Concealed Data Aggregation for Multiple Application Using Distributed Data Scheduling Algorithm

J.Mumtaj Begum[1] Mr .G.Ravi[2]
[1]Research Scholar [2]Associate Professor & Head of Department
[1,2]Department of Computer Science
[1,2]Jamal Mohamed College, Trichirapalli, Tamil Nadu, India

Abstract— 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. Therefore, we propose a new concealed data aggregation scheme extended from homomorphic public encryption system. Main objective of this project to aggregate for multi application data and provide security using PH.

Key words: Concealed Data Aggregation, homomorphic public encryption, SSL, Diffie Helman Algorithm

I. INTRODUCTION

Existing aggregate encrypted messages directly from SN, avoiding the forgery of aggregated result. Since Cluster Heads are not capable of encrypting messages, compromising a CH earns nothing in forging aggregated results and CHs to classify encrypted data without decrypting them. This Concealed data aggregation (CDA) supporting richer operations on aggregation. CDA utilizes the privacy homomorphism encryption (PH) to facilitate aggregation in encrypted data. CHs are able to execute algebraic operations on encrypted numeric data. Public-key based PH encryptions to construct their systems but these Techniques doesn't applicant for multi application. These approach only for transmitting separate aggregate function so, increase communication cost also.

II. LITERATURE SURVEY

A. CDA for Reverse Multicast Traffic in Wireless Sensor Networks

Analysis in most scenarios presumes computation of an optimum, e.g., the minimum or maximum, the computation of the average, or the detection of movement pattern. Precomputation of these operations may be either fulfilled at a central point or by the network itself. The latter is beneficial in order to reduce the amount of data to be transmitted over the wireless connection. Since the energy consumption increases linearly with the amount of transmitted data, an aggregation approach helps increasing the WSN's overall lifetime. Another way to save energy is to only maintain a connected backbone for forwarding traffic, whereas nodes that perform no forwarding task persist in idle mode until they are re-activated.

1) Algorithm Using

- Privacy Homomorphism
- Aggregation

B. A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack

All of the previously known schemes provably secure under standard intractability assumptions are completely impractical (albeit polynomial time), as they rely on general and expensive constructions for non-interactive zero knowledge proofs. This includes non-standard schemes like Rackoff and Simon's as well.

Practical Schemes. Damgard proposed a practical scheme that he conjectured to be secure against lunch-time attacks; however, this scheme is not known to be provably secure, and is in fact demonstrably insecure against adaptive chosen cipher text attack.

C. Classify 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. Since supporting In-network processing can significantly improve the performance of extremely resource-constraint sensor networks featuring many-to-one traffic pattern. It is an open problem of how to protect the traffics and to support In-network processing at the same time.

1) Algorithm Using:

- Diffie Helman Algorithm

D. Public Key Based Cryptoschemes for Data Concealment in Wireless Sensor Networks

Secure aggregation is the absence of solutions involving public-key encryption schemes. However, public-key based solutions provide a higher level of system security, since nodes would not be equipped with private keys, which would limit the advantage gained by an attacker compromising some of the nodes. It is therefore important to note why public-key encryption schemes have not yet been deployed. The reason is two-fold: (1) they are deemed too costly for computationally weak devices and (2) the expansion in bit size during the transformation of plaintext to ciphertext introduces costly communication overhead, which directly translates to a faster depletion of the sensor's energy.

1) Algorithm Used:

- Additively Homomorphic Encryption
- Elliptic Curve Naccache-Stern (EC-NS) Encryption

E. E_cient Aggregation of encrypted data in Wireless Sensor Networks

Although simple and well-understood, aggregation becomes problematic if end-to-end privacy between sensors and the sink is required. If we assume that all sensors are trusted, sensors could encrypt data on a hop-by-hop basis. For an intermediate sensor (i.e., one that receives and forwards data), this would entail: 1) sharing a key each neighboring sensor, 2) for each downstream1 neighbor, decrypting the received encrypted value, 3) aggregating all received values, and 4) encrypting the result for transmission upstream. Though viable, this approach is fairly expensive and complicated. The former because of having to decrypt each received value before aggregation and the latter due to the overhead imposed by key management.

1) Algorithm:

AGG protocol, HBH (hop-by-hop encryption and aggregation.

III. SYSTEM ANALYSIS

A. Existing System

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 set. Although data aggregation could significantly reduce transmission, it is vulnerable to some attacks. For instance, compromising a CH will allow adversaries to forge aggregated results as similar as compromising all its cluster members. An alternative approach for this problem is to aggregate encrypted messages directly from SN, thereby avoiding the forgery of aggregated result. Since CHs are not capable of encrypting messages, compromising a CH earns nothing in forging aggregated results. The cipher texts of different applications cannot be aggregated together; otherwise, the decrypted aggregated result will be incorrect. The only solution is to aggregate the cipher texts of different applications separately. The transmission cost grows as the number of the applications increases. The second scenario is designed for single application WSNs. Compared with conventional schemes; CDAMA mitigates 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 capability. In previous schemes, the base station does not know how many messages are aggregated from the decrypted aggregated result; leaking count knowledge will suffer maliciously selective aggregation and repeated aggregation.

B. Proposed System

The CDAMA base station exactly knows the number of messages aggregated to avoid above attacks 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 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 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). PH schemes are classified to symmetric cryptosystem when the encryption and decryption keys are identical, or asymmetric cryptosystem (also called public key cryptosystem) when the two keys are different.

The most notable asymmetric PH schemes are based on elliptic curve cryptography (ECC). Compared with RSA cryptosystems, ECC provides the same security with a shorter key size and shorter cipher texts. The AG aggregates those cipher texts through modular addition. And the BS decrypts the cipher text received by modular subtraction with all the temporal keys. Their scheme cannot prevent the adversary from injecting forged data packets into the legitimate data flow. In addition, key synchronization must be guaranteed because each SN must rekey after each encryption.

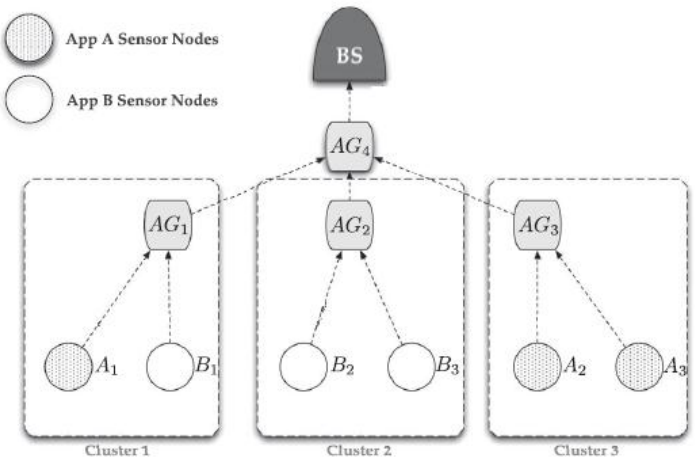
IV. SYSTEM SPECIFICATION

A. Software Requirement

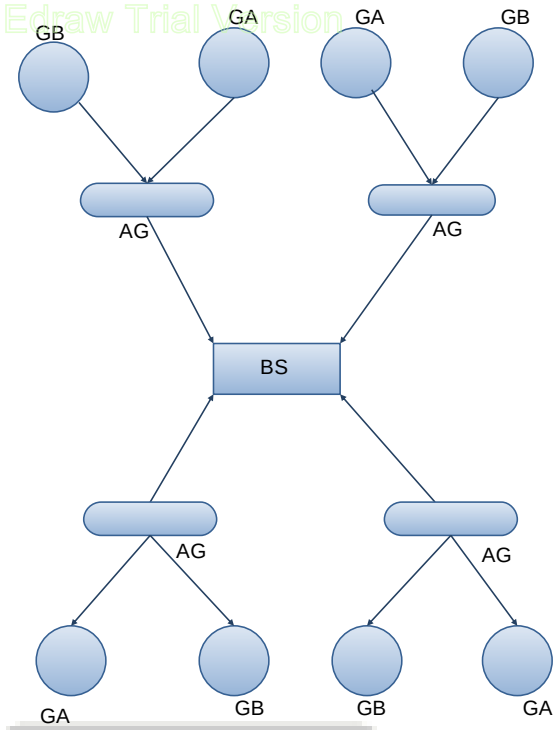
Front End/GUI Tool	: Microsoft Visual studio 2008
Operating System	: Windows Family
Language	: C#
Application	: C#.NET
Back end	: SQL-Server 2005

V. SYSTEM DESIGN

System design is the process of defining the architecture, components, modules, and data for a system to satisfy specified requirements. One could see it as the application of systems theory to product development. There is some overlap with the disciplines of systems analysis, systems architecture and systems engineering. If the broader topic of product development blends the perspective of marketing, design, and manufacturing into a single approach to product development, then design is the act of taking the marketing information and creating the design of the product to be manufactured. System design is therefore the process of defining and developing systems to satisfy specified requirements of the user.



A. System Architecture:



VI. System Implementation

A. Modules And Explanation

- Network Evaluation Module
- CDAMA Construction Module
- Key Distribution Module
- Data Aggregation Module
- Secure Counting Module

B. Algorithm

- Homomorphic Public Encryption
- CDAMA
- Aggregation with Secure Counting

C. Homomorphic Public Encryption

Homomorphic encryption (PH) is an encryption scheme with homomorphic property. The homomorphic property implies that algebraic operations on plaintexts can be executed by manipulating the corresponding ciphertexts.

PH schemes are classified to symmetric cryptosystem when the encryption and decryption keys are identical, or asymmetric cryptosystem (also called public key cryptosystem) when the two keys are different.

D. CDAMA

Assume that all SNs are divided into two groups, G_A and G_B. CDAMA contains four procedures: Key generation, encryption, aggregation, and decryption, CDAMA (k = 2) is implemented by using three points P,Q, and H whose orders are q1, q2, and q3, respectively.

E. Aggregation with Secure Counting

The main weakness of asymmetric CDA schemes is that an AG can manipulate aggregated results without encryption capability. An AG is able to increase the value of aggregated result by aggregating the same cipher text of sensed reading repeatedly, or decrease the value by selective aggregation. Since the BS does not know the exact number of cipher texts aggregated repeated or selective aggregation may happen

F. Expected Outcome

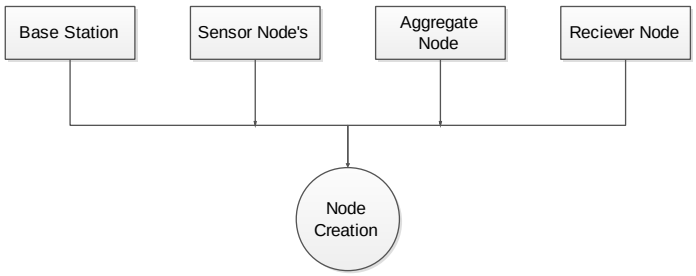
This project implemented for .NET application and language C#. The CDAMA are all built on elliptic curves, encryption and aggregation are based on two kinds of operations, point addition and point scalar multiplication. In elliptic curve arithmetic, two basic operations are point doubling and adding.

These inputs are given sensed data, these data only sense the system based sensors like Desktop capture and Folder Sensing software has been implement for this application.

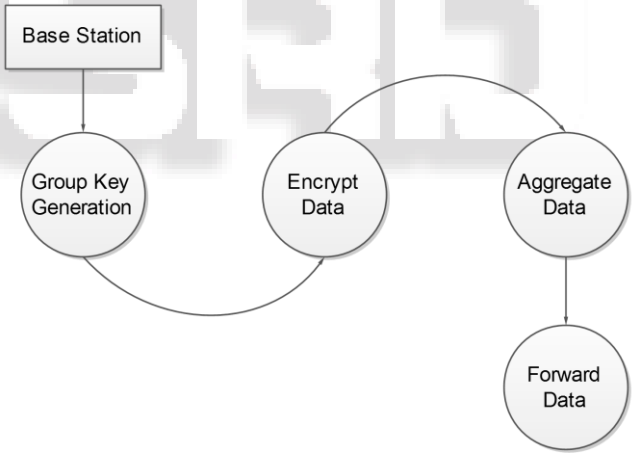
Outputs are secure data access for base station and securely counting the how many data has been aggregated.

G. Flow Diagram

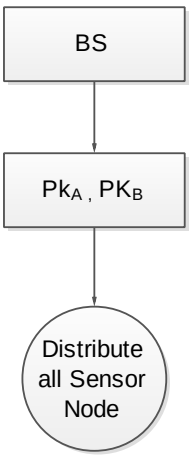
- Network Evaluation Module



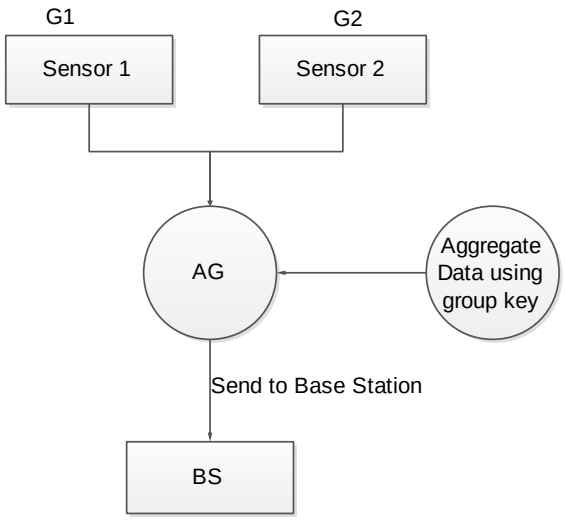
- CDAMA Construction Module



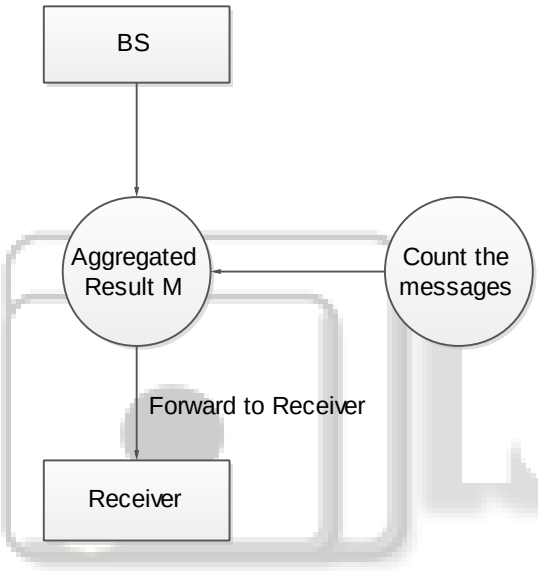
- Key Distribution Module



- Data Aggregation Module



– Secure Counting Module



VII. CONCLUSION

A multi-application environment, CDAMA is the first CDA scheme. Through CDAMA, the cipher texts from distinct applications can be aggregated, but not mixed. For a single-application environment, CDAMA is still more secure than other CDA schemes. When compromising attacks occur in WSNs, CDAMA mitigates the impact and reduces the damage to an acceptable condition. Besides the above applications, CDAMA is the first CDA scheme that supports secure counting. The base station would know the exact number of messages aggregated, making selective or repeated aggregation attacks infeasible. Finally, the performance evaluation shows that CDAMA is applicable on WSNs while the number of groups or applications is not large.

VIII. FUTURE WORK

Attribute-aware data aggregation (ADA) scheme, which can make the packets with the same attribute convergent as much as possible to improve the efficiency of data aggregation. ADA to collect packets and aggregate them before they reach the sink. Attribute-aware data aggregation consisting of PBDR protocol and packet-driven timing control algorithm. Packets are treated as ants, and then the basic mechanism for finding paths. Packet-driven adaptive timing scheme. The node maintains a timer for the packets with the same attribute in its queue.

REFERENCES

[1] 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.

a. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks," Comm. ACM, vol. 47, no. 6, pp. 53-57, June 2004.

[4] L. Hu and D. Evans, "Secure Aggregation for Wireless Networks," Proc. Symp. Applications and the Internet Workshops, pp. 384-391, 2003.

[5] H. Cam, S. O ¨ zdemir, P. Nair, D. Muthuavinashiappan, and H.O. Sanli, "Energy-Efficient Secure Pattern Based Data Aggregation for Wireless Sensor Networks," Computer Comm., vol. 29, no. 4, pp. 446-455, 2006.

[6] H. Sanli, S. Ozdemir, and H. Cam, "SRDA: Secure Reference-based Data Aggregation Protocol for Wireless Sensor Networks," Proc. IEEE 60th Vehicular Technology Conf. (VTC 04-Fall), vol. 7, 2004.

[7] Y. Wu, D. Ma, T. Li, and R.H. Deng, "Classify Encrypted Data in Wireless Sensor Networks," Proc. IEEE 60th Vehicular Technology Conf., pp. 3236-3239, 2004.

[8] 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.

[9] J. Girao, D. Westhoff, M. Schneider, N. Ltd, and G. Heidelberg, "CDA: Concealed Data Aggregation for Reverse Multicast Traffic in Wireless Sensor Networks," Proc. IE

