A Survey on Spatiotemporal Approaches in Sensor Networks

1 K.Sreekanth 2 Rapalli Rakesh

Abstract

Spatial-temporal reasoning is based on qualitative abstractions of temporal and spatial aspects of the common-sense background knowledge on which our human perspective .

We describes sensor networks with resource rich master nodes at the upper tier and resource-poor sensor nodes at the lower tier. Master nodes collect data from sensor nodes and answer the queries from the network owner.

We proposes the spatiotemporal approach to provide secure range queries in event-driven two tier sensor networks. It offers data confidentiality by preventing master nodes from reading hosted data and also enables efficient range-query processing. The compromised master node may leak hosted sensitive data to the adversary; it may also return juggled or incomplete data in response to a query.

which allows the network owner to verify with very high probability whether a query result is authentic and complete by examining the spatial and temporal relationships among the returned data.

Related work

Event-Driven Application Model

In this subsection, we clarify the event-driven application model used throughout the paper. Similar to [5], we assume that time is divided into epochs and that sensor and master

nodes are loosely synchronized. We assume there are totally$F$ events observed in a target cell during epoch t, where F ∈[0, Fm] is a random number, and Fm is the maximum number

of events that can be observed in a cell during each epoch. Let nf denote the number of distinct sensor nodes detecting event f, $1 \le f \le F$. It is worth noting that one sensor node may detect multiple events in the same epoch. F and nf may vary in different cells and epochs and follow some distributions which depend on concrete applications.

RANGE QUERIES OVER ENCRYPTED DATA

In this section, we illustrate how to realize data confidentiality,efficient range queries, and query-result authentication, which is the basis for our spatiotemporal crosscheck scheme. We assume that each epoch consists of three phases. In the longest detection phase, each sensor node performs sensing. In the subsequent reporting phase, each sensor node submits to its master node all the data (if any) it produced during that epoch. Depending on concrete applications, each data itemmay comprise multiple attributes such as the weight of an observed object, its location, its speed and moving trajectory, and its appearance and lingering times. In the final query phase, the network owner may issue queries for data generated in that epoch. During the relatively much shorter reporting and query phases, some nodes may generate some data which will be carried over to the next epoch. In this paper, we aim to support only epoch-based and cell-based single-attribute range queries, e.g., “Return all the data items generated uring epoch t in cell $idcell$ whose weight attribute is between 100 and 120pounds.”

SPATIOTEMPORAL APPROACH TO SECURE RANGE QUERIES

In this section, we present a novel spatiotemporal approach allowing the network owner to verify the completeness of range queries, which includes a spatial crosscheck technique, a temporal crosscheck technique, and their combination.A. Spatial Crosscheck (SC)

We first introduce a novel spatial crosscheck (SC) technique. We consider cell $idcell$ which consists of master node$\mathcal{M}$ and sensor nodes $\{Si\}N$ i=1. The key idea of spatial crosscheck is to embed some relationships among data generated by different nodes during each epoch, e.g., embedding the information about node Sj ’s data into node Si’s data buckets. Under this technique, if $\mathcal{M}$ omits data from some sensor nodes, the network owner can decide with high probability that the query result is incomplete by inspecting the spatial relationships among the returned data. $\mathcal{M}$ is thus forced to either return all the data satisfying the query or none of them in order to escape the detection. To realize the SC technique, each node need disseminate the information about its own data which can then be embedded into other nodes’ data. How to disseminate such information is critical in designing SC, which determines the efficacy and efficiency of SC. In the following, we detail three versions of SC, including a broadcast-based spatial crosscheck method (BSC), a neighbor-based one (NSC), and a hybrid one (HSC) which is the combination of BSC and NSC.

In BSC, before submitting its data to$\mathcal{M}$, every sensor node broadcasts the information about its data (if any) within cell $idcell$. The broadcasted information consists of its ID and avector of g bits, called data index, where each bit indicateswhether the node has detected data in the corresponding bucket or not. We denote the data index of Si at epoch t by Vi,t. For example, if g = 8 and Vi,t = 10101000, then Si only detected data for buckets 1|3|5 during epoch t. Every node with data for submission sets a timer to the estimated longest end-to-end message transmission time in cell $idcell$ to allow enough time for receiving other nodes’ data indexes. Then it embeds its own data index and all the received ones along with the corresponding node IDs into each of its own data buckets. Finally, it sends the encrypted buckets to $\mathcal{M}$ as in

Section III. For example, assume that Si has 3|2|1 data items in buckets 1|3|5, respectively, and has data indexes $\{Vl,t\}kl=1$ before submission, including the received ones and its own,

i.e., $Si \in \{Sl\}kl =1$. It finally sends the following message to $\mathcal{M}$ during the reporting phase.

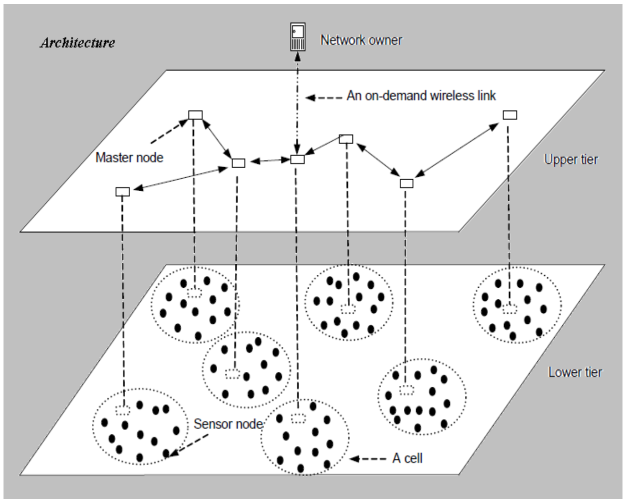
$Si \rightarrow \mathcal{M}$: i, t, $\langle 1, (data1, data2, data3, \{jl, Vl,t\}kl=1)Ki,t \rangle, \langle 3, (data4, data5, \{jl, Vl,t\}kl$

$=1)Ki,t\rangle, \langle 5, (data6, \{jl, Vl,t\}kl=1)Ki,t\rangle$.

The effectiveness of BSC can be easily seen through the following example. Assume that the network owner sends a query only for bucket 5; nodes $\Theta \subseteq \{Si\}N\ i=1$ have data in bucket 5; and $\mathcal{M}$ drops the data bucket of $Si \in \Theta$. Since$\langle i, Vi,t\rangle$ is embedded in bucket 5 of every other node in

$\Theta \setminus \{Si\}$, it can reach the network owner as long as $\mathcal{M}$ does not drop all the data buckets atisfying the query. If the network owner finds $\langle i, Vi,t\rangle$ in any received bucket and does not receive the bucket from Si, it can determine that $\mathcal{M}$ must be malicious. Therefore, $\mathcal{M}$ has to drop all the data bucketsto escape detection.

Architecture



Technique Used

Bucketing technique:

The bucketing technique to store encrypted data at master nodes and also ensure rang-query efficiency. If the encryption algorithm is an OCB-like authenticated encryption primitive their scheme can ensure data confidentiality and query-result authenticity. To permit query-result completeness verification, they propose that every sensor node that has no data satisfying the range query return some verifiable information through the involved master node to the network owner. We adopt the bucketing technique to strike a balance between data confidentiality and query efficiency. Our major contribution is a novel spatiotemporal approach for the network owner to verify query-result completeness.

Existing System

The reliance on master nodes for data storage and query processing raises serious security concerns. In particular, many target application environments of WSNs such as forests and oceans are unattended and hostile in nature.

Disadvantages:

1. juggled and/or incomplete data
2. complexity
3. No secure range query processing

Proposed System and its approaches

Master nodes are attractive targets of attack and might be compromised by the adversary. Let master nodes store encrypted data for which they do not hold the decryption keys, while enabling efficient query processing. our technique allows the network owner to verify the authenticity and completeness of any query result. In this paper, we focus on supporting range queries which are an important and common type of queries in sensor networks and ask for data within a certain range.

Advantages:

1. increasing network capacity and scalability
2. reducing system complexity, and prolonging network lifetime
3. Apply Encrypt/Decrypt Method
4. secure range query processing

Approaches

1. General Approach
2. Adversary Model
3. Range Queries Over Encrypted Data
4. Master Node – Network Owner

1. General Approach

The lower tier comprises a large number of resource-constrained sensor nodes, while the upper tier contains fewer relatively resource-rich *master node*s. Sensor nodes are mainly responsible for sensing tasks, while master nodes perform more resource-demanding computation and communication tasks. Master nodes also form a multi-hop wireless mesh network via long-range high-bandwidth radios. The network field is partitioned into physical *cell*s, each containing a master node in charge of sensor nodes in that cell. Master nodes collect data from affiliated sensor nodes and store them locally for extended periods of time. The network owner can query data through an on-demand communication link (e.g., a satellite link) to some master node(s).

2. Adversary Model

We refer to the existing rich literature for effective defenses against other attacks. We assume that the adversary can compromise an arbitrary number of master nodes. Once compromising a master node, the adversary can access data stored there and also instruct it to return juggled and/or incomplete data in response to range queries from the network owner. The adversary may also compromise sensor nodes and access any information stored on them. Since a compromised sensor node only has very limited information and there are many more sensor nodes than master nodes with more important roles, the adversary will be motivated to compromise master nodes in order to do more damage.

3. Range Queries Over Encrypted Data

We assume that each epoch consists of three phases. In the longest *detection* phase, each sensor node performs sensing. In the subsequent *reporting* phase, each sensor node submits to its master node all the data (if any) it produced during that epoch. Depending on concrete applications, each data item may comprise multiple attributes such as the weight of an observed object, its location, its speed and moving trajectory, and its appearance and lingering times. In the final *query* phase, the network owner may issue queries for data generated in that epoch. During the relatively much shorter reporting and query phases, some nodes may generate some data which will be carried over to the next epoch. In this paper, we aim to support only epoch-based and cell-based single-attribute range queries.

4. Master Node – Network Owner

The data is encrypted when we are uploading in Master Node. The Network Owner view the encrypted file details after that they request for the files on the particular Master Node. Network Owner has a grant permission to check the received files are coming for the authenticated requested Master Node. The files are decrypted when received from Master Node - Network Owner.

VI. CONCLUSION

In this paper, we presented a novel spatiotemporal technique to secure range queries in event-driven two-tier sensor networks. Our technique can prevent compromised master nodes from reading hosted data and also achieves high query efficiency. In addition, our technique allows the network owner to verify the authenticity and completeness of any query result. Compared with prior work, our technique can achieve a comparable detection probability with much lower communication overhead in even-driven WSNs. The efficacy and efficiency of our technique are confirmed by detailed evaluations.

REFERENCES

[1] J. Shi, R. Zhang, and Y. Zhang, "Secure range queries in tiered sensor

networks," in IEEE INFOCOM'09, Rio de Janeiro, Brazil, Apr. 2009.

[2] P. Desnoyers, D. Ganesan, and P. Shenoy, "TSAR: a two tier sensor storage architecture using interval skip graphs," in Proc. ACM SenSys'05,

San Diego, California, USA, Nov. 2005, pp. 39–50.

[3] M. Shao, S. Zhu, W. Zhang, and G. Cao, "pDCS: security and privacy

support for data-centric sensor networks," in Proc. IEEE INFOCOM'07,

Anchorage, Alaska, USA, May 2007, pp. 1298–1306.

[4] N. Subramanian, C. Yang, and W. Zhang, "Securing distributed data

storage and retrieval in sensor networks," in IEEE PerCom'07, White

Plains, NY, Mar. 2007.

[5] B. Sheng and Q. Li, "Verifiable privacy-preserving range query in sensor

networks," in Proc. IEEE INFOCOM'08, Phoenix, AZ, Apr. 2008, pp.

46–50.

[6] Q. Wang, K. Ren, W. Lou, and Y. Zhang, "Dependable and secure sensor

data storage with dynamic integrity assurance," in IEEE INFOCOM'09,

Rio de Janeiro, Brazil, Apr. 2009.

[7] O. Gnawali, K.-Y. Jang, J. Paek, M. Vieira, R. Govindan, B. Greenstein,

A. Joki, D. Estrin, and E. Kohler, "The tenet architecture for tiered

sensor networks," in Proc. ACM SenSys'06, Boulder, Colorado, USA,

Oct. 2006, pp. 153–166.

[8] X. Li, Y. J. Kim, R. Govindan, and W. Hong, "Multi-dimensional range

queries in sensor networks," in Proc. ACM SenSys'03, Los Angeles,

California, USA, Nov. 2003, pp. 63–75.

[9] H. Hacig¨um¨us¸, B. Iyer, C. Li, and S. Mehrotra, "Executing SQL over

encrypted data in the database-service-provider model," in Proc. ACM

SIGMOD'02, Madison, Wisconsin, June 2002, pp. 216–227.

[10] B. Hore, S. Mehrotra, and G. Tsudik, "A privacy-preserving index for range queries," in Proc. VLDB'04, Toronto, Canada, Aug. 2004, pp.

720–731

Author's profiles

Rapalli Rakesh
MTech student
Department: CSE Dept
MALLA REDDY COLLEGE
OF ENGINEERING & TECHNOLOGY

k.sreekanth

Asst Professor
Department: CSE Dept
MALLA REDDY COLLEGE
OF ENGINEERING & TECHNOLOGY