Information Sciences 284 (2014) 130–141

Contents lists available at ScienceDirect

Information Sciences

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

PHDA: A priority based health data aggregation with privacy preservation for cloud assisted WBANs

Kuan Zhang [a,*], Xiaohui Liang [a], Mrinmoy Baura [a], Rongxing Lu [b], Xuemin (Sherman) Shen [a]

[a] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada
[b] School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore 639798, Singapore

ARTICLE INFO

Article history:
Received 26 August 2013
Received in revised form 26 May 2014
Accepted 4 June 2014
Available online 20 June 2014

Keywords:
Wireless body area network
Cloud
Priority
Aggregation
Privacy preservation

ABSTRACT

Wireless Body Area Networks (WBANs), as a promising health-care system, can timely monitor human physiological parameters. Due to the limitation of communications, power, storage and computation in WBANs, a cloud assisted WBAN flourishes and provides more reliable, real-time, and intelligent health-care services for patients and mobile users. However, it is still critical to efficiently aggregate the different types of WBAN data to the cloud server. In addition, security and privacy concerns are also of paramount importance during the communications between WBAN and cloud. In this paper, we propose a priority based health data aggregation (PHDA) scheme with privacy preservation for cloud assisted WBANs to improve the aggregation efficiency among different types of health data. Specifically, we first explore social spots to help forward health data and enable users to select the optimal relay according to their social ties. According to different data priorities, the adjustable forwarding strategies can be selected to forward the user's health data to the cloud servers with the reasonable communication overheads. The security analysis demonstrates that the PHDA can achieve identity and data privacy preservation, and resist the forgery attacks. Finally, the performance evaluation shows that the PHDA achieves the desirable delivery ratio with reasonable communication costs and lower delay for the data in different priorities.

1. Introduction

Wireless Body Area Networks (WBANs) which can real-timely monitor patients or users' health status play an essential role in heath-care systems as the phenomenon of aging population and the demands of remote health monitoring in our daily life [24]. WBANs provide a variety of services in diverse fields including medical or personal health monitoring, consumer electronics, entertainment, sports or fitness, and military applications. Different physiology parameters, such as temperature, blood pressure, and electrocardiography (ECG) can be collected by WBANs [18]. With the increasing demands from customers and patients, the sensing data is required to be timely processed and the feedback from the doctors is also desirable. Since it requires more network resources, i.e., storage, computation and communication power, it is difficult to achieve these goals only relying on the traditional WBANs [9]. Therefore, the cloud computing is introduced to assist WBANs to store and process the sensing data in a real time fashion.

* Corresponding author. Tel.: +1 5198884567.
E-mail addresses: k52zhang@bbcr.uwaterloo.ca (K. Zhang), x27liang@bbcr.uwaterloo.ca (X. Liang), mbarua@bbcr.uwaterloo.ca (M. Baura), rxlu@ntu.edu.sg (R. Lu), xshen@bbcr.uwaterloo.ca (X. (Sherman) Shen).

http://dx.doi.org/10.1016/j.ins.2014.06.011
0020-0255/

Taking the advantage of the cloud server to store the large volume of sensing data and process them for doctor's diagnosis [2,8], cloud assisted WBANs become more robust and provide the desirable services for patients and users. For example, in a gym or conference environment, many people have some social activities [27], and wear WBANs to sense their health data and to periodically report them to the cloud servers. The hospital or doctors to access the data stored in the cloud servers in a real time pattern. Then, the doctors (trusted authorities) are able to timely detect the abnormal phenomenon and feedback the corresponding diagnosis. Once a user has an emergency, WBANs can help him call the hospital and continuously upload the real-time health data. However, when a large number of users located at the same place upload their data at the same time, the connection between WBANs and cloud servers might be intermittent. The available bandwidths from WBANs to cloud servers for each individual user are also limited so that the network performance is considerably degraded. Therefore, the communications between WBANs and cloud servers is the bottleneck with the perspective of efficiency and reliability.

Some existing research works [13,15] utilize cooperation among users to improve the reliability. Recent emergency call schemes [12] for health-care applications usually adopt the epidemic dissemination to deliver the general emergency information to the cloud server or hospitals. Even though it can guarantee the emergency call's delivery ratio and minimal delay, the communication costs are still very high. In the above example, some detailed physiology parameters of the patients with the emergency should be continuously uploaded to the cloud server for the further diagnosis and monitoring. If this portion of data is still epidemically disseminated in the network, it consumes an extreme large number of network resources. Therefore, the health data should be classified into different categories with different requirements (i.e., delay) and communication strategies. As communications are deeply involved in cloud assisted WBAN, security and privacy are of paramount importance [23]. All the data transmitted in health-care applications should be authenticated and secure against malicious modification. For example, an attacker might forge a fake emergency call and make it distributed in the network to degrade the network performance. In addition, privacy is also a primary concern from customers point of view, as health data is highly relevant to users themselves, for example, the ECG can reflect people's some specific behaviors, such as sleeping, having meals etc. As a result, the reveal of such health data might violate user's privacy. Therefore, how to efficiently aggregate different types of data and preserve user's privacy is still challenging in cloud assisted WBANs.

In this paper, we propose a priority based health data aggregation scheme (PHDA) with privacy preservation for cloud assisted WBANs to reduce the aggregation overheads and preserve user privacy. The health data is divided into different types, and each type of data is assigned a specific priority. When a user wants to upload his data, he can select different forwarding strategies according to his data's priority. The intuition is that the data with higher priority can be forwarded in a smaller delay. Furthermore, the data with the same priority can be efficiently aggregated which significantly reduces the communication overheads. Specifically, the major contributions of this paper are threefold.

- Firstly, we propose a priority based data aggregation scheme (PHDA) for cloud assisted WBANs. The health data is divided into different types assigned corresponding priorities. Different forwarding strategies are selected according to the data priority. Furthermore, the PHDA enables social spots to help mobile users forward the data to the cloud servers. An eligible relay can be selected based on his social tie to the social spots, which reflects the relay's forwarding capability.
- Secondly, we investigate a lightweight privacy-preserving aggregation scheme with aggregate authentication. The cloud servers can only learn the statistical information without knowing the exact data of individual user. The proposed aggregate authentication scheme can validate the data priority for users which resists the forgery attack, while reducing the authentication overhead.
- Finally, we provide the security and privacy analysis to show that the PHDA can achieve identity and data privacy preservation and resist the forgery attack. In additional, the performance evaluation shows that the PHDA satisfies the delay and delivery ratio requirements for the data with different priorities and consumes lower communication overheads compared with other schemes.

The remainder of this paper is organized as follows: The related works are investigated in Section 2. Network model and design goals are presented in Section 3. In Section 4, we propose the detailed PHDA, followed by the security analysis and performance evaluation in Sections 5 and 6, respectively. Finally, Section 7 concludes the paper.

2. Related work

Recently, there are several research works [1,28] on data forwarding different applications. An effective approach is to pre-deploy some fixed nodes in the network to help mobile users forward their data. Aviv et al. [1] investigate the human mobility patterns and propose a forwarding protocol, named Return-to-Home, which enables the fixed social spots to help mobile users store-and-forward the packets and improves the forwarding efficiency. Lu et al. [15] propose a social spot aided packet forwarding protocol (SPRING) in vehicular ad hoc networks. The SPRING follows the Return-to-Home principle and preserves user privacy at the same time. Zhang et al. [28] investigate a novel social spot deployment to preserve the location privacy for both the users and social spots. Despite the social spots, our PHDA also enables mobile users to help forward the data to social spots so that the data forwarding efficiency is further improved. In addition, some research efforts are paid to investigate data forwarding in health-care systems. Borrego et al. [7] investigate a new paradigm, called store-carry-process-and-forward, based on mobile code to improve the integration of wireless sensor networks and grid computing