Improved Data Client Security of DAS Model Using CDAMA in Wireless Sensor Network

[1] Satyaprakash Mishra, [2] Sheela Verma

[1]Department of Computer Science &Engineering
Shri Shankaracharaya College of Engineering and Technology Bhilai, India

[2]*Assistant Professor,*
Department of Computer Science &Engineering
Shri Shankaracharaya College of Engineering and Technology Bhilai, India

Abstract - Wireless sensor networks is different from that in commonsense mobile ad-hoc networks.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 homomorphism 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 homomorphism public encryption system. CDAMA is designed by using multiple points, each of which has different order. DAS model are the bandwidth overhead between the server and client The security of CDAMA are based on the hardness assumption of subgroup decision problem. 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.

Keywords - *Homomorphism encryption, Concealed data aggregation, wireless sensor networks.*

1. 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, accident reporting, and military investigation Like living organisms, a variety of modern devices and equipments relies on the sensory data from the real world around it. These sensory data comes is provided by Wireless Sensor Networks, which consists of several tiny sensor nodes to monitor physical or environmental conditions, such as temperature, vibration, pressure, sound or motion, and then collectively send these information to a central computing system, called the base station or sink. Different routing protocols govern the movement of this information. Depending on the purpose of each application, SN is customized to read different kinds of data (e.g., temperature, light, or smoke). Typically, SN are restricted by the resources due to limited computational power and low battery supply; thus, energy saving technologies must be considered when design the protocols. For better energy utilization, cluster-based WSNs [2] have been proposed. In cluster-based WSNs, 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 .In cluster-based WSNs, 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 set**.**

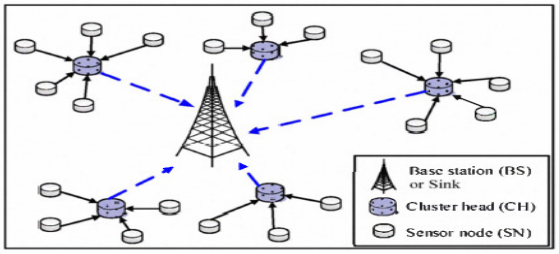

Figure 1: Cluster-based WSN

In particular, we cannot assume a sensor node to comprise a tamper-resistant unit. Such sensor nodes are envisioned to be spread out over a geographical area to form in an indeed self-organizing manner a multihop network. Most frequently, such WSNs are stationary, although mobile WSNs are also conceivable. Potential applications for WSNs—besides military ones—can be found in monitoring environmental data with the objective to understand complex and geographical widespread interdependencies of nature. Examples are the detection of fire in huge forest areas, the monitoring of wildlife animals' movement patterns, or the incremental shift of snow and rocks in the alpine mountains further applications for WSNs are envisioned to be on the biomedical sector, public safety, and safety support for vehicles. One major application scenario for a WSN is to monitor environmental data and to transmit it to a central point .Here; the data are analyzed and eventually serve to initiate some action. 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. 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].

2. Basic Principles

2.1 Homomorphism Encryption Techniques

In WSNs, Privacy homomorphism 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]

2.2 Privacy homomorphism Cryptosystem

PH is contain an encryption scheme with homomorphism 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].

2.3. 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 homomorphism PHs support additive operations on encrypted data, where multiplicatively homomorphism PHs allows for multiplicative operations on the cipher text. 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 cipher text attacks. 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].

2.4. 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.

2.5 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 cipher text 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 know 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 cipher text how to deliver the group public keys to SNs securely. There are two main approaches.

1] Key pre distribution.- If we know the locations of deployed SNs then 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 post distribution- 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. 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.

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.

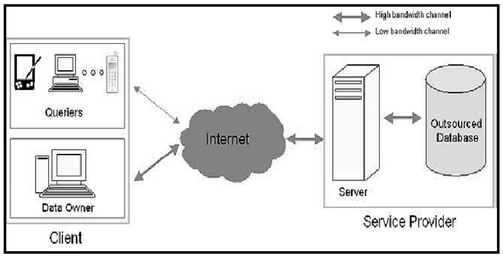

Figure2 DAS .Model

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).

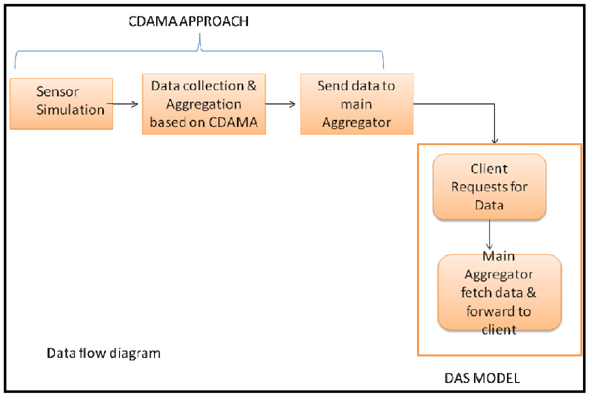
CDAMA APPROACH
Sensor Simulation
Data collection & Aggregation based on CDAMA
Send data to main Aggregator
Client Requests for Data
Main Aggregator fetch data & forward to client
Data flow diagram
DAS MODEL

Figure.3. Block diagram of CDAMA approach with DAS model

5. Conclusion

In this paper various aspects of data gatherings schemes and Aggregation Scheme like, Privacy Homomorphism, CDA, and 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. 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 Converge cast 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 “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