International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com

Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks

[a]Dr.Sheeja, [b]P.Karthikeyani

[a]Assistant Professor, Department of Computer Science, Karpagam Academy of Higher Education
[b]PG Student, Department of Computer Science, Karpagam Academy of Higher Education

A B S T R A C T

Irrecoverable concealed data aggregation for data integrity in wireless sensor network (RCDA) a base station can recover each sensing data generated by all sensors even if these data have been aggregated by cluster heads (aggregators). With these individual data, two functionalities are provided. First, the base station can verify the integrity and authenticity of all sensing data. Second, the base station can perform any aggregation functions on them. Then, we propose two RCDA schemes named RCDA-HOMO r and RCDA-HETE for homogeneous and heterogeneous WSN respectively. In the security analysis, we demonstrate that the proposed schemes are secure under our attack model. Through experiments, we show that the performance of our design is reasonable and affordable. We also provide detailed comparisons with other schemes.

Keywords: RCDA, WSN, Data Integrity, Security

1. Introduction

Wireless sensor networks (WSN) have been widely deployed in many applications, e.g., military field surveillance, health care, environment monitor, accident report, etc. A WSN is composed of a large number of sensors which collaborates with each other. Each sensor detects a target within its radio range, performs simple computations, and communicates with other sensors. Generally, sensors are constrained in battery power, communication, and computation capability; therefore, reducing the power consumption is a critical concern for a WSN. Recently, a practical solution called data aggregation was introduced. The original concept is to aggregate multiple sensing data by performing algebraic or statistical operations such as addition, multiplication, median, minimum, maximum, and mean of a data set, etc. Normally, data aggregation is performed by cluster heads if the whole network is divided into several groups known as clusters. For example, in military fields, sensors are deployed to measure radiation or chemical pollution. The base station (sink) may require the maximum value of all sensing data to trigger the immediate response; thus, each cluster head selects the maximum value of multiple sensing data of its cluster members and sends the result to the base station. Obviously, communication cost is reduced since only aggregated results reach the base station. Unfortunately, an adversary has the ability to capture cluster heads. It would cause the compromise of the whole cluster; consequently, several schemes, such as ESPDA and SRDA, have been proposed. However, these schemes restrict the data type of aggregation or cause extratransmission overhead. Besides, an adversary can still obtain the sensing data of its cluster members after capturing a cluster head. To solve above problems completely, two ideas are usedin recent research. First, data are encrypted during transmission. Second, cluster heads directly aggregate encrypted data without decryption. A well-known approach named Concealed Data Aggregation (CDA) has been proposed based on these two ideas. CDA provides both end-to-end encryption and in-networking processing in WSN. Since CDA applies privacy homomorphism (PH) encryption with additive homomorphism, cluster heads are capable of executing addition operations on encrypted numeric data. Later, several PH-based data aggregation

schemes [4], [3] have been proposed to achieve higher security levels. In the above PH-based schemes , the base station receives only the aggregated results. However, it brings two problems. First, the usage of aggregation functions is constrained. For example, these schemes only allow cluster heads to perform additive operations on cipher texts sent by sensors; therefore, they are ineffective if the base station desires to query the maximum value of all sensing data. Second, the base station cannot verify the integrity and authenticity of each sensing data. These problems seem to be solved if the base station can receive all sensing data rather than aggregated results, but this method is in direct contradiction to the concept of data aggregation that the base station obtains only aggregated results. Thus, we attempt to design an approach that allows the base station to receive all sensing data but still reduce the transmission overhead Contributions.

These data aggregation schemes provide better security compared with traditional aggregation since cluster heads (aggregator) can directly aggregate the cipher texts without decryption; consequently, transmission overhead is reduced. However, the base station only retrieves the aggregated result, not individual data, which causes two problems. First, the usage of aggregation functions is constrained. For example, the base station cannot retrieve the maximum value of all sensing data if the aggregated result is the summation of sensing data. Second, the base station cannot confirm data integrity and authenticity via attaching message digests or signatures to each sensing sample. In this paper, we attempt to overcome the above two drawbacks. In our design, the base station can recover all sensing data even these data has been aggregated. This property is called "recoverable." Experiment results demonstrate that the transmission overhead is still reduced even if our approach is recoverable on sensing data. Furthermore, the design has been generalized and adopted on both homogeneous and heterogeneous wireless sensor networks

2. Methodology

A well-known approach named Concealed Data Aggregation (CDA) has been proposed based on these two ideas. CDA provides both end-to-end encryption and in-networking processing in WSN. Since CDA applies privacy homomorphism (PH) encryption with additive homomorphism, cluster heads are capable of executing addition operations on encrypted numeric data. The base station receives only the aggregated results. However, it brings two problems. First, the usage of aggregation functions is constrained. Second, the base station cannot verify the integrity and authenticity of each sensing data. These problems seem to be solved if the base station can receive all sensing data rather than aggregated results, but this method is in direct contradiction to the concept of data aggregation that the base station obtains only aggregated results. Thus, we attempt to design an approach that allows the base station to receive all sensing data but still reduce the transmission overhead. We introduce a concept named Recoverable Concealed Data Aggregation (RCDA). In RCDA, a base station can recover each sensing data generated by all sensors even if these data have been aggregated by cluster heads. With these individual data, two functionalities are provided. First, the base station can verify the integrity and authenticity of all sensing data. Second, the base station can perform any aggregation functions on them. Then, we propose two RCDA schemes named RCDA-HOMO and RCDA-HETE for homogeneous and heterogeneous WSN respectively. In the security analysis, we demonstrate that the proposed schemes are secure under our attack model. Through experiments, we show that the performance of our design is reasonable and affordable. We also provide detailed comparisons with other schemes.

2.1 MODULES DESCRIPTION

1. Sensor Node Creation

- In this module We have Registered the sensor node ip address and port number this detail store the Database
- After click Login page Enter the node name and port no, Main server verify the Database.
- Finally created sensor node.When a sensor decides to send sensing data to itsCH(Cluster Header), it performs Encrypt Data and sends the result to the CH(Cluster Header).

2.Cluster Header Creation

- In this module We have Registered the Cluster Headerip address and port number this detail store the Database
- After click Cluster Header Login page Enter the node name and port no, Main server verify the Database.
- Cluster Header means Group of Sensor node handled or Header of Sensor node.

3.Base Station Activation

- In this module We have Registered the Base Station Ip address and port number this detail store the Database
- After click Base Station Login page Enter the Base Station name and port no, Main server verify the Database.
- Base Station Control the all Cluster Header and Sensor node, Monitoring the each sensor node

4. Aggregation and Temporal key generation & Signature generation

- proposed an aggregate signature scheme which merges a set of distinct signatures intoone.
- The aggregated signature,This scheme consists of five procedures: key generation (KeyGen), signing (Sign), verifying (Verify), aggregation (Agg), and verifying aggregated signature (Agg-Verify).

5. Verify the integrity of the Data

- The BS first extracts individual sensing data by decrypting the aggregated cipher text.
- Afterward, the BS verifies the authenticity and integrity of the decrypted data based on the corresponding aggregated signature.

3 Results and Discussion

System Implementation is the stage in the project where the theoretical design is turned into a working system. The most critical stage is achieving a successful system and in giving confidence on the new system for the user that it will work efficiently and effectively The existing system was long time process. The proposed system was developed using Java Swing. The existing system caused long time transmission process but the system developed now has a very good user-friendly tool, which has a menu-based interface, graphical interface for the end user. After coding and testing, the project is to be installed on the necessary system. The executable file is to be created and loaded in the system. Again the code is tested in the installed system. Installing the developed code in system in the form of executable file is implementation.

4. Conclusion

Recoverable concealed data aggregation schemes for homogeneous WSNs. A special feature is that the base station can securely recover all sensing data rather than aggregated results, but the transmission overhead is still acceptable. Moreover, we integrate the aggregate signature scheme to ensure data authenticity and integrity in the design. Even though signatures bring additional costs, the proposed schemes are still affordable for WSNs after evaluation. The collaborative nature of these applications makes multicast traffic very common. Securing such traffic is of great importance, particularly authenticating the source and message to prevent any infiltration attempts by an intruder. Contemporary source authentication schemes found in the literature either introduce excessive overhead or do not scale for large networks which pursues a two tired hierarchical strategy combining both time and secret-information asymmetry in order to achieve scalability and resource efficiency.

REFERENCES

[1] R. Rajagopalan and P. Varshney, "Data-Aggregation Techniques in Sensor Networks: A Survey," IEEE Comm. Surveys Tutorials,vol. 8, no. 4, pp. 48-63, Oct.-Nov. 2006.

[2] S. Madden, M.J. Franklin, J.M. Hellerstein, and W. Hong, "TAG:A Tiny Aggregation Service for Ad-Hoc Sensor Networks,"Proc. Fifth Symp. Operating Systems Design and Implementation,2002.

[3] J.-Y. Chen, G. Pandurangan, and D. Xu, "Robust Computation of Aggregates in Wireless Sensor Networks: Distributed Randomized Algorithms and Analysis," IEEE Trans. Parallel Distributed Systems, vol. 17, no. 9, pp. 987-1000, Sept. 2006.

[4] H. C¸ am, S. O ¨ zdemir, P. Nair, D. Muthuavinashiappan, and H.OzgurSanli, "Energy-Efficient Secure Pattern Based Data Aggregation for Wireless Sensor Networks," J. Computer Comm., vol. 29, pp. 446-455, 2006.

[5] H. Sanli, S. Ozdemir, and H. Cam, "SRDA: Secure Reference-Based Data Aggregation Protocol for Wireless Sensor Networks,"Proc. IEEE 60th Int'l Conf. Vehicular Technology (VTC '04-Fall),vol. 7, pp. 4650-4654, Sept. 2004.

[6] Praneesh, M., and R. Annamalai Saravanan. "Deep Stack Neural Networks Based Learning Model for Fault Detection and Classification in Sensor Data." *Deep Learning and Edge Computing Solutions for High Performance Computing*. Springer, Cham, 2021. 101-110.