IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 4, April 2015.
www.ijiset.com
ISSN 2348 – 7968

Concealed Data Aggregation Scheme for Wireless Sensor Network Applications

R.Raguraman[1] and S.Priya[2]

[1] Post Graduate Scholar, Department of Computer Science & Engineering, SRM University, Chennai, Tamilnadu, India
[2]Assistant Professor, Department of Computer Science & Engineering, SRM University, Chennai, Tamilnadu, India

Abstract

Data aggregation scheme is a technique which reduces the large amount of transmission in wireless sensor networks. In the existing system, homomorphic encryptions are used to conceal communication during aggregation. The enciphered data can be aggregated algebraically without decryption, hence compromising the security issues and adversaries are able to collect valuable data. Hence these schemes become insecure in case some sensor nodes are compromised, it does not satisfy multi-application environment and they do not provide secure counting which may lead to unauthorized aggregation attacks. Therefore , we propose a new concealed data aggregation scheme extended from Boneh et al.'s homomorphic public encryption system. First, it is designed for a multi-application environment. The base station extracts application-specific data from aggregated cipher texts. Secondly it reduces the impact of compromising attacks. Finally, it degrades the damage from unauthorized aggregations, hence providing the security.

Keywords— *Wireless Sensor Network, Concealed Data Aggregation, Homomorphic Encryption, CDAMA, Secure Counting.*

1. INTRODUCTION

In general, Wireless sensor networks (WSNs) consist of thousands of sensor nodes (SN) that gather data from deployed environments. Environment monitoring, accident reporting and military investigation [1] are some examples of Wireless Sensor Networks. They sense data accordingly to the environment which they are deployed .Limited computational power and low battery supply are the factors which gives restriction to sensor networks and also gives evolution for new energy saving technique. We follow cluster-based WSNs for efficient consumption of energy. In cluster-based WSNs[2], Sensor Network resident in nearby area would form a cluster and it chooses one among them to be their cluster head (CH).The data pieces received from SN is organized into an aggregated result by cluster Head(CH), and then forwards the result to the base station depending on regular routing paths. In general, aggregative operations are algebraic, such as the addition or multiplication of received data, or statistical operation, such as a median, a minimum, or a maximum of a data set[3]. Even though Data aggregation has an advantage of reducing Data transmission, it is exposed to different kind of attacks. For example, compromising a CH will give access adversaries to forge aggregated data results as similar as compromising all its cluster members. To solve this problem, several studies, such as the delay aggregation, CDAMA, have been proposed. To protect against such problems, the scheme, called CDAMA, provides CDA between multiple groups is proposed. It has three practical application scenarios for CDAMA. The first scenario is designed for multi-application WSNs. SN with different purposes (e.g., smoke alarms and thermometer sensors) would be deployed in the same environment. If we apply conventional concealed data aggregation schemes[4] [9], the cipher texts of different applications cannot be aggregated together as well as the decrypted aggregated result will be incorrect. The only solution is to aggregate the cipher texts of different applications separately which results in the transmission cost as the number of the applications increases.

By the concept of CDAMA, the cipher texts from different applications are encapsulated into one cipher text. Conversely, the base station extracts application-specific plain texts with the help of corresponding secret keys. The second scenario is for single application WSNs. Compared with conventional schemes[9], CDAMA degrades the impact of compromising SN through the construction of multiple groups. An adversary can forge data only in the compromised groups, not the whole system The last scenario is designed for secure counting. The previous schemes has the disadvantage of unknown

ISSN 2348 – 7968

message count. The base station is not aware of the number of messages aggregated from the decrypted result; leaking of count knowledge will be subjected to malicious selective aggregation and repeated aggregation. By using CDAMA, the base station is capable of knowing the number of messages aggregated.

These are the schemes performed by CDAMA to solve these issues and the scheme also uses the system model, which is further divided into Aggregation model and Attack model. In aggregation model to enhance the lifetime, tree-based or cluster networks force the intermediate nodes (cluster head) to perform aggregation, i.e., to act as aggregators. After aggregation is done, AGs would direct the results to the next hop. Basically, the data can be aggregated via algebraic operations (e.g., addition or multiplication) or statistical operations (e.g., median, minimum, maximum, or mean). The attack model defines what kinds of attacks a secure data aggregation scheme should protect itself from exposing to attacks.

The remainder of this paper is organized as follows. In Section 2, the objective of the project is being explained. The existing system and the techniques used as well its disadvantages is explained in Section 3. In section 4 the problem in the existing system is defined. The related work of the paper and concepts of the related work is being explained in section 5. The concept of CDAMA is being explained in section 6. The architecture of the CDAMA system is being explained in section 7. The section 8 deals with explanations of each model of the system and its design. Section 9 evaluates the performance of CDAMA. Section 10 concludes the CDAMA and its future work is described.

2. OBJECTIVE

The purpose of including CDAMA Technique in the existing protocol is to improve the overall performance of the Sensor network, extract application specific data and to provide multi-application environment with secure transfer of data between the nodes.

3. EXISTING SYSTEM

For wireless sensor networks, data aggregation scheme that reduces a large amount of transmission is the most practical technique. In previous studies, homomorphic encryptions have been applied to conceal communication during aggregation such that enciphered data can be aggregated algebraically without decryption. Since aggregators collect data without decryption, adversaries are not able to forge aggregated results by compromising them. However, these schemes are not satisfy multi-application environments. Second, these schemes become insecure in case some sensor nodes are compromised. Third, these schemes do not provide secure counting; thus, they may suffer unauthorized aggregation attacks.

3.1 DISADVANTAGES OF EXISTING SYSTEM

- These schemes do not satisfy Multi-application environment**.** If so it cannot extract application specific data.
- Data are insecure and can be forged if the sensor nodes are compromised. Thus it does not provide security to the data.

4. PROBLEM DEFINITION

Homomorphic encryptions have been applied to conceal communication during aggregation such that enciphered data can be aggregated algebraically without decryption. Since aggregators collect data without decryption, adversaries are not able to forge aggregated results by compromising them. It does not satisfy multi-application environment which are done using homomorphic encryption. These schemes become insecure in case some sensor nodes are compromised. They may suffer unauthorized aggregation attacks.

5. RELATED WORK

5.1 Classification of Encrypted Data in Wireless Sensor Networks

End-to-end security mechanisms like SSL [1], which are popular on Internet, may seriously limit the capability of Innetwork processing that is the most critical function in sensor network. This paper proposes a model of categorizing encrypted messages in wireless sensor networks. A classifier, an intermediate sensor node in our setting, is embedded with a set of searching keywords in encrypted format. Upon receiving an encrypted message, it matches the message with the keywords and then processes the message based on certain policies such as forwarding the original message to the next hop, updating it and forwarding or simply dropping it on detecting

ISSN 2348 – 7968

duplicates. The messages are encrypted before being sent out and decrypted only at its destination. Although the intermediate classifiers can categorize the messages, they learn nothing about the encrypted messages except several encrypted keywords, even the statistic information.

It uses Sensor Network Model. The hierarchical architecture has three levels where the base station, fusion point and sensor node stay respectively. Being queried, the sensor will act on collecting raw data and generate reading reports. The sensor reading is then sent out toward the fusion point. The fusion point can aggregation the readings and send the data upward to some base station. The path of data flowing relies further on the routing protocol and the network topology. It deals with encrypting and authenticating of the messages. The presented scheme is efficient, flexible and resource saving. The performance analysis shows that the computational cost and communication cost are minimized. Adversary can easily eavesdrop on, intercept, inject and alter the data transmitted The adversary can jam a sensor node by repeatedly sending packets to it, the sensor will soon run out of battery

5.2 Reverse Multicast Traffic in Concealed Data Aggregation of Wireless Sensor Network

Wireless sensor networks (WSN) are a particular class of ad hoc networks that attract more and more attention both in academia and industry. The sensor nodes themselves are preferably cost-cheap and tiny consisting of application specific sensors, a wireless transceiver, a simple processor, and an energy unit which may be battery or solar driven. This paper presents privacy homomorphism (PH) is an encryption transformation that allows direct computation on encrypted data. Encryption transformation and decryption transformation is performed. It conceals sensed data end-to-end, by still providing efficient in-network data aggregation.

The aggregating intermediate nodes are not required to operate on the sensed plain text data. We apply a particular class of encryption trans- formation and exemplarily discuss the approach on the basis of two aggregation functions. We use actual implementation to show that the approach is feasible and flexible and frequently even more energy efficient than hop-by-hop encryption. The proposed solution assumes passive adversaries. In practice, there are several other security goals that should be fullfill by combining other mechanisms, e.g., authentication of communicating sensors, protection of data integrity, and plausibility of sensed data. The proposals regarding other protection goals in WSNs especially focus on integrity and plausibility of sensed data. The proposed PH is unsecure against chosen plaintext attacks for some parameter settings. A single corrupted node would reveal the information of the whole network. Hence it reveals the results of the aggregated data and also it does not fulfill the security mechanism. Compromising of one node may lead to retrieve data from many applications and it leads to the insecure system. Thus is uses the nodes with

5.3 SRDA: Secure Reference-Based Data Aggregation Protocol for Wireless Sensor Networks.

It presents a secure data aggregation protocol, called SRDA, for wireless sensor networks. SRDA establishes secure connectivity among sensor nodes. In order to reduce the number of bits transmitted, sensor nodes compare their raw sensed data value with their reference data value and then transfer only the difference data. SRDA also establishes secure connectivity among sensor nodes . This is how the process in which the secure reference based data aggregation protocol is carried out in wireless sensor network.

In SRDA, raw data sensed by sensor nodes are compared with reference data values and then only the difference data are transmitted. Reference data is taken as the average value of a number of previous sensor readings. It also uses the term differential data to refer the difference between the reference value and the sensed data value. The proposed protocol in this paper provides a key distribution scheme with low memory overhead to establish secure communication links in the network and then, to save energy, applies variable strength security at different levels of the clustering hierarchy. By using SRDA, we cannot extract the Application Specific data. Hence it cannot be used for Multi-application environment.

6. CDAMA

BGN is implemented by using two points of different orders so that the effect of one point can be removed by multiplying the aggregated cipher text with the order of the point, and then the scalar of the other point can be obtained. Based on the same logic of BGN, CDAMA is designed by using multiple

ISSN 2348 – 7968

points, each of which has different order. We can obtain one scalar of the specific point through removing the effects of remaining points (i.e., multiplying the aggregated cipher text with the product of the orders of the remaining points). The security of CDAMA and BGN are based on the hardness assumption of subgroup decision problem, whereas CDAMA requires more precise secure analysis for parameter selections. We use CDAMA (k = 2) to explain how it works in multiple groups.

Assume that all SNs are divided into two groups, GA and GB. CDAMA contains four procedures: Key generation, encryption, aggregation, and decryption. As we can see, CDAMA (k = 2) is implemented by using three points P;Q, and H whose orders are q1;q2, andq3, respectively. The scalars of the first two points carry the aggregated messages in GA and GB, respectively, and the scalar of the third point carries randomness for security. By multiplying the aggregated cipher text with q2q3 (i.e., the SK in GA), the scalar of the point P carrying the aggregated message in GA can be obtained. Similarly, by multiplying the aggregated cipher text with q1q3 (i.e., the SK in GB), the scalar of the point Q carrying the aggregated message in GB can be obtained. In this way, the encryptions of messages of two groups can be aggregated to a single cipher text, but the aggregated message of each group can be obtained by decrypting the cipher text with the corresponding SK. Considering deployment, the private keys should be kept secret and only known by the BS. SNs in the same group share the same public key and no other entities outside the group knows the group public key. Another major change is the decryption procedure. By performing individual decryption, the BS extracts individual aggregated results of different groups from an aggregated cipher text.

7. SYSTEM ARCHITECTURE

Design is the only way that can accurately translating a customer's requirements in to a finished software product. Fig. 1 shows the process through which the requirements are translated in to a representation of the software i.e. the blue print for constructing software. The system architecture explains what are all the process, data in the sensor node is being undergone and Fig. 1 also shows the process of aggregation of data and retrieving the application specific data back after decrypting.. The system architecture also explains about the process in which the data flow happens.

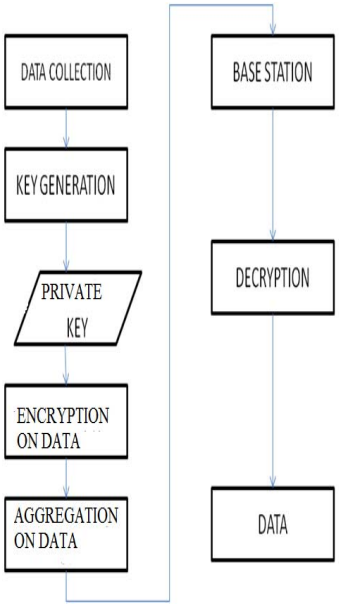

Fig. 1 System Architecture.

8. DESIGN FOR SYSTEM MODEL

This describes how each nodes carry information in it and how they are secured from the attacks. It also explains how the sensor nodes aggregate the data and how it is retrieved in a application specific manner.

8.1 MODEL NAMES

1. Aggregation model.
2. Attack Model.
3. Grouping of Data in Sensor.
4. Secure Extraction of Data

These are the models in the process of performing secure transmission of data to the base station. Each model carries unique task on data.

8.2 MODEL EXPLANATION

Aggregator Model:

In WSNs, SN collect information from deployed environments and forward the information back to base station (BS) via multi-hop transmission based on a tree or a cluster topology. The accumulated transmission carries large energy cost for intermediate nodes. To increase the lifetime, tree-based or cluster networks force the intermediate nodes (a sub-tree node or a cluster head) to perform aggregation, i.e., to be aggregators (AG). After

ISSN 2348 – 7968

aggregation done, AGs would forward the results to the next hop. In general, the data can be aggregated via algebraic operations (e.g., addition or multiplication) or statistical operations (e.g., median, minimum, maximum, or mean). For example, an AG can simply forward the sum of numerical data received instead of forwarding all data to the next hop.

Attack Model:

First of all, we categorize the adversary's abilities as follows:

1. Adversaries can eavesdrop on transmission data in a WSN.
2. Adversaries can send forged data to any entities in a WSN (e.g., SN, AG, or BS).
3. Adversaries can compromise secrets in SNs or AGs through capturing them.

Second, we define the following attacks to qualify the security strength of a CDA scheme. Part of these attacks refer to Peter et al.'s analysis [6]. Based on adversary's abilities and purposes.

Grouping of Data in Sensor:

This module helps the Sensor Nodes to be grouped as Group A, Group B. SN resident in nearby area would form a cluster and select one among them to be their cluster head(CH).The CH organizes data pieces received from SN into an aggregated result, and then forwards the result to the base station based on regular routing paths. Generally, aggregative operations are algebraic, such as the addition or multiplication of received data, or statistical operation, such as a median, a minimum, or a maximum of a data. Fig 2 explains how the nodes are grouped. Data are forwarded to Base Station after completing the aggregation process in the aggregator.

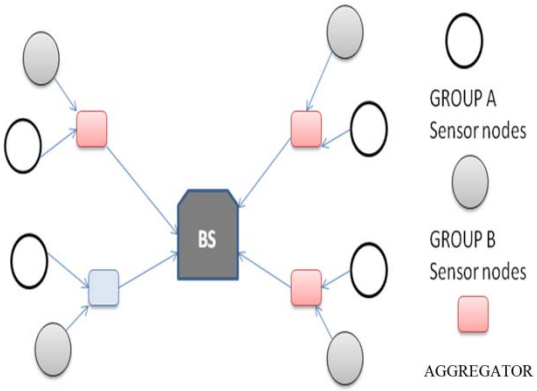

Fig. 2 Grouping of sensor Networks.

Secure Extraction Of Data:

This model describes how the multi-parameter data from the sensor node is being retrieved from the Base Station. The data for security reasons as well to extract application specific data it is being provided a key and using the key the data is extracted. If a single sensor node is compromised then data can be forged. Hence the Cipher data is sent to base station in a encrypted form.

9. EVALUVATION

We have shown the cost relation between point addition and scalar multiplication. Next, we show how to estimate the cost of scalar multiplication on different finite fields. In general, the cost depends on the size of the scalar and the size of underlying finite field. If the size of scalar doubles, the cost doubles too (i.e., linearly inclining). Moreover, if the size of the finite field doubles, the computation cost is almost four times the original (i.e., increasing by a power of 2). Based on these two rules, the cost of scalar multiplication on a 1,024-bit field is estimated to be 247.84 times greater than that on a 163-bit field, where the scalar is chosen from the underlying field.

10. CONCLUSION AND FUTURE WORK

A new mechanism is proposed for a multi-application environment. With the help of CDAMA the cipher texts of different applications are aggregated in a secure way and they are not mixed. CDAMA reduces the impact and also blocks damages from occurring. It provides the knowledge of knowing the exact number of messages aggregated and sends the information of it to the base station.. Hence it provides security and enhances the performances of the application. In the future, we wish to apply CDAMA to realize aggregation query in Database-As-a-Service (DAS) model[7]. In DAS model, a client stores her database on an untrusted service provider. Therefore, the client has to secure their database through PH schemes because PH schemes keep utilizable properties than standard ciphers. Based on PH schemes, the provider can conduct aggregation queries without decryption. The most important of all is that we do not have to consider the computation cost and the impact of compromising secret keys . Those drawbacks will no longer be issues in CDAMA.

ISSN 2348 – 7968

REFERENCES

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A Survey on Sensor Networks,” IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002.

[2] R. Min and A. Chandrakasan, “Energy-Efficient Communication for Ad-Hoc Wireless Sensor Networks,” Proc. Conf. Record of the 35th Asilomar Conf. Signals, Systems and Computers, vol. 1, 2001.

[3] B. Przydatek, D. Song, and A. Perrig, “SIA: Secure Information Aggregation in Sensor Networks,” Proc. First Int’l Conf. Embedded Networked Sensor Systems, pp. 255-265, 2003.

[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] J. Girao, D. Westhoff, M. Schneider, N. Ltd, and G. Heidelberg, “CDA: Concealed Data Aggregation for Reverse Multicast Traffic in Wireless Sensor Networks,” Proc. IEEE Int’l Conf. Comm. (ICC ’05), vol. 5, 2005.

[6] S. Peter, D. Westhoff, and C. Castelluccia, “A Survey on the Encryption of Convergecast-Traffic with In-Network Processing,” IEEE Trans. Dependable and Secure Computing, vol. 7, no. 1, pp. 2034, Jan.-Mar. 2010.

[7] B. Iyer, C. Li, and S. Mehrotra, “Executing Sql over Encrypted Data in the Database-Service-Provider Model,” Proc. ACM SIGMOD Int’l Conf. Management of Data, pp. 216-227, 2002

[8] H. Hacigu ¨mu ¨s¸ “Efficient Execution of Aggregation Queries over Encrypted Relational Databases,” Proc. Ninth Int’l Conf. Database Systems for Advanced Applications (DASFAA ’04), vol. 9, p. 125, 2004.

[9] 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: Networking and Services (MobiQuitous ’05), pp. 109-117, 2005.

[10] D. Boneh, E. Goh, and K. Nissim, “Evaluating 2-DNF Formulas on Ciphertexts,” Proc. Second Int’l Conf. Theory of Cryptography (TCC), vol. 3378, pp. 325-341, 2005.