ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Reading Based Anonymization Method in Which the Query Result Integrity Can Be Guaranteed By Verifiable Top-K Query (VQ) Schemes

P.Divyateja
M.Tech Student,
Dept of CSE,
St.Martin's Engineering College,
Dhulapally, Hyderabad, Telangana.

U.Sivaji
Professor,
Dept of CSE,
St.Martin's Engineering College,
Dhulapally, Hyderabad, Telangana.

Abstract:

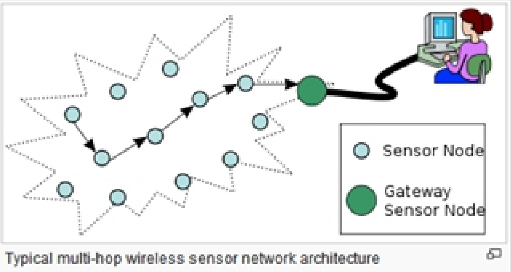
A wireless sensor networks are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location.Storage nodes are predictable to be located as an intermediate tier of huge scale sensor networks for caching the composed sensor readings and responding to queries with benefits of influence and storage reduction for standard sensors. Nevertheless, an essential issue is that the compromised storage node may not only source the privacy problem, but also arrival fake/curtailed query results. We propose a graceful yet competent dummy reading based anonymization constitution, beneath which the query result steadfastness can be certain by our proposed verifiable top-k query (VQ) schemes. Compared with accessible machinery, the VQ schemes have an essentially different design attitude and realize the lower communication complexity at the cost of slight exposure capability degradation. Analytical studies, geometric simulations, and archetype implementations are conducted to exhibit the practicality of our proposed methods.

Keywords:

Sensor networks, Storage node, Top-k query result completeness, VQ scheme.

Introduction:

Wireless Sensor Networks (WSN) have recently been the focus of a significant amount of attention and effort of the research community. The main motivation has been to address the challenges posed by the WSN paradigm, i.e., limited node power, processing, and communication capabilities, dense network deployment, multi-hop Communications and heterogeneous application-specific requirements. The vast majority of these studies applies to conventional WSN applications which need reliable and efficient communication of scalar event features and sensor data such as temperature, pressure, humidity.The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.



Typical multi-hop wireless sensor network architecture

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created.

The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

The main characteristics of a WSN include:

- Power consumption constraints for nodes using batteries or energy harvesting
- Ability to cope with node failures (resilience)
- Mobility of nodes
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Ease of use
- Cross-layer design

To motivate effective dummy reading based anonymization framework, under which the query result integrity achieve the lower communication complexity at the cost detection. OPE has been applied widely to encrypted catalog reclamation. Regrettably, in the literature, the information is all assumed to be generated and encrypted by a single authority, which is not the case in our consideration. In addition, because the number of possible sensor readings could be limited and known from hardware specification, the relation between plaintexts and cipher texts might be exposed. For example, if the sensors can solitary spawn 20 kinds of possible outputs, then practically the adversary can derive the OPE key by investigating the numerical order of the eavesdropped cipher texts despite the theoretical security guarantee. The genuine top-k results are distributed to several sensor nodes. Through assured prospect, the influence will find query result incompleteness by checking the other sensor nodes' sensor readings.

Amalgam routine is a collective use of supplementary facts and crosscheck, attempting to equilibrium the communiqué cost and the query result incompleteness detection capability. Top-k query result integrity was also addressed in where distributed data sources generate and forward the sensed data to a proxy node. The query result completeness is achieved by requiring sensors to send cryptographic one-way hashes to the storage node even when they do not have fulfilling readings. In SMQ apiece sensor applies muddle operation to the received data and its hold data, generating a certifiable entity of the sensor readings of the entire network. The basic idea behind SMQ is to construct an aggregation tree over the sensor nodes.

RELATED WORK:

Fast Privacy-Preserving Top-k Queries using Secret Sharing Over the past several years a lot of research has focused on distributed top-k division. In this work we are fascinated in the next privacy-preserving distributed top-k quandary. A situate of parties grasp secretive lists of keyvalue pairs and want to find and disclose the k key-value pairs with largest aggregate values without revealing any further information. We use sheltered multiparty computation (MPC) techniques to solve this problem and design two MPC protocols, PPTK and PPTKS, putting prominence scheduled their effectiveness. PPTK uses a chop table to squeeze a probably large and sparse space of keys and to probabilistically estimate the aggregate values of the top-k keys. PPTKS uses manifold botch tables, i.e., sketches, to progress the inference precision of PPTK. We estimate our protocols with real interchange traces and show that they accurately and efficiently aggregate distributions of IP addresses and port numbers to find the globally most frequent IP addresses and port numbers.

Privacy and Integrity Preserving Range Queries in Wireless Sensor Networks:

Two tiered sensor network architecture, someplace storage nodes proceed as an intermediary tier between sensor nodes and sink which is act as a receiver for storing data items and calculating queries. I propose beneficial techniques to save power consumption and memory space consumption and buildup efficient query processing.

For preserve privacy, I propose a technique named SafeQ. SafeQ is a protocol, which is used to detect misbehavior of attackers. And storage node can perfectly process queries issued from sink and data items sent by sensor nodes without knowing their inventive values. For care for veracity, I intend two methods namely Merkle hash tree and vicinity manacles. Mutually be used for corroborate whether the query result of data items that satisfy the query. For reduce communiqué cost, I propose flourish filters for diminish the communiqué cost between sensor nodes and storage nodes in sensor networks.

SafeQ: Secure and Efficient Query Processing in Sensor Networks:

The architecture of two-tiered sensor networks, somewhere storage nodes give out as a transitional tier between sensors and a sink for storing data and doling out queries, has been extensively adopted since of the reimbursement of power and storage saving for sensors as well as the efficiency of query meting out. Conversely, the magnitude of storage nodes also makes them striking to attackers. In this paper, we intention SafeQ, aetiquetteso as to prevents attackers on or after gaining information from both sensor collected data and sink issued queries. SafeQ too allows a fall to perceive compromised storage nodes when they act up. To preserve privacy, SafeQ uses a novel technique to encode both data and queries such that a storage node can correctly process encoded queries over encoded data without knowing their ideals. To preserve integrity, we intend a novel data structure called neighborhood chains that allow a sink to verify whether the result of a query contains exactly the data items that gratify the query. In toting up, we intend a clarification to acclimatize SafeQ for event-driven sensor networks.

Top-k Monitoring in Wireless Sensor Networks:

Top-k monitoring is important to many wireless sensor applications. This term paper exploits the semantics of top-k query and proposes an energy-efficient monitoring loom called FILA. The essential initiative is to establish a sieve at each sensor node to suppress unnecessary sensor updates. Sieve scenery and query reassessment in front updates are two fundamental issues to the correctness and efficiency of the FILA loom. We enlarge a query reassessment algorithm that is capable of handling concurrent sensor updates. In finicky, we turnout optimization techniques to shrink the prying cost. We devise a skewed sieve locale scheme, which aims to steadiness energy expenditure and prolong network existence. Besides, two sieves revise strategies, explicitly, fervent and sluggish, are anticipated to favor different relevance scenarios. We as well widen the algorithms to quite a few variants of topk query, that is, classify numb, rough, and value monitoring. The performance of the proposed FILA approach is extensively evaluated using factual data traces. The consequences show that FILA significantly outperforms the existing TAG-based approach and range caching approach in terms of both network lifetime and energy consumption under various network configurations.

Secure Top-k Query Processing via Untrusted Location-based Service Providers:

Distributed system for collaborative location-based information generation and sharing which become increasingly popular due to the explosive growth of Internet-capable and location-aware itinerant devices. The arrangement consists of a data aerial, data contributors, location-based overhaul providers (LBSPs), and system users. The data collector gathers reviews about points-of-interest (POIs) from data contributors, whilst LBSPs acquire POI data sets as of the data collector and allow users to perform location-based top-k queries which ask for the POIs in a certain region and with the highest k ratings for an interested POI trait. In carry out, LBSPs are untreated and can return fake query results for various bad motives, e.g., in favor of POIs agreeable to pay. This dissertation presents two novel schemes meant for users to detect fake top-k query results as an effort to foster the practical deployment and use of the wished-for system. The effectiveness and good organization of our schemes are thoroughly analyzed and evaluated.

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.

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.

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 multihop 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.

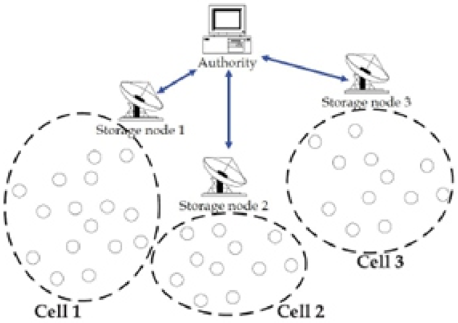
ADVANTAGES OF PROPOSED SYSTEM:

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

SYSTEM ARCHITECTURE:



Modules:

Middle tier storage node access
Evaluating Data Anonymity
Authentication for false injected reading
Result verification

CONCLUSION:

A novel dummy reading-based anonymization framework is proposed to design Verifiable top- k Query (VQ) schemes. In picky, AD-VQ-static achieves the inferioSr communiqué complexity with only minor detection aptitude consequence, which might be of both speculative and down-to-earth interests. Accompanied by only symmetric cryptography implicated and their low realization obscurity, the VQ schemes are apposite and sensible for current sensor networks.

REFERENCES:

1. Yu, C., G. Ni, I. Chen, ErolGelenbe, and S. Kuo. "Top-k Query Result Completeness Verification in Tiered Sensor Networks." (2014): 1-1.

2. E. Gelenbe and G. Loukas, "A self-aware approach to denial of service defence," Comput.Netw., vol. 51, no. 5, pp. 1299–1314, 2007.

3. 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.

4. H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in Proc.ICPS, Jul. 2005, pp. 88–97.

5. M. Burkhart and X. Dimitropoulos, "Fast privacy preserving top-k queries using secret sharing," in Proc. 19th ICCCN, 2010, pp. 1–7.

6. 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.

7. F. Chen and A. X. Liu, "SafeQ: Secure and efficient query processing in sensor networks," in Proc. 24th IEEE Conf. Comput. Commun.,Mar. 2010, pp. 1–9.

8. M. Wu, J. Xu, X. Tang, and W.-C.Lee, "Top-k monitoring in wireless sensor networks," IEEE Trans. Knowl. Data Eng., vol. 19, no. 7, pp.962–976, Jul. 2007