ARTICLE IN PRESS

Pervasive and Mobile Computing ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

journal homepage: www.elsevier.com/locate/pmc

An energy conservation indexing method for secure XML data broadcast in mobile wireless networks

Leila Fathi, Hamidah Ibrahim *, Meghdad Mirabi

Department of Computer Science, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400, Serdang, Selangor, Malaysia

ARTICLE INFO

Article history:
Received 15 February 2013
Received in revised form 24 August 2013
Accepted 29 August 2013
Available online xxxx

Keywords:
Access control
Data confidentiality
Indexing
Mobile wireless broadcast
XML query processing
XML stream

ABSTRACT

Secure broadcasting of XML data is becoming an essential requirement for many applications in mobile wireless networks. Several indexing methods have been proposed to reduce the tuning time in processing the XML queries over the wireless XML stream. Tuning time is the sum of period of times which a mobile client stays in active mode in order to retrieve the required data over the wireless stream. Therefore, it is frequently used to estimate the energy consumption of a mobile client. The problem of existing indexing methods is that they cannot directly be applied to an encrypted XML stream since mobile clients can only access the authorized parts of the XML data in an encrypted XML stream. In this paper, we define a unit structure of an XML stream called SecNode which guarantees confidentiality of the XML data in the wireless stream. We also define two indexes called Min (NCS) and Min (NIS) for the SecNode structure based on the set of access authorizations specified in the original XML document in order to efficiently process the XML queries over the encrypted XML stream. Experimental results show that the use of the SecNode structure for secure XML data broadcast improves the performance of XML query processing in terms of tuning time and therefore reduces the power consumption at mobile clients.

1. Introduction

As XML (eXtensible Markup Language) [1] is emerging as a standard for data dissemination over the Internet, the use of XML for data broadcasting in wireless networks is rapidly increasing. Recently, many applications are using XML for data broadcasting in wireless environments such as traffic and travel information systems and weather information systems.

Generally, data access via wireless networks can be classified into two categories: point-to-point data access and broadcast data access [2–4]. In the point-to-point data access, mobile clients send their queries to the server and the server processes these queries and returns the query results to mobile clients over a point-to-point channel. In the broadcast data access, the broadcast server disseminates information to a large number of mobile clients through a public broadcast channel which is shared by mobile clients and mobile clients listen to the channel and retrieve their desired information without consuming energy to send their requests to the broadcast server. Therefore, data broadcasting can reduce network bandwidth and energy consumption of mobile devices.

In mobile wireless networks, access efficiency and energy conservation of mobile clients are two important issues since mobile clients carry small, battery powered hand-held devices with limited data processing capability [4,5].

* Corresponding author. Tel.: +60 3 89471713.
E-mail addresses: leila.fathi67@gmail.com (L. Fathi), hamidah@fsktm.upm.edu.my, hamidah.ibrahim@upm.edu.my (H. Ibrahim), meghdad.mirabi@gmail.com (M. Mirabi).

1574-1192/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.pmcj.2013.08.004

Two different performance metrics are used to measure the access performance of a stream in a wireless broadcast channel: Access Time and Tuning Time [2,4,6]. Access time is the period of time from the moment a mobile client submits a query to the moment the query results are retrieved by the mobile client. Therefore, it is used to measure access efficiency in a wireless broadcast channel. Tuning time is the sum of period of times which a mobile client stays in active mode in order to retrieve the required data which are index information and query results. Therefore, it is frequently used to estimate the energy consumption of a mobile client. When a mobile client listens to the broadcast channel and receives its requested data from the stream in the energy consumption mode (active mode), it consumes much more energy than when it is in the energy saving mode (doze mode).

In public networks like a wireless broadcast network, the XML data must be encrypted before sending the XML data over the network in order to guarantee data confidentiality. In these networks, the delivery of the XML data to the mobile clients must obey a set of access authorizations specified on the XML data [7–9]. Mobile clients must only access the authorized parts of the XML data based on their access authorizations.

Several indexing methods are proposed to reduce the tuning time such as those proposed by [4,5,10,11]. However, these indexing methods are not applicable to be used for the XML data since they are designed for flat data records identified by keys while the XML data are semi-structured and can be accessed by XML query languages like XPath [12] and XQuery [13].

A lot of researches have been done to efficiently process XML queries over the XML data in wired networks with high bandwidth and server processing capacity such as the approaches proposed by [14–28] but they cannot be used for XML query processing over an XML stream in a wireless broadcast channel since the wireless broadcast channel has low bandwidth capacity and mobile clients carry battery powered hand-held devices with limited data processing capacity.

Recently, several indexing methods have been proposed to selectively access the XML data over an XML stream in a mobile wireless broadcast network such as the methods proposed by [29–31]. However, these indexing methods cannot directly be applied to an encrypted XML stream since mobile clients can only access the authorized parts of the XML data in an encrypted XML stream instead of accessing the whole of the XML stream. In order to selectively access the XML data over an encrypted XML stream, an efficient indexing method is required to specify the authorized parts of the XML data in the stream.

Let us consider an XML tree as shown in Fig. 1. In Fig. 1, each XML node is assigned with three rectangles where the left, middle, and right rectangles represent the accessibility of the XML node to mobile clients of groups g_1, g_2, and g_3, respectively. In Fig. 1, the gray rectangles represent accessibility of the XML nodes to mobile clients of the different groups while the white rectangles represent non-accessibility of the XML nodes to mobile clients of the different groups. For example, the node "Border" is accessible to the mobile clients of group g_2 but not to the mobile clients of groups g_1 and g_3.

Fig. 2 shows a broadcast stream of the XML tree illustrated in Fig. 1. The broadcast server first encrypts all of the XML nodes separately with different keys and then organizes the encrypted XML nodes in the preorder sequence and broadcasts them on the air. In Fig. 2, it is assumed that all of the XML nodes are labeled with the pre/post labeling scheme proposed in [32] since the XML nodes in the stream are encrypted separately and the structural relationships between the different XML nodes in the stream must be determined during the process of XML querying over the stream. The pre/post labeling scheme is able to determine all types of structural relationships between the different XML nodes. An example of an XML tree labeled by the pre/post labeling scheme is illustrated in Fig. 1 where the preorder, postorder, and depth values are assigned to each XML node in the XML tree.

In the conventional approach to process an XML query over an encrypted XML stream, each mobile client first decrypts each encrypted XML node in the stream if it has the appropriate key for decryption and then searches the XML nodes in the stream satisfying the XML query path. Assume that a mobile client c_1 which is a member of the group g_1 listens to the broadcast channel and queries "/Mondial/Country/City/Name" before the root node is broadcast. The mobile client c_1 can only decrypt the gray nodes in the stream shown in Fig. 2 since it only has the set of keys for decrypting them based on the set of access authorizations specified for the members of the group g_1 in the XML tree shown in Fig. 1. In this case, the mobile client c_1 must decrypt 15 encrypted XML nodes (the number of gray nodes is 15) in the stream to find three candidate nodes "Name" (i.e. the nodes with the preorder 7, 10, and 14). Such a process consumes a lot of energy to decrypt the XML nodes and find all of the candidate nodes satisfying the XML query "/Mondial/Country/City/Name".

Motivated by the above example, this paper considers efficient ways to guarantee confidentiality of the XML data in the stream and selectively access the XML data over the XML stream in a wireless broadcast channel. Hence, the main contributions of this paper are summarized as follows:

- We define a unit structure of XML stream called SecNode which guarantees confidentiality of the XML data in the wireless stream. The SecNode structure contains the XML data and index information.
- We define two indexes called Min (NCS) and Min (NIS) for the SecNode structure based on the set of access authorizations specified in the original XML document in order to selectively access the XML data over the encrypted XML stream. The Min (NCS) index is used to jump forward to the next accessible candidate node which may be the query answer while the Min (NIS) index is used to skip the irrelevant accessible nodes of the XML query.
- We propose algorithms to generate an encrypted XML stream based on the SecNode structure and process the simple path XML queries over the encrypted XML stream.
- We propose a method to process the twig pattern XML queries having predicate conditions at the different steps of the XPath expression by decomposing the twig pattern XML query into several simple path XML queries.

Please cite this article in press as: L. Fathi, et al., An energy conservation indexing method for secure XML data broadcast in mobile wireless networks, Pervasive and Mobile Computing (2013), http://dx.doi.org/10.1016/j.pmcj.2013.08.004