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. 4, April 2014, pg.1013 – 1018

RESEARCH ARTICLE

Secure and Energy Efficient CDAMA Scheme in Wireless Sensor Network Using DAS Model

Nidhi Mouje
Department of Computer Science & Engineering,
G. H. Raisoni College of Engineering & Technology, Nagpur, India
nmouje@gmail.com

Nikita Chavhan
Assistant Professor, Dept. of Computer Science & Engineering
G. H. Raisoni College of Engineering & Technology, Nagpur, India
niki.chavan@gmail.com

Abstract-Wireless sensor networks (WSNs) are ad-hoc networks composed of tiny devices with limited computation and energy capacities. For such devices, data transmission is a very energy-consuming operation. It thus becomes essential to the lifetime of a WSN to minimize the number of bits sent by each device. Concealed data aggregation (CDA) schemes that are based on the homomorphic characteristics of a privacy homomorphism (PH) enable end-to-end encryption in wireless sensor networks CDAMA is designed by using multiple points, each of which has different order. 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 to maintain data privacy, clients need to outsource their data to servers in encrypted form. So that time, clients must still be able to execute queries over encrypted data.

Key Words: data aggregation; wireless sensor networks; Security; privacy

1. Introduction

Wireless sensor networks (WSN) are a particular class of ad hoc networks that attract increasing attention, both in academia and industry. WSN has used in many applications such as environment monitoring, forest fire detection etc. It is widely used network as the data gathering paradigm. This may include sensing motion, measuring temperature, humidity, etc. Data monitored by the sensors is sent to a sink that is responsible for collecting the information. To collect the information from the given network many sensor nodes can be deploy in the network [1]. An aggregate (or summarized) value is computed at the data sink by applying the corresponding aggregate function, for example MAX, COUNT, AVERAGE or MEDIAN to the collected data. Aggregation techniques are used to reduce the amount of data communicated within a WSN and thus conserves battery power. The aggregators can either be special more powerful nodes or regular sensors nodes. Aggregation becomes problematic if end-to-end privacy between sensors and the sink is required[2]. All sensors are trusted, sensors could encrypt data on a hop-by-hop basis. In WSNs, PH can be prominently applied for concealed data aggregation with simple in network processing at aggregating intermediate nodes. Such an approach is termed as CDA. Encryption and decryption transformation of the symmetric reference PH proposed by Domingo-Ferrer[4]. Privacy Homomorphic is probabilistic, it contains that the encryption transformation involves some randomness that chooses the ciphertext corresponding to a given cleartext from a set of ciphertexts. There are many conventional techniques have been applied to conceal communication during aggregation such that enciphered data can be aggregated algebraically without decryption. CDAMA is designed by using multiple points, each of which has different order. One scalar of the specific point through removing the effects of remaining points . The security of CDAMA is based on the hardness assumption of subgroup decision problem.

The Database-as-a-Service (DAS) model [1] is a manifestation of the more general Software-as-a-Service trend which is becoming increasingly popular. In this model, the client stores the encrypted database at the DAS server and locally stores some information which is referred to as metadata. The types of queries that can be run at the server over the encrypted data are limited to logical comparisons, thereby greatly reduces the usefulness of the server in the query processing.

2. Previous Work

2.1 Privacy Homomorphisms

PH is an encryption transformation that allows direct computation on encrypted data. Rivest, Adleman, and Dertouzos have proposed four different additive privacy homomorphisms. two of them are insecure under a ciphertext only attack and the other two can be broken by a known plaintext attack. Conventional privacy homomorphism is introduced which has the novel property of seeming secure against a known-clear text attack. A uniform application to multilevel statistical calculation is presented, namely classified retrieval of exact statistics from unclassified computation on disclosure-protected (perturbed) data. A privacy homomorphism (PH) is an encryption transformation which allows direct computation on encrypted data using this scheme for the WSN data aggregation scenario results in a higher level of security than solutions based on hop-by-hop encryption. For an adversary aiming to obtain confidential information, it is only reasonable to break a mechanism if the cost of breaking is less than the value of the revealed information. An efficient public-key-based PH would be advantageous for the desired data aggregation in WSNs, so sensor nodes would need to store the nonsensitive public key, whereas the private key would solely be stored in the tamper-resistant sink node.

2.2 Concealed Data Aggregation on Cryptosystem

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[4[. 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. neither the encryption keys nor the sensed plaintext information need to be available at aggregating nodes. This differs from a hop-by-hop encryption approach, where captured aggregator node would reveal this information.

2.3 BGN Scheme

The cryptosystem devised by Boneh, Goh, and Nissim [1] was the to allow both additions and multiplications with a constant-size ciphertext. There is a catch, however: while the additive property is the same as for the ElGamal variant, only one multiplication is permitted.BGN system is to use elliptic curve groups whose order is a composite number n that is hard to factor. In all previous systems we required the group order to be prime. if factor the group order n in the BGN cryptosystem, then the secret key q and the system is broken. Also, if we can compute discrete logarithms in the group G, then we can compute r = logP (Q) and q = n=r. So necessary conditions for security are that factoring n is hard and computing discrete logarithms in G is hard.

2.3 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]So performing securely decryption, the BS extracts individual aggregated results of different groups from an aggregated ciphertext how to deliver the group public keys to SNs securely. 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.

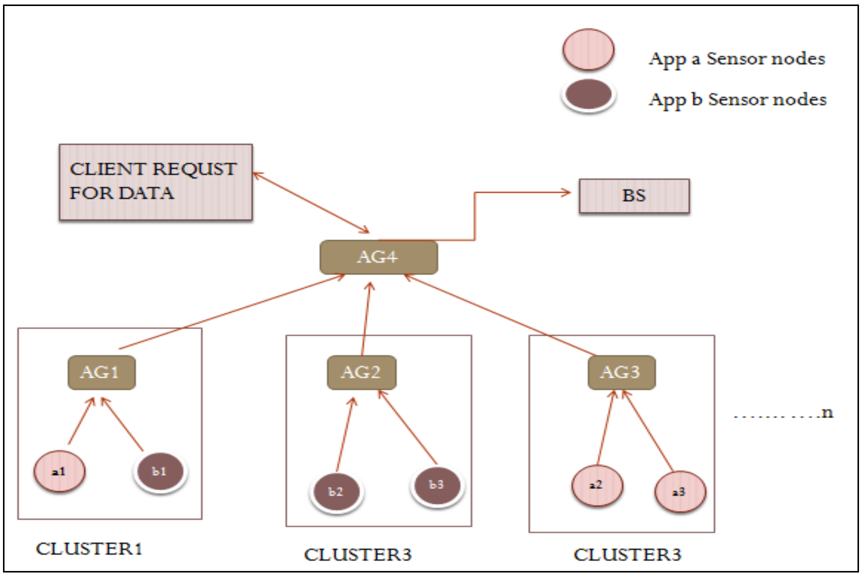


Fig.1. Proposed System

3. Database-As-a-Service (DAS) model

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[14]. 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
3.1.3Mapping 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.

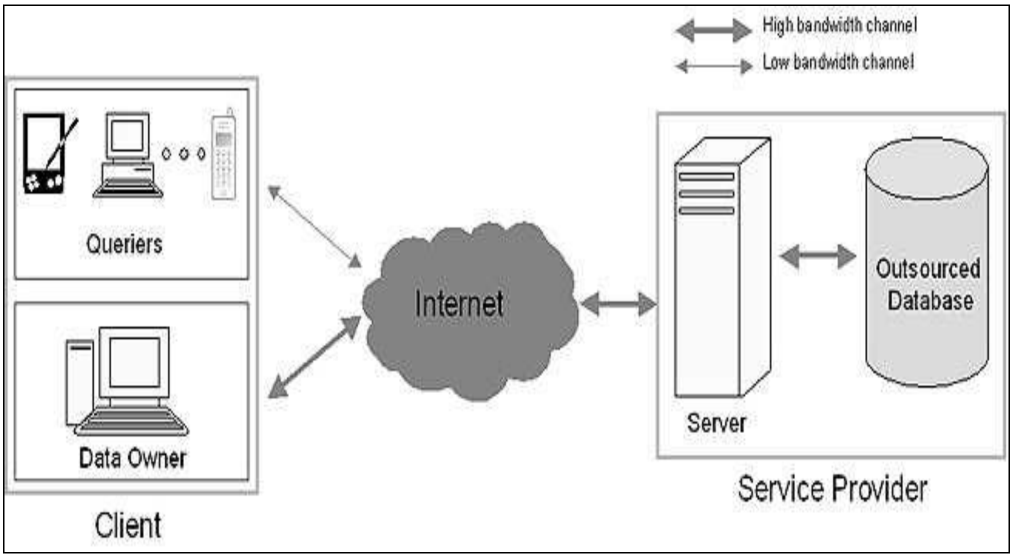


Fig.2.DAS Model

4. 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).

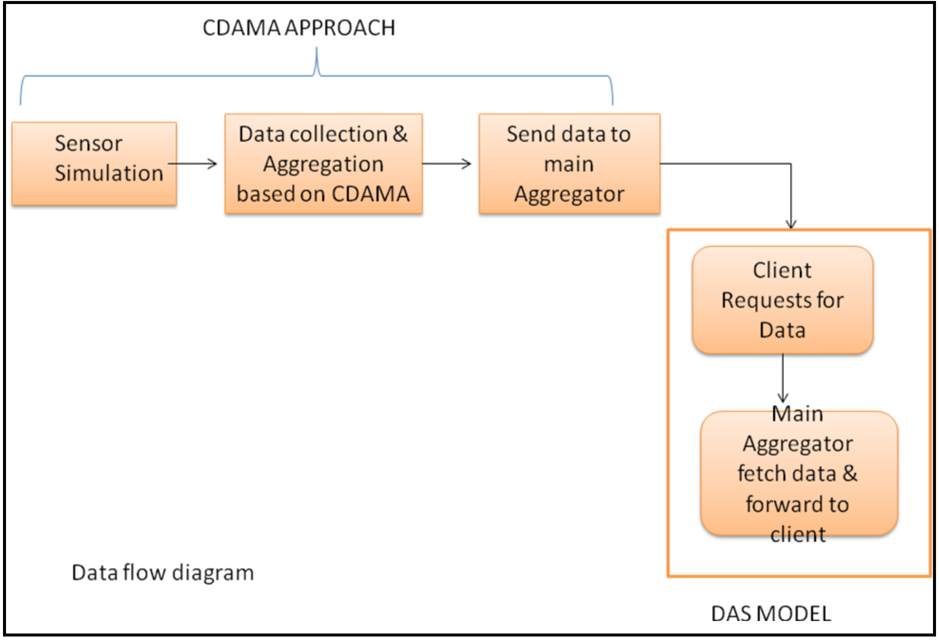
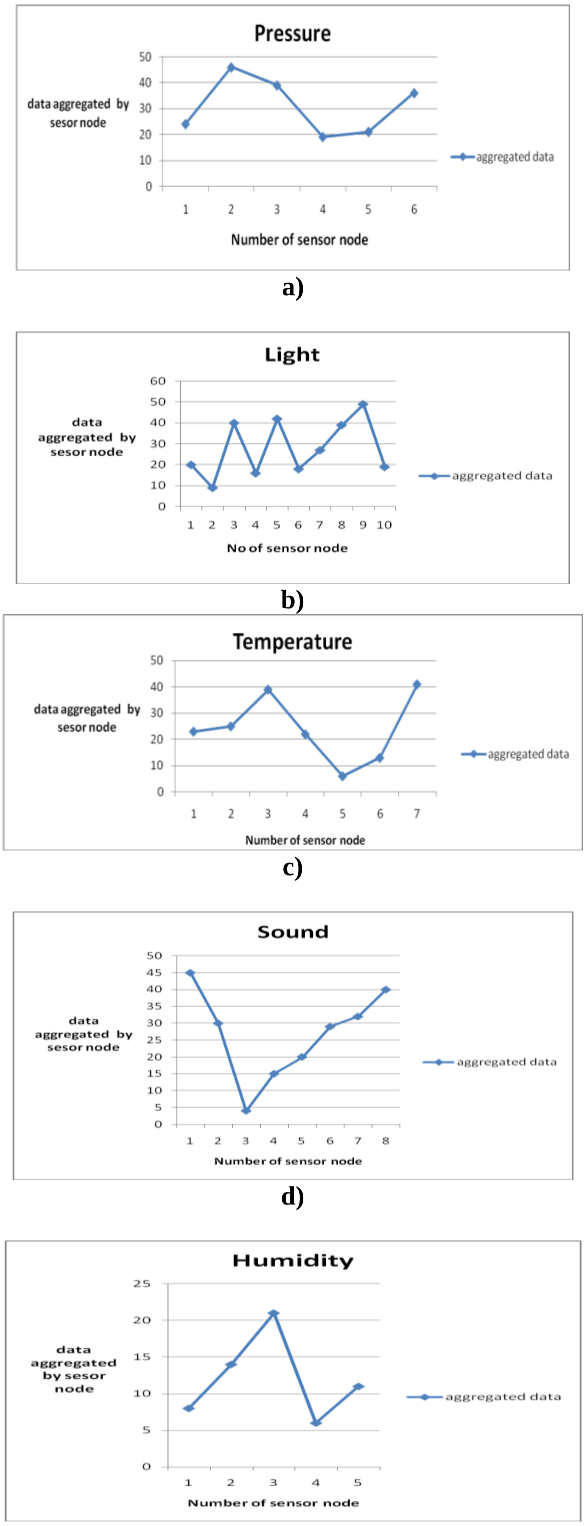

CDAMA APPROACH
Sensor Simulation
Data collection & Aggregation based on CDAMA
Send data to main Aggregator
Client Requests for Data
Main Aggregator fetch data & forward to client
Data flow diagram
DAS MODEL

Fig.3.block diagram of CDAMA approach with DAS model

5. Evalution Results

In this section for simulation used VB.net The simulation results validate the following aspects sensor nodes aggregated data through concealed data aggregation for multiple nodes which are considered as aggregation . Here, we consider parameter like temperature ,pressure, humidity , Light, sound for measuring following parameter in" Celcius", "Candella", "%", "Pascals", "dB" here Concealed Data Aggregation performed by using parameters. The graphical representation shows how much data can be aggregated.



a)

b)

c)

d)

e)

Fig.3 Shows aggregated data by sensor node for five parameter like pressure, humidity, temperature, light, sound

After collection of database this aggregated data stored by server. Database service model scenario happens client request for database through PH schemes. Next server fetches data to client in encrypted way so that maintain Data Privacy.

6. Conclusion

In this paper various aspect of data gatherings schemes and Aggregation Scheme like, Privacy Homomorphic, CDA, CDAMA has been discussed. After that overview of DAS model has been discussed. Security Analysis gives detail information about all scheme and there are Comparison distinct type of attacks with CDAMA and other conventional schemes.. 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 and network performance and Maintain Data Privacy.

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] A. 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 “Incorprating 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

[15] S. Zhu, S. Setia, and S. Jajodia, “LEAP+: Efficient Security Mechanisms Distributed Sensor Networks,”ACM Trans. Sensor Networks, vol. 2, no. 4 pp. 500-528, 2006.

[16] I. Akyildiz, W. Su, Y. Sankarasu bramaniam, and E. Cayirci, “ASurvey on Sensor Networks,” IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002.