Research on the path selection of mobile sink in dynamic sensor networks

Du Jie, Sang Kai

1.PINGDINGSHA INSTITUTE OF EDUCATION, Ping Ding Shan city ,HeNan, China

Key words: wireless sensor networks; range query; energy consumption; privacy protection

Abstract. put forward an agreement of safety range query that possesses privacy and completeness protection aiming at low-energy and high-privacy protection required by range query in two-level wireless sensor networks: SPQ（Secure probabilistic range query）. SPQ consists of technologies like data encryption, prefix member verification, probability neighbor validation and query transformation process separation and can ensure to complete range query in the circumstance of not disclosing privacy. Analysis and simulation results show: compared with other safety agreement, SPQ possesses lower energy consumption on the condition of safety guarantee of range query.

Introduction

With the continuous application and development of wireless sensor networks (Wireless Sensor Networks，WSNs）, data query tasks on them are increasing greatly and safety requirement in data query process is more and more important. WSNs data query can quickly gather partial effective data collected by WSNs or specific data to Sink (aggregation node) and then Sink will analyze and calculate query results to control WSNs or make other decisions. WSNs data query can be mainly divided into two kinds: firstly, sample query, carry out sample query operastion to data collected by WSNs. Present research hotspots mainly are range query, Top-k query, skyline query and based on type query. This kind of query is sample, universe and can be applicable to different WSNs; possess fine research value; secondly, complex query, process of query is complex and requires special query strategy; its university is not strong enough and generally aims at special WSNs.

Network model

Safety data query of WSNs (namely, research of privacy protection) is mainly based on two-level sensor networks model[10] (Fig.1）, without exception for query range. SPQ is agreement based on this model.
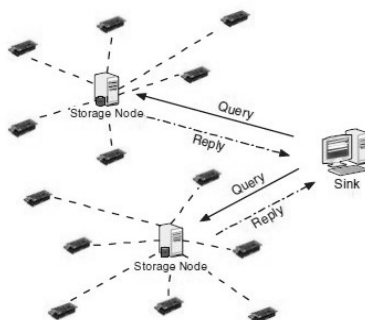

Fig1 Two-level Wireless Sensor Networks Model

As shown in Fig.1, high-level of this networks model consists of Storage Node; Storage Node (Storage Node) is sensor node with lager storage space and stronger calculating ability; basement consists of ordinary sensor node and ordinary node is resource-limited and low-cost. Query process of data is as follows: query (Query) requirements of users are transmitted to storage node by Sink and ordinary node transmits data to storage node for storage after ordinary node collects data; inquire and calculate on storage node; transmit the query reply (Reply) back to Sink and to users in the end.

WSNs data query possesses the following advantages if selecting two-level model: ① ordinary sensor node only needs to transmit collected data to nearby storage node, not transmitting to Sink node by long path, which decreases energy-consumption greatly and avoids Sink node encountering communication bottleneck; ② Sink can only communicate with storage node and get query result, which makes query process more efficient.

Query agreement of WSNs safety range

As for WSNs, amount of energy-consumption is constraints for considering whether to carry out safety strategy. Objective of SPQ is to try to decrease energy-consumption on the condition of guarantee query safety.

3.1 Key technology

3.1.1 Data encryption

In SPQ, every ordinary sensor node s_i will share a secret key k_i with Sink and k_i shall be replaced regularly. Data $d_1,\cdots,d_n$ collected by s_i ordinary node will be encrypted by k_i in the process of query. Even storage node that completes query process and collects query results to be uploaded to Sink cannot obtain specific data information. This ensures privacy of data.

3.1.2 Premix member verification

Storage node still needs to complete query process in the condition that specific data cannot be identified, which makes use of verification technology of premix member.

Verification technology of premix member transforms the condition whether verification data conforms to query range to compare the size of data items, for example, judging whether data 12 conforms to range query [11, 15]. Binary representation of 12 is 1100, firstly, establishing premix family and getting ｛1100 110* 11** 1*** ****｝, then carrying out premix numeralization and obtaining ｛11001 11010 11100 11000 10000｝; at the same time, binary representation of [11,15] is [1011,1111], namely, ｛1011 1100 1101 1110 1111｝, firstly, carrying out premix transformation and getting ｛1011 11**｝, then carrying out premix numeralization and obtaining ｛10111 11100｝. In the final premix numeralization sets, they have the same item 11100, which means data 12 conforms to range query [11, 15]. On the opposite, if there is no same item, this data does not conform to the condition of query range.

In SPQ，apply verification technology of premix member with three hash functions. Three hash functions [11-13] respectively are Φ，Ψ，Ω.

3.1.3 Probability neighbor validation

Completeness verification of SPQ query results will be realized by technology of probability neighbor validation. Namely, ordinary node s_i generates message $(t,i,len$）after getting search result and transmits this message to nearby neighbor validation. Therein, t is time period, i is No. of sensor and l is number of data item that meets query. Then every neighbor validation is randomly added （t,i,len) to its query results and encrypted to upload qith certain probability p ; Sink carries out completeness verification of query results according to every （t,i,len) after receiving query results.

3.2 SPQ one-dimensional data query process

WSNs range query can be divided into one-dimensional data query and multi-dimensional data query according to different dimensions of data item. The process of multi-dimensional data query is the most simple. With the increase of dimension, generally, energy consumption of multi-dimensional data query presents exponential growth. SPQ shall try to avoid this circumstance and improve energy consumption of different dimensions.

During one-dimensional data query, realization process of SPQ is as shown in the following pseudocode. Therein, Sink is aggregation node, Storage Node is storage node and s_i、s_j are ordinary node.

① Sink→Storage Node: $t, \Omega([a,b])$
　　s_i→Storage Node: $i,t, \Psi(d_1,\cdots,d_n)$

② Storage Node:

```
for j=1 to n do
    if(F(j, Ψ(d₁,···,dₙ), Ω([a,b]))=1)
        len++
        min_d=min(min_d,j)
        max_d=max(max_d,j)
    endif
next j
Storage Node→sᵢ:i,t,min_d,max_d,len
```

③ $s_i \to s_{i\_neighbor}$: t,i,len

④ $s_i \to$ Storage Node $\to$ Sink:

$\{(t, i\_neighbor,len)_p, d_{min\_d-1}, \cdots, d_{max\_d+1}\}_{ki}$

Specific query details are as follows:

① Ordinary node s_i gets $d_1, \cdots, d_n$, after collecting certain data and ranking order; apply the first hash function Ψ and encrypt to get fix-length message code $\Psi(d_1, \cdots, d_n)$; send $\Psi(d_1, \cdots, d_n)$ to storage node. When Sink will carry out query $\{t,[a,b]\}$, Sink will settle query range with another function Ω and will finally send $\{t, \Omega([a,b])\}$ to storage node.

② As for the third function Φ when storage node settles query, when $\Phi(j, \Psi(d_1, \cdots, d_n), \Omega([a,b]))$ is true, then d_j meets query condition; when $\Phi(j, \Psi(d_1, \cdots, d_n), \Omega([a,b]))$ is false, then d_j does not meets query condition and shall be abandoned. Storage node will meet the minimum data and maximum No. of query condition and data number $(min\_d, max\_d, len)_i$ will be fed back to s_i.

③ After s_i receiving feedback result, find out all middle data $d_{min\_d}, \cdots, d_{max\_d}$ including min_d and max_d and add d_{min-1}（if $min\_d-1<1$，then select $d_{min\_d-1} = -1$）, d_{max_d+1}（if $max\_d+1>n$，then select $d_{max\_d+1} = \infty$）. s_i generates message (t,i,len) and sends this message to nearby neighbor node. Therein, t is time period, i is No. of sensor and len is data number that meets query.

④ If s_i receives message $(t, i\_neighbor,len)$ sent by neighbor node $s_{i\_neighbor}$, it will add this message to query result that needs to be uploaded by itself with certain probability p, namely, it will upload $\{(t, i\_neighbor,len)_p, d_{min\_d}, \cdots, d_{max\_d}\}_{ki}$ in the end. Therein, k_i is shared secret key of s_i and Sink.

Uploading data will be sent to Sink through storage node; Sink will carry out completeness verification to all query results and then SPQ is in the end.

3.3 Query process of SPQ multi-dimensional data

Because in real application, application scenarios of range query generally aims at multi-dimensional data, it is necessary to apply SPQ agreement to multi-dimensional data query. Next, briefly describe SPQ query process:

① After ordinary node s_i collects n of m-dimension data $(d_1^1, d_1^2, \cdots, d_1^m), \cdots, (d_n^1, d_n^2, \cdots, d_n^m)$, apply the first hash function to encrypt to get m of fixed-length message codes $\Psi(d_1^1, \cdots, d_n^1)$, $\Psi(d_1^2, \cdots, d_n^2)$, $\Psi(d_1^m, \cdots, d_n^m)$ and send to storage node. When Sink will carry out query $\{t,([a^1,b^1], \cdots, [a^m,b^m])\}$, Sink will process query range with another function Ω and will finally send $\{t, \Omega([a^1,b^1]), \cdots \Omega([a^m,b^m])\}$ to storage node.

② As for the third function Φ when storage node processes query, when $\Phi(j, \Psi(d_1^t, \cdots, d_n^t), \Omega([a^t,b^t]))$ (therein, $1=<t<=m$) is true, then d_j meets query condition on dimension t; when $\Phi(j, \Psi(d_1^t, \cdots, d_n^t), \Omega([a^t,b^t]))$ is false, then d_j does not meets query condition on dimension t and shall be abandoned. When completing all dimensions, intersection that seeks for No. will obtain final search result; storage node will feed back data No. max and min value $\{(min\_d^1, max\_d^1), \cdots, (min\_d^m, min\_d^m), len\}$ that meets query condition to s_i.

s_i rank orders for uploading data in query process according to a value on dimension t randomly. After receiving feedback result, find out all data that conforms to conditions and encrypts the data according to query results.

③、④ are the same with query process of one-dimensional data.

Performance analysis

This paper simulates SPQ and SafeQ by using original data sets on MATLAB platform; 100 ordinary nodes randomly distributed in area with length and width both of 300m. 4 storage nodes are distributed relatively even and a Sink node is placed in the middle. Suppose that the effective transmission distance of sensor nodes is 75m; establish route and path by making use of TAG （tiny aggregation service for ad hoc sensor networks） algorithm. It needs averagely 1.8 sauts that every ordinary node transmitting data to storage node. Every node averagely has 20 neighbor nodes. Probability of sending verification message to every neighbor node is 0.4.

Inn simulation experiment, energy consumption value refers to specific energy consumption divided by time, namely, a value that analogy power measures energy consumption level; effective query ratio is specific ratio between effective data size and consumptive energy that are obtained by final query result of storage node, which reflects utilization efficiency of networks energy of the agreement.

Experiment mainly compares energy consumption when SPQ and SafeQ inquire different dimension data. In order to ensure correctness of experimental result, all experiments adopt same real data sets; one-dimensional data sets and two-dimensional data sets are one dimension and two dimensions that are peeled off from three-dimensional data sets, namely, the number of data item of query results received in unit time in the experiment with different dimensions shall be the same.

Energy consumption contrast condition of SPQ and SafeQ of the first group of experiment on the condition of one-dimensional data:
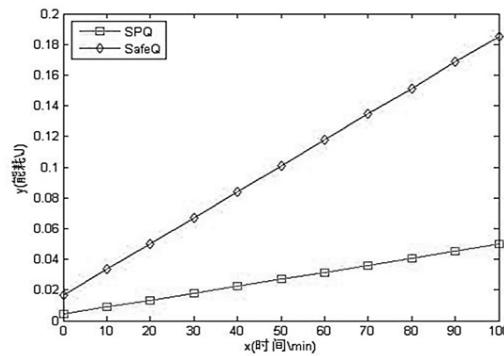

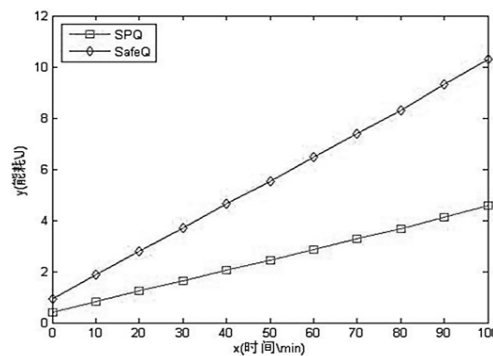Fig. 2 Average Energy Consumption Contrast of Ordinary Node of One-dimensional Data Query

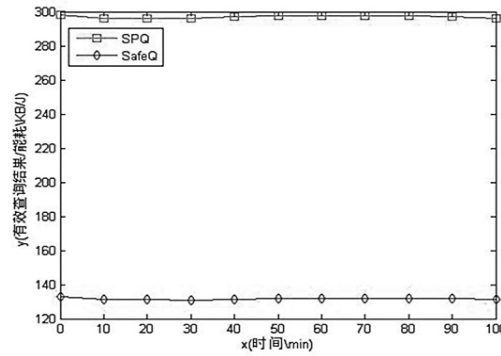Fig. 3 Average Energy Consumption Contrast of Storage Node of One-dimensional Data Query

Fig. 4 Contrast of Effective Query Ratio of One-dimensional Data Query

By comparing results of experiment, when aiming at one-dimensional data query, in the condition of same data sets source, energy consumption of SPQ ordinary node is 3.2 times lower than that of SafeQ; energy consumption of SPQ storage node is 2.5 times lower than that of SafeQ. Effective query ratio of SPQ is 2.2 times that of SafeQ. On the condition of one-dimensional data, energy consumption of SPQ is obviously lower than that of SafeQ.

Conclusion

Privacy protection of SPQ agreement put forward by this paper will be realized by verification technology of premix member; completion verification of data will be accomplished mainly by probability neighbor verification technology and communication traffic (namely, energy consumption) will be decreased by a series of communication strategy. The objective is to make it superior to exsisting SafeQ and based on barrel-mode range query. Although exsisting agreement has lower energy consumption and better safety performance compared with SPQ, it still has higher energy consumption compared with query strategy without privacy protection. Safety strategy or communication method shall be further sought for in order to better promote safety data query.

Reference

[1] Jinyu Hu and Zhiwei Gao. Distinction immune genes of hepatitis-induced heptatocellular carcinoma[J]. Bioinformatics, 2012, 28(24): 3191-3194.

[2] Jinyu Hu, Zhiwei Gao and Weisen Pan. Multiangle Social Network Recommendation Algorithms and Similarity Network Evaluation[J]. Journal of Applied Mathematics, 2013 (2013).

[3] Lv Z, Li X, Zhang B, et al.. Managing Big City Information Based on WebVRGIS. IEEE Access, 2016, 4: 407-415.

[4] Yang J, Lin Y, Gao Z, et al. Quality Index for Stereoscopic Images by Separately Evaluating Adding and Subtracting[J]. PloS one, 2015, 10(12): e0145800.