VOL. 10, NO. 9, MAY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

AUTHENTICATION OF K NEAREST NEIGHBOR QUERY ON ROAD NETWORKS

S. Angel Latha Mary and Krishana Prasath
Department of Computer Science Engineering, Karpagam College of Engineering, Coimbatore, Tamilnadu, India
E-mail: xavierangellatha@yahoo.com

ABSTRACT

This work specifically focus on the k-nearest-neighbor (kNN) query verification on road networks and design verification schemes which support both distance verification and path verification. That is the k resulting objects have the shortest distances to the query point among all the objects in the database, and the path from the query point to each k-nearest-neighbor result is the valid shortest path on the network. In order to verify the kNN query result on a road network, a naïve solution would be to return the whole road network and the point of interest (POI) dataset to the client to show correctness and completeness of the result.

Keywords: k-nearest-neighbor (kNN), road networks.

1. INTRODUCTION

The combination of mobile devices and Cloud-based solutions is creating a versatile ecosystem for reshaping the way geospatial data are stored, managed, served, and shared [8]. Consequently, outsourcing databases to the Cloud is becoming increasingly popular and has received considerable attention from the research community [1]. Although database outsourcing provides data owners with a more efficient, economical, and flexible solution, it also introduces new concerns. In this paper, we study one of those concerns, in particular, the query integrity concern [7]. That is, how to ensure that the query results returned by SP are still trustworthy. As SP is not the real owner of the data, it might return incorrect results to mobile clients out of its own interests, for example, an SP which hosts a collection of restaurants might favor some restaurants that pay more advertisement fees. Moreover, an SP might return suboptimal results to query clients by applying flawed or inferior algorithms in order to save computation resources [2]. For example, as of today, the Google Maps online service still provides users with k-nearest-neighbor results based on their Euclidean distances instead of their road network distances, not because they cannot compute the road network distances, but because it is much less expensive to compute the Euclidean distances. On the other hand, with the growing popularity of the Cloud, more and more security breaches and attacks on such systems have been brought to people's attention [3]. The experiment results show that our approach leads to compact verification objects (VO) and the verification algorithm on mobile devices is efficient, especially for queries with low selectivity.

2. RELATED WORKS

Authenticated query processing ensures the client that the received result complies with the validated DB [5]. An adaptation of a multistep algorithm that is optimal in terms of DST computations. AMN requires transmissions of false hits, i.e., records that are not in the result, but are nevertheless necessary for its verification. In addition to the network overhead, false hits impose a significant burden to the client, which has to verify them. C-AMN alleviates this problem through an elaborate scheme that reduces the size of false hits [2]. The database is horizontally partitioned over several servers. Addressing authenticated similarity retrieval from such sources using the multistep kNN framework [3]. We developed C-AMN, a technique that addresses the communication specific aspects of NN, and minimizes the transmission overhead and verification effort of the clients. We propose ID-AMN, which retrieves distance information from distributed servers, eliminating those that cannot contribute results. The main drawback is Computational complexity and there is a lack of result in verification process [12, 13, 14].

3. PROPOSED SYSTEM

This system subsumes and extends our earlier work by providing a sound proof for our *k*NN query verification scheme, which utilizes the network Voronoi [9] diagram to generate a compact *VO*, as well as ensuring the completeness and correctness of the *k*NN query result with regard to both distances and paths. Furthermore, this paper proposes a pre-computation based verification scheme to accelerate the verification on mobile clients by utilizing the distance pre-computation. In addition, this paper includes a discussion on updates of the outsourced database. Subsequently, we propose two update modes: the one-by-one update mode and the batch update mode. Finally, we conduct extensive experiments using real-world and synthetic datasets to evaluate the verification performance and the database update cost.

4. IMPLEMENTATION

The Presence Cloud server overlay construction algorithm organizes the PS nodes into a server-to-server overlay, which provides a good low-diameter overlay property. The low-diameter property ensures that a PS node only needs two hops to reach any other PS nodes. To improve the efficiency of the search operation, Presence

Cloud requires a caching strategy to replicate presence information of users. In order to adapt to changes in the presence of users, the caching strategy should be asynchronous and not require expensive mechanisms for distributed agreement. In Presence Cloud, each PS node maintains a *user list* of presence information of the attached users, and it is responsible for caching the *user list* of each node in its PS list, in other words, PS nodes only replicate the *user list* at most one hop away from itself. The cache is updated when neighbors establish connections to it, and periodically updated with its neighbors. Therefore, when a PS node receives a query, it can respond not only with matches from its own *user list*, but also provide matches from its caches that are the user lists offered by all of its neighbors

a) Authentication data structure

To support the query verification, we need a well-defined authentication data structure (ADS) built on the outsourced data, which should be cryptographically signed by DO to ensure data integrity. Consider the outsourced database with a set of POIs P over an underlying road network G. In this work, we propose an elaborate authentication data structure in order to support k-nearest-neighbor query verification on road networks where the distances [10] from the query point to objects are measured by the shortest path on the graph with regard to the edge weight W. Given a set of POIs and the graph G, the network Voronoi diagram can be computed by applying parallel Dijkstra's algorithm where POIs are treated as multiple sources. In this algorithm, we employ a Fibonacci heap to expand the shortest path tree from all POIs in the graph until shortest path trees meet. For each POI, a set of border points is discovered and all the road segments in between the border points from the network Voronoi cell for that POI (generator). Note that the network Voronoi cell for any generator on the graph is unique because it contains a unique set of road segments.

b) Network kNN verification at the client

Generally, a query verification process consists of two sequential steps, that is, signature verification and geometry verification. As the signature verification step is a standard and straightforward procedure, it is only briefly discussed here and omitted from the following sections. On receiving the result of a kNN query, the client first examines the signature attached to the VO to ensure that all objects in the result set originated from DO. On receiving an aggregate signature, the client verifies the signature by employing the corresponding aggregate signature verification algorithm. Signature verification can ensure the proof data has not been falsified by SP or malicious attackers. Next, the client verifies the geometry property of the kNN result. The verification starts with verifying the first NN of the result. Recall that in the VO returned by the SP server, each POI p in the kNN result set is accompanied by its network Voronoi cell V(p) and its Voronoi neighbors Nbr(p). According to Property 5, we know that the query point q must be on a road segment inside the Voronoi cell of its first NN. Therefore, given the first NN p1 and its Voronoi cell V(p1), a client verifies that the query point q falls on one of the road segments inside V(p1). If this is true, the generator p1 is the first NN of q. Otherwise, p1 is not the first NN of q and the result is not correct. The actual distance and the shortest path from q to the generator p1 can be verifies using Dijkstra's algorithm or A* algorithm on the sub graph inside V(p1). Note that Lemma 1 ensures the shortest path from q to p1 is fully contained in V (p1). Therefore, the Voronoi cell V (p1) is sufficient for computing the shortest path from q to p1 on the client. As a result, both the first NN p1 and the shortest path from query point q to p1 can be verifies.

c) Top k-Query processing, VO construction, and verification

We assume the Power Diagram, together with its authenticated data structure, has been materialized on external storage [6]. Any data object, including its Power Voronoi cell, digest and signature, can be efficiently accessed using the corresponding id. As such, a top-k query can be incrementally processed. We introduce a formal security model and design two cryptographic building blocks (namely PPB and PLB) that can prove to the client the relation of rank values of two objects w.r.t. a query point without disclosing the locations and non-spatial scores[4]. We develop a complete set of authentication schemes for both the R-tree and Power Diagram based indexes. We propose strategies for both the data owner and the SP to optimize the storage cost of the PLB method. We conduct extensive experiments and security analysis to evaluate the performance and robustness of the proposed authentication schemes.

d) Performance comparison

In this section, we evaluate the performance of the network Voronoi diagram-based *k*-nearest-neighbor query verification approach through experiments. Our database outsourcing framework contains two phases: the offline database transformation phase on DO, and the online phase on SP and clients. In the offline phase, DO computes the network Voronoi diagram on the POI set and the underlying road network, and it then generates a signature for each POI by incorporating the authentication information into each POI object. In the online phase, SP evaluates queries and sends results to query clients on behalf of the DO, and then the client verifies the query result.

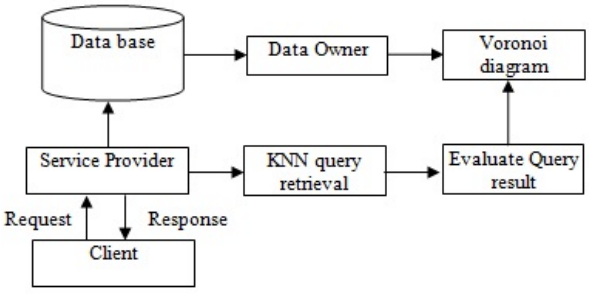

Figure-1. Proposed work.

The query Q is executed by the service provider (SP) on the dataset D, which is authorized and signed by the data owner (DO). The authentication problem is for the querying client to verify that the SP executes Q faithfully. For that we develop a complete set of authentication schemes for both the R-tree and Power Diagram based indexes. To this end, we design two new cryptographic building blocks, one with optimized online computation (the private-Paillier based method, or PPB) and the other with optimized offline computation (the pre-signed line based method, or PLB).

5. EXPERIMENTAL RESULTS AND DISCUSSION

Our implementation for the online query evaluation and verification is in Java. The server-side program (SP) runs on a Linux Server with an Intel Core2 Duo 2.13GHz CPU and 4GB memory. Meanwhile, the client-side query verification program runs on a HTC EVO 3D mobile device with the Google Android OS which communicates with the SP server via Internet connections through WiFi. The cryptographic operations are implemented using the SHA-256 digest algorithm (with 32-byte hash digest) and RSA-1024 signature algorithm (with 128-byte keys) from. Our experiments were performed on two real-world road networks obtained from: (i) **CA** which consists of the major freeways and highways in the state of California with a total of 21, 048 nodes and 22, 830 edges, and (ii) **BAY** which contains highways as well as surface streets with 174, 956 nodes and 223, 001 edges in the San Francisco Bay Area, California. Although the second network (BAY) covers a smaller geospatial region, the size of the network is larger than the California road network due to the inclusion of surface streets. Red color represents the proposed work and green is the existing work. Throughput Vs Time graph is shown below in Figure-2 that takes time along X-axis ranging from 0 to 50 ms and throughput of transmission along Y-axis ranging from 0 to 28 Kbps. It can be observed initially the throughputs of both existing and proposed are almost same. But when, time progress there is a significant throughput increase in proposed method (Figure-2).

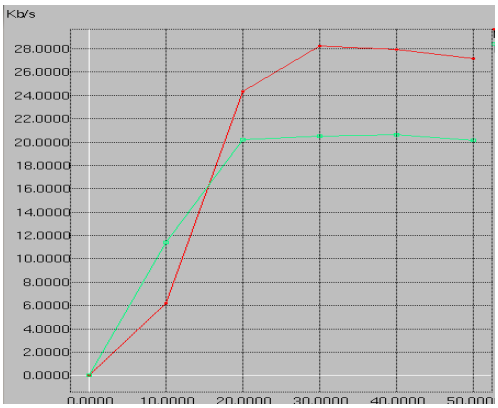

Figure-2. Throughput Vs Time.

In Figure-3, Packet Delivery Ratio (PDR) Vs Time graph is shown, where time ranging from 0 to 50 ms is taken along X-axis and PDR which is the ratio of successful packet reception to the total number of packet is taken along Y-axis ranging from 0 to 1. Rather than like throughput metric of previous graph, PDR of the proposed seems to be high even from the beginning over the existing system.

It is also essential to consider number of packets dropped similar to considering of packet delivered (i.e.., PDR). The following Figure-4, shows that maximum number of packets are dropped in existing but the proposed have very fewer packet drop achieving high packet delivery ratio with decrease in average packet drop ratio in the range of 0 to 1 along Y-axis where time as same as above graphs.

Figure-3. PDR Vs Time.

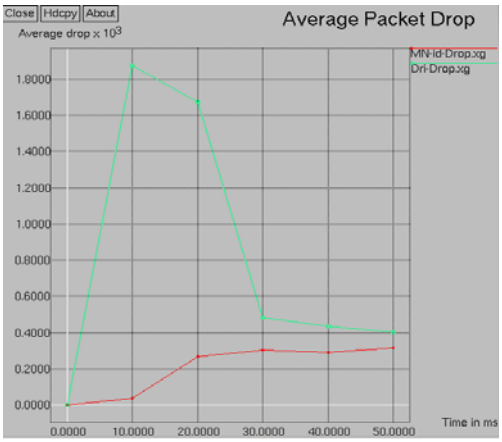

Figure-4. Average Packet Drop Vs Time.

6. CONCLUSIONS

In this paper, we studied the query verification problem for *k*-nearest-neighbor queries on road networks. While existing approaches proposed in this domain cannot verify both the distance and the shortest path to the *k*NN results simultaneously, we present a network Voronoi diagram-based verification approach that utilizes the network Voronoi cell of each result object to verify the

correctness and completeness of the *k*NN result with regard to both distance and path. In addition to the basic verification algorithm (NVD), an improved version (DIST) with pre-computed distances within each network Voronoi cell is presented for *k*NN query verification to further reduce the verification cost on mobile clients. Our experiments on real-world road networks show that both verification schemes generate compact verification objects and allow for efficient verification processes on modern mobile devices. In Future research will focus cryptographic building blocks of private ranking-value comparisons can be presented two authentication schemes based on modified multi-dimensional R-tree and Power Diagram indexes.

REFERENCES

[1] C. Cachin and M. Schunter. 2011. "A cloud you can trust," IEEE Spectrum, vol. 48, no. 12, pp. 28–51, December.

[2] A. Fiat. 1997. "Batch RSA," Journal of Cryptology, vol. 10, no. 2, pp. 75–88.

[3] W. Cheng and K.-L. Tan. 2009. "Query assurance verification for outsourced multi-dimensional databases," Journal Computer Security., vol. 17, no. 1, pp. 101–126.

[4] Y. Yang, S. Papadopoulos, D. Papadias and G. Kollios. 2008. "Spatial outsourcing for location-based services," in Proc. IEEE 24th ICDE, Cancun, Mexico, pp. 1082–1091.

[5] Y. Yang, S. Papadopoulos, D. Papadias and G. Kollios. 2009. "Authenticated indexing for outsourced spatial databases," VLDB J., Vol. 18, no. 3, pp. 631–648, June.

[6] K. Mouratidis, D. Sacharidis and H. Pang. 2009. "Partially materialized digest scheme: An efficient verification method for outsourced databases," VLDB J., Vol. 18, no. 1, pp. 363–381.

[7] W.-S. Ku, L. Hu, C. Shahabi and H. Wang. 2009. "Query integrity assurance of location-based services accesses outsourced spatial databases," in Proc. 11th Int. Symp. SSTD, Aalborg, Denmark, pp. 80–97.

[8] D. Papadias, J. Zhang, N. Mamoulis and Y. Tao. 2003. "Query processing in spatial network databases," in Proc. 29th VLDB, Berlin, Germany, pp. 802–813.

[9] M. R. Kolahdouzan and C. Shahabi. 2004. "Voronoi-based K nearest neighbor search for spatial network databases," in Proc. 13th Int. Conf. VLDB, Toronto, ON, Canada, pp. 840–851.

[10] H. Hu, D. L. Lee and V. C. S. Lee. 2006. "Distance indexing on road networks," in Proc. 32nd Int. Conf. VLDB, pp. 894–905.

[11] H. Samet, J. Sankaranarayanan and H. Alborzi. 2008. "Scalable network distance browsing in spatial databases," in Proc. SIGMOD, New York, NY, USA, pp. 43–54.

[12] K. C. K. Lee, W.-C. Lee, B. Zheng and Y. Tian. 2012. "ROAD: A new spatial object search framework for road networks," IEEE Trans. Knowl. Data Eng. Vol. 24, no. 3, pp. 547–560, March.

[13] H. Hacigümüs, B. R. Iyer, C. Li and S. Mehrotra. 2002. "Executing SQL over encrypted data in the database-service-provider model," inProc. SIGMOD, Madison, WI, USA, pp. 216–227.

[14] H. Pang and K.-L. Tan. 2004. "Authenticating query results in edge computing," in Proceedings of ICDE, Washington, DC, USA, pp.560–571.