Lu and Sun *EURASIP Journal on Wireless Communications and Networking* (2018) 2018:157
https://doi.org/10.1186/s13638-018-1173-7

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

A resilient data aggregation method based on spatio-temporal correlation for wireless sensor networks

Yong Lu* and Na Sun

Abstract

In wireless sensor networks, the existing data aggregation algorithms usually cannot evaluate the extent of data damage in presence of additive attacks. To resolve such problem, a resilient data aggregation method based on spatio-temporal correlation for wireless sensor networks is presented in this paper. On the basis of the distributed data convergence model, the algorithm combines the centroid distance and similarity to measure the attack degree of each cluster node's perceived data, and the weighted calculation can improve the convergence precision of data recovery. In addition, this method can obtain the estimated value of data sample of all clusters according to the temporal correlation characteristic of the nodes' perceived data at different time. Using the chi-square fitting, the extent of the data being tampered in each cluster can be measured effectively. Theoretical analysis and simulation results show our method can improve the restoration convergence precision as the attack increment is small. Also, it can enhance the robustness from noise interference.

Keywords: Wireless sensor networks, Resilient data aggregation, Similarity, Security

1 Introduction

In most applications of wireless sensor networks (WSNs), data aggregation is critical for reducing the transmission of redundant data effectively and prolonging the network lifetime. Due to the impact of node's deployment and transmission channel, data aggregation is always facing a severe challenge on security issues [1]. Especially as some nodes in WSN being captured, the input values of aggregation function will be modified involuntarily, which will increase the output error of the result. Therefore, the input values should be verified before aggregating the data being collected by sensor nodes. However, in traditional methods, once the malicious attacks being monitored, the perceived data of the sensor nodes will be discarded directly [2]. That will cause a great waste of resources and reduce utilization rate of sensor node's energy.

At present, the important issue is that the perceptual data is vulnerable to malicious tampering for data aggregation. Broadly, there are two different categories about those attacks. One is that the data is modified during the transmission process, which mostly can be detected by encryption technology. The other is that the data will be tampered with before the aggregation, and this kind of attack cannot be detected or blocked effectively by encoding [3]. Therefore, the data aggregation algorithms are proposed to solve this problem by validating the perceived data before entering the aggregate function. However, once the attack is detected, the traditional method will discard the data being collected by monitoring nodes directly [4]. This process mode can lead to a lot of waste of resources and reduce the utilization of network energy. In order to solve this problem, a variety of simple method of restoration and aggregation is proposed by using the samples that are not attacked [5], such as truncation method and shear mechanism, which can improve the energy utilization of the network. But those methods have some limitations. In this paper, we focus on spatio-temporal correlation of the perceptual data in cluster-based WSNs. In particular, we cope with the centroid distance and similarity to measure the attack degree of each cluster node's perceived data and

* Correspondence: yl_cun@yeah.net
School of Information Engineering, Minzu University of China, Beijing 100081, China

present a resilient data aggregation method based on spatio-temporal correlation (RDAS) for WSNs.

The rest of this paper is organized as follows: In Section 2, we review the related work. We describe the network model and assumptions and explain the details of our method in Section 3. Section 4 presents a thorough experimental evaluation and compares our solution with the state-of-the-art. Finally, we conclude this paper in Section 5.

2 Related works

Wireless sensor nodes are often deployed in a relatively open environment with self-organized architecture [6]. Owing to lack of physical link or fixed special protection equipment, a greater deal of security threat often confronts more severely in WSNs than traditional network [7]. From the perspective of secure routing, a special monitoring node is set up in WSN network to implement target monitoring. In order to solve the problem of high cost and difficulty to achieve, some security data fusion method is proposed.

Lv et al. [8] proposed a secure routing algorithm for WSNs based on credibility and gave a hierarchical routing trust model to eliminate malicious nodes through establishing secure routing. However, the main disadvantage is that the data correlation is ignored in spite of the trusted model being built from multiple perspectives. Safa et al. [9] is a cluster-based trust-aware routing protocol, which includes a hierarchical routing algorithm based on node's trust value. Each adjacent node conducts mutual trust value evaluation and then clusters in a self-organizing way. The intra-cluster nodes send the data to the trusted cluster head by directional diffusion, which can effectively guarantee the security of data transmission. Hu et al. [10] proposed a creditability-based data aggregation (CBDA) model based on trusted data fusion to ensure the authenticity and reliability of the generated aggregated data.

Zhang et al. [11] presented data fusion mechanisms based on immune in WSN, which uses the hierarchical distributed strategy to reduce the energy consumption of the network to the maximum extent and improves the reliability of the data fusion results by employing the adaptive characteristics of the immune system. However, the above mechanism cannot solve external malicious attacks effectively. Liu et al. [12] proposed a high-efficient and real-time data aggregation algorithm based on data integrity. The algorithm employs redundant theorems on sink node to verify the consistency of data to evaluate the reliability of the result. Also, a homomorphic encryption mechanism is conducted to provide security for data forwarding.

To improve the accurate rate of the data fusion results, Qiu et al. [13] presented a data aggregation in WSNs based on a deep learning model. By designing the stacked automatic encoders, the feature extraction classification model is established for all clusters, and the feature data is extracted and classified to aggregate the characteristic information of the same kind. Cui et al. [14] presented a malicious node detection algorithm based on secure data fusion in WSNs, which combines a false data filtering method for different geographic locations. The node's location is verified according to the data sent by the node to identify the malicious nodes that may exist in different regions according to the forged data. Du et al. [15] proposed a dynamic data fusion algorithm based on hierarchical routing queue. By setting a dynamic queue in the filtering node, the historical interactive data among the adjacent nodes can be stored and the redundant data of the network will be filtered, which can reduce the interference of redundant data to final fusion results.

Wager [16] first introduced the concept of resilient data aggregation and presented the specific issues that need to be resolved. Some simple solutions have put forward such as cutting method and truncated mechanism. Based on the random sample consensus paradigm, Buttyan et al. [17] proposed a resilient data aggregation mechanism in WSNs. This method checks consistency between model and sample by random sampling and constantly eliminates abnormal node data. After some experiments repeatedly, the remaining data set can be used as input of aggregate function. However, since the centralized data processing is conducted, the energy consumption of nodes is much higher. Especially when the attack does not exist in the network, still a large amount of data should be removed, and it result in low convergence precision. Luo et al. [18] presented a gray relationship degree and probability density parallel distance-based resilient data aggregation, which uses a distributed aggregation model to measure the degree of attack in view of gray correlation and probability density interval. The convergence precision has been improved, but its anti-noise performance is poor. Based on the above research, they proposed a similarity-based resilient data aggregation for WSNs [19]. The restoration precision of the method is high, and the robustness to the noise interference of the network is stronger. But when the amount of attack imposed on the perceived data is smaller, the expectation model cannot be selected accurately, and it results in the convergence of the reconstruction precision being not improved efficiently. To aim the problem of privacy preservation in intermediate nodes, Parmar et al. [20] proposed a data aggregation method with malleability resilient concealment to avoid loss of packets under active or passive attacks. The method can effectively protect the network from internal and external opponents and also implement conflicting objectives.

3 A resilient data aggregation method based on spatio-temporal correlation

3.1 Network model

By clustering method [21], the whole network can be divided into several clusters, where each node only belongs to one cluster and each cluster is assigned to one cluster head. All the data being collected by member nodes will be gathered by the cluster head, and then, the results will be transmitted to the base station by a multi-hop routing [22]. Considering that the attackers actually only has limited energy, it can be assumed as follows:

(1) Incremental attack, that is, the same value is added to the readings of each captured node.
(2) Constant attacks that modify the readings of the captured nodes to a certain constant.
(3) The attacker may not choose to capture the nodes at any position instead of the ones in the range of convenient operation nearby. Therefore, we can assume that the distribution of captured nodes located in the network is relatively concentrated.

3.2 Data similarity

Vuran et al. [23] have explicitly proposed the concept of data time-spatial correlation in the field of WSNs. Due to the dense deployment, the data collected by sensor nodes have spatial correlation. If the sampling interval is small enough, the sampling data between adjacent intervals demonstrates time correlation simultaneously.

For simplicity, M represents the total number of nodes in WSN and r represents the number of clusters. Besides, C_i denotes the i-th cluster with m_i member nodes and x_{ij} indicates the reading of the node j in the cluster C_i, and S_i indicates the set of perceived data by all nodes in the cluster C_i at a certain time, i.e., $\{x_{i1}, x_{i2}, \cdots, x_{ij}, \cdots\}$. Suppose that if the sensor nodes not be attacked, x_{ij} obeys independent co-distribution and the mathematical expectation μ and variance δ^2 are unknown. k represents the proportion of the nodes being attacked to all nodes.

By adopting the method of distribution fitting test [24], a cluster C_q by no attack or the weakest attack can be selected as the reference by expected model. Then, the data similarity in C_p and C_q will be measured to evaluate the degree of attack for cluster C_p. Assume that the monitoring data in cluster C_q is $x_{ij}^{(q)} (j = 1, 2, \cdots, n)$, which represents the historical data of i-th member node of cluster C_q at time j. Considering the discrete degree of the comparison of two groups, the influence of data units and measurement scales should be eliminated by standard deviation as much as possible. Also, the time variant property of the process should be highlighted. Hence, we have

$$\begin{cases} \mu_i = \dfrac{1}{N}\sum_{j=1}^{N} x_{ij}^{(q)} \\ \sigma_i = \sqrt{\dfrac{1}{N}\sum_{j=1}^{N}\left(x_{ij}^{(q)} - \mu_{ij}\right)^2} \end{cases} \tag{1}$$

Further, the coefficient of variation can be obtained as:

$$Corr_i = \frac{\sigma_i}{\mu_i} = \frac{\sqrt{N\sum_{j=1}^{N}\left(x_{ij}^{(q)} - \mu_{ij}\right)^2}}{\sum_{j=1}^{N} x_{ij}^{(q)}} \tag{2}$$

Suppose that the mean values of the data in the cluster C_p and C_q are $\overline{X}^{(p)}$ and $\overline{X}^{(q)}$, respectively, the centroid distance between C_p and C_q can be estimated as

$$dist(cp, cq) = \left|\overline{X}^{(p)} - \overline{X}^{(q)}\right| \tag{3}$$

In addition, the correlation coefficient of clusters C_p and C_q can be obtained based on the perceived data of nodes.

$$rel(cp, cq) = \frac{\sum_{j=1}^{N} Corr_i \times \left(x_{ij}^{(p)} - \overline{X}^{(p)}\right) \times \left(x_{ij}^{(q)} - \overline{X}^{(q)}\right)}{\sqrt{Corr_i \times \sum_{j=1}^{N}\left(x_{ij}^{(p)} - \overline{X}^{(p)}\right) \times \left(x_{ij}^{(q)} - \overline{X}^{(q)}\right)}} \tag{4}$$

Finally, the data similarity between the clusters C_p and C_q can be given as

$$\rho = \theta \times dist(p, q) + (1 - \theta) \times rel(cp, cq) \tag{5}$$

where θ is a tune parameter to allocate the weight value of correlation coefficient function and centroid distance.

Apparently, the data similarity can be used to represent the degree of similarity between two samples. By formula 5, it shows that the greater the correlation coefficient of the two samples, the greater the similarity between the two samples will be. In addition, if the greater the center of gravity between the two samples, the smaller the similarity is. In brief, the centroid distance reflects the difference between the mean value between C_p and C_q, and the correlation coefficient represents the degree of the comparison of monitoring data in clusters C_p and C_q. When the attack increment is small, the correlation coefficient can reflect the difference of the data being distorted and expectations in the reference model. Also, while there is noise interference in the network, the disturbance of each node's perceptual data can also accurately reflect the change of the correlation coefficient.

However, as the attack increment is large, the centroid distance can reflect the similarity between clusters C_p and C_q more accurately than the correlation coefficient.

3.3 Chi-square fitting degree

When the amount of attack behaviors is small, the chi-square statistic method can be conducted to evaluate the measurement of convergence in each cluster. By dividing the node's data of cluster C_i into c groups with equal interval, o_j and T_j denote the theoretical and actual frequency of the measured values for the interval j, respectively. Then, the chi-square statistics of the cluster i can be estimated as:

$$\chi_i^2 = \sum_{j=1}^{c} \frac{\left(o_j - T_j\right)^2}{T_j} \tag{6}$$

Hence, the chi-square fitting degree of cluster i can be obtained.

$$F_i = \frac{1}{1 + \chi_i^2} \tag{7}$$

From the above equation, it can be seen that the effect of fitting degree is similar to the utility estimation of information quality. As the assailant increases the increment of the attack on the captured nodes' perceived data, the discrepancy between the cluster and the reference model is more obvious. In contrast, when the attack increment is smaller, the parallel distance between the cluster's mean value and the probability density of mathematical expectation is almost the same [25]. However, the utility estimation of information quality should be obtained by means of the integration of covariance and a priori probability. It will result in long time for calculation and high energy consumption. Comparatively, the operation of chi-square fitting is much more oversimplified and the energy consumption can be reduced.

Further, the weight value corresponding to the fitting degree F_i of the cluster C_i chi-square can be obtained according to Lagrange's extreme value method.

$$\omega_i = \frac{F_i^2}{\sum_{j=1}^{r} F_i^2} \tag{8}$$

The chi-square value reflects the degree of coincidence between the actual frequency and the theoretical value. If it is assumed that the sample obeys the theoretical distribution, the difference between the actual frequency and the theoretical value will not be very large and vice versa. Thus, the smaller the χ_i, the actual sample is close to the theoretical value.

3.4 Resilient data aggregation method

When the amount of distort exerted by the attackers on the captured node's perceiving data is large, the difference between the cluster under attack and the normal cluster is more obvious. Therefore, the expected cluster C_q can be selected to reflect the degree of attack on the node's data in the cluster by using the centroid distance between them.

Considering the case of the aggregated function as the mean, X denotes the true value of the target variable to be obtained by the aggregation function and $\hat{X}$ represents the estimated value of the target variable. Suppose $\hat{X}_i$ to be the estimated value of the target variable of data sample in each cluster, the estimated value of the cluster i can be given as:

$$\hat{X}_i = \sum_{i=1}^{m_i} w_j \times x_{ij} \tag{9}$$

where m_i is the number nodes in cluster C_i and w_i is the weight value of member node j in the cluster i.

The entropy theory has been widely applied in engineering applications for probability inference based on incomplete samples and deal with uncertainty in intelligent systems [26]. If the entropy of a variable is smaller, the greater the amount of information provided by the variable will be. Considering the effect of the variable on the final result, a larger weight should be given. Based on entropy method, the weight value of the member node j in the cluster i can be determined.

$$\begin{cases} \gamma_j = -\frac{1}{\ln m_i} \sum_{i=1}^{m_i} \left(x_{ij} - \hat{X}_i^{(t-1)}\right) * \ \ln\left(x_{ij} - \hat{X}_i^{(t-1)}\right) \\ w_j = -\frac{1-\gamma_j}{\sum_{i=1}^{m_i} \left(1-\gamma_j\right)} \end{cases} \tag{10}$$

where $\hat{X}_i^{(t-1)}$ denotes the aggregated result at the previous interval.

The estimated values of the cluster samples will be calculated with weight value, then

$$\widehat{X'} = \sum \rho_i{}^* \omega_i{}^* \hat{X}_i \tag{11}$$

Next, the final aggregation results can be obtained by the cluster of the expected model and the value obtained by above formula.

$$\hat{X} = f\left(\widehat{X'}, \hat{X}_q\right) \tag{12}$$

4 Simulation results

There are 400 sensor nodes randomly deployed in a region with 100m × 100m square, and the whole network will be evenly divided into nine clusters. If there is no attack in WSNs, the data samples of the sensor nodes obey the distribution $N(0, \delta^2)$ and significance level $\alpha = 0.05$. In the following simulation experiments, the aggregation function is defined as the mean value and the attack mode is a constant attack, and 200 Monte Carlo experiments will be conducted in evaluation process. The attacks applied to the node are confined to additive attack, and the specific method is about constant accumulation, namely, the attackers will modify each of the reading of the captured nodes to achieve the same constant d.

Figure 1 shows the comparison of performance in aspect of absolute deviation when attack nodes are distributed in different numbers of clusters. The horizontal axis represents the value of the attack node ratio k, and the longitudinal axis indicates the absolute deviation between the result and the real value of different value of k. Besides, $\delta^2 = 4$ and constant d is equal to 10. It can be observed from the experimental results that when the malicious nodes are restricted to fewer clusters, its influence is relatively small and the final absolute deviation is lower. In addition, when the density of the attack node increases, the absolute deviation is also promoted fairly smoothly. It indicates that our resilient data aggregation algorithm can detect the extent of the data being tampered in time and effectively correct the fusion results.

Next, we compare the cluster weights in the process of data aggregation. Suppose the number of the clusters not being attacked is 3 and the value of d is set to 0.5 and a cluster that is not attacked is selected as the expected object. The weight assigned to other clusters in RDAS and LARA (linear approaches resilient aggregation) [27] is shown in Figs. 2 and 3, respectively. In LARA, there is no obvious difference in terms of the similarity between the attacked clusters and the expected one, and it shows LARA cannot determine the degree of attack of each cluster accurately. Comparatively, the clusters being attacked can be allocated as low weight value in RDAS. With the increase of the proportion of attack nodes, it illustrates more obviously. It can reduce the effects of the clusters being attacked on the final fusion results.

Figures 4 and 5 show the comparison in aspect of convergence restoration between RDAS, LARA, and ADDA (Attack Detectors Data Aggregation) [28]. When the attack increment is 0.5 and 10, the performance of RDAS is better than that of ADDA and LARA. In LARA, the correlation coefficient is defined as the convergence of weighted value for data aggregation. As can be seen from the results, when the attack increment is high, the correlation coefficient is not very suitable and the difference of weight value of each cluster is too large to affect the final result. With the use of gray relational degree, ADDA also needs to select the expected cluster. When the node's data fluctuation is small, the determination of the desired model will produce a great deal of error. RDAS makes use of the perceived data of all nodes so that the attacked nodes are concentrated in some clusters, and the more concentrated the attack nodes are, the smaller the convergence error is.

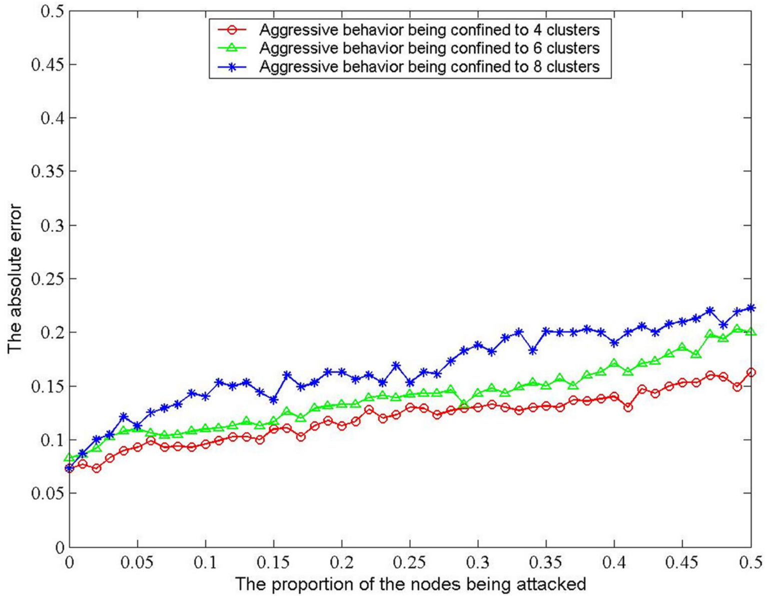

Fig. 1 Absolute error as attacks being occurred in different clusters

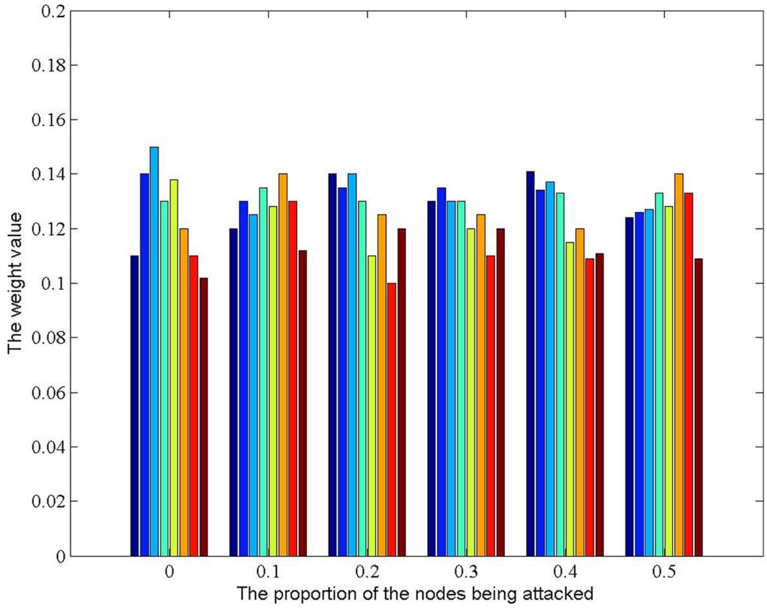

Fig. 2 The weight value of all clusters in LARA

As can be seen from Fig. 4, as $d = 0.5$, the error range of data reconstruction is about 0.08~ 0.28 in ADDA and 0.07~ 0.22 in LARA. Comparatively, the absolute error in RDAS can vary between 0.07 and 0.16. If $d = 10$, the absolute error in ADDA maintains between 0.15 and 0.27 as the proportion of attack nodes is small. With the increase of the number of attack nodes, it fluctuates at the range of 0.2~ 0.25 sharply. In general, the absolute error of LARA has the lower level of 0.13~ 0.31 than that of ADDA. Compared with LARA and ADDA, RDAS also shows better performance of different proportion of the attacked nodes in aspect of the absolute error as $d = 10$. The reason is that ADDA and LARA utilize the mean to represent the estimated value of the target variable of the cluster. However, the estimated value of target variables of all clusters by RDAS is obtained by

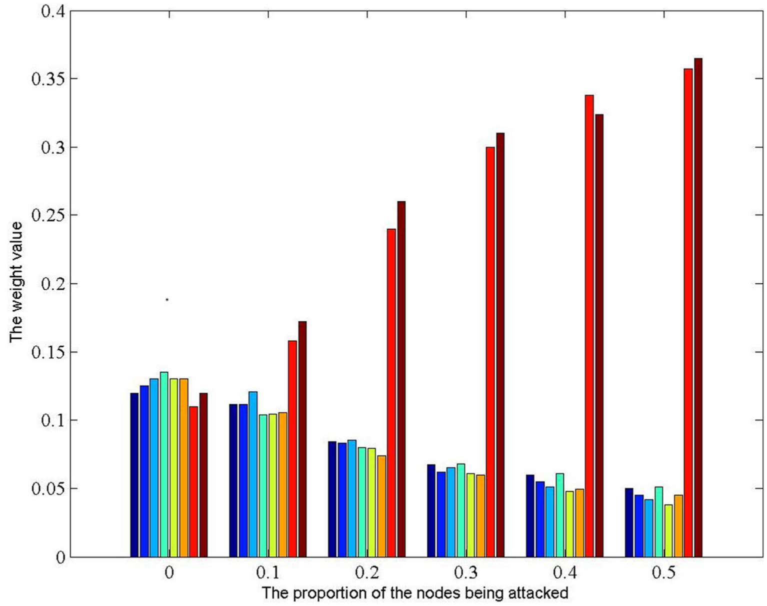

Fig. 3 The weight value of all clusters in RDAS

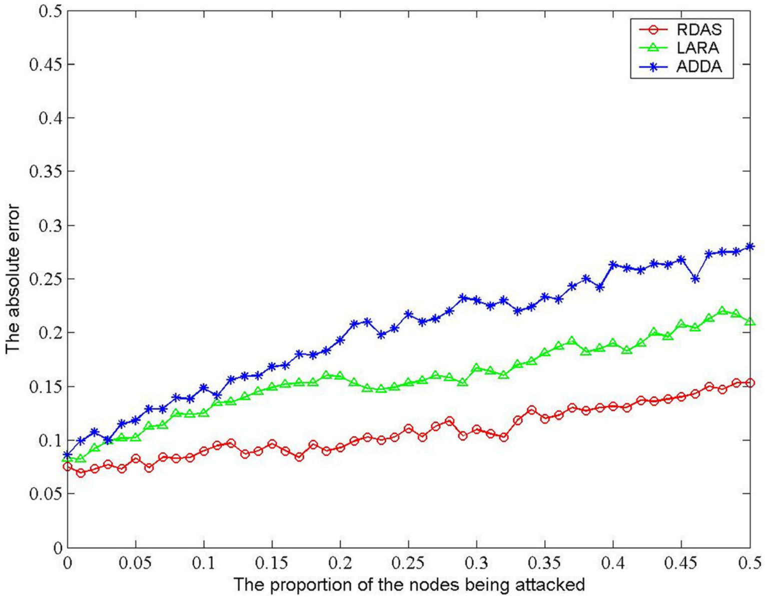

Fig. 4 The absolute error ($d = 0.5$)

using the time correlation of node's data, which can be aggregated in each cluster separately.

Figures 6 and 7 show the absolute error as a Gauss white noise N applied to each node's perceptual signal, and the signal-to-noise ratio is 0 and − 5 dB. As the signal-to-noise ratio is − 5 and 0 dB, RDAS can achieve better performance in terms of anti-noise than LARA and ADDA. It should be noted that the anti-noise performance of RDAS is weakened with the increase of the value k. That is because there is little difference between the data of each cluster when the amount of attack is small, and it is impossible to select the expected cluster correctly. In general, the chi-square fitting can accurately represent the weight during the phase of data aggregation, which can avoid the error caused by the improper selection of expectation model in LARA and ADDA.

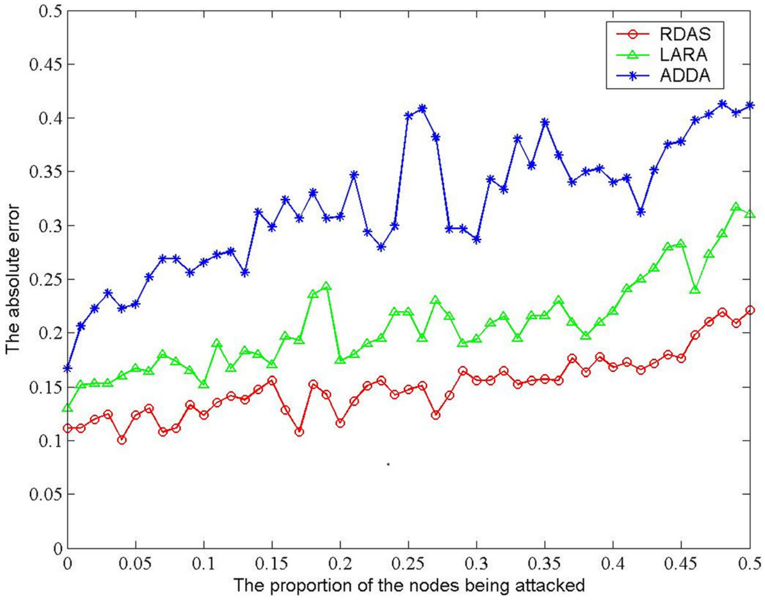

Fig. 5 The absolute error ($d = 10$)

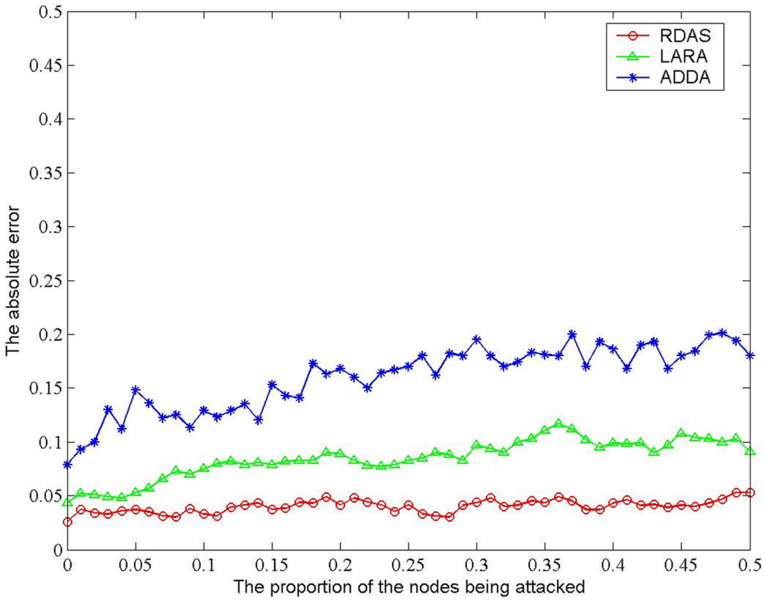

Fig. 6 Anti-noise performance (SNR = − 5 dB)

5 Conclusions

In this paper, we contributed with a resilient data aggregation algorithm based on spatio-temporal correlation for WSNs. On the basis of the distributed data convergence model, the algorithm combines the centroid distance and similarity to measure the attack degree of each cluster node's perceived data, and the weighted calculation can improve the convergence precision of data recovery. In addition, this method can obtain the estimated value of data sample of all clusters according to the temporal correlation characteristic of the nodes' perceived data at different time. Using the chi-square fitting, the extent of the data being tampered in each cluster can be measured effectively. Both analysis and extensive simulations support the quality and viability of our proposal.

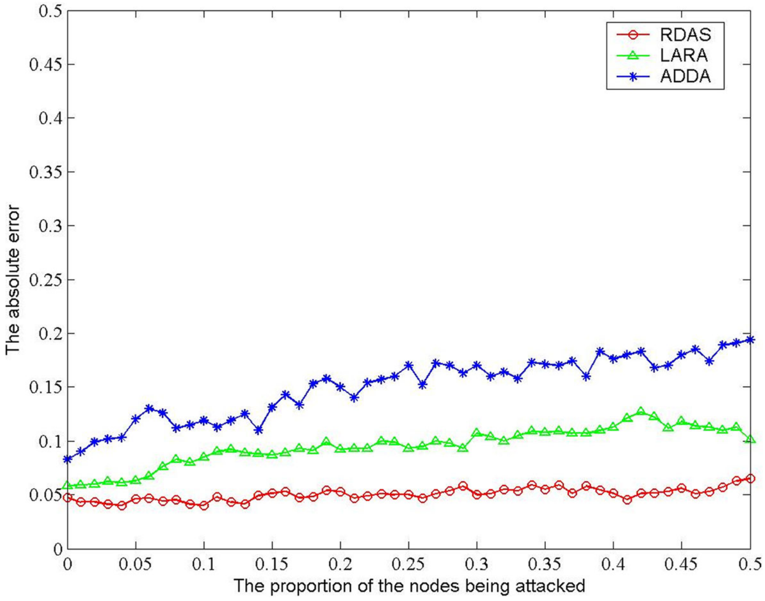

Fig. 7 Anti-noise performance (SNR = 0 dB)

Abbreviations

ADDA: Attack detectors data aggregation; CBDA: Creditability-based data aggregation model; LARA: Linear approaches resilient aggregation; RDAS: Resilient data aggregation method based on spatio-temporal correlation; WSN: Wireless sensor network

Acknowledgements

The authors acknowledged the anonymous reviewers and editors for their efforts in valuable comments and suggestions.

Funding

This work was supported by the project of the First-Class University and the First-Class Discipline (No. 10301-017004011501) and the National Natural Science Foundation of China.

Availability of data and materials

The datasets supporting the conclusions of this article are included within the article.

Authors' contributions

YL contributed to the conception and algorithm design of the study. NS contributed to the acquisition of simulation. YL and NS contributed to the analysis of simulation data and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Received: 5 March 2018 Accepted: 1 June 2018
Published online: 18 June 2018

References

1. A Apavatjrut, W Znaidi, A Fraboulet, C Goursaud, et al., in *Proceedings of the 4th international conference on network and system security, NSS'10*. Energy friendly integrity for network coding in wireless sensor networks (IEEE, Melbourne, 2010), pp. 223–230
2. K Parmar, DC Jinwala, in *Proceedings of the 20th EUNICE/IFIP workshop on advances in communication networking, EUNICE'14, Lecture Notes in Computer Science*. Malleability resilient concealed data aggregation, vol 8846 (2014), pp. 160–172
3. MA Simplicio Jr, BT De Oliveira, CB Margi, et al., Survey and comparison of message authentication solutions on wireless sensor networks. Ad. Hoc. Netw.. **11**(3), 1221–1236 (2013)
4. D Westhoff, O Ugus, in *Proceedings of the 4th IEEE international workshop on data security and privacy in wireless networks, D-SPAN'13*. Malleability resilient (premium) concealed data aggregation (IEEE, Madrid, 2013), pp. 1–6
5. S Sicari, LA Grieco, G Boggia, et al., DyDAP: a dynamic data aggregation scheme for privacy aware wireless sensor networks. J. Syst. Softw. **85**(1), 152–166 (2012)
6. M Mansouri, L Khoukhi, H Nounou, Secure and robust clustering for quantized target tracking in wireless sensor networks. J. Commun. Netw. **15**(2), 164–172 (2013)
7. G Han, J Jiang, L Shu, J Niu, HC Chao, Managements and applications of trust in wireless sensor networks: a survey. J. Comput. Syst. Sci. **80**(3), 602–617 (2014)
8. L Lv, L Hong, N Zhang, Hierarchical routing trust model for wireless sensor networks. Comput. Eng. **23**, 101–103 (2010)
9. H Safa, H Artail, D Tabet, A cluster-based trust-aware routing protocol for mobile ad hoc networks. Wirel. Netw **16**, 969–984 (2010)
10. H Xiangdong, W Qinfang, T Hui, Model and simulation of creditability-based data aggregation for the internet of things. Chin. J. Sci. Instrum. **31**(11), 2636–2640 (2010)
11. Z Nan, Z Jianhua, L Zhishu, Data fusion mechanisms based on immune in wireless sensor network. J. Chin. Comput. Syst. **30**(3), 454–459 (2009)
12. K Liu, T Du, S Qu, The research of high efficient and real time data aggregation method applied in WSNs. J. Sens. Technol. Appl. **3**(3), 33–46 (2015)
13. L Qiu, T Liu, D Lin, et al., Data aggregation in wireless sensor network based on deep learning model. Chin. J. Sens. Actuators **12**, 1704–1709 (2014)
14. H Cui, J Pan, D Yan, Malicious nodes detection algorithm based on secure data fusion in wireless sensor networks. Chin. J. Sens. Actuators **5**, 664–669 (2014)
15. T Du, S Qu, Q Guo, et al., in *Proc. of IEEE Fourth International Conference on Big Data and Cloud Computing*. A high efficient real time data aggregation algorithm for WSNs (2014), pp. 594–598
16. D Wager, in *Proc. of the 2nd ACM Workshop on Security in Ad Hoc and Sensor Networks*. Resilient aggregation in sensor networks (ACM Press, New York, 2004), pp. 78–87
17. L Buttyan, P Schaffer, I Vajda, *in Proceedings of the Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks*. RANBAR: RANSAC-based resilient aggregation in sensor networks (ACM, Alexandria, 2006), pp. 83–90
18. YJ Luo, XY Ding, XG Luo, et al., Effective method for resilient data aggregation in wireless sensor networks. J. Data Acquis. Process. **1**, 90–94 (2011)
19. YJ Luo, DY Shi, YT Hou, et al., Resilient data aggregation method based on similarity in wireless sensor networks. Appl. Res. Comput. **9**, 3405–3407 (2012)
20. K Parmar, DC Jinwala, Malleability resilient concealed data aggregation in wireless sensor networks. Wirel. Pers. Commun. **87**(3), 971–993 (2016)
21. WR Heinzelman, A Chandrakasan, H Balakrishnan, in *Proc. of the 33rd Hawaii Int'l Conf. on System Science (HICSS 2000)*. Energy-efficient communication protocol for wireless microsensor networks (2000), pp. 3005–3014
22. P Kuila, SK Gupta, PK Jana, A novel evolutionary approach for load balanced clustering problem for wireless sensor networks. Swarm Evol. Comput. **24**(12), 48–56 (2013)
23. MC Vuran, B Akan, F Akyildizl, Spatio-temporal correlation: theory and applications for wireless sensor networks. Comput. Netw. **45**(3), 245–259 (2004)
24. C Mi, D Zhu, BA Engel, et al., Research on probability distribution of extreme wind speed in maize growth period. Sens. Lett. **10**(1), 535–540 (2012)
25. HC Ma, PK Sahoo, YW Chen, Computational geometry based distributed coverage hole detection protocol in wireless sensor networks. J. Netw. Comput. Appl. **34**(5), 1743–1756 (2011)
26. S Ridvan, L Peide, Maximizing deviation method for neutrosophic multiple attribute decision making with incomplete weight information. Neural Comput. Appl. **27**(7), 2017–2029 (2016)
27. KJ Henry, DR Stinson, Linear approaches to resilient aggregation in sensor networks. J. Math. Cryptol. **9**(4), 245–272 (2015)
28. R Lopez-Valcarce, D Romero, in *Proc. of 23rd European Signal Processing Conference (EUSIPCO), Nice, France, Aug 31-Sep 04*. Attack detectors for data aggregation in clustered sensor networks (2015), pp. 2053–2057