ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Improved Client Data Security with Aggregated Query Using CDAMA

Ms.S.Kanimozhi[1], Mrs.K.Makanyadevi[2]

PG Scholar[1], Department of CSE, M.Kumarasamy College of Engineering, Karur, Tamilnadu, India[1]

Assistant Professor, Department of CSE, M.Kumarasamy College of Engineering, Karur, Tamilnadu, India [2]

ABSTRACT - One of the major problems in data mining is security. In the existing framework implementation was done in wireless sensor network. Existing system provides three contributions: 1. it is designed for multi-application environment, 2. it mitigates the impact of compromising attacks in single application environments and 3. it degrades the damage from the unauthorized aggregations. The two drawbacks in this scheme are, this CDAMA technique cannot be used for Database as a Service model and compromising the secret keys in sensor are very easy. In the proposed framework, Database as a Service model can be implemented through the bucketization algorithm and in the existing framework as sensors are easily compromised the secret keys are not secured whereas in the proposed framework trusted service providers are used to secure the secret keys. So the security level is increased in the proposed system when compared with the existing system.

KEYWORDS: Concealed data aggregation for multiple application, bucketization algorithm, wireless sensor networks, Database as a Service model, trusted service provider.

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, accident reporting, and military investigation. Depending on the purpose of each application, SN is customized to read different kinds of data. SN is restricted by the resources due to limited computational power and low battery supply; thus, energy saving technologies must be considered when I 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. 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. To solve this problem, several studies, such as the delay aggregation, SIA, ESPDA, and SRDA have been proposed.

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. Based on this concept, Wu et al. gave the proposal to allow CHs to classify encrypted data

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

without decrypting them. The proposed scheme, called CDAMA, provides CDA for multiple groups. Basically, CDAMA is a modification from Boneh et al.'s PH scheme. Here, It also suppose three practical application scenarios for CDAMA, all of which can be realized by only CDAMA.

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. RELATED WORKS

A novel framework was designed by Bartosz przydatek et al (2003) for secure information aggregation in large sensor networks. In our framework 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, enable the user to verify that the astir 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, it 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.

Wireless Sensor Network (WSN) is an emerging technology is designed by A. Perrig et al (2004) that show great promise for various futuristic applications both for mass public and military. The sensing technology combined with processing poitr and wireless communication makes it lucrative for being exploited in abundance in future. The inclusion of wireless communication technology also incurs various types of security threats. The intent of this paper is to investigate the security related issues and challenges in wireless sensor networks.

A protocol was designed by Lingxuan Hu et al (2003) that provide 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, memory and poitr consumption limits of inexpensive sensor devices, but takes advantage of the properties of wireless networking, as it will act as the pointer asymmetry to the devices and the base station.

Data aggregation in wireless sensor networks was designed by H.O. Sanli et al (2006) in eliminates redundancy to improve bandwidth utilization and energy-efficiency of sensor nodes. This paper presents a secure energy-efficient data aggregation protocol called ESPDA (Energy-Efficient Secure Pattern based Data Aggregation). Unlike conventional data aggregation techniques, ESPDA prevents the redundant data transmission from sensor nodes to cluster-heads. If sensor nodes sense the same data, ESPDA first puts all but one of them into sleep mode and generate pattern codes to represent the characteristics of data sensed by sensor nodes.

SRDA is designed by Hasan Cam in 2004 establishes secure connectivity among sensor nodes by taking advantage of deployment estimation and not performing any online key distribution. The incremental security requirement due to the nature of the data aggregation process is met by an aggregation specific security technique. Simulation results show that SRDA yields significant savings in the energy consumption while preserving the data security. YongKong Du was designed by 2004 in a classifier, an intermediate sensor node in our setting, is embedded with a set of searching keywords in encrypted format. Upon receiving an encrypted message, it matches the message with the keywords and then processes

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

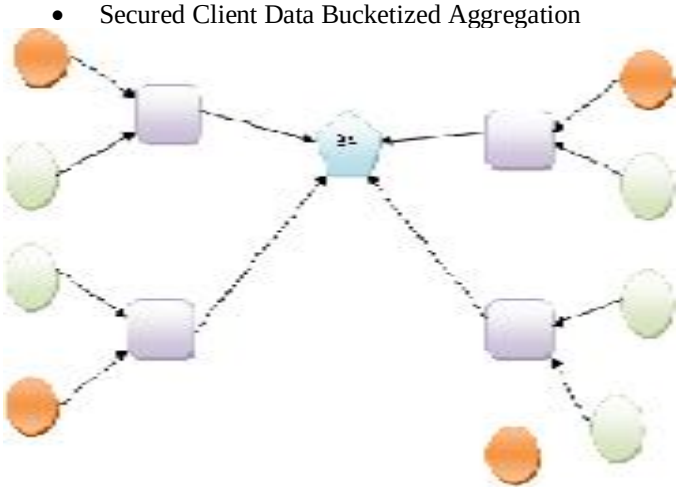
the message based on certain policies such as forwarding the original message to the next hop, updating it and forwarding or simply dropping it on detecting duplicates.

Routing in wireless sensor networks is designed by Mithun Acharya (2006) in commonsense mobile ad-hoc networks. It mainly needs to support reverse multicast traffic to one particular destination in a multihop manner. For such a communication pattern, end-to-end encryption is a challenging problem. To save the overall energy resources of the network, sensed data needs to be consolidated and aggregated on its way to the final destination. It present an approach that 1) conceals sensed data end-to-end by 2) still providing efficient and flexible in-network data aggregation. The aggregating intermediate nodes are not required to operate on the sensed plaintext data. It apply a particular class of encryption transformations and discuss techniques for computing the aggregation functions "average" and "movement detection."

III. OVERVIEW

In the proposed system a new concealed data aggregation scheme extended from Boneh et al.'s homomorphism public encryption system. The proposed scheme has three contributions. First, it is designed for a multi-application environment. The base station extracts application-specific data from aggregated cipher texts. Next, it mitigates the impact of compromising attacks in single application environments. Finally, it degrades the damage from unauthorized aggregations.

- These three applications that are realized by only CDAMA multi group construction.
- WSN Aggregation Model
- Concealed Data Aggregation
- Aggregation with Secure Counting
- Database as a Service Model for CDAMA
- Trusted Service Provider
- Secured Client Data Bucketized Aggregation



Group A Sensor nodes

Group B Sensor nodes

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

- Aggregator

WSN AGGREGATION MODEL

In WSNs, SN collect information from deployed environments and forward the information back to base station (BS) via multihop transmission based on a tree or a cluster topology. The accumulated transmission carries large energy cost for intermediate nodes. To increase the lifetime, tree-based or cluster networks force the intermediate nodes.

The multi-application WSNs, the scenario of a single application is more commonly discussed in WSNs. However, the scenario of multiple applications working concurrently is more realistic in most cases. Study indicates that deploying multiple applications in a shared WSN can reduce the system cost and improve system flexibility. The reason is because an SN supports multiple applications and can be assigned to different applications dynamically.

To maintain data privacy and reduce the communication overhead, sensed reading should be encrypted by SNs and the corresponding cipher texts must be aggregated. The solution satisfying this requirement has already been proposed, called CDA. Even if aggregation on cipher texts is possible, aggregation of multi-application is still hard because the decryption cannot extract application-specific aggregated result from a mixed cipher text.

CONCEALED DATA AGGREGATION

Interestingly, applying CDAMA to the conventional aggregation model can mitigate the impact from compromising attacks. Each group could be assigned a distinct group public key. Once an adversary compromised a SN in group A; it only reveals PKA, not PKB. Since the adversary can only forge messages in group A, not group B, the SNs in group B can still communicate safely.

CDAMA assigns every node for its own group, resulting in the strongest security CDAMA ever offered. However, this is impractical because the size of cipher text becomes extremely large when it construct groups with a huge group number. Thus, assigning a reasonable number of groups for a single application not only keeps the overhead acceptable but also mitigates the impact of compromising attacks.

AGGREGATION WITH SECURE COUNTING

An 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 ciphertexts aggregated, repeated or selective aggregation may happen. To avoid this problem, it adopt CDAMA (k ¼ 2) scheme to provide secure counting for single application case, i.e., the BS exactly knows how many sensed readings are aggregated while it receives the final result. The BS obtains the aggregated result M and its count.

If a malicious AG launches unauthorized aggregations, such as repeated or selective aggregation, s value would be changed to a bigger or smaller value than the reference. Since the AG does not know the base points P and Q, unauthorized aggregations have to alter the values M simultaneously; it is impossible to alter M without changing. Meanwhile, the BS knows the number of deployed sensors through gathering topology information; the BS can detect unauthorized aggregation.

DATABASE AS A SERVICE MODEL FOR CDAMA

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

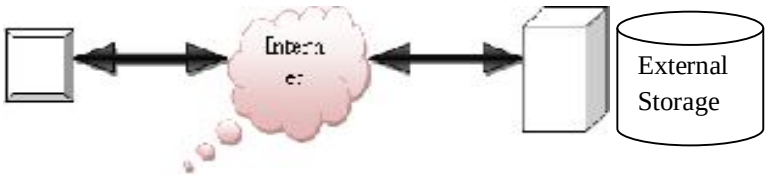
Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

DAS involves clients outsourcing their private databases to database service providers (servers) who offer storage facilities and necessary expertise. Clients, in general, do not trust service providers with the contents of their databases and, therefore, store the databases in encrypted format. The central challenge is how to enable a UN trusted service provider to run SQL-style queries over encrypted data.

It proposes a very simple alternative for handling aggregation queries at the server, which does not involve homomorphic encryption functions. It further describes the protocols for formulating and executing queries as itll as updating encrypted tuples.



TRUSTED SERVICE PROVIDER

DAS model involves bucketizing (partitioning) attributes upon which range queries will be based. This involves dividing the range of values in the specific domains of the attribute into buckets and providing explicit labels for each partition. These bucket labels are then stored along with the encrypted tuples at the server. Based on the same bucketization strategy, the follow-on work in addresses aggregation queries in DAS by proposing the use of a particular homomorphic encryption function. In general, homomorphic encryption is a technique that allows entities who only possess encrypted values (but no decryption keys) to perform certain arithmetic operations directly over these values.

SECURED CLIENT DATA BUCKETIZED AGGREGATION

In contrast, equi-depth bucketization attempts to avoid this problem by having each bucket contain the same number of items, thereby hiding the actual distribution of values. The downside of this approach is that, in the presence of frequent database updates, the equi-depth partition needs to be adjusted periodically. This requires additional (and non-trivial) interaction between the server and the client (database owner).

Bucketization has an unavoidable side-effect of privacy loss since labels (bucket id-s) disclose some information about the clear text. Unless there are as many buckets as there are distinct values in the domain of an attribute, some statistical information about the underlying data is disclosed through bucket id-s.

IV. PERFORMANCE ANALYSIS

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 CDAMA.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

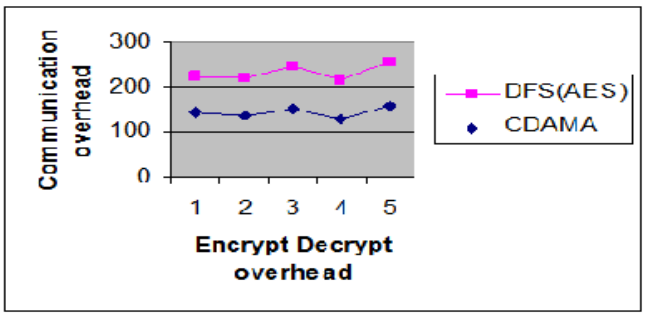


Fig 4.1 CDAMA of Encrypt Decrypt Overhead and Communication Overhead

Fig 4.1 CDAMA is several thousand times greater than that in DFS because the encryption cost of CDAMA is significantly greater than the cost of AES. For an AG, the communication overhead in DFS is increased tenfold whenever the AG reaches to the next layer, whereas the communication overhead in CDAMA are all kept the same. The reason for this is because the i th layer AG must forward 10i messages in DFS but only 10 messages in CDAMA. For a forwarder, the main energy consumption depends on transmission; therefore, CDAMA allows the forwarder to spend only 1 percent of transmission cost in DFS.

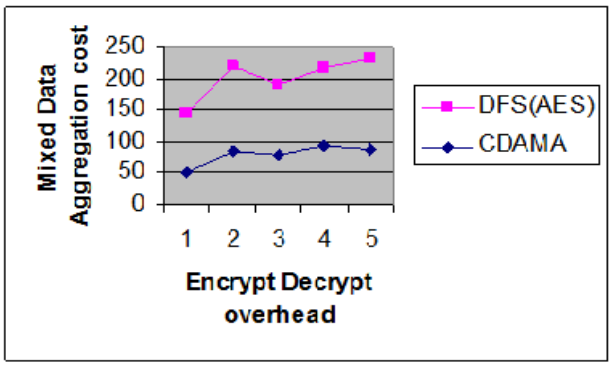


Fig 4.2 CDAMA of Encrypt Decrypt Overhead and Mixed Data Aggregation Cost

The CDAMA is Comparison between Encrypt Decrypt Overhead and Mixed Data Aggregation Cost is DFS is high level and CDAMA is low level position. In DFS, a leaf node encrypts its sensed reading by symmetric encryption schemes and forwards the cipher text to its parent AG. AGs and forwarders just transmit the received data without any in-network processing. Both schemes (rather than hop-by-hop aggregation) provide end-to-end security, thereby avoiding the forgery of aggregated result.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

V. CONCLUSION

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, Finally, the performance evaluation shows that CDAMA is applicable on WSNs while the number of groups or applications is not large.

CDAMA to realize aggregation query in Database-As-a-Service (DAS) model. In DAS model, a client stores her database on a 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 it do not have to consider the computation cost and the impact of compromising secret keys.

REFERENCES

[1] 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.
[2] A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks," Comm. ACM, vol. 47, no. 6, pp. 53-57, June 2004.
[3] L.Hu and D. Evans, "Secure Aggregation for Wireless Networks," Proc. Symp. Applications and the Internet Workshops, pp. 384-391, 2003.
[4] 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.
[5] 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.
[6] 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.
[7] D. Itsthoff, 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.
[8] J. Girao, D. Itsthoff, M. Schneider, N. Ltd, and G. Heidelberg, "CDA: Concealed Data Aggregation for Reverse Multicast Traffic in Wireless Sensor Networks," Proc. IEEE Int'l Conf. Comm. (ICC '05), vol. 5, 2005.
[9] Yue-Hsun Lin, Shih-Ying Chang, and Hung-Min Sun, "CDAMA: Concealed Data Aggregation Scheme for Multiple Applications in Wireless Sensor Networks", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 25, NO. 7, JULY 2013.
[10] I.Akyildiz and E.Cayirci, "A Survey on Sensor Networks", IEEE comm., Magazine, vol.40, no.8, pp.102-114, Aug. 2002.