Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.881 – 888

RESEARCH ARTICLE

CONCEALED CLIENT DATA AGGREGATION FOR DATABASE-AS-SERVICE (DAS)

JEBARANJANI.B
M.E/CSE
V.S.B Engineering College
Karur, TamilNadu
jebaranjani@gmail.com

SANGEETHA.S
AP/CSE
V.S.B Engineering College
Karur, TamilNadu
sangi.vs@gmail.com

Abstract---Data aggregation scheme reduces the large amount of transmission in Wireless Sensor Networks (WSN). Concealed Data Aggregation schemes that are extended from homomorphic public encryption system are designed for a multi-application environment. The drawbacks of existing work include address aggregation security for Database As Service (DAS) Model. Client query aggregation increases the computation cost. Compromised secret keys affect the sensor node aggregations that are loosed. In DAS client stores database are on an entrusted service provider. The proposed work presented Concealed Data Aggregation for Database-AS-Service. It establishes the trusted database server for the client data storage. The aggregation of client queries for multiple applications is made with private homomorphic encryption standards. The client query responsive data are extracted from trusted data server with authenticated concealment. PH scheme contains utilizable properties to conceal data of respective clients. It minimizes the computation cost due to the client query aggregates. The uncompromised secret key improves the client query response for multiple groups.

Index Terms---Concealed data aggregation, elliptic curve cryptography, homomorphic encryption, wireless sensor networks.

I. INTRODUCTION

Wireless sensor networks (WSNs) consist of thousands of sensor nodes (SN) that gather data from deployed environments. Currently, there are plenty of rich applications proposed for WSNs, such as environment monitoring,

© 2014, IJCSMC All Rights Reserved

accident reporting, and military investigation. Depending on the purpose of each application, SN is customized to read different kinds of data (e.g., temperature, light, or smoke). Typically, SN is restricted by the resources due to limited computational power and low battery supply; thus, energy saving technologies must be considered when we design the protocols. 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. To solve this problem, several studies, such as the delay aggregation, SIA, ESPDA and SRDA have been proposed. The proposed scheme, called CDAMA, provides CDA between multiple groups. Basically, CDAMA is a modification from Boneh et al.'s PH scheme. Here, we also suppose three practical application scenarios for CDAMA, all of which can be realized by only CDAMA.

The first scenario is designed for multi-application WSNs. In practice, SN having different purposes the only solution is to aggregate the cipher texts of different applications separately. As a result, the transmission cost grows as the number of the applications increases. By CDAMA, the cipher texts from different applications can be encapsulated into "only" one cipher text. Conversely, the base station can extract application-specific plaintexts via the corresponding secret keys.

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. In CDAMA, the base station exactly knows the number of messages aggregated to avoid above attacks.

II. PRELIMINARIES

The Sensor Network framework is designed by W. Su et al., (2002) can be used for various applications areas. The current state of the art of sensor networks is captured in this article, where solution is discussed under their related protocol stack layer sections. This article also points out the open research issues and intends to spark new interests and development in these fields.

We propose a novel framework for secure information aggregation in large sensor networks. In our framework is designed by D. Song et al., (2003) certain nodes in the sensor network, called aggregators, help aggregating information requested by a query, which substantially reduces the communication overhead. By constructing efficient random sampling mechanisms and interactive proofs, we enable the user to verify that the answer given by the aggregator is a good approximation of the true value even when the aggregator and a fraction of the sensor nodes are corrupted. In particular, we present efficient protocols for secure computation of the median and the average of the measurements, for the estimation of the network size, and for finding the minimum and maximum sensor reading. Our protocols require only sub linear communication between the aggregator and the user. To the best of our knowledge, this paper is the first on secure information aggregation in sensor networks that can handle a malicious aggregator and sensor nodes.

We show possible attack scenarios is designed by L. E. Palafox et al., (2004) and evidence the easiness of perpetrating several types of attacks due to the extreme resource limitations that wireless sensor networks are subjected to. Nevertheless, we show that security is a feasible goal in this resource-limited environment; to prove that security is possible we survey several proposed sensor network security protocols targeted to different layers in the protocol stack. The work surveyed in this chapter enable several protection mechanisms vs. well documented network attacks. Finally, we summarize the work that has been done in the area and present a series of ongoing challenges for future work.

An emerging class of important applications uses ad hoc wireless networks of low-power sensor devices is designed by D. Hu et al., (2003) to monitor and send information about a possibly hostile environment to a powerful base station connected to a wired network. To conserve power, intermediate network nodes should aggregate results from individual sensors. However, this opens the risk that a single compromised sensor device can render the network useless, or worse, mislead the operator into trusting a false reading.

We present a protocol that provides a secure aggregation mechanism for wireless networks that is resilient to both intruder devices and single device key compromises. Our protocol is designed to work within the computation,

© 2014, IJCSMC All Rights Reserved

memory and power consumption limits of inexpensive sensor devices, but takes advantage of the properties of wireless networking, as well as the power asymmetry between the devices and the base station.

III.CONCEALED CLIENT DATA AGGREGATION FOR DATABASE-AS-SERVICE (DAS)

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 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).

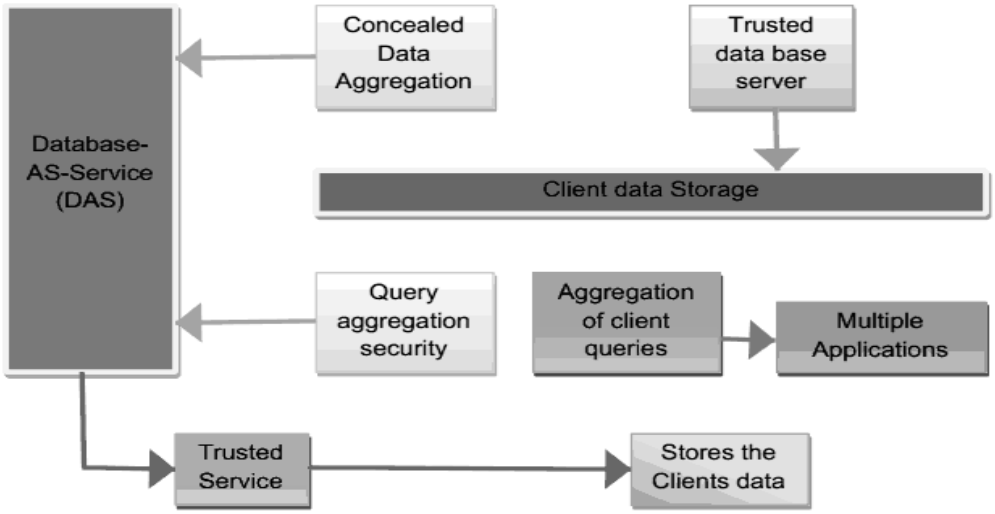

Fig 3.1 Architecture Diagram of Concealed Client Data Aggregation for Database-AS-Service (DAS)

The order of E should be large enough. Therefore, when k becomes large, the length of ciphertext will also expand. The analysis on this overhead is stated in Section 6.2. For multi-application WSNs, the SNs belonging to one specific application are assigned the same group public key. Under CDAMA, the ciphertexts from different applications can be aggregated together, but they are not mixed. The ciphertexts can be integrated into a ciphertext and transmitted to the BS. The BS then individually decrypts the aggregated ciphertext to extract the aggregated value of each application.

- Multiple Application WSN
- Concealed Data Aggregation
- Aggregation with Secure Counting
- Database as a Service Model
- Trusted Database Server
- Concealed Client Key and Data Aggregation

A. Multiple Application WSN

Deployment of multiple applications in a shared WSN. Reduce system cost, improve system flexibility, sensor nodes supports multiple applications. Assigned to different applications dynamically, sensing different data i.e., temperature, light, accelerometer.

© 2014, IJCSMC All Rights Reserved

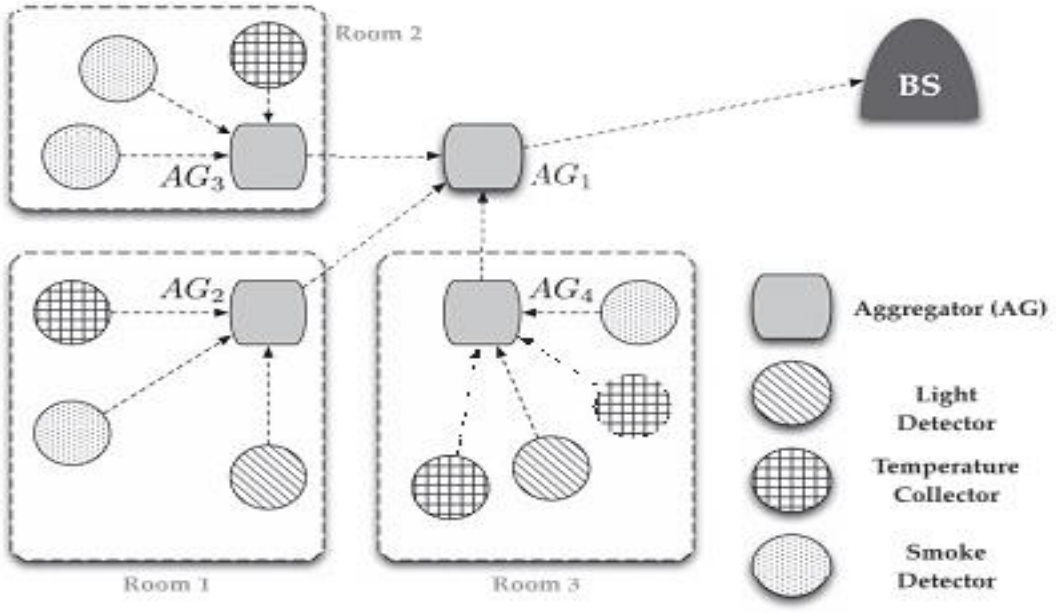

Fig 3.2 Multiple Application WSN

Aggregate sensed readings from different applications to mixed aggregated result. Sensed reading encrypted by SNs corresponding cipher texts aggregated, maintain data privacy, reduce communication overhead. Decryption cannot extract application-specific aggregated result from a mixed cipher text.

B. Concealed Data Aggregation

Concealed data aggregation model mitigate the impact from compromising attacks. All SN s arranged into two groups through C DAMA construction. Each group assigned a distinct group public key. Once an adversary compromised a SN in group A it only reveals PK of A not PK of B. Adversary can only forge messages in group A not group B sensor nodes in group B can still communicate safely CDAMA assigns every node for its own group resulting in strongest security.

CDAMA is designed by using multiple points each has different order. Obtain one scalar of the specific point by removing the effects of remaining points. Multiply aggregated cipher text with product of the orders of the remaining points CDAMA contains four procedures key generation, encryption, aggregation, and decryption. Scalars of the first two points carry aggregated messages; scalar of the third point carries randomness for security. Multiplying the aggregated cipher text scalar of the point carrying aggregated message can be obtained. Encryptions of messages of two groups aggregated to single cipher text. Aggregated message of each group obtained by decrypting cipher text with the corresponding secured key.

C. Aggregation with Secure Counting

Aggregation (AG) is able to increase value of aggregated result by aggregating same cipher text of sensed reading repeatedly or decrease the value by selective aggregation. Base Station (BS) does not know exact number of cipher texts aggregated / repeated / selective aggregation. CDAMA scheme provide secure counting BS exactly knows how many sensed readings are aggregated while it receives the final result, BS obtains the aggregated result and its count.

If malicious AG launches unauthorized aggregations value changed to a bigger or smaller value than reference count i.e., the number of deployed sensors AG does not know the base points. Unauthorized aggregations have to alter

© 2014, IJCSMC All Rights Reserved

the values simultaneously. Meanwhile BS knows the number of deployed sensors through gathering topology information BS detect unauthorized aggregation. For each application one group sums its messages other group counts number of messages aggregated, unauthorized aggregation by AG is mitigated.

D. Database as a Service Model

DAS provides an effective mechanism for organizations to purchase data management as a service freeing them to concentrate on their core businesses. DAS overhead are remote access to data an infrastructure to guarantee data privacy, user interface for such a service. Identify data privacy as a particularly vital problem. In database service provider model user data needs to reside on premises of database service provider. Most corporations view their data as a very valuable asset. Service provider would need to provide sufficient security measures to guard the data privacy.

E. Trusted Database Server

Trusted database server modeled as set of security requirements presented a concrete construction provably satisfies trustworthiness of database accessibility from remote. Each client employs a distinct key Client revocation does not entail updating of query keys re-encryption of the database, transparent to the non revoked client.

Trusted database server allows a group of client each possessing a distinct secret key to insert their encrypted data records to the database while every user in the group is able to search all the records using her chosen keywords with assistance from a semi-trusted database server. Allows the client management of the database owner organization to dynamically and efficiently revoke clients. Revocation does not require distribution of new keys did not need to update the encrypted database. After a revocation revoked clients are no longer able to search the database while revocation process is transparent to those non-revoked clients. Allows for dynamic client enrollment since a client joining does not affect other client's settings.

F. Concealed Client Key and Data Aggregation

Concealed client key and data aggregation is effective for DAS client privacy is maintained with his private key associated to the aggregation data. Once an adversary compromised column value in the database it only reveals data identity key and not the client key. Adversary forge messages in aggregated data not on the specific client's aggregated data client in the group, still access the data from service provider safely.

Key Setup:

k = (p , q), where p and q are large secret primes.

Their product: n = pq is made public.

Encryption:

Given plaintext (an integer) a,

$E_k(a) = C = (c_1, c_2) = (a \pmod p)+R(a) \times p$,

$a \pmod q+R(a) \times q$), where a Є Zn and R(x)

is a pseudorandom number generator (PRNG)

seeded by x.

Decryption:

© 2014, IJCSMC All Rights Reserved

Given ciphertext (c_1; c_2),

Dk(c_1; c_2) = (c_1 mod p)qq□1 + (c_2

mod q)pp^{-1} (mod n)

Algorithm 3.1: Concealed Client Key

Scalars of the first two points carry aggregated messages; scalar of the third point carries randomness for security. Multiplying the aggregated client key scalar of the point carrying aggregated data is accessible. Encryptions of client key of two groups aggregated to corresponding data items. Aggregated data of each group obtained by decrypting corresponding client key with the item identity.

IV. PERFORMANCE RESULTS AND DISCUSSION

The computation cost of CDAMA is significantly large. Although data aggregation can reduce the communication effectively, sensors must pay higher computation cost for encryption and aggregation. To argue with this point, we estimate the performance gain from the whole WSN based on CDA

Fig 4.1 a leaf node, the energy consumption in CDAMA is several number times greater than that in DFS because the encryption key size of CDAMA is significantly greater than the groups of AES.

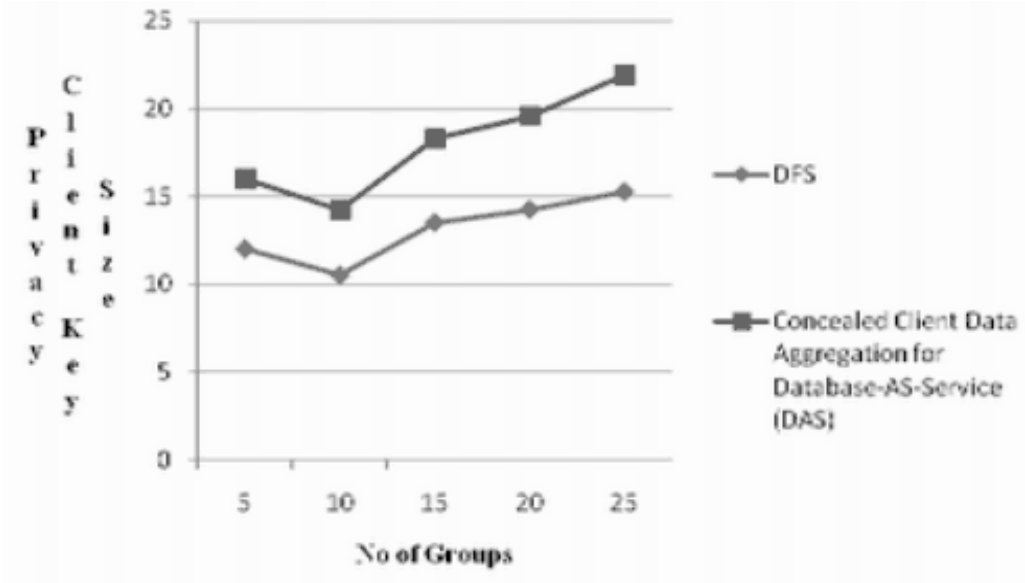

Fig 4.1 Concealed Client Data Aggregation for DAS of Number of groups and Privacy Client Key Size

For an AG, the energy consumption in DFS is increased tenfold whenever the AG reaches to the next layer, whereas the energy consumption in CDAMA are all kept the same.

© 2014, IJCSMC All Rights Reserved

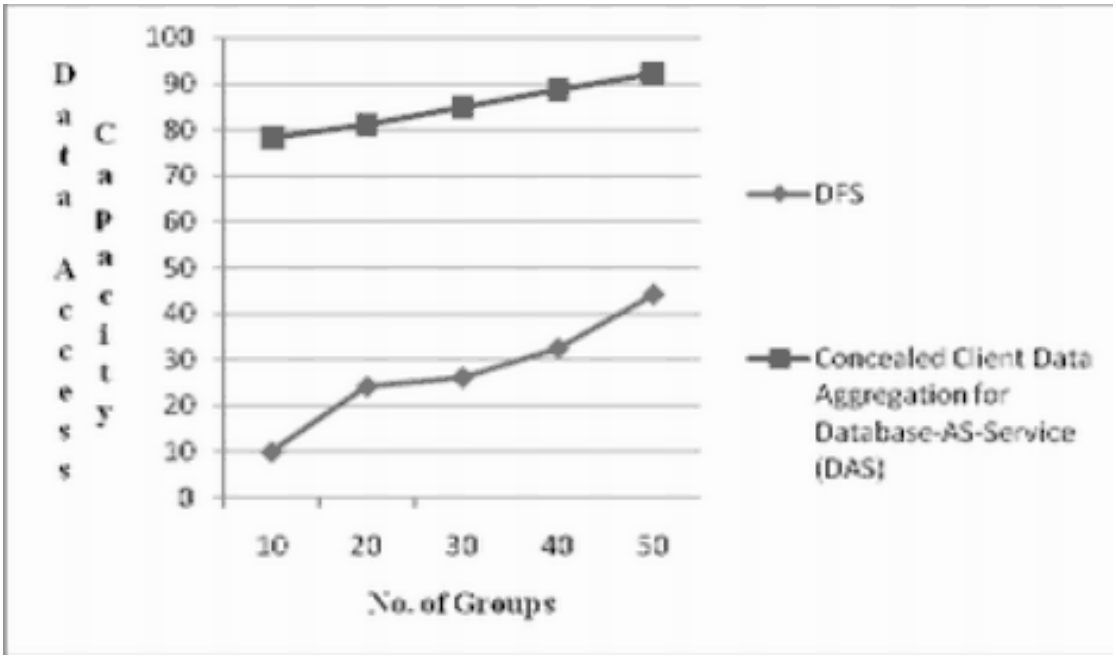

Fig 4.2 Concealed Client Data Aggregation for DAS of Number of groups and Data Access Capacity

Moreover, depending on the result of a MICAz node (8- bit microcontroller) and TelosB node (16-bit microcontroller), TelosB requires approximately 14 computation cost of MICAz to execute the same cryptographic operations, but the Data Access Privacy (receiving/transmitting one bit) in both devices are almost the same. This suggests that secure data aggregation schemes that rely on higher computation ability would be more practical in the near future.

V. CONCLUSION

CDAMA is the first CDA scheme. Through CDAMA, the ciphertexts 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.

In DAS model, a client stores her database on an un trusted 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.

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, pp. 255-265, 2003.

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

© 2014, IJCSMC All Rights Reserved

[5] L. Hu and D. Evans, "Secure Aggregation for Wireless Networks," Proc. Symp. Applications and the Internet Workshops, pp. 384-391, 2003.
[6] H. Cam, S. O ¨ zdemir, P. Nair, D. Muthuavinashiappan, and H.O. Sanli, "Energy-Efficient Secure Pattern Based Data Aggregation for Wireless Sensor Networks,", pp. 446-455, 2006.
[7] 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.

© 2014, IJCSMC All Rights Reserved