Future Generation Computer Systems 52 (2015) 125–136

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

A reliable recommendation and privacy-preserving based cross-layer reputation mechanism for mobile cloud computing

Hui Lin[a], Li Xu[a,*], Yi Mu[a,b], Wei Wu[a]

[a] Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou, China

[b] School of Computer Science and Software Engineering, University of Wollongong, Wollongong, NSW 2522, Australia

HIGHLIGHTS

- A recommendation and privacy based cross-layer reputation mechanism (RP-CRM).
- The RP-CRM is secure, privacy preserving and efficient.
- Rapid and accurate detection and management of malicious node.
- The effective recommendation rate of RP-CRM is higher than that of SLCRM and FSLR.
- The successful acceptation rate of RP-CRM is better than that of SLCRM and FSLR.

ARTICLE INFO

Article history:
Received 27 June 2014
Received in revised form
19 September 2014
Accepted 25 October 2014
Available online 11 November 2014

Keywords:
Mobile cloud computing
Security
Privacy preserving
Reputation mechanism

ABSTRACT

Mobile cloud computing (MCC) is gaining popularity due to anywhere anytime data access. However, at the same time it also introduces the new privacy and security threats that have become an obstacle to the widespread use and popularity of MCC. In this paper, we propose a reliable recommendation and privacy preserving based cross-layer reputation mechanism (RP-CRM) to provide secure and privacy-aware communication process in wireless mesh networks (WMNs) based MCC (WM-MCC). RP-CRM integrates the cross-layer design with recommendation reputation reliability evaluation mechanism and the privacy preserving scheme to identify and manage the internal malicious nodes and protect the security and privacy against internal multi-layer attack, bad mouthing attack and information disclosure attack. Simulation results and performance analysis demonstrate that RP-CRM can provide rapid and accurate malicious node identification and management, and provide security and privacy protection against aforementioned attacks more effectively and efficiently.

1. Introduction

Mobile cloud computing (MCC) is a new computing paradigm that combines cloud computing with mobile devices and ubiquitous wireless infrastructure [1,2]. MCC has wide applications in various different areas [3] such as entertainment, health, games, business, and social networking. At the same time, the wireless mesh networks (WMNs) have been accepted as a promising low-cost and efficient solution for next-generation wireless networking, with the ability to provide high-speed Internet access and support mobile applications. Thus, WMNs have been deployed in a broad range of applications such as MCC [4,5]. Therefore, building WMNs based MCC (WM-MCC) will be a viable solution for MCC to implement the fast large-scale application. The architecture of the WM-MCC is depicted in Fig. 1. The mobile client is connected with the base transceiver station (BTS) and accesses to the mesh backbone via the mesh router; while mesh routers connect to each other and communicate with the cloud by accessing the Internet via the gateway.

Due to its features of shared medium, multi-hop decentralized architecture and special communication mode, WM-MCC is vulnerable to different security and privacy threats, especially those arising from internal attacks launched by internal malicious nodes [1,2,6–10]. Now, the privacy and security threats have become an obstacle to the widespread use and popularity of the WM-MCC. According to the survey in [11,12], 74% of IT Executives and Chief Information Officers are not willing to adopt mobile cloud services due to the risks associated with security and privacy.

* Corresponding author.
E-mail address: xuli@fjnu.edu.cn (L. Xu).

http://dx.doi.org/10.1016/j.future.2014.10.032

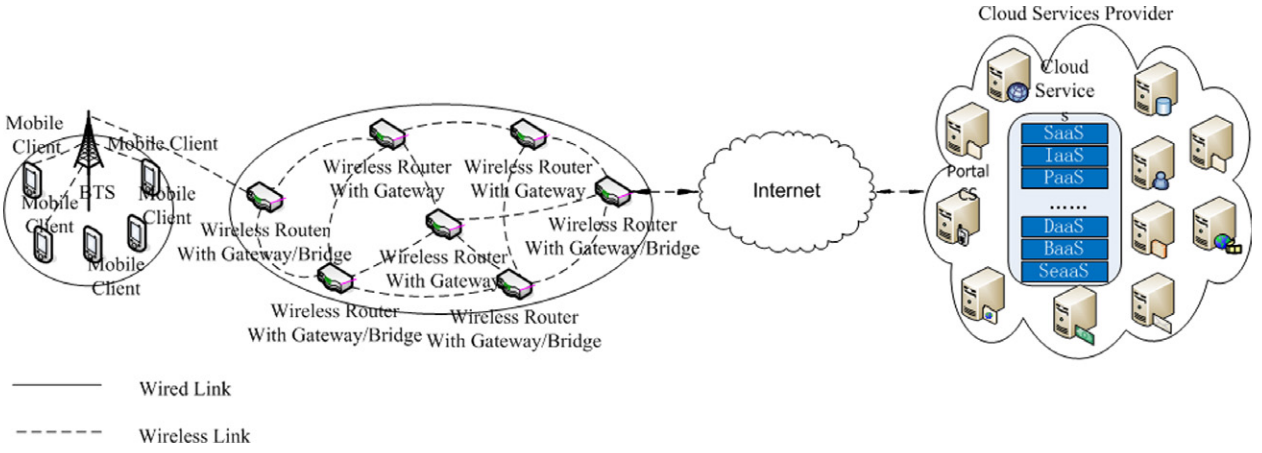
Cloud Services Provider
Cloud Service s
SaaS
IaaS
PaaS
......
DaaS
BaaS
SeaaS
Portal CS
Internet
Mobile Client
Mobile Client
BTS
Mobile Client
Mobile Client
Mobile Client
Wireless Router With Gateway
Wireless Router With Gateway
Wireless Routen With Gateway/Bridge
Wireless Router With Gateway
Wireless Router With Gateway/Bridge
Wireless Router With Gateway/Bridge
Wireless Router With Gateway/Bridge
Wired Link
Wireless Link

Fig. 1. WM-MCC architecture [2].

Security and privacy protection in WM-MCC are closely related to trust [13]. Trust can characterize and learn the nodes' actions and the evolution of these actions over time, which facilitates secure cooperation and is vital to construct an efficient and robust solution for security and privacy-sensitive applications. The lack of trust will restrict the users using the mobile cloud services. Therefore, establishing trust among nodes is one of the most challenging issues in WM-MCC.

As a key scheme for managing trust, the reputation mechanism has been introduced as an effective approach to characterize and quantify nodes behaviors for MCC. Although a number of reputation mechanisms and reputation-based trust functions have been proposed in the literature, all existing reputation mechanisms were based on the direct observation of layer-specifics to evaluate the node reputation, thus ignoring many key factors of reputation in other layers [9,10,13,14]. Moreover, they did not take into account privacy preserving and dishonest recommendations that are used to frame up good parties and/or boost trust values of malicious peers.

To overcome the above mentioned shortcomings, a reliable recommendation and privacy preserving based cross-layer reputation mechanism (RP-CRM) is proposed in this paper. To the best of our knowledge, the RP-CRM is the first cross-layer reputation mechanism in MCC considering the recommendation reputation reliability and privacy protection during the reputation computation process. The major contributions of this work include:

(1) A cross-layer reputation mechanism integrating node forwarding at network-layer with channel collision at MAC-layer and channel quality at physical-layer is proposed to resist multi-layer attacks, preserving privacy and make the detection of malicious nodes more effectively and accurately.

(2) A node security relevance computation method is introduced into the computation of the recommendation reputation to make the recommendation information and the recommenders credibility more accurate. In addition, it will further enhance the reliability and validity of the RP-CRM and defend against the bad mouthing attack.

(3) A malicious node classification and management mechanism based on the node security level (*sl*) and security class (*sc*) is proposed, which makes the malicious nodes management more accurately and flexibly and also improves the fault-tolerance and the survivability of RP-CRM. Moreover, a new design of hierarchical key management protocol HKMP based on the node *sl* and *sc* is proposed to protect the privacy and defend against the information disclosure attack.

(4) Extensive OPNET simulation experiments are conducted to investigate the performance of RP-CRM. Experimental results demonstrate that RP-CRM outperforms the existing mechanism in terms of the reputation update, effective recommendation rate, malicious node detection management and the successful acceptation rate in the presence of multi-layer, bad mouthing and information disclosure attacks.

The remainder of this paper is organized as follows. In Section 2, we review some important related work. In Sections 3 and 4, we present the proposed RP-CRM and the privacy preserving scheme, respectively. In Section 5, we verify the effectiveness of our model through extensive simulations. Finally, we conclude the paper in Section 6.

2. Related work

Reputation mechanisms or reputation based trust models have been widely studied in various fields of distributed networks to support secure and trustworthy communications and enhance collaborations among participants [9,10,13–20].

Li et al. [16] presented a hierarchical account-aided reputation management system (ARM) to efficiently and effectively provide cooperation incentives. The ARM built a hierarchical locality-aware dynamic hash table infrastructure for efficient and integrated operations of both reputation and price systems. Liu et al. [17] proposed a reputation mechanism to help nodes recognize selfish nodes much earlier and decrease the convergence time for isolating selfish nodes by combining familiarity values with subjective opinions. The familiarity value represents a nodes familiar degree with another individual node and is used to calculate the weighting factor that determines how much the node recommendation opinion impacts on the reputation computation result. Sicari et al. [18] proposed DARE (evaluating data accuracy using node reputation), an architecture addressing both node reputation and run-time data trustworthiness. DARE is based on a hybrid wireless sensor/mesh networks architecture and the use of the secure verifiable multilateration technique to provide secure data aggregation and node reputation, and allows the network to retain the trustworthiness of aggregated data even in the presence of malicious nodes. Shen et al. [19] presented a manual model and an automatic model for P2P networks to accurately reflect node trust and provide guidance for high-QoS server selection. The two models study the relationship between node trust, reputation, and additional factors, and derive accurate node trust of additional factors on reputation to truly reflect node trust by removing the impact of additional factors on reputation. Moati et al. [20] proposed a motivation and detection model to motivate nodes during selection to behave normally by