International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-2, May 2015
ISSN: 2395-3470
www.ijseas.com

Top-k Query Result Completeness Verification in Tiered Sensor Networks

ABSTRACT

Storage nodes are expected to be placed as an intermediate tier of large scale sensor networks for caching the collected sensor readings and responding to queries with benefits of power and storage saving for ordinary sensors. Nevertheless, an important issue is that the compromised storage node may not only cause the privacy problem, but also return fake/incomplete query results. We propose a simple yet effective dummy reading based anonymization framework, under which the query result integrity can be guaranteed by our proposed verifiable top-k query (VQ) schemes. Compared with existing works, the VQ schemes have a fundamentally different design philosophy and achieve the lower communication complexity at the cost of slight detection capability degradation. Analytical studies, numerical simulations, and prototype implementations are conducted to demonstrate the practicality of our proposed methods

\

INTRODUCTION

In sensor networks for data collection, since there could be unstable connection between the authority (or network owner) and network, a middle tier with the purpose of caching the sensed data for data archival and query response becomes necessary. The network model of this paper is illustrated in Fig. 1, where the authority can issue queries to retrieve the sensor readings. The middle tier is composed of a small number of storage-abundant nodes [24], called *storage nodes*. The bottom tier consists of a large number of resource-constrained ordinary sensors that sense the environment.

In tiered sensor networks, the authority issues proper queries to retrieve the desired portion of sensed data. We restrict ourselves in this paper to discussing top-*k* query, which is one of the most intuitive and commonly used queries.

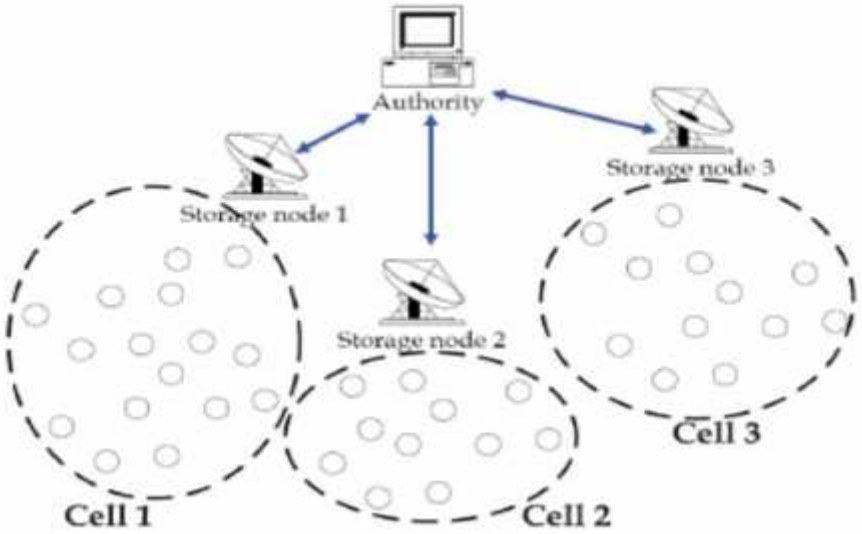
Two schemes, *additional evidence* and *crosscheck*, were tiered sensor networks. While the former generates hashes for each consecutive pair of sensed data for verification purpose, the latter performs network-wide broadcast such that the information about the readings is distributed over the entire network and therefore the query result cannot be manipulated. Despite the prior works on verifiable queries, we still have the following concerns: In a network of *n* sensors, Hybrid method [35] incurs tremendous $O(n2)$ communications.Although SMQ [34] can be adapted to verify the top-*k* query result, an aggregation tree not only needs to be constructed but also needs to remain intact and unchanged.

The exact information about the tree topology is also required by the authority. In real world deployment, these requirements are difficult to meet. Although the method in [35] can be extended in some straightforward way to the method with data confidentiality guarantee, such extension actually implies some of the other severe weaknesses, which are unacceptable in the design of a verifiable query scheme

In the above tiered architecture, sensor nodes are usually partitioned into disjoint groups, each of which is associated with a storage node. Each group of sensor nodes is called a *cell*. The

sensor nodes in a cell form a multi-hop network and always forward the sensor readings to the associated storage node. The storage node keeps a copy of received sensor readings and is responsible for answering the queries from the authority. An example of the tiered architecture can be found in Fig. 1

SYSTEM ARCHITECTURE:



EXISTING SYSTEM

Two schemes, additional evidence and crosscheck, were proposed in as solutions for securing top-k query in tiered sensor networks. While the former generates hashes for each consecutive pair of sensed data for verification purpose, the latter performs network-wide broadcast such that the information about the readings is distributed over the entire network and therefore the query result cannot be manipulated. In particular, the idea behind additional evidence is that if each consecutive pair of sensed data is associated with a hash, once an unqualified sensor reading is used to replace the genuine query result, the authority may know because it can find that there are some missing sensor readings for hash verification. On the other hand, the idea behind crosscheck is that the genuine top-k results are distributed to several sensor nodes. With certain probability, the authority will find query result incompleteness by checking the other sensor nodes' sensor readings. Hybrid method is a combined use of additional evidence and crosscheck, attempting to balance the communication cost and the query result incompleteness detection capability.

PROPOSED SYSTEM:

The Verifiable top-k Query (VQ) schemes based on the novel dummy reading-based anonymization framework are proposed for privacy preserving top-k query result integrity verification in tiered sensor networks. A randomized and distributed version of Order Preserving Encryption, rdOPE, is proposed to be the privacy foundation of our methods.AD-VQ-static achieves the lower communication complexity at the cost of slight detection capability degradation, which could be of both theoretical and practical interests. Analytical studies, numerical simulations, and prototype implementation are conducted to demonstrate the practicality of our proposed methods. A cell is a connected multi hop network composed of a storage node and a number of ordinary sensors. Storage nodes are storage-abundant, can communicate with the authority via direct or multi-hop communications, and are assumed to know their affiliated cells. Time on the nodes has been synchronized and is divided into epochs. Note that time synchronization among nodes can be achieved by using algorithms.

ADVANTAGES OF PROPOSED SYSTEM:

1. The message m to be communicated is associated with H M ACK , the use of HMAC naturally guarantees the data authenticity and integrity.

2. Hybrid Crosscheck incurs tremendous communication cost because it involves the data broadcast over the cell.

3. SMQ achieves the data confidentiality through the use of bucket index

DISADVANTAGES OF EXISTING SYSTEM:

1. There is no trusted central authority like proxy node in for such responsibility.

2. In real world deployment, these requirements are difficult to meet.

3. The methods do not handle the data privacy issue.

CONCLUSION AND FUTURE ENHANCEMENT

A novel dummy reading-based anonymization frame workis proposed to design Verifiable top-*k* Query (VQ) schemes. In particular, AD-VQ-static achieves the lower communication complexity with only minor detection capability penalty, which could be of both theoretical and practical interests. With only symmetric cryptography involved and their low implementation difficulty, the VQ schemes are suitable and practical for current sensor networks.