ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (17-22), Month: October - December 2014, Available at: www.researchpublish.com

Secure and Effective Technique CDAMA Scheme in Wireless Sensor Network Using DAS Model

[1]Satyaprakash Mishra, [2]Sonu Agrawal

[1]Department of Computer Science &Engineering, Shri Shankara charaya College of Engineering and Technology Bhilai, India
[2]Associate Professor, Department of Computer Science &Engineering, Shri Shankaracharaya College of Engineering and Technology Bhilai, India

***Abstract*: For wireless sensor networks, data aggregation scheme minimize a large amount of transmission data to the base station, so that improve the energy efficiency and prolong the wireless network lifetime.CDA provides end-to-end security.ie. even though the sensed data are encrypted on the sensor nodes and not decrypted before the sink node In this paper, all the homomorphic encryption techniques and various attacks is categorized, but CDA schemes are not satisfy multi-application environments and not provide secure counting; so they may suffer unauthorized aggregation attacks Therefore, a new concealed data aggregation scheme based on homomorphic public encryption system. CDAMA is designed by using multiple points, each of which has different order. The security of CDAMA are based on the hardness assumption of subgroup decision problem Database-as-a-Service model is a specific instance of an outsource database model where by clients do not have the necessary resources to manage their own databases choose to outsource them to database service providers**

***Keywords:* Homomorphic encryption, Concealed data aggregation, wireless sensor networks**

I. INTRODCTION

Wireless sensor networks are an emerging technology, poised for rapid market growth. The combination of multiple user applications, the development of communication protocols for self-organizing ad hoc networks, high levels of product integration, and standardization is expected to lead to high manufacturing volumes and their associated economies of scale. It truly is an exciting time for the wireless industry, which has suffered lately due to the maturity of its existing markets. The development of wireless sensor networks will be its next major growth area.

Six major market classifications for wireless sensor networks were presented:

1. Industrial control and monitoring

2. Home automation and consumer electronics

3. Security and military sensing

4. Assjet tracking and supply chain management

5. Intelligent agriculture and environmental sensing

6. Health monitoring

The database generic query interface for data aggregation can be applied to dedicated networks of sensor devices. Aggregation is used as a data reduction tool. Networking approaches have focused on application specific solutions. In the data aggregation of WSN, two security requirements are confidentiality and integrity, should be fulfilled. An adversary can require the data confidentiality by the following attacks: a) eavesdropping the messages in the wireless channel; b) compromising a node and obtaining all keys stored in it; c) using the compromised node's keys to deduce the keys employed elsewhere in the network; d) using the compromised node's keys to inject unauthorized malicious sensor nodes in the network. The data aggregation can significantly reduce the amount of data transmitted to the base station so that improve the energy efficiency and prolong the wireless network lifetime [9] [10]. Sometime the sensor nodes may be deployed in remote and hostile environments where attackers may inject false information or forge aggregation values without being detected. so security issue becomes an important research field in data aggregation for WSNs. Typically, a sensor node is rearly constrained in terms of computation capability and energy reserves. A optimal method to collect the sensed information from the network is to allow each sensor node.

II. TYPE OF ATTACKS

The main types of attacks in wireless sensor networks are Listed 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.

2.1. Adversaries can eavesdrop on transmission data in a WSN

In the first category, An adversary wants to deduce the secret key (i.e., decrypting arbitrary ciphertexts). First Category consists of four attacks that are generally used in qualifying an encryption scheme .here in this category following attacks are as follows

2.1.1-. Ciphertext only attack.--An adversary can affect the key from only the encrypted messages.

2.1.2. Known plaintext attack-- Given some samples of plaintext and their ciphertext, an adversary can deduce the key or decrypt any ciphertext.

2.1.3. Chosen plaintext attack-- Given some samples of chosen plaintext and their ciphertext, an adversary can deduce the key or decrypt any ciphertext.

2.1.4. Chosen ciphertext attack-- Given some samples of chosen ciphertext and their plaintext, an adversary can deduce the key or decrypt any ciphertext she has not chosen before.

2.2 Adversaries can send forged data to any entities in a WSN (e.g., SN, AG, or BS)

In this category, an adversary wants to send the forged messages to cheat the BS even though she does not know the secret key. Second category consists of two attacking scenarios based on specific features deriving from PH schemes.

2.2.1. Unauthorized aggregation--An adversary can aggregate sniffed ciphertexts into forged but format-valid ciphertexts.

2.2.2. Malleability-- An adversary can alter the content of a ciphertext.

2.3. Adversaries can compromise secrets in SNs or AGs through capturing them

The last category consists of three attacks and considers the impact of node compromising attacks. The initial most attack is the case of compromising an AG, and the last two attacks are cases of compromising an SN. We discuss them separately because they store different secrets in the PH schemes.

2.3.1 B2/B3 attacks --with higher probability of success.

2.3.2 Unauthorized decryption-- under compromised SN. When an adversary captures an SN and compromises its secret,they can decrypt not only the ciphertexts from that SN but also the ciphertexts from the other remaining SNs.

Asymmetric schemes can follow unauthorized decryption under compromised secrets.

III. HOMOMORPHIC ENCRYPTION TECHNIQUES

In WSNs, Privacy homomorphic can be applied for concealing converge cast traffic with simple in network processing at aggregating intermediate nodes. Such an approach is known as CDA[2]. The topology-aware key pre distribution provides the best achievable security in an environment with no tamper resistant devices and still ensures the application of CDA for reverse multicast traffic protocol. Such a key pre distribution scheme is also applicable to a CDA based on the the comparison operation that we provided in our earlier work.[3]

3.1 Privacy Homomorphic Cryptosystem

PH is centain an encryption scheme with homomorphic property. PH schemes are classified to symmetric cryptosystem when the encryption and decryption keys are identical, or asymmetric cryptosystem (also known public key cryptosystem) when the two keys are different[2].

3.2. CDA Based on PH

In Conventional schemes are insecure because an adversary is able to forge aggregated results hop-by-hop aggregation[5] such as compromising all the Aggregator’s child nodes when he compromises the secret of an Aggregator’s. CDA provides end-to-end security.ie. even though the sensed data are encrypted on the sensor nodes and not decrypted before the sink node, This scheme can be aggregated on the intermediate nodes. They make use of the algebraic properties of the applied PH: Additively homomorphic PHs support additive operations on encrypted data, where multiplicatively homomorphic PHs allow for multiplicative operations on the ciphertext. CDA is the first work focusing on end-to-end encryption in WSNs by still providing in-network processing. The applied PH from Domingo-Ferrer is secure against adversaries that exclusively carry out chosen ciphertext attacks.

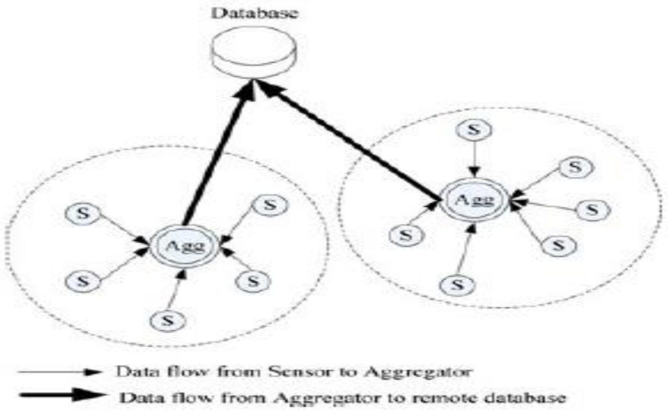
Database
S
Agg
Data flow from Sensor to Aggregator
Data flow from Aggregator to remote database

FIG 1: Data aggregation through CDA

CDA-based end-to-end encryption is much more flexible for varying connected backbones over different epochs. only nodes storing the corresponding key can perform the decryption and aggregate data in hop-by-hop encryption. In CDA node can be selected as an aggregator node, so the aggregating nodes do not need to store the key to operate on the incoming message. So that, the election process of a node per epoch is based on the remaining energy levels of the nodes. CDA provides confidentiality by not restricting aggregator-node-election algorithms This give robustness and reliability of the WSN [1][2].

3.3. BGN Scheme

BGN provides additive and multiplicative homomorphism. Since the multiplicative property, based on the bilinear pairing [2] is much expensive and inefficient for Sensor node. BGN is constructed on a cyclic group of elliptic curve points. Precisely, these points form an algebraic group, where the identity element of the group is the infinite point[1] only utilize the additive homomorphism of BGN. Here first provide a possible application for BGN, data aggregation. modify BGN to fit multigroup construction for stronger security and better applicability in CDA.

3.4 CDAMA

CDAMA is designed by using multiple techniques, and all of has different order. Here obtain one scalar of the specific point through removing the effects of remaining points (i.e.multiplying the aggregated ciphertext with the product of the orders of the remaining points).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.[14] Another major change is the decryption procedure. By performing individual decryption, the BS extracts individual aggregated results of different groups from an aggregated ciphertext how to deliver the group public keys to SNs securely. There are two main approaches.

1] Key predistribution.- If we know the locations of deployed SNsthen preload necessary keys and functions into SNs and AGs so that they can work correctly after being spread out over a geographical region.

2] Key postdistribution- Before SNs are deployed to their geographical region, they are capable of nothing about CDAMA keys. These SNs only load the key shared with the BS prior to their deployment therefore the individual key in LEAP [4] and the master secret key in SPINS [6]. Once these SNs are deployed, they can run the LEACH protocol [2] to elect the AGs and construct clusters. After that, the BS sends the corresponding CDAMA keys, encrypted by the sheared key, to SNs and AGs.

3.5 DAS model

DAS model are the bandwidth overhead between the server and client[15] It is a manifestation of the more general Software-as-a-Service trend which is becoming increasingly popular. However, providers who gain complete access to the clients' data may not be trustworthy as they might store databases belonging to competing clients or simply have their own malicious intentions. This might be acceptable if the client is using a desktop/laptop with a high-speed network connection, but not so in case the client is a weak device such as a cell phone or low-end PDA, where battery power and computational resources are limited. It contains following function

3.1.1. Partition Functions

3.1.2. Identification Functions

3.1.3. Mapping Function

3.1.4. Storing Encrypted Data

3.1.5. Decryption Function

Natural choice for ensuring data privacy is to use a strong encryption algorithm. The client encrypts the database using a symmetric-key encryption algorithm– such as AES[11] which is ideal for bulk data encryption – and stores the it at the service provider. Each time the client needs to execute a SQL query, it first obtains required tables from the server, decrypts the data and runs the query locally.

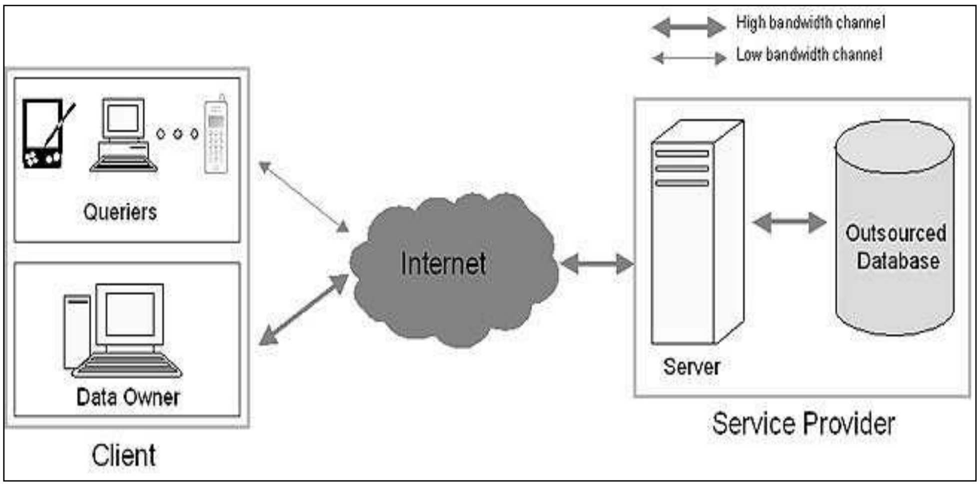

Fig.2.DAS Model

IV. DISCUSSION

4.1 Efficient Aggregation Techniques

It is a challenging task to securely aggregate information SIA [4] ESPDA[5] SRDA[6] in large sensor networks when the aggregators and some sensors may be malicious. Here propose the *aggregate-commit-prove* framework for designing secure data aggregation protocols and concrete protocols within this framework for securely computing the median, securely finding the minimum and maximum values securely estimating (counting) the number of distinct elements (and the network size) and securely computing the average of measurements). Here introduces the problem of secure information aggregation to the community and encourages other researchers to consider this important problem.

4.2 Effective Encryption

Here introduced the problem of end-to-end encrypted data aggregation in WSNs. We showed that privacy homomorphism are encryption transformation with particular characteristics valuable for concealed data aggregation. By applying the additive PH from Domingo-Ferrer as a reference PH our proof of concept indicates the principle suitability of symmetric additive PHs to aggregation functions average and movement detection. Actual implementation and its performance comparison with a hop-by-hop encryption scheme confirms that the approach is feasible and for a broad range of realistic encryption. [9]

4.3 Candidate Scheme

In wireless sensor networks design, implementation, and evaluation of Tiny ECC, is configurable library for ECC operations. Tiny ECC is important feature its configurability. It provides a number of optimization switches, which can specific optimizations on or off based on needs. Different combinations of the optimizations have different execution time and resource consumptions, and so give the developers great flexibility in integrating TinyECC into sensor network applications. A series of experiments to evaluate the performance and resource consumptions of TinyECC with different combinations of enabled optimizations. In particular, experiment results gave the most computationally efficient and the most storage efficient configurations of Tiny ECC..[10]

4.4. Performence Analysis

A homomorphic encryption scheme that supports addition or multiplication techiqes for effective results. The values being encrypted lie in a small range as is the case when encrypting bits. homomorphic properties not evaluate multi-variant polynomials of total degree 2 given the encrypted inputs. Here described a number of applications of the system.using our encryption scheme, we 1) reduced the amount of communication in the basic step of the Kushilevitz-Ostrovsky PIR, 2) improved the efficiency of election systems based on homomorphic encryption, and 3) implemented universally verifiable secure computation.[12][11]

V. CDAMA APPROACH TO AGGREGATION QUERY APPLY IN DAS MODEL

CDAMA to realize aggregation query in Database-As-a-Service (DAS) model.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 (i.e., compromising a client in DAS model is harder than compromising a sensor).

VI. CONCLUSION

In this paper various aspect of Aggregation Scheme like, Privacy Homomorphic, BGN Scheme, CDA Based on PH,CDAMA has been discussed; furthermore various type of attacks have been listed in wireless sensor network . homomorphic encryptions have been applied to conceal communication during aggregation such that enciphered data can be aggregated without decryption. Since aggregators collect data without decryption. CDA schemes are not satisfy multi-application environments. And not provide secure counting a new concealed data aggregation scheme i.e. CDAMA extended from homomorphic public encryption system. it is designed for a multi-application environment. it mitigates the impact of compromising attacks in single application environments and degrades the damage from unauthorized aggregations. In the database-service-provider model, user's data resides on the premises of the provider. Both corporations and individuals view their data as a very valuable asset. CDAMA to realize aggregation query in DAS model. Result shows client has to secure their database through PH schemes because PH schemes reduces Communication Overhead,the system cost , improve system flexibility.

REFERENCES

[1] Yue-Hsun Lin, Shih-Ying Chang, and Hung-Min Sun"CDAMA: Concealed Data Aggregation Scheme for Multiple Application" IEEE Transaction on knowledge and data engineering,vol.25 no,7 july 2013

[2] Steffen Peter, Dirk Westhoff, Member, and Claude Castelluccia, "A Survey on the Encryption of Convergecast Traffic with In-Network Processing," IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 7, NO. 1, JANUARY-MARCH 2010

[3] 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.

[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. 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] B. Iyer, C. Li, and S. Mehrotra, "Executing Sql over Encrypted Data in the Database-Service-Provider Model," Proc. AC 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] 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.

[10] J. Girao, D. Westhoff, E. Mykletun, and T. Araki, "Tinypeds: Tiny Persistent Encrypted Data Storage in Asynchronous Wireless Sensor Networks," Ad Hoc Networks, vol. 5, no. 7, pp. 1073-1089 2007

[11] 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.

[12] Sanjeev SETIA a,Sankardas ROY and Sushil JAJODI "Secure Data Aggregation in Wireless Sensor Networks" Proc. of 33rd STOC, pages 266–275, 2001.

[13] Gabrieli, L. Mancini, S. Setia, and S. Jajodia. "Security topology maintenance protocols for sensor networks: Attacks & countermeasures" .First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005. IEEE, 2005.

[14] Einar Mykletun and Gene Tsudik "Incorporating a Secure Coprocessor in the Database-as-a-Service Model" Proceedings of the Innovative Architecture for Future Generation High-Performance Processors and Systems (IWIA'05)IEEE 2005