Privacy and Integrity Preserving Top-k Query Processing for Two-Tiered Sensor Networks

ABSTRACT

Privacy and integrity have been the main road block to the applications of two-tiered sensor networks. The storage nodes, which act as a middle tier between the sensors and the sink, could be compromised and allow attackers to learn sensitive data and manipulate query results. Prior schemes on secure query processing are weak, because they reveal non-negligible information, and therefore, attackers can statistically estimate the data values using domain knowledge and the history of query results.

EXISTING SYSTEM

In Existing System, Sensor networks have been widely adopted for their scalability and energy efficiency. A large number of sensors equipped with limited storage and computing capacity are deployed in fields. Some storage nodes, equipped with large storage and powerful computating capacity, are deployed among sensors for storing measurement data from the neighboring sensors. We address the problem of privacy and integrity preserving top-*k* queries in two-tiered sensor networks to protect against storage node compromise. Our goal is to design scheme to enable storage nodes to process top-k queries correctly without knowing the actual value of data stored in them and allow the sink to detect misbehavior of storage nodes. Top-k query processing, *i.e.*, finding the *k* smallest or largest data items collected from a specified sensed area, is a fundamental operation in sensor networks.

DIS ADVANTAGES

- Privacy and integrity preserving top-*k* queries in two-tiered sensor networks to protect against storage node compromise problem occurs.
- It cannot prevent the privacy leakage.

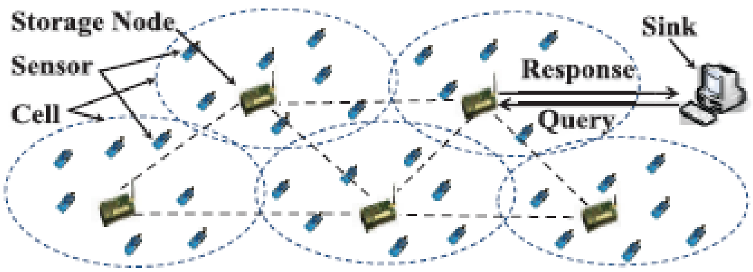
PROPOSED SYSTEM

In Proposed System, first top-*k* query processing scheme that protects the privacy of sensor data and the integrity of query results. To preserve privacy, we build an index for each sensor collected data item using pseudo-random hash function and Bloom filters and transform top-*k* queries into top range queries. To preserve integrity, we propose a data partition algorithm to partition each data item into an interval and attach the partition information with the data. The attached information ensures that the sink can verify the integrity of query results. We formally prove that our scheme is secure under IND-CKA security model. Our experimental results on real-life data show that our approach is accurate and practical for large network sizes.

ADVANTAGES

- It detects misbehavior of storage nodes.
- It facilitates the secure queries.

SYSTEM ARCHITECTURE



Architecture of two-tiered sensor networks

SYSTEM REQUIREMENTS

H/W System Configuration:-

Processor	-	Pentium –III
RAM	-	256 MB (min)
Hard Disk	-	20 GB
Key Board	-	Standard Windows Keyboard
Mouse	-	Two or Three Button Mouse
Monitor	-	SVGA

S/W System Configuration:-

Operating System	:	Windows95/98/2000/XP
Application Server	:	Tomcat5.0/6.X
Front End	:	HTML, Jsp
Scripts	:	JavaScript.
Server side Script	:	Java Server Pages.
Database	:	MySQL 5.0
Database Connectivity	:	JDBC