RESEARCH ARTICLE

International Journal of Multidisciplinary and Scientific Emerging Research

Available at http://www.ijmser.com/ (ISSN 2349 – 6037)

Aggregation of Recoverable Concealed Data in Homogeneous Wireless Sensor Networks

Mr. Harsha S[1], Dr. Khalid Nazim Abdul Sattar[2], Dr. Hani Alquhayz[3], Mr. Theja N[4] and Mr. Shailesh Kumar[5]

[1]Associate Professor, Department of Information Science & Engineering, Vidya Vikas Institute of Engineering & Technology, Mysuru,
[2]Assistant Professor, Department of CSI, College of Science in Az zulfi, Al- Majmaah University, KSA
[3]Assistant Professor, HOD, Department of CSI, College of Science in Az zulfi, Al- Majmaah University, KSA
[4]Assistant Professor, Department of Computer Science and Engineering Vidya Vikas Institute of Engineering & Technology, Mysuru,
[5]Assistant Professor, Department of Information Science & Engineering, Vidya Vikas Institute of Engineering & Technology, Mysuru,

Accepted **15** November 2015, Available online **17** December 2015, **Vol.4, No.2 (December 2015)**

Abstract

Several data aggregation schemes based on privacy homomorphism encryption result in a better security compared with traditional aggregation. In the proposed Recoverable Concealed Data Aggregation scheme, the Cluster Heads can aggregate the sensing data of the individual Sensor Node present in the cluster without decryption which reduces the transmission over head. The Concealed Data Aggregation is extended with symmetric key encryption. The base station can retrieve or recover the application specific data from the aggregated cipher text. The contribution of this scheme is that it mitigates the impact of compromising attacks.

Keywords: *Base Station, Data integrity, Concealed data aggregation, Security, Wireless Sensor Networks, Data Aggregation, Wireless Sensor Networks (WSNs)*

1. INTRODUCTION

A wireless sensor network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. Commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions. A sensor network consists of multiple detection stations called sensor nodes, each of which is small, lightweight and portable. Wireless Sensor Networks 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 [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.] 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 extra transmission 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 used in 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 [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.] 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 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, in this paper, 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 (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 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 can show that the performance of our design is reasonable and affordable. We also provide detailed comparisons with other schemes.

2. LITERATURE SURVEY

This section describes the work related to data aggregation schemes and security mechanisms for data transmissions.

S. Ozdemir's Concealed Data Aggregation in Heterogeneous Wireless Sensor Networks Using Privacy Homomorphism

The data aggregation [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.][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.][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.][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.]can be implemented in WSNS to reduce data redundancy and summarize necessary information without requiring all pieces of data. The data aggregation can be maximized by implementing it at every data aggregator along the path to the base station. Before transmission to the base station, each sensor node encrypts data and it will be decrypted by the base station to maintain end to end security. But, the data aggregation requires the encrypted data to be decrypted. In order to achieve data aggregation and secure communication, Privacy Homomorphism [S. Ozdemir, "Concealed Data Aggregation in Heterogeneous Sensor Networks Using Privacy Homomorphism," Proc. IEEE Int'l Conf. Pervasive Services, pp. 165-168, July 2007.] is employed which offers end-to-end concealment of data and ability to operate on cipher texts. The computational overhead imposed by the privacy homomorphism encryption functions is tolerated by employing a set of powerful nodes, called AGGNODEs.

2.1 Secure encrypted-data aggregation scheme for wireless sensor networks

Most of the conventional aggregation functions operate when readings are received in plaintext. If readings are in the encrypted form, the aggregation function requires decryption creating extra overhead and key management issues. The Secure Encrypted Data Aggregation Scheme allows duplicate instances of original readings to be packed into a packet there by providing security and privacy. The scheme can reduce the communication overhead and can be resilient to known-plaintext attacks, chosen-plaintext attacks [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.], cipher text-only attacks and man-in-the-middle attacks

2.2 D Bohen's Aggregate and Verifiably Encrypted Signatures from Bilinear Maps

The aggregate signatures [D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt), pp. 416-432, 2003.] are useful for reducing the size of certificate chains by aggregating all signatures in the chain and for reducing message size in secure routing protocols. An aggregate signature scheme is a digital signature that supports aggregation: Given signatures on n distinct messages from n distinct users, it is possible to aggregate all these signatures into a single short signature. An efficient aggregate signature can be constructed from short signature scheme bilinear maps due to Boneh, Lynn, and Shacham. It can be shown that a given cipher text C is the encryption of a signature on a given message M and the short signature scheme can be extended to give simple ring signatures.

2.3 Data aggregation in wireless sensor networks—exact and approximate algorithms

The data aggregation is one of the basic approaches in the wireless sensor [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.] network to reduce the number of transmissions of sensor nodes and the overall power consumption can be reduced. Several factors affect such as placement of aggregation points, the aggregation function, and the density of sensors in the network affect the data aggregation. There are exact and approximate algorithms for finding the minimum aggregation points to maximize the network lifetime.

2.4 Concealed Data Aggregation (CDA)

A well-known approach named Concealed Data Aggregation (CDA) [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.][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.] 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.

Proposed Scheme: Recoverable Concealed Data Aggregation (RCDA) for Homogeneous Wireless Sensor Networks (RCDA – HOMO)

We introduce a concept named Recoverable Concealed Data Aggregation (RCDA) for homogeneous wireless sensor networks (RCDA – HOMO). 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, RCDA scheme WSN. The proposed schemes can be secure under different attack models. Through experiments, we can show that the performance of the proposed design is reasonable and affordable.

The following figure shows the homogeneous wireless sensor networks in which all sensors have the same storage, processing, battery power, sensing, and communication capabilities.

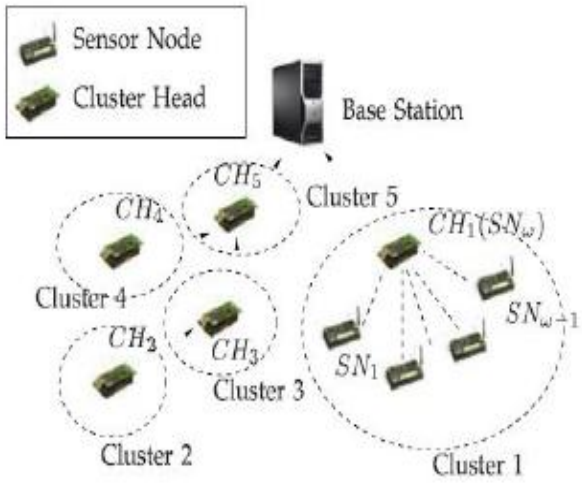

Figure 1: Homogeneous Wireless Sensor Network.

The diagram shown below is the architectural model of the proposed system. The wireless sensor network is controlled by a base station. All Senor Nodes in the network may be divided into several clusters[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.] after being deployed. Each cluster has a cluster head responsible for collecting and aggregating sensing

data from Senor Nodes within the same cluster. A cluster head then sends the aggregation results to the base station. The base station verifies the integrity of the data.

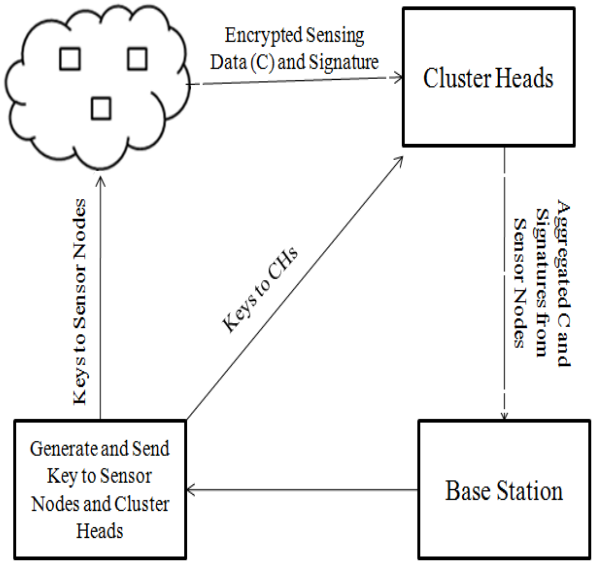

Figure 2: System Architecture.

- **Sensor Nodes:** Sensor nodes are deployed to sense and gather responsible results for the base station. The sensor nodes are grouped into a cluster which is controlled by a Cluster Head.
- **Cluster Head:** It is responsible for collecting and aggregating sensing data from sensor node within the same cluster
- **Base Station:** It has a large bandwidth, strong computing capability, sufficient memory, and stable power to support the cryptographic and routing requirements of the whole WSN

The keys are generated for each sensor of the cluster by using public key encryption algorithm. The cluster member encrypts sensing data and sends it to the cluster head. The signature is added to all the sensing data of the node. The result is aggregated (encrypted data and signature) and sent to the cluster head. The base station performs signature verification process. After receiving the aggregated result from the cluster head, it decrypts the data and verifies the signature of the individual nodes of the network (signature verification). Boneh proposed an aggregate signature scheme which merges a set of distinct signatures into one aggregated signature. This scheme consists of five procedures: key generation (KeyGen), signing (Sign), verifying (Verify), aggregation (Agg), and verifying aggregated signature (Agg -Verify) and the aggregation scheme proposed by Mykletun is based on the elliptic curve ElGamal (EC - EG) cryptosystem. It consists of four procedures: key generation (KeyGen), encryption (Enc), aggregation (Agg), and decryption (Dec).

RCDA-HOMO is composed of four procedures: Setup, Encrypt-Sign, Aggregate, and Verify. The Setup procedure is to prepare and install necessary secrets for the BS and each sensor. When a sensor decides to send sensing data to its CH, it performs Encrypt-Sign and sends the result to the CH. Once the CH 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 BS. The last procedure is Verify. 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. SECURITY ANALYSIS

The assumption is that the adversary does not compromise the sensors in the network. The proposed scheme is secure as each sensor node encrypts sensing data before transmission to the base station. The adversary can't modify the messages and inject forged messages as he can't sign the message. Based on the attack model, data aggregation must satisfy the following requirements.

Data Privacy: All sensing data must be encrypted and concealed from CH. The CH must aggregate the cipher texts without decryption.

Data Integrity: The base station must be able to detect the altered data by an authorized entity during transmission and to verify the data sender.

Prevent Decryption with Compromised Secrets: An adversary cannot decrypt the cipher text or aggregated results after compromising sensors
Prevent Encryption with Compromised Secrets: An adversary cannot generate the forged cipher text through compromised secrets
Prevent Unauthorized Aggregation: An adversary cannot aggregate the cipher text and modify aggregate results if he does not compromise sensors or cluster heads

CONCLUSION

The special feature of the proposed scheme is that the base station can securely recover all sensing data rather than aggregated results, but the transmission overhead is still acceptable. The signature scheme is integrated 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.

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] 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.

[5] 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.

[6] 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.

[7] S. Ozdemir, "Concealed Data Aggregation in Heterogeneous Sensor Networks Using Privacy Homomorphism," Proc. IEEE Int'l Conf. Pervasive Services, pp. 165-168, July 2007.

[8] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt), pp. 416-432, 2003.

[9] 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.

[10] 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.

[11] 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.

[12] 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.