

## Authentication Using RDOPE In Tiered Sensor Network

C.Nandini<sup>#1</sup>, A. Agalya<sup>#2</sup>, S.Sri Devi<sup>#3</sup>  
PG Scholar<sup>#1#2</sup>, Assistant Professor<sup>#3</sup>

*Department of CSE, Vels University, Pallavaram, Chennai*

### Abstract

In three tier wireless sensor network, the storage node are suppose to be placed as an middle tier for collecting and caching the sensor reading and responding to the queries with benefits of storage and power saving for sensors. The problem is if the storage node is compromised will cause not only the privacy issue and also return incomplete or fake result. In existing it has higher communication complexity and does not have a design principle. The effective dummy reading based anonymization framework is proposed, under this the query integrity can be guaranteed and the scheme used have a fundamentally design principle and achieve the lower communication complexity at the cost of slight detection capability degradation. Numerical simulation is conducted to demonstrate practically.

**Index term:** query result completeness, sensor networks, and authentication.

### Introduction

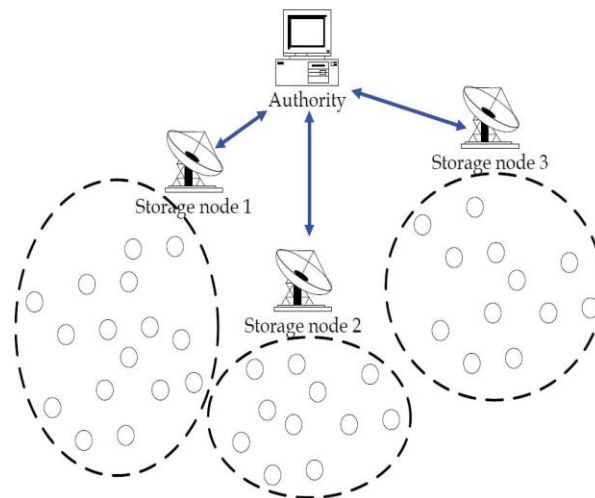
#### Three Tiered Sensor Networks:

The network which is placed in some harsh (cruel) or hostile region (military enemy) for data collection or environment monitoring is called sensor network. Hence there is the possibility of unstable connection in sensor network.

In three tier architecture, first one is the authority or the network owner who is responsible for maintenance, intermediatetier is for query response and catching the sensed data. The network model is illustrated in fig.1; the authority will issue the query for retrieve the sensor reading form the middle tier [1]. The middle tier is filled with few storage abundant nodes called storage nodes. The last segment is called bottom tier which consists of a large number of sensor that sense the reading of environment [1].

In the fig.1, sensor nodes are divided into disjoint groups. The group of sensor nodes is a cell [1]. The cell which contains sensor nodes forms a multi hop network. The middle tier which contains the storage node holds the copy of received sensor

readings, it forwards to the authority and answering the query to the network owner [1].



**Figure 1:** A Concept of The Tiered Sensor Network

### **Empirical Work In Tiered Sensor Network:**

- In April 2013 [3] a paper was published where two tier sensor networks is used, this method uses safeQ protocol, Merkle hash tree, neighborhood chain and bloom filters [3]. SafeQ is used for detecting attackers and improper sensor networks, while Merkle hash tree is employed for integration purpose. Finally bloom filters technique is used for minimizing communication cost [3].
- In June 2011 [4] a paper regarding multidimensional query in tiered sensor network was published. The two-tier architecture holds large number of storage nodes and sensor nodes [4]. Here, the entire sensor have several sensing abilities, it regularly sends multidimensional sensed data to the storage node. [4] If the storage node is compromised by adversary the sensed data will gets leaked, to overcome this effective hash tree-based framework is suggested, by this data confidentiality, genuine query result and completeness of query result can be assured.
- In 2012 [5] top k query in entrusted LBSP is stated. The system contains the information collector, knowledge contributors, location based service provider and system user. The information collector collects the review concerning POI (points-of-interest) from knowledge contributors and permit user to do the location based top-k queries which invite the POI in actually existing region with the best k rating of POI quality [5]. The paper gives two systems to find pretend top-k query results an attempt to foster the sensible preparation and use of the proposed system [5].
- In 2004 [2] OPE for numerical data is explained. Normally encryption is very good method for safeguarding sensitive data. If the data is encrypted,

information will not be simply queried rather than actual matches [2]. A tendency to gift associate degree order-preserving encryption theme for numeric information that permits any comparison operation to be directly applied on encrypted information [2]. The query outcomes produced are sound and complete. The proposed theme has been designed to be deployed in application environments within which the unwelcome person will get access to the encrypted database, however doesn't have previous domain data like the distribution of values and can't encipher or rewrite arbitrary values of his alternative [2]. The cryptography is powerful against estimation of the true worth in such environments [2].

- In September 2011[6] privacy in sensor storage for range query is established. A hybrid two-tiered sensor architecture consisting of normal sensors and special sensors with massive storage capacity, known as storage nodes. The regular sensors “push” their information to near storage nodes and therefore the sink diffuses queries alone to storage nodes and “pulls” the reply [6]. To examine security and privacy threats once the detector network should be deployed in an untrusted or unfriendly surrounding. The most important concern is that storage nodes may simply become the target for the unauthorized to surrender due to their vital role [6]. A compromised storage node will leak the information hold and breach the information privacy. The answered framework includes a privacy-preserving storage theme which utilizes a bucketing technique and a verifiable question protocol that hires encryption numbers to modify the sink to verify the response [6].

## System Model

There are following models in the three tired architecture:

### A. Architecture Model:

The large number of resource-constrained sensors and very less number of storage abundant nodes are used [1]. A cell which holds the large number of sensors is connected to form the multi hop network. The authority is nothing but network owner will issue the query to the storage node which has the sensor reading will reply to the authority [1]. The time on the nodes has been divided into epochs. The time synchronization is achieved by the algorithm”global clock synchronization in sensor network” [7] and” secure and resilient time synchronization in wireless sensor network” [8].

By various types of data flow, two aspects are considered; first one is information submission, in this the sensor will submit the sensed information to the nearest storage node [1]. The second one is query response to authority, here the storage node will respond according to the query given by authority [1].

### B. Security Model:

In this phase the security is given to the data which is saved in the storage node. Each sensor in this architecture shares the key with authority at each time slot. If the node is

compromised, then all the data stored in the middle tier is completely breached [1]. The unauthorized person will take the full in charge of storage node and be able to control, manipulate the computation reports and communication result [1].

The keyed-hash function used here are keyed-hash message authentication code. The data authenticity and integrity is guaranteed by HMAC.

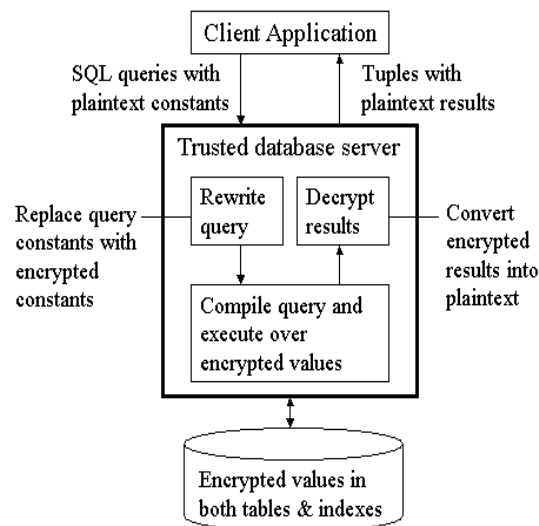
### C. Query Model:

This is the last model in the three tiered architecture, to make top-k query rank function want to consider [29]. Authority asks the storage node to response the query. The storage node will answer to the query which is given by the authority or by the network owner [1].

## Comparison Between OPE and RDOPE

### A. OPE scheme:

The OPE (Order Preserving Encryption Scheme) encryption technique that allows to evaluate operations to be straightly applied on encrypted data, without decrypting the operands [2]. Therefore, equality and range queries in addition MAX, MIN, and COUNT queries can be directly applied over encrypted data. The data encrypted using OPES are promise [2]. OPES make updates balanced. OPES can easily be composed with existing database systems as it has been created to employee with the existing sequence structures.



When processing with responsive numeric data, an unauthorized person does not have to figure the exact data value of plain text equivalent to an encrypted value of cipher text [2]. A leak might occur if the adversary achieves an exact estimate of plaintext.

The OPE algorithm is used to encrypt database; regrettably all the data's are figured by a single network owner is not used in our consideration [1]. The sensor readings which are used here is limited and known from hardware product, the connection between the cipher texts and plain texts is shown [1]. For example the sensor will generate only 30 types of certain outputs, sure the unauthorized person will get OPE key by inquiring the numerical order of listening the cipher texts insults the empirical security guarantee [1].

### B. RDOPE Algorithm Description:

RDOPE is the technique gives randomness in encryption outputs and is good for using in distributed information generation with less input value. The important strategy of rdOPE is to develop the numerical orders of encryption from various sensors that access various OPE. The cipher text is decided before by the sensor deployment. So, the cipher texts in various sensors are preserved.

The RDOPE contains  $n$  types of sensors and  $r$  certain sensor reading is define as

$$\sum k(i)(x1) < \sum k(j)(x2) \text{ if } x1 < x2, 1 \leq i, j \leq n,$$

The  $k(i)$  and  $k(j)$  refers the rdOPE keys maintained by  $s_i$  and  $s_j$ , value ranges of hash output  $hrdOPE(\cdot)$  and encryption function output[1].

### Notation Table

$k$	The top $k$ query
$n$	The number of sensor nodes
$S_i$	The $i$ -th sensor node
$S_m$	The storage node
$A$	The authority
$K(i)$	rdOPE key possessd by $i$ -th sensor

## Basic Idea of The System

### A. Description of RDOPE:

Using RDOPE (randomized and distributed order preserving encryption) algorithm is used for privacy guarantee in verifiable top-k Query schemes [1]. The rdOPE will produce the random encryption values for the sensor and maintain the numerical order of encryption. Here the authority  $A$  will fix the relationship between the plain text and cipher text [1]. So the privacy is guaranteed in this phase.

### B. Description GD-VQ:

GD-VQ is the algorithm which provides privacy guarantee, query completeness verification and authenticity by using rdOPE hashing mechanism and adding dummy reading [1]. The sensor data which is encrypted by  $S_i$  using  $K(i)$  rdOPE key and it generates the random dummy reading [1].The dummy data is mingled with cipher text

and it is encrypted. The problem is the adding dummy data endows A authority to check the result completeness. GD-VQ is communication incapable, because the authority needs to issue the unsteady number of top queries to get very good top k result. Next is dummy data wants to be returned in worst case, proceeding to the staggering communication load.

### C. AD-VQ algorithm:

The AD-VQ overcomes the problems in communication and the security completely depends on proposition of local adversary. In AD-VQ the data sensed by sensor is encrypted and advance dummy data is added with the cipher text.

The AD-VQ algorithm overcomes the attacks which want to corrupt sensor networks task. The following attacks are false data injection attack, wormhole attack, Sybil attack, and replication attack. In false data injection attack the fake data is injected to the original data it does battery power reducing and network life time [9], the wormhole attack drops the packet and sends to another wormhole node [10]. The Sybil attack is nothing but the nodes which have different legal IDs are displayed in the network [11], in the node replication attack, the legal sensors are compromised and replicated [12].

### Conclusion

Finally, the rdOPE establish the privacy guarantee for verifiable top-k query scheme, AD-VQ advanced dummy based anonymization is proposed for the reducing the communication overhead. The Sybil attack, wormhole attack, replication attack, and false data injection attack are defeated by proposed method.

### References

- [1] Chia-Mu Yu, Guo-Kai Ni, Ing-Yi Chen, Erol Gelenbe, Life Fellow, and Sy-Yen Kuo, Fellow, IEEE “Top-k Query Result Completeness Verification in Tiered Sensor Networks,” in *Proc. IEEE Info. Forensics and Security. Trans.*, pp. 109–124.
- [2] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, “Order preserving encryption for numeric data,” in *Proc. ACM SIGMOD*, 2004, pp. 63–574.
- [3] Y.-T. Tsou, C.-S. Lu, and S.-Y. Kuo, “Privacy- and integrity-preserving range query in wireless sensor networks,” in *Proc. IEEE Global Commun. Conf.*, Dec. 2012, pp. 328–334.
- [4] Y.-T. Tsou, C.-S. Lu, and S.-Y. Kuo, “Privacy- and integrity-preserving range query in wireless sensor networks,” in *Proc. IEEE Global Commun. Conf.*, Dec. 2012, pp. 328–334.
- [5] R. Zhang, Y. Zhang, and C. Zhang, “Secure top-k query processing via untrusted location-based service providers,” in *Proc. 24th IEEE Conf. Comput. Commun.*, Mar. 2012, pp. 1170–1178.

- [6] Bo Sheng, Member, IEEE, and Qun Li, Member, IEEE “Verifiable Privacy-Preserving Sensor Network Storage for Range Query” in *Proc IEEE Mobile Commun.*, Sep. 2011, pp. 1312–1326.
- [7] Q. Li and D. Rus, “Global clock synchronization in sensor networks,” in *Proc. IEEE Conf. Comput. Commun. INFOCOM*, Jan. 2004, pp. 1–11.
- [8] K. Sun, P. Ning, C. Wang, A. Liu, and Y. Zhou, “TinySeRSync: Secure and resilient time synchronization in wireless sensor networks,” in *Proc. 13th ACM Conf. CCS*, Feb. 2006, pp. 264–277.
- [9] F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical en-route filtering of injected false data in sensor networks,” in *Proc. IEEE 23rd Annu. Joint Conf. Comput. Commun. INFOCOM*, Mar. 2004, pp. 2446–2457.
- [10] Y.-C. Hu, A. Perrig, and D. Johnson, “Packet leashes: A defense against wormhole attacks in wireless networks,” in *Proc. 22nd Annu. Joint Conf. IEEE Comput. Commun. INFOCOM*, Apr. 2003, pp. 1976–1986.
- [11] B. Parno, A. Perrig, and D. Johnson, “Distributed detection of node replication attacks in sensor networks,” in *Proc. IEEE Symp. Security Privacy*, May 2005, pp. 49–63.
- [12] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar, “SPINS: Security protocols for sensor networks,” in *Proc. ACM Conf. Mobile Comput. Netw.*, 2001, pp. 521–534.

