Computer Communications 65 (2015) 27–34

Contents lists available at ScienceDirect

Computer Communications

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

Social role-based secure large data objects dissemination in mobile sensing environment

Mande Xie [a,*], Urmila Bhanja [b], Guoping Zhang [c], Guiyi Wei [a], Yun Ling [a]

[a] School of Computer Science and Information Engineering, Zhejiang Gongshang University, Hangzhou, Zhejiang 310018, PR China
[b] Dept. of Electronics and Telecommunication Engineering, Indira Gandhi Institute of Technology, Sarang, Odisha 759146, India
[c] School of Information Science and Technology, Zhejiang Sci-Tech University, Hangzhou, Zhejiang 31001, PR China

ARTICLE INFO

Article history:
Available online 21 February 2015

Keywords:
Network coding
Authentication
Hash function
Proxy re-signature

ABSTRACT

At present, in mobile sensing environment, almost all the existing secure large data objects dissemination algorithms are centralized. The centralized servers publicize the sensing tasks and are also the authorized parties to initiate sensed data dissemination. This paper proposes a novel social role and network coding based security distributed data dissemination algorithm referred as PRXeluge to overcome the shortcomings of existing centralized data dissemination algorithms. Unlike the existing participatory sensing applications, in PRXeluge, service provider just publicizes the sensing tasks and utilizes a conditional proxy re-signature technique to authorize different social roles such as authorized smartphone users to be utilized as a contracted picture reporters, which sense the data and directly disseminate the sensed large data. Furthermore, PRXeluge proposes the XOR (Exclusive-OR) network coding scheme on the basis of Seluge security framework. To maximize the number of successfully decoded packets, PRXeluge introduces a neighbor node table to determine the optimal coding scheme. Experimental results reveal that the proposed PRXeluge shows better performance in terms of lower data packet transmission and dissemination delay compared to that of Seluge. Furthermore, it is observed from the experiment that the proposed algorithm is stronger as compared to that of centralized scheme and performs the fine grain access control without giving any additional load to subscriber nodes.

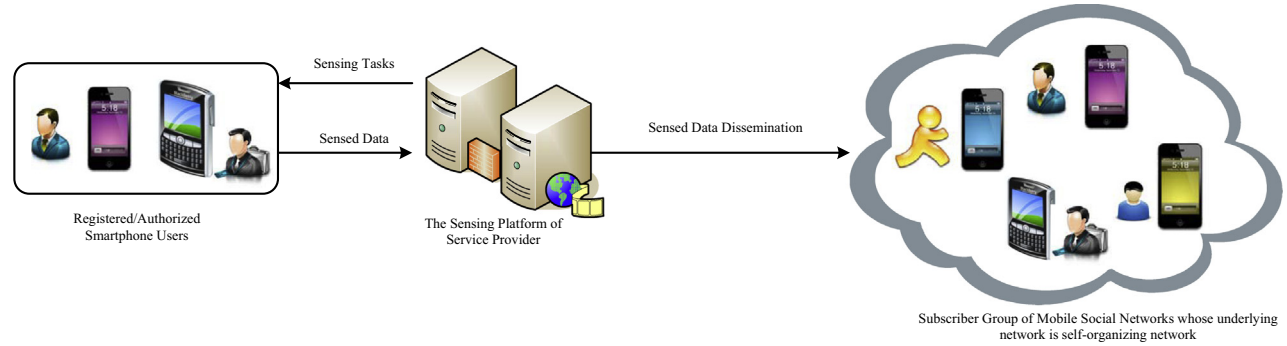
1. Introduction

With growing popularity of smartphones, according to statistics till date, the current global smartphone ownership has exceeded 1.9 billion and mobile data traffic is predicted to grow further by over 100 times in the next ten years. Various sensors embedded in smartphones such as photosensitive sensors, Global Position System (GPS), accelerometer, bidirectional microphone and high-resolution cameras, provide smartphone users very convenient and powerful data-aware capabilities. Mostly participants in social networking applications share real-time perceived multimedia data or participate in a variety of hot events multimedia data-aware services through smartphones or other mobile sensing devices [1]. The great potential of the mobile phone sensors led the researchers to develop various related applications and systems. Fig. 1(a) shows a traditional framework of these applications. These systems generally consist of a service provider, which consists of multiple sensing servers, many smartphone users, and the subscriber group of mobile social networks. First, the service provider discloses the sensing tasks and then the registered or authorized smartphone users such as the contracted picture reporters send the sensed data to the corresponding service provider. Finally, the service provider disseminates the sensed data such as the pictures of hot event to the subscribers. In the centralizing framework, the centralized servers are highly susceptible to attack targets and it is easy to produce a single point failure (such as Deny of Service (DoS) attack).

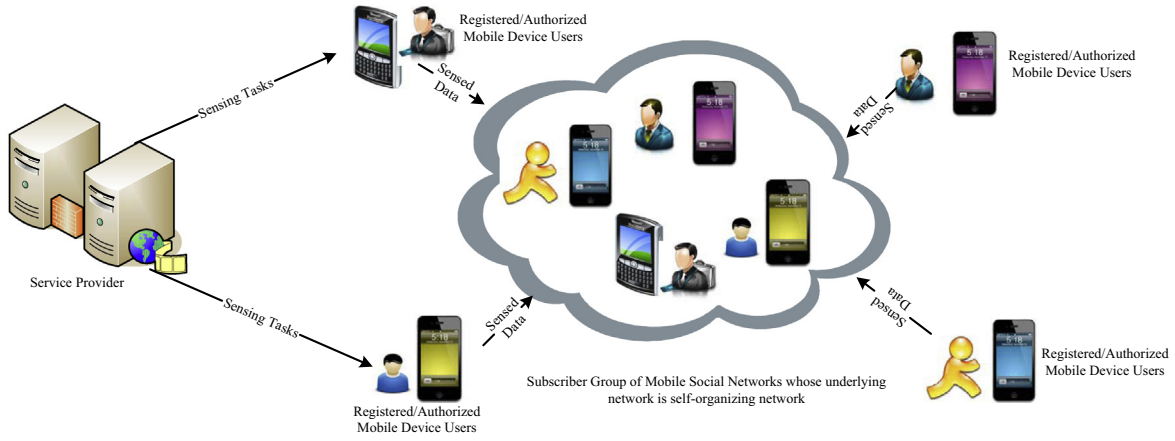
In this paper, as shown in Fig. 1(b), the framework of the distributed data dissemination is employed. In the distributed framework, the service provider only publicizes the sensing tasks and the registered or authorized smartphone users sense the data and disseminate directly the sensed data to the subscribers. In the distributed framework, the secure transmission or dissemination of large data objects is very significant and hot topic these days. This paper mainly discusses the following four significant points.

* Corresponding author.
E-mail addresses: berniexie@gmail.com (M. Xie), urmilabhanja@gmail.com (U. Bhanja), zgp4508@zstu.edu.cn (G. Zhang).

http://dx.doi.org/10.1016/j.comcom.2015.02.007
0140-3664/



(a) The Framework of centralized sensed large data dissemination in mobile sensing envirnoment



(b) The framework of distributed sensed large data dissemination in mobile sensing environment

Fig. 1. The framework of sensed large data dissemination in mobile sensing environment.

(1) The authentication of the smartphone users.
(2) To withdraw the malicious authorized users.
(3) To verify the authentication of the received sensed data immediately after reception.
(4) To perform the fine grain access control. For example, the authorized smartphone users just are permitted to disseminate the sensed data to the special subscriber group.

This paper proposes a social role-based secure distributed large data dissemination algorithm in mobile sensing environment to address the above mentioned four issues. The main contributions of the proposed algorithm are as follows.

- A social role based distributed Large Data Object (LDO) dissemination framework, named PRXeluge, is proposed involving the service provider or network owner, authorized smartphone users, and the subscriber groups of mobile social networks. In the new framework, the service provider is not directly involved in the sensed data dissemination and a conditional proxy re-signature technique is utilized to authorize different smartphone users. By the conditional proxy re-signature technique, the fine-grain access control is performed. For example, the authorized smartphone users just are permitted to disseminate the sensed data to the special subscriber group.
- A XOR network coding method is introduced in the proposed algorithm. The neighbor node table is proposed to find the optimal coding scheme. With just one data packet transmission, each node can obtain required packet through the optimal coding scheme. Hence, there is a reduction in the number of transmitted packets. Furthermore, the neighbor node table is extended where, two additional fields SC (Sending Counter) and RC (Receiving Counter) are introduced. Based on the extended neighbor table, a counter method for Anti-DOS attacks is proposed.
- The security framework of Seluge [2] and XOR network coding method are seamlessly integrated into PRXeluge. PRXeluge shows similar security performance as that of Seluge and exhibits better performance than Seluge in terms of reduction in the transmitted data packets and dissemination delay. Furthermore, compared to the centralized scheme, PRXeluge does not bring any additional load to the subscriber nodes, and exhibits stronger performance in terms of fine grain access control.

The rest of this paper is organized as follows: Section 2 introduces the related work. Section 3 gives out the framework of the PRXeluge protocol. In Section 4, the preprocessing of sensed LDO is described. Section 5 describes networking coding and transmission of packets. The security analysis is given in Sections 6 and 7 explains the experimental results. At last, a brief summary is drawn in Section 8.

2. Related work

In mobile sensing environment, participatory sensing applications in the social networks have attracted great attention from researchers. In [3–5], some incentive mechanisms for participatory sensing are proposed. For example, Wang et al. propose a mechanism based on anonymous reputation and trust to solve the problem of "trust without identity" in participatory sensing networks [3]. Yang et al. propose an auction-based incentive mechanism and an incentive mechanism using a Stackelberg game for the mobile phone sensing [4]. Koutsopoulos et al. focus on the optimal