$P(q) = q^{J-1} \sum_{k=0}^{d_{in_max}} P(\text{in-degree} = k)q^k \tag{5.1}$$

d_{in_max} represents the maximum in-degree value of nodes in the network in the formula. The value of d_{in_max} in the SMART algorithm is determined by J ; $p(\text{in-degree} = k)$ represents the probability of the node in-degree value k ; $\sum_{k=0}^{d_{in_max}} P(\text{in-degree} = k)q^k$ represents the probability of all the out-degree links between the nodes are eavesdropped; q^{J-1} represents the probability that all in-degree links between the nodes are eavesdropped. In the D-SMART algorithm, J represents the maximum number of slices generated by the leaf node; j represents the actual number of slices generated by the leaf node. It can be seen that the formula of the probability of the node privacy exposure $P(q, j)$ in the D-SMART algorithm as follow:

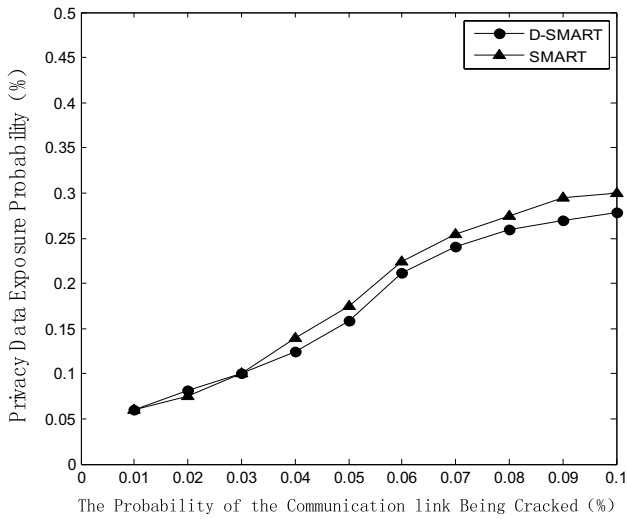


Fig. 6 Data privacy protection of SMART and D-SMART

$$P_D(q, J) = \sum_{j=1}^J P(\text{out-degree} = j)q^{j-1} * \sum_{k=0}^{d_{in,max}} P(\text{in-degree} = k)q^k \tag{5.2}$$

In the above formula, $P(\text{out-degree} = j)$ represents the probability that the number of out-degree links of the sensor node is equal to j ; $\sum_{k=0}^{d_{in,max}} P(\text{out-degree} = k)q^k$ represents the probability that all out-degree links in the node are eavesdropped.

From Fig. 6, with the increase of the probability of communication link being cracked, the privacy data exposure probability of the two algorithms is increasing rapidly. It can be seen that data exposure probability of D-SMART algorithm is higher than SMART algorithm until the probability of communication link being cracked is up to 0.03%. We can see that when the probability of communication link being cracked is up to 0.02%, the privacy data exposure probability is up to 0.082 in D-SMART algorithm, the privacy data exposure probability is up to 0.073% in SMART algorithm. After the point of 0.03%, data exposure probability of SMART algorithm is higher than D-SMART algorithm. We can see that when the probability of communication link being cracked is up to 0.07%, the privacy data exposure probability is up to 0.261 in D-SMART algorithm, the privacy data exposure probability is up to 0.273% in SMART algorithm. It is obvious that the probability of privacy exposure of node data in D-SMART algorithm is obviously lower than the SMART algorithm after the point of 0.03%.

5.2 The Data Communication Overhead

The data transmission between sensor nodes will consume a lot of energy, it is one of the key factors to prolong the network life cycle by reducing the energy consumption between nodes as much as possible. This chapter compares the data transmission overhead of TAG, SMART, and D-SMART algorithms by the simulation.

In the TAG algorithm, the sensor node directly forward its collected data to upper nodes in the network, and its data traffic is N . In the SMART algorithm, the data traffic is $N * J$, due to node data slicing and sending. In the D-SMART algorithm, the aggregator node does not slice and send the packet, only transmitting packet in the data aggregation phase, so the data transmission traffic is $N * P_a$. The number of leaf nodes are $N * (1 - P_a)$, and the number of out-degree links for each leaf node is J_i , J_i is the number of data slices of node i . So the data communication overhead of the D-SMART algorithm is:

$$N * P_a + \sum_{i=1}^{N(1-P_a)} J_i \quad (J_i \in 2, 3, 4) \tag{5.3}$$

$\sum_{i=1}^{N(1-P_a)} J_i$ ($J_i \in 2, 3, 4$) represent the number of slices send by leaf nodes.

The above Fig. 7 shows the network communication overhead of the three security data aggregation algorithms in the simulation environment. The network communication overhead of TAG algorithm is the lowest, keeping at 600 slices, the SMART algorithm is the highest, keeping at 1800 slices, the node slicing into [2–4] slices change in the D-SMART algorithm, the simulation results show that the D-SMART algorithm communication overhead is fluctuating between

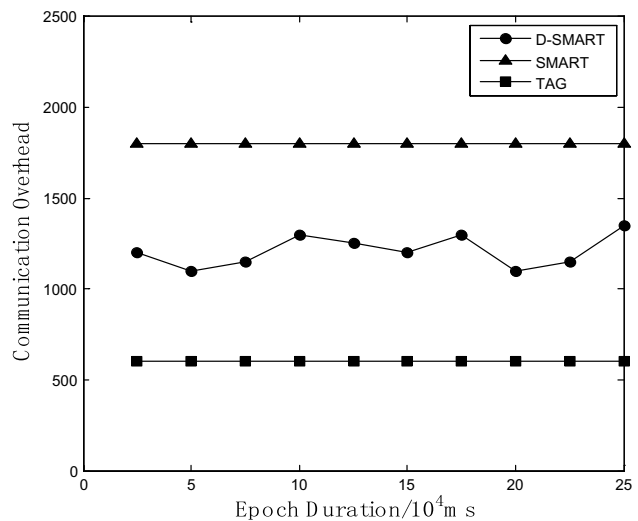


Fig. 7 Communication overhead of TAG, SMART and D-SMART

1200 and 1400 slices, so the network communication overhead between the TAG and SMART algorithm.

5.3 The Computation Overhead Analysis

One of the limitations of the wireless sensor network is the energy limitation of the sensor nodes. Although the data communication is the main energy consumption mode in the network, however, the energy consumption caused by the calculation load in the network can not be neglected, The computation overhead is also one of the factors that must be considered in the data aggregation security algorithm based on privacy protection in the network. In this section, we will discuss the calculation of the computational load and the effect on the energy consumption of the two algorithm in the network. Table 1 defines several different types of computation overhead.

Then, for the SMART algorithm, N sensor nodes perform N data slice calculation at the stage of data slicing, and at the same time these nodes need to encrypt and decrypt $N * (J - 1)$ slice data; In the process of data mixing, the sensor nodes need to perform $N * (J - 1)$ arithmetic computation. Then in the process of data aggregation, the nodes perform N arithmetic, encryption and decryption calculation. The computation load of the SMART algorithm— C_{smart} can be expressed as the follow equation

$$C_{SMART} = N * C_{div} + N * J * (C_{enc} + C_{dec} + C_{cal}) \quad (5.4)$$

In the process of data slicing of D-SMART algorithm, only $N * (1 - Pa)$ nodes perform $S_{D-SMART}$ data slice calculation at the stage of data slicing, then these nodes encrypt and encrypt $S_{D-SMART}$ slice data, In the process of data mixing, the sensor nodes need to perform $S_{D-SMART}$ arithmetic computation. Then in the process of data aggregation, the nodes perform N arithmetic, encryption and decryption calculation, thereinto, Pa represents the proportion of aggregation nodes and $a2, a3, a4$ respectively represents the ratio of different level nodes, so $Pa + a2 + a3 + a4 = 1$.

$$C_{D-SMART} = N * (1 - Pa) * C_{div} + (N + S_{D-SMART}) * (C_{enc} + C_{dec} + C_{cal}) \quad (5.5)$$

$$S_{D-SMART} = \sum_{i=1}^{N(1-Pa)} j_i \quad (j_i \in 2, 3, 4)$$

Equations 5.4 and 5.5 are the comparison between SMART algorithm and D-SMART algorithm. It can be seen from Eqs. 5.4 and 5.5 that $C_{SMART} - C_{D-SMART}$ have a close correlation between Pa and the number of slices j for each original data in the two algorithms, with the increase of j , the difference of $C_{SMART} - C_{D-SMART}$ will become bigger and bigger. In other word, the advantage of D-SMART algorithm computation load lowering SMART algorithm computation load will become more and more obvious.

$$C_{SMART} - C_{D-SMART} = N * Pa * C_{div} + [N * (j - 1) - S_{D-SMART}] * (C_{enc} + C_{dec} + C_{cal}) \quad (j \geq 3) \quad (5.6)$$

5.4 The Data Aggregation Accuracy

Data aggregation accuracy is one of the important indexes that reflects the accuracy performance of the security data aggregation algorithm. It is defined as the ratio of the actual aggregation result to the theoretical aggregation result:

$$Pa = \frac{D^*}{\sum_{i=1}^N Di}, \quad (5.7)$$

D^* represents the final aggregation result of the BS node; $\sum_{i=1}^N Di$ represents the theoretical aggregation. However, the

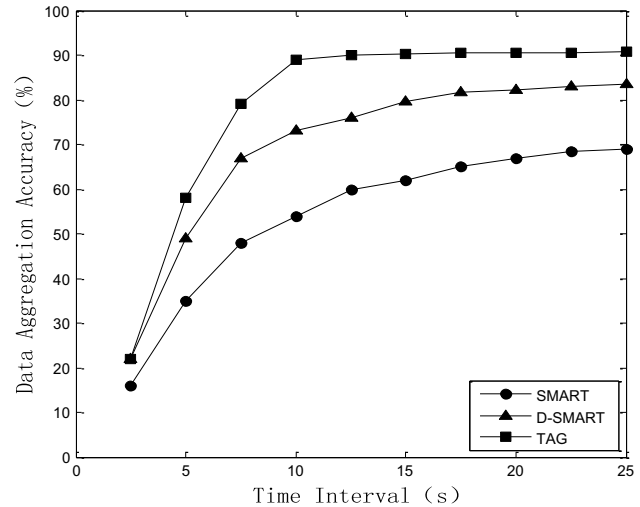


Fig. 8 Data aggregation accuracy of TAG, SMART and D-SMART (BER = 0.03)

Table 1 the sign of computation load

C_{div}	The energy consumption of a node performing a slice calculation
C_{cal}	The energy consumption of a node performing an arithmetic calculation
C_{dec}	The energy consumption of a node performing a decryption calculation
C_{enc}	The energy consumption of a node performing an encryption calculation

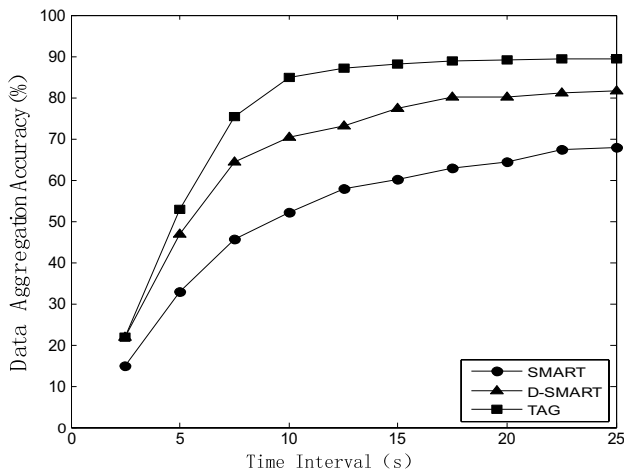


Fig. 9 Data aggregation accuracy of TAG, SMART and D-SMART (BER = 0.04)

process of data aggregation can not avoid the data collision, delay, retransmission and error of data transmission and so on. Different bit error rate (BER) will influence the aggregation result.

As can be seen from the two above graphs. From Fig. 8, when the BER is 0.03, with the increase of data aggregation time interval, the data aggregation accuracy of the three algorithms is increasing rapidly, in which the TAG algorithm is the fastest and the data aggregation accuracy up to 90% at 10 s; While the SMART algorithm increases at the slowest pace, the data aggregation accuracy up to approximately 54% at 10 s, the D-SMART algorithm growing between the TAG algorithm and the SMART algorithm. The three aggregation accuracy almost does not changes after 10 s, the data aggregation accuracy of SMART algorithm is the lowest up to 68.7%, the TAG algorithm data aggregation accuracy is highest up to 90.2%, the D-SMART algorithm data aggregation accuracy is still between the two algorithms up to 83.4%. From Fig. 9, when the BER is 0.04, with the increase of data aggregation time interval, the data aggregation accuracy of the three algorithms is increasing rapidly, in which the TAG algorithm is the fastest and the data aggregation accuracy up to 88% at 10 s; While the SMART algorithm increases at the slowest pace, the data aggregation accuracy up to approximately 52.1% at 10 s, the D-SMART algorithm growing between the TAG algorithm and the SMART algorithm. The three aggregation accuracy almost does not changes after 10 s, we can know that different BER cause different results, the BER is also a key factor to the aggregation accuracy.

6 Conclusion

Based on the analysis and study of other wireless sensor network security protection algorithms in terms of communication overhead, aggregation accuracy and the performance of privacy protection. We propose the D-SMART algorithm which improves the disadvantage of data aggregation accuracy and privacy protection of the SMART algorithm. Meanwhile reducing the data traffic, saving the energy consumption and prolonging the network lifetime.

Data integrity is also a challenge for data security protection. In the future, we will extend the data integrity on the basis of the D-SMART algorithm, we will protect the data integrity while protecting data privacy.

Acknowledgements This paper is supported by the project of Natural Science Foundation of Liaoning Province (2015020082, 2015020643), Liaoning BaiQianWan Talents Program, Liaoning Innovative Talents Program, Liaoning Special Professor Project and Shenyang program for scientific and technological innovation talents of middle and young people.

References

1. T. Ko, J. Hyman and E. Graham, Embedded imagers: detecting, localizing, and recognizing objects and events in natural habitats, *Proceedings of the IEEE*, Vol. 98, No. 11, pp. 1934–1946, 2010.
2. R. Szwedczyk and A. Ferencz, Energy implications of network sensor designs. Berkeley Wireless Research Center Report, 2000.
3. W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, PDA: privacy-preserving data aggregation in wireless sensor network. In *Proceedings of the 26th IEEE International Conference on Computer Communications*, Anchorage, AK, pages 2045–2053, 2007.
4. L. I. Sen and Yang Geng, Research on precision aggregation privacy-preserving algorithm in wireless sensor networks, *Computer Technology and Development*, Vol. 23, pp. 139–142, 2013.
5. Geng Yang, Sen Li and Zheng-yu Chen, High-accuracy and privacy-preserving oriented data aggregation algorithm in sensor networks, *Chinese Journal Of Computers*, Vol. 36, pp. 188–200, 2013.
6. Lu-sheng Shi and Xiao-lin Qin, Privacy-preserving data aggregation algorithm with integrity verification, *Computer Science*, Vol. 40, pp. 197–202, 2013.
7. Yong-jian Fan, Hong Chen and Xiao-ying Zhang, Data privacy preservation in wireless sensor networks, *Chinese Journal Of Computers*, Vol. 35, pp. 1141–1146, 2012.
8. Jiang-hong Guo and Jian-feng Ma, Efficient encrypted data aggregation algorithm for wireless sensor networks, *Journal of Xidian University*, Vol. 40, pp. 95–101, 2013.
9. Sun Long and Xu Ting-rong, A new uneven clustering routing protocol in WSN based on chain-cluster type, *Computer Applications and Software*, Vol. 32, pp. 106–109, 2015.
10. L. Wang and S.Y. Zhao, Research and application of key technology of secure data aggregation in wireless sensor network, *Computer Engineering and Applications*, pp. 63–79, 2016.
11. Zheng-yu Chen and Geng Yang, Survey of data aggregation for wireless sensor networks, *Application Research of Computers*, Vol. 28, pp. 1601–1604, 2011.

12. Sumedha Sirsikar and Samarth Anavatti, Issues of data aggregation methods in wireless sensor network: a survey, *Procedia Computer Science*, Vol. 49, pp. 194–201, 2015.
13. S. Roy, M. Conti and S. Setia, Secure data aggregation in wireless sensor networks: filtering out the attacker's impact, *IEEE Transactions on Information Forensics and Security*, Vol. 9, No. 4, pp. 681–694, 2014.
14. C.-X. Liu, Y. Liu and Z.-J. Zhang, High energy-efficient privacy secure data aggregation for wireless sensor networks, *International Journal of Communication Systems*, Vol. 26, No. 3, pp. 380–394, 2013.
15. M. Rezvani, A. Ignjatovic, E. Bertino and S. Jha, Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks, *IEEE Transactions on Dependable and Secure Computing*, Vol. 12, No. 1, pp. 98–110, 2015.
16. J. Girao, D. Westhoff, and M. Schneider, CDA: concealed data aggregation for reverse multicast traffic in wireless sensor networks. In *IEEE International Conference on Communications, 2005. ICC 2005*. 2005, vol. 5, pages 3044–3049, 2005.
17. Sankardas Roy, Mauro Conti and Sushil Jajodia, Secure data aggregation in wireless sensor networks, *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 3, pp. 1040–1052, 2012.
18. M. Conti, L. Zhang, S. Roy and R. DiPietro, Privacy-preserving robust data aggregation in wireless sensor networks, *Security and Communication Networks*, Vol. 2, pp. 195–213, 2009.
19. M. Yu, C. Li, G. Chen and J. Wu, An energy efficient clustering scheme in wireless sensor networks, *Journal of Control Theory and Applications*, Vol. 9, No. 1, pp. 99–119, 2011.
20. T.W. Kuo and M.J. Tsai, On the construction of data aggregation tree with minimum energy cost in wireless sensor networks: NP-completeness and approximation algorithms. In *IEEE INFOCOM*, pages 2591–2595, 2012.
21. C. M. Chao and T. Y. Hsiao, Design of structure-tree and energy-balanced data aggregation in wireless sensor networks, *Journal of Network and Computer Applications*, Vol. 12, pp. 2012–2030, 2012.
22. H. Yousefi, M. H. Yeganeh and N. Alinaghypour, Structure-free real-time data aggregation in wireless sensor networks, *Computer Communication*, Vol. 35, pp. 1132–1140, 2012.
23. S. Peter, K. Piotrowski, and P. Langendoerfer, On concealed data aggregation for WSNs. In *IEEE Consumer Communication and Networking Conference*, pages 192–196, 2007.
24. C. Castelluccia, E. Mykletun, and G. Tsudik, Efficient aggregation of encrypted data in wireless sensor networks. In *The Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services*, pages 109–117, 2005.
25. S.R. Madden and M.J. Franklin, TAG: a tiny aggregation service for ad hoc sensor networks. In *OSDI*, 2002.
26. Adwitiya Sinha and D. K. Iobiyal, Prediction models for energy efficient data aggregation in wireless sensor network, *Wireless Personal Communications*, Vol. 84, pp. 1325–1343, 2015.
27. Qi-biao Guo, Wireless sensor network based on homomorphic encryption security data aggregation analysis, *Network Security Technology and Application*, pp. 76–77, 2015.
28. H. Bao and R.A. Lu, A lightweight data aggregation scheme achieving privacy preservation and data integrity with differential privacy and fault tolerance, *Peer-to-Peer Networking and Applications*, pp. 1–16, 2015.
29. A. Sinha and D. K. Lobiyal, Prediction models for energy efficient data aggregation in wireless sensor network, *Wireless Personal Communication*, Vol. 72, No. 2, pp. 1–19, 2015.
30. A. Awang and S. Agarwal, Data aggregation using dynamic selection of aggregation points based on RSSI for wireless sensor network, *Wireless Personal Communication*, Vol. 80, No. 2, pp. 611–633, 2015.



Jun Wang is currently a professor at Shenyang University of Chemical Technology, PRC. He has received the B.Sc. and M.Sc. degrees in computer science from the Shenyang Institute of Chemical Technology, PRC in 2001 and 2005, respectively, and the Ph.D. degree from Shenyang Institute of Automation of CAS, PRC in 2009. Currently, He is a Vice-dean in Computer Science and Technology College, and leads the Internet of things and Cyberspace Security Lab. Since January 2010, he has been

invited as an Academic Visitor (including post-doctoral project as a post-doctor) at De Montfort University, UK. Since August 2012, he has been working as a post-doctor in Shenyang Institute of Automation of CAS. His research interests include wireless network, network cyberspace security and the Internet of things, etc.



Yu Chen is a Master student at Shenyang University of Chemical Technology. He received his Bachelor degree from Shenyang University of Chemical Technology in 2016, and started his master studying in 2016. His research interests are network security, Industrial Internet of things, etc.