ISSN NO: 9726-001X
Volume 03 Issue 01 January 2015

JOURNAL OF CURRENT SCIENCE

Verifying the Integrity of the Top k Search Results in a Hierarchical Sensor Network

Mahesh Wagh
Energy Technology, Shivaji University, Maharashtra, India

ABSTRACT

With the potential to save both power and space, storage nodes are increasingly being included into large-scale sensor networks as an intermediary layer for storing sensor data and responding to requests. However, the hacked storage node may not only lead to the privacy issue but also provide false or partial query results. We present a simple but effective dummy reading based anonymization framework, under which our proposed verified top-k query (VQ) techniques may ensure the integrity of the query results. The VQ schemes have a fundamentally different design philosophy than previous efforts, and they are able to reduce communication complexity at the expense of a little loss of detection capabilities. Our suggested methodologies are tested using analytical investigations, numerical simulations, and prototype implementations.

Introduction

Since the link between the authority (or network owner) and the network in a data-gathering sensor network is not always solid, a caching layer in the intermediate is required for archiving sensed data and responding to queries. To obtain sensor readings, the authority may query the network, as shown in Fig. 1 of this research. A modest number of storage nodes [24] make up the nodes in the intermediate layer. In the lowest rung, several regular sensors with little resources collect data about their immediate surroundings.

In hierarchical sensor networks, the authoritative node sends relevant queries to get the sought-after subset of the sensed data. In this work, we focus only on the top-k question, one of the simplest and most practical inquiries.

Sensor networks with several layers were used in two approaches (additional evidence and crosscheck). The former creates hashes for each subsequent pair of sensed data for verification, while the latter broadcasts the data across the network so that no one node can falsify the query result.

Despite the research done on verified questions before, we are nonetheless worried about the following. With n sensors, the Hybrid approach [35] results in prohibitively expensive O(n2) communications.The top-k query result may be verified using a modified version of SMQ [34], but this requires not only the construction of an aggregation tree, but also its preservation and integrity.

ISSN NO: 9726-001X
Volume 03 Issue 01 January 2015

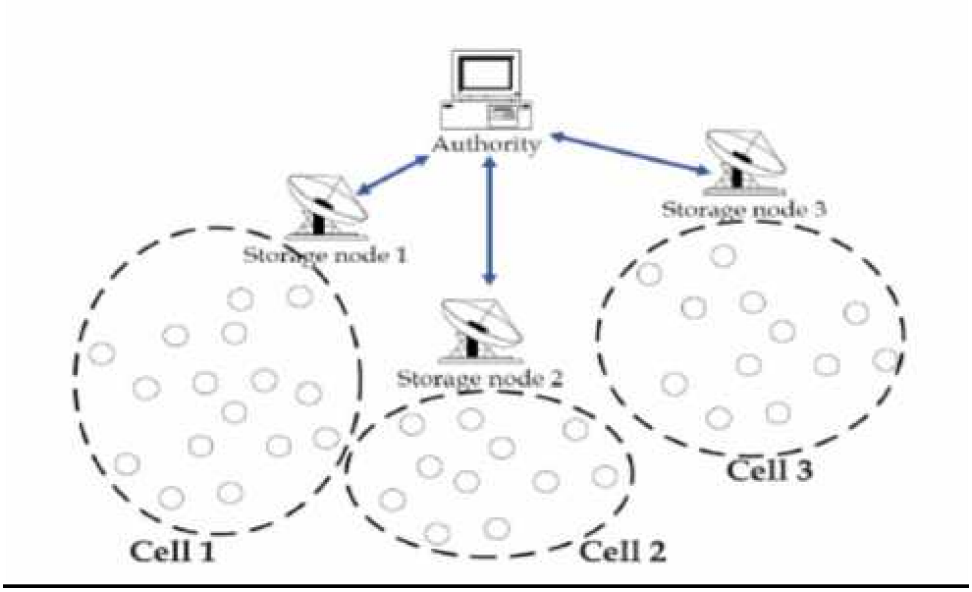
The proper authorities also need to know the specifics of the tree's topology. It is challenging to achieve these standards in a production environment. While it may seem possible to simply add a data-confidentiality guarantee to the approach in [35], doing so would imply additional grave shortcomings that cannot be tolerated in the design of a verifiable query strategy.

Separate sets of sensor nodes, each with its own storage node, are a common feature of the aforementioned tiered design. A cell is any collection of sensor nodes working together. The

The cell's sensor nodes work together to establish a multi-hop network that reliably relays data to the storage node. The storage node acts as a repository for collected sensor data and responds to authoritative inquiries.

An example of the tiered architecturecan be found in Fig. 1

SYSTEM ARCHITECTURE:



ISSN NO: 9726-001X
Volume 03 Issue 01 January 2015

EXISTING SYSTEM

In order to protect the results of a top-k query in a hierarchical sensor network, the authors of offer two schemes: extra evidence and crosscheck. The former creates hashes for each subsequent pair of sensed data for verification, while the latter broadcasts the data across the network so that no one node can falsify the query result. When an unqualified sensor reading is substituted for the genuine query result, the authority may discover that there are some missing sensor readings for hash verification if each consecutive pair of sensed data is associated with a hash. Crosscheck, on the other hand, involves sending the authentic top-k findings to several sensor nodes. Incomplete query results are likely to be discovered by the authority once they compare their data to that of other sensor nodes. The goal of the hybrid approach is to strike a compromise between the communication cost and the capacity to identify incompleteness in the query results.

PROPOSED SYSTEM:

Verifiable top-k Query (VQ) techniques are provided for privacy-preserving top-k query result integrity verification in tiered sensor networks, and they are built on the new dummy reading-based anonymization framework. Our suggested privacy backbone is rdOPE, a randomized and distributed variant of Order Preserving Encryption.Theoretical and practical goals may be served by the decreased communication complexity achieved by AD-VQ-static at the expense of a modest reduction in detection capabilities. To prove the viability of our approaches, we do analytical analyses, run numerical simulations, and put together working prototypes. The components of a cell are a storage node and a set of regular sensors linked in a multi-hop network. It is expected that storage nodes know whose cells they are associated with and that they have access to direct or multi-hop connections with the authority. All of the nodes' clocks are now in sync and time is tracked in epochs. Keep in mind that techniques may be used to synchronize the time of many nodes.

ISSN NO: 9726-001X
Volume 03 Issue 01 January 2015

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

To construct VQ schemes, an innovative dummy-reading based anonymization framework is given. AD-VQ-static in particular may be of theoretical and practical importance due to its capacity to reduce communication complexity while incurring just a small cost in detecting capabilities. The VQ methods are applicable to real-world sensor networks since they use just symmetric cryptography and have a minimal implementation complexity..