S Mounika* et al.
(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH
Volume No.6, Issue No.5, August - September 2018, 8573-8574.

Query Analysis For Two-Level Sensor Topologies With Data Protection And Reliability

S.MOUNIKA
M.Tech Student, Dept of CSE, Malla Reddy Engineering College for Women, Hyderabad, T.S, India

Dr. KIRUBAKARAN
Professor, Dept of CSE, Malla Reddy Engineering College for Women, Hyderabad, T.S, India

Abstract: **The storage nodes, which act as an intermediate layer between the sensors and the sink, can be hacked, allowing attackers to learn sensitive data and process query results.Privacy and integrity were the cornerstones of the application of sensor networks with two levels. Prior schedules for secure query processing are weak because they reveal very little information, so attackers can estimate statistical data based on domain knowledge and the date of query results. In this study we propose the first top-k query processing system that protects the privacy of the sensor data and the integrity of the query results. To maintain privacy, we build an index for each data element collected by the sensor using a semi-random hash function and Blom filters and converting top-k queries to queries in the upper range. To maintain integration, we propose that the data partition algorithm divide each data element into a time interval and associate the partition data with the data. The attached information ensures that the repository can verify the integrity of the query results. We officially show that our software is protected under the IND-CKA security model. Our empirical results from real-life data show that our approach is rigorous and practical for large network size.**

Keywords: **Synchronization; Localization; Sensor Node; Joint Solution; Propagation Delay;**

I. INTRODUCTION:

Two-tier sensor networks have been widely adopted because of their scalability and energy efficiency. A large number of sensors equipped with limited storage spaceAnd computing capabilities, are spreading in the fields. Some storage nodes, equipped with large storage capacity and powerful computing capability, are used between sensors to store measurement data from adjacent sensors, such as shown in Figure 1. The sink acts as a terminal device that queries sent to storage nodes and sensors retrieves data from interest. Due to the importance of dual sensor network architecture, many commercial storage units, such as StarGate and RISE, have also been developed. Storage points provide two main advantages compared to a non-built sensor network model [1]. First, storage nodes are responsible for collecting, storing and transmitting sensory data from sensors to the aquarium. The sensors are reduced to eliminate a large amount of energy by sensing the transmission of the relay sensor to the aquarium, and prolong the life of the grid. Second, storage units have greater computing power and greater storage capacity than sensors. Therefore, the sink can perform complex queries, such as group queries or higher as to retrieve multiple data items in a single query. This saves the power bandwidth and network sensor nodes needed to answer the aquarium queries. However, because of its importance in network operations, storage points are more vulnerable to attacks and compromises. Attackers cannot steal sensitive information on the storage node, but also use query processing functions of the storage node to send false information to the sink.

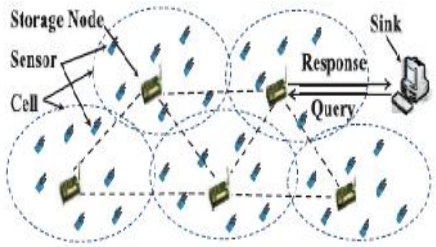

Fig. 1. Architecture of two-tired sensor networks.

II. METHODOLOGY:

In this work, the source activates all sensors and sets the temperature for all cells and uploads their data to the assigned storage node. Is stored in the cell. The service provider can view the attacker's file in the storage node, replace the malicious files injected into the original file in the cells, and notify the authority of malicious files in the cells [2]. The main part can send questions to retrieve sensor measurements. The middle level consists of a small number of abundant storage nodes, called a storage contract. The lower level consists of a large number of ordinary sensors with limited resources that are influenced by the environment. The Authority shall issue an appropriate investigation to request the desired part of the observed data. In this system we limit ourselves to the top-k-query, one of the most frequently used queries. The storage node keeps a copy of the received sensor measurements and is responsible for answering questions from the authority. The temperature is stored with its characters such as node name, temperature, status, digital marking, temperature adjusted in storage node, data file will also be stored with their tags such as node name, file name, secret key, status, In

the storage node storage nodes are abundant in storage, they can communicate with the power via direct or multiple connection hopping, presumably to know its own cells [3][4]. The storage node can also see details of the attacker. In this unit, the sensor nodes are usually divided into separate groups, each connected to a storage node. Each set of sensor points is called a cell. The sensor node in the cell forms a network with multiple hop points and always sends sensor values and file data back to the associated storage node. The end user has access to the details of the top-k file and the highest k-temperatures of the cells in the corresponding storage node (SN1, SN2 and SN3), and the end user can request a response to the contents of the file at the corresponding storage node. If the file name and the secret key are correct, the user receives the file response from the reference and the storage node. Topk queries in a centralized unconfirmed database, providing a good background for the problem of distributed processing [5]. The query response can be obtained by testing the groups in order of the descending order from the sorted table (which is still known as T for simplicity). We can easily determine that the groups with the highest ranking are certainly in the answer group, as long as their qualifications are greater than p, since their qualifications such as PT-Topk answers are not dependent on another group [6].

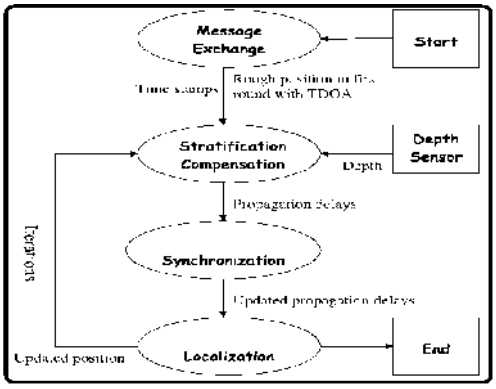

Fig.2.System architecture

III. CONCLUSION:

During the identification phase, JSL compensates, instead of other algorithms, for assuming that the waves move in straight lines in the water atmosphere, the effect of layers in the underwater acoustic performance ranges, i.e. the delay estimate, will be a greatly improved effort. In this work we concentrate on domain-based localization algorithms. Technologies are generally based on communication or communication. Although the submerged sensor network is three-dimensional, no two network nodes are known as the plane perpendicular to the ocean floor. Within this work, estimates of settlements arise from a combination of suspicions and measurements. Given the possibility of multiple movement patterns in each node, the comparison of the global situation is not possible. JSL is extended to a network-wide solution with a frequent strategy request. The error around the reference position in the anchor follows the normal distribution: 1 for the average value and: 01 for the standard derivation. We evaluated the effect of water flow using two different models, namely the random walk along the model of current mobility aliasing. Assuming that the speed profile seems the only depth-dependent, please note that both the transmitter and the receiver need a two-dimensional surface on the countertop.

IV. REFERENCES:

[1] B. Sheng and Q. Li, "Verifiable privacy-preserving range query in twotieredsensor networks," in Proc. 27th INFOCOM, Apr. 2008, pp. 46–50.

[2] B. Sheng, Q. Li, and W. Mao, "Data storage placement in sensornetworks," in Proc. 7th ACM MobiHoc, May 2006, pp. 344–355.

[3] I. F. Ilyas, G. Beskales, and M. A. Soliman, "A survey of top-k queriesprocessing techniques in relational database system," ACM Comput.Surv., vol. 40, no. 4, pp. 11:1–11:58, Oct. 2008.

[4] A. S. Silberstein, R. Braynard, C. Ellis, K. Munagala, and J. Yang,"A sampling-based approach to optimizing top-k queries in sensornetworks," in Proc. 22nd ICDE, Apr. 2006, p. 68.

[5] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preservingmulti-keyword ranked search over encrypted cloud data," IEEE Trans.Parallel Distrib. Syst., vol. 25, no. 1, pp. 222–233, Jan. 2014.

[6] B. Bezawada, A. X. Liu, B. Jayaraman, A. L. Wang, and R. Li, "Privacypreserving string matching for cloud computing," in Proc. 35th ICDCS,Jun./Jul. 2015, pp. 609–618.

