ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 6, June 2013

RENDERING INTEGRITY AND RELIABILITY THROUGH RECOVERABLE CONCEALED DATA AGGREGATION IN WIRELESS SENSOR NETWORKS

Chethana E [1], Mrs.Srividya B V [2]

P.G.Student, Department of Telecommunication Engineering,Dayanand Sagar College of Engineering,Bangalore,India[1]

Assistant Professor,Department of Telecommunication Engineering,Dayanand Sagar College of Engineering, Bangalore India[2]

Abstract: In Wireless sensor networks (WSN) 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 is introduced. By performing data aggregation we can reduce the number of packets transmitted to the base station resulting in conservation of energy and bandwidth. In this paper, we are going to recover the concealed data aggregation for reliability and data integrity in wireless sensor networks where a base station can recover each sensing data generated by all sensors even if these data have been aggregated by cluster heads. This approach allows the aggregation of data packets that are encrypted with different encryption keys. In addition, during the decryption of aggregated data, the base station is able to classify the encrypted and aggregated data based on the encryption keys. Moreover, by generating the temporal key of each aggregated data and signature to ensure data reliability and integrity in wireless sensor networks. Results obtained by this method will show that recoverable concealed data aggregation approach provides good results making it an alternative to existing aggregation algorithms.

Keywords: Data integrity, Concealed data aggregation, Security, Wireless sensor networks.

INTRODUCTION

A Wireless sensor networks 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. Data gathering is defined as the systematic collection of sensed data from multiple sensors to be eventually transmitted to the base station for processing. Since sensor nodes are energy constrained, it is inefficient for all the sensors to transmit the data directly to the base station. Data generated from neighbouring sensors is often redundant and highly correlated. In addition, the amount of data generated in large sensor networks is usually enormous for the base station to process. Hence, we need methods for combining data into high-quality information at the sensors or intermediate nodes which can reduce the number of packets transmitted to the base station resulting in conservation of energy and bandwidth. This can be accomplished by data aggregation. Data aggregation is defined as the process of aggregating the data from multiple sensors to eliminate redundant transmission and provide fused information to the base station. Data aggregation usually involves the fusion of data from multiple sensors at intermediate nodes and transmission of the aggregated data to the base station (sink).

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. 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; to solve above problems completely, two ideas are used in recent research [3], [4]. First, data are encrypted during transmission. Second, cluster heads directly aggregate encrypted data without decryption.

To solve above problems completely, two ideas are used in recent research. First, data are encrypted during transmission. Second, cluster heads directly aggregate encrypted data without decryption

I. EXISTING SYSTEM

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 [5]. 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 have been proposed to achieve higher security levels [6]. 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, these 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 [7].

II. PROBLEM DESCRIPTION

In this paper, new approach is used to solve the problem of restricted usage of aggregation function 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, attempt to design an approach that allows the base station to receive all sensing data but still reduce the transmission overhead. Here introduce a concept named Recoverable Concealed Data Aggregation (RCDA) [13].

III. PROPOSED SYSTEM

In this paper, recover the concealed aggregated data with authenticity and data integrity in wireless sensor networks. The base station can recover all sensing data even these data has been aggregated in cluster head. The aim of this paper is to provide security and authenticity in wireless sensor network by generating temporary key for aggregated data.

IV. ARCHITECTURE MODEL

The diagram below represents the architecture model of the paper. WSN is controlled by a base station. All Senor node's in a WSN may be divided into several clusters after being deployed. Each cluster has a cluster head responsible for collecting and aggregating sensing data from senor node's within the same cluster. A cluster head then sends the aggregation results to the base station.

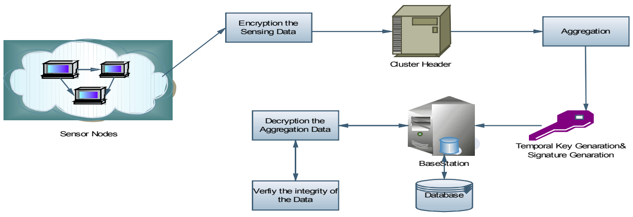

Encryption the Sensing Data
Cluster Header
Aggregation
Sensor Nodes
Decryption the Aggregation Data
BaseStation
Temporal Key Genaration& Signature Genaration
Verfiy the integrity of the Data
Database

Fig 1: Proposed Architecture Model

The proposed approach is composed of four procedures: Setup, Encrypt, Aggregate-Sign, and Verify.

A. SETUP:-To prepare and install necessary secrets for the base station and each sensor. In this module, we create many sensor nodes. Users enter name, ip address and port number of sensor to register in the database. While entering the next node user has to database whether the node already exists in the database as shown in fig2.Later for activation of the sensor nodes the user has to enter the details of that particular node which user wants to activate and after entering the correct details the nodes gets activated.

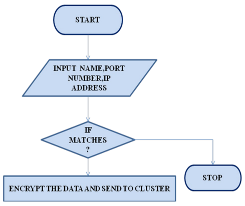

START
INPUT NAME,PORT NUMBER,IP ADDRESS
IF MATCHES ?
ENCRYPT THE DATA AND SEND TO CLUSTER
STOP

Fig 2: Set up procedure of sensor nodes

B. ENCRYPT:-After the sensor nodes are activated, the sensor decides to send sensing data to its cluster head, it performs encrypt and sends the result to the cluster head.

C. AGGREGATION AND TEMPORAL KEY GENERATION AND SIGNATURE GENERATION: - Once the cluster head receives all results from its members, it activates aggregate to aggregate what it received, and then sends the final results (aggregated cipher text and signature) to the base station.

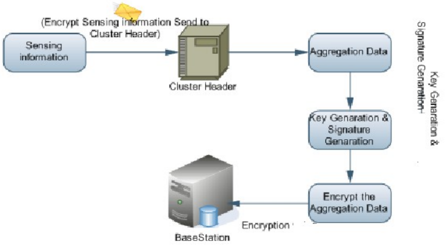

(Encrypt Sensing information Send to Cluster Header)
Sensing information
Cluster Header
Aggregation Data
Key Genaration & Signature Genaration
Encrypt the Aggregation Data
Encryption
BaseStation
Key Genaration & Signature Genaration

Fig 3: Aggregation and Temporal Key Generation & Signature Generation

D. VERIFYING INTEGRITY OF THE DATA: - The base station first extracts individual sensing data by decrypting the aggregated cipher text. Afterward, the base station verifies the reliability and integrity of the decrypted data based on the corresponding aggregated signature.

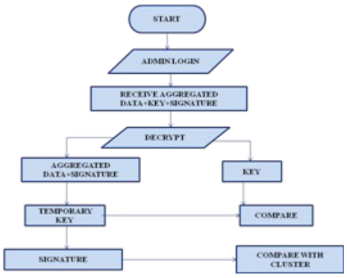


Fig 4: Verifying Integrity of the Data

V. RECOVERY PROPERTY

The Recovery property attempts to provide two functionalities. First, BS can verify the integrity and reliability of all sensing data. Second, BS can perform arbitrary aggregation operations on these data.

VI. SECURITY ANALYSIS

We first assume that an adversary does not compromise sensors. The proposed schemes are secure because sensing data are encrypted. In this approach, each sensor encrypts their data with private key of base station before transmitting. Besides, our design generates the corresponding signature for each sensing data. Consequently, an adversary cannot modify messages and inject forged messages since he cannot sign forged messages without private keys. If an adversary has the ability to compromise sensors, we consider the following situations. An adversary can compromises a sensor and perform it as a legal one. Detecting compromised sensors that still act normally is infeasible in all existing detection mechanisms in WSN. Also, if the value of a forged message is in a reasonable range, detecting it is still infeasible. An adversary can also try to manipulate the aggregated result. He may generate false data, modify legal messages or impersonate other sensors.

The proposed schemes are still secure against above attacks because of the signature required for each generated message. A malicious sender cannot impersonate other legal sensors because he lacks the corresponding keys of legal sensors. Based on the attack model, data aggregation scheme must satisfy the following security requirements [8] [9] [10].

1) Data Privacy: All sensing data must be encrypted and concealed from *CH*, especially in homogeneous WSN. It implies that a *CH* must have an ability to aggregate the cipher texts without decryption.
2) Data Integrity/Authenticity: The integrity ensures the base station can detect altered data by unauthorized entity during transmission. Besides, authenticity can trace the source of data; the base station can verify the data sender.
3) Prevent Decryption with Compromised Secrets: An adversary cannot decrypt the cipher text or aggregated results after compromising sensors [10].
4) Prevent Encryption with Compromised Secrets: An adversary cannot generate the forged cipher text through compromised secrets.
5) Prevent Unauthorized Aggregation: An adversary cannot aggregate the cipher text and modify aggregate results if he does not compromise sensors or cluster heads [11]. These security requirements may broaden the scope of the assumptions defined in the past research. For example, CDA cannot satisfy all these requirements, but it can be solved by combining other mechanisms such as node authentication approaches. However, in this analysis, our design can achieve all security requirements without collaborating with other mechanisms. It seems more cost efficient.

VII. EXCEPTED RESULTS

Fig 5 shows the sensor node creation and Fig 5a shows the sensor node activation and then node selects the file and encrypts the file and sends this data to cluster head.

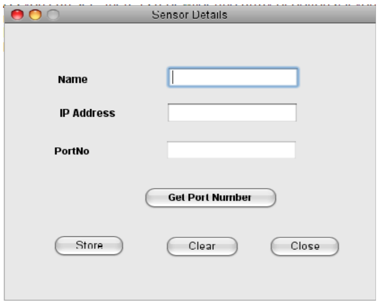
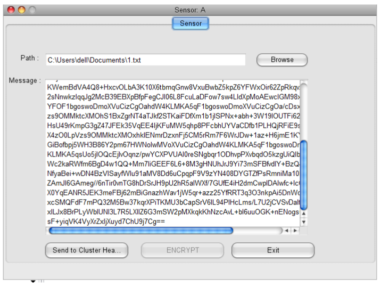


Fig 5: Senor Node Registration



Path : C:\Users\dell\Documents\1.txt

Message :

KWemBdVA4Q8+HxcvOLbA3K10X6tbmqGnw8VxuBwbZ5kpZ6YFWxOir62ZpRkqv
2sNnwkzIqqJg2McB39EBXpBfpFegCJI06L8FcuLaDFow7sw4LIdXpMoAEwcIGM98x
YFOF1bgoswoDmoXVuCizCgOahdW4KLMKA5qF1bgoswoDmoXVuCizCgOa/cDsx
zs9OMMktcXMOhS1BxZgrNT4aTJkf2STKaiFDfXm1b1jlSPNx+abh+3W19IOUTFi62
HsU49rKmpG3gZ47JFEk35VqEE4IjKFuMW5qhp8PFcbhUYVaCDfb1PLHQjRFiE9s
X4zO0LpVzs9OMMktcXMOxhklENmrDzxnFj5CM5rRm7F6WrJDw+1az+H6jmE1K
GiBofbpj5WH3B86Y2pm67HWNolwMVoXVuCizCgOahdW4KLMKA5qF1bgoswoDr
KLMKA5qsUo5jIOQcEjlvOqnz/pwYCXPVUAI0reSNgbqr1ODhvpPXvbqdO5kzgUiQIb
Wc2kaRWfm6BgD4w1QQ+Mm7IiGEEF6L6+8M3gHNUhJrJ9Yi73mSFBfvdIY+BzQ
NfyaBei+wDN4BzVISayfWlu91aMV8Dd6uCpqpF9V9zYN408DYGTZfPsRmniMa10
ZAmJI6GAmeg//6nTir0vnTG8hDrSrJH9pU2hR5alWXf/7GUfE4iH2dmCwplDAlwfc+Ic
X0YqEANR5JEK3meFBj62mBiGnazhWav1jW5qr+azz25YfRRT3q3O3nkpAi5DnW
xcSMQFdF7mPQ32M5Bw37kqrXPiTKMU3bCapSrV6IL94PlHcLms/L7U2jCVSvDal
xlLJx8BrPLyWblUNl3L7R5LXllZ6G3mSW2pMXkqkKhNzcAvL+bl6uuOGK+nENogs
sF+yiqVK4VyXrZxljXuyd7ChU9j7Cg==

Fig 5a: Sensor Node Activation

Fig 6 represents the cluster head which receives the data and displays each sensor node information and file received. For this received data, aggregation is performed then temporary key and signature is generated. Later it is sent to base station.

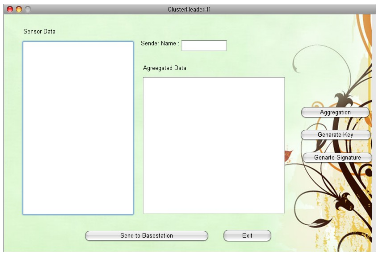


Fig 6: Data Received At Cluster Head

Fig 7 represents base station where all aggregated data key signature is received. At the base station, the aggregated data is decrypted and hence it displays the cluster head information, node from which file was received. Thus providing integrity and reliability by verifying the key and signature which was generated at cluster head.

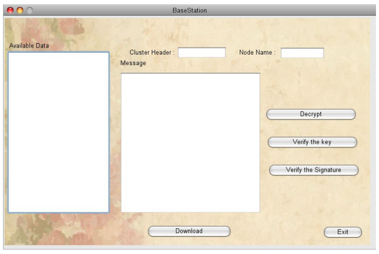


Fig 7: Verifying Integrity at Base Station

VIII. CONCLUSION

In this paper, we have proposed recoverable concealed data aggregation scheme provides a secure and reliable data aggregation in wireless sensor network. 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, by generating the temporal key of each aggregated data and integrates the aggregate signature to ensure data reliability and integrity in the design. Even though signatures bring additional costs, the proposed schemes are still affordable for WSNs after evaluation.

REFERENCES

[1] R. Rajagopalan and P. Varshney, “Data-Aggregation Techniques in Sensor Networks: A Survey,” IEEE Comm. Surveys Tutorials, vol. 8, no. 4, pp. 48-32, Oct.-Nov. 2006.

[2] 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. 14, no. 9, pp. 984-1000, Sept. 2006.

[3] H. Cam, S.Ozdemir, P. Nair, D. Muthuavinashiappan, and H.Ozgur Sanli, “Energy-Efficient Secure Pattern Based Data Aggregation for Wireless Sensor Networks,”J. Computer Comm., vol. 29,pp. 446-455, 2006.

[4] 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.

[5] D.Westhoff, J. Girao, and M. Acharya, “Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution, and Routing Adaptation,” IEEE Trans. Mobile Computing, vol. 5, no. 10, pp. 1417-1431, Oct. 2006.

[6] C.Castelluccia, E.Mykletun, and G.Tsudik, “Efficient Aggregation of Encrypted Data in Wireless Sensor Networks,” Proc. Second Ann. Int’l Conf. Mobile and Ubiquitous Systems, pp. 109-117, July 2005.

[7] E.Mykletun, J.Girao, and D.Westhoff, “Public Key Based Cryptoschemes for Data Concealment in Wireless Sensor Networks,” Proc. IEEE Int’l Conf. Comm., vol. 5, pp. 2288-2295, June 2006.

[8] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “An Application-Specific Protocol Architecture for Wireless Microsensor Networks,” IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-670, Oct. 2002.

[9] M. Demirbas, A. Arora, V. Mittal, and V. Kulathumani, “A Fault-Local Self-Stabilizing Clustering Service for Wireless Ad Hoc Networks,”IEEE Trans. Parallel Distributed Systems, vol. 17, no. 9,pp. 912-922, Sept. 2006.

[10] B. Yu and B. Xiao, “Detecting Selective Forwarding Attacks in Wireless Sensor Networks,” Proc. IEEE 20th Int’l Symp. Parallel and Distributed Processing (IPDPS’ 06), Apr. 2006.

[11] G. De Meulenaer, F. Gosset, F.X. Standaert, and L. Vandendorpe,“On the Energy Cost of Communication and Cryptography in Wireless Sensor Networks,” Proc. IEEE Int’l Conf. Wireless and Mobile Computing, Networking and Comm., pp. 580-585, 2008.