Computer Networks 65 (2014) 56–72

Contents lists available at ScienceDirect

Computer Networks

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

Peer-to-peer publication, search and retrieval using the Android mobile platform

Isaí Michel Lombera *, Louise E. Moser, P. Michael Melliar-Smith, Yung-Ting Chuang

Department of Electrical and Computer Engineering, University of California, Santa Barbara, Santa Barbara, CA 93106, USA

ARTICLE INFO

Article history:
Received 23 August 2013
Received in revised form 3 March 2014
Accepted 4 March 2014
Available online 12 March 2014

Keywords:
Peer-to-peer network
Mobile ad hoc network
Wi-Fi Direct
Android mobile platform
Decentralized publication
Search and retrieval

ABSTRACT

In this paper, we present the iTrust over Wi-Fi Direct system, which is a peer-to-peer publication, search and retrieval system for mobile ad hoc networks. We describe the iTrust over Wi-Fi Direct architecture and components, as implemented on the Android platform for mobile devices, and show how user applications can easily interface with iTrust over Wi-Fi Direct. We also describe the iTrust over Wi-Fi Direct networking model, and the interactions with the Android and Linux stacks. In addition, we describe the peer management protocol for iTrust over Wi-Fi Direct on the Android platform, which enables peers to construct a mobile ad hoc network by automatically discovering and connecting peers. We discuss deficiencies of the Android platform for Wi-Fi Direct, and present our solution to address those limitations. Finally, we present a performance evaluation of iTrust over Wi-Fi Direct in terms of the match probabilities without and with message forwarding, the peer management overhead, and the resource transfer latency.

1. Introduction

Traditional access to information from desktop and laptop computers is transitioning to mobile phones, tablets and other devices. While the uses of these devices continue to follow the habits of their users, traditional sources of information have not adapted to a world, where users actively participate in the search for information. Indeed, the era of passively watching the broadcast evening news on television is giving way to the online active news aggregator accessible from a mobile phone or tablet. Users are sharing their own unedited and uncensored information, rather than information from a controlled and vetted source. Why wait for the 6 o'clock evening news with its 2-minute summary of the morning's political upheaval when you can watch the event unfold live from a bystander's mobile phone camera?

The paradigm of serving data from a server's central repository to a client (one way) is transitioning to the clients' serving data to each other (both ways), which results in a change in the information as well. Instead of a central news source dictating which information is served to clients or users, now users decide which information to share among themselves. The transition from the client–server model to the peer-to-peer (P2P) model has placed new demands not only on the network but also on the sources or generators of information. While a desktop user at home searching for pictures of his/her favorite travel destination expects a Google search to be fast and effective, a mobile phone user in the field expects his/her mobile device, enabled with a Facebook app, to be fast and effective, and also to show pictures that friends took at that destination. Similarly, a desktop user might save a picture from a Web server before departing to his/her destination (one-way information retrieval), but a mobile phone user may share

* Corresponding author. Tel.: +1 760 468 2828.
E-mail addresses: imichel@ece.ucsb.edu (I. Michel Lombera), moser@ece.ucsb.edu (L.E. Moser), pmms@ece.ucsb.edu (P.M. Melliar-Smith), ytchuang@ece.ucsb.edu (Y.T. Chuang).

http://dx.doi.org/10.1016/j.comnet.2014.03.002
1389-1286/

his/her own pictures taken from a camera after arriving at the destination (two-way information sharing).

The twin drivers of emerging networks – increased peer-to-peer information sharing and increased sharing of personal information – will continue to play an increased role in the lives of most users and, thus, in the creation and development of those networks. Traditionally, network technology was developed to enable the transfer of information between devices, and was intentionally biased to favor mass transfers of information from the server to the clients. Now, as new technology is developed to increase the interactions between clients, care must be taken to address new issues that arise. The simultaneous transition from client–server to peer-to-peer networks and from public to private stores of information fits well with the transition from wired to wireless networks and from structured to unstructured networks. The convenience of mobile ad hoc networks to mobile phone users that share information among themselves cannot be overstated. With this freedom of direct sharing of information among peers, the threat of censorship appears to be nonexistent. However, history has shown that restriction and control of information are pervasive enough within autocratic societies, governments and organizations to encroach on even the most free and uncontrolled communication media. In short, a software architecture that enables personal sharing of information in mobile ad hoc networks must also address censorship and filtering of information.

To address the need for sharing of personal information and simultaneously to prevent a third party from censoring information or preventing the dissemination of information, we created iTrust over Wi-Fi Direct. Wi-Fi Direct [1–3] is a relatively new wireless technology, based on the IEEE 802.11 standard, that enables devices to form a peer-to-peer network without the need for a third intermediary device, such as a Wi-Fi access point. The previous name of Wi-Fi Direct was Wi-Fi P2P; in this paper, we use both terms interchangeably. The iTrust over Wi-Fi Direct system that we developed enables users with Wi-Fi Direct enabled mobile devices to publish, search for, and retrieve information among themselves. In the rest of this paper, we describe the design of the iTrust over Wi-Fi Direct system, the architecture and components as implemented on the Android mobile platform [4], the associated networking model, and the peer management protocol. We also present performance evaluation results.

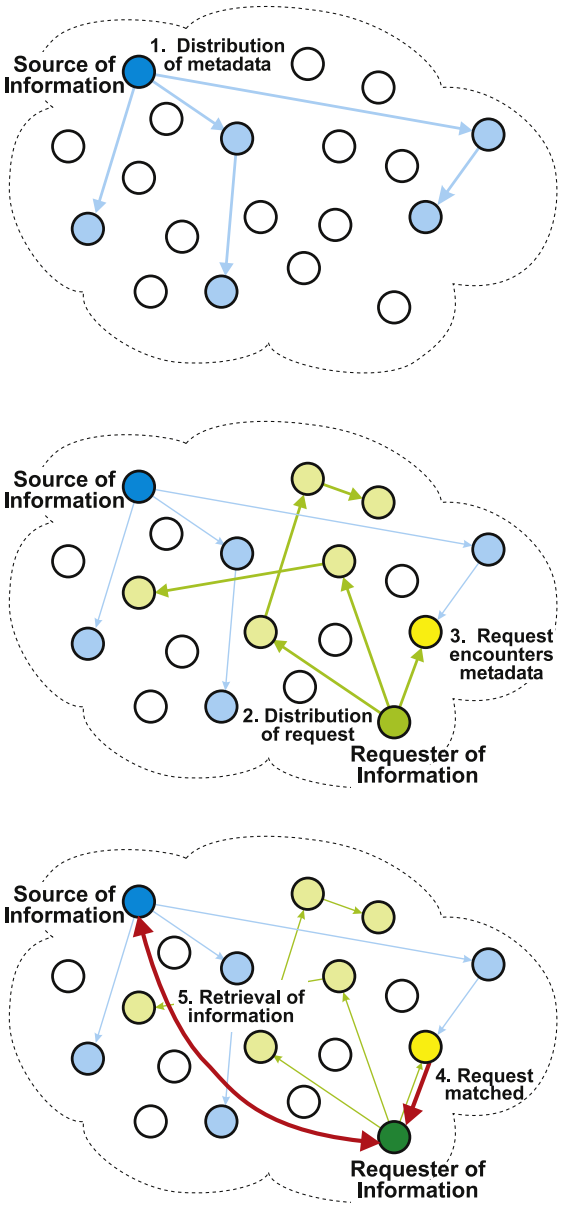

Fig. 1. Publication, search and retrieval in the iTrust over Wi-Fi Direct network.

2. Design of iTrust over Wi-Fi Direct

The iTrust over Wi-Fi Direct network consists of peers that form a mobile ad hoc network. Multiple iTrust over Wi-Fi Direct networks may exist simultaneously, and a peer may join any such network(s) over time. Peers in the same network are said to be in the same *membership*, although they need not *all* necessarily be within range of each other. Fig. 1 illustrates how information is published, searched for, and retrieved in the iTrust network.

Any peer with information to share (which we call a *source* peer) generates metadata describing that information and distributes that metadata to a subset of the membership chosen at random (1). A peer interested in querying or *requesting* information distributes a query to a subset of the membership chosen at random (2). In both the distribution of the metadata and the distribution of a query, a peer that receives the message may *forward* the message to yet another subset of the membership chosen at random. Prevention of message flooding is incorporated into iTrust over Wi-Fi Direct, as explained below.

When a peer finds a match between a query it receives and the metadata it holds, we say that an *encounter* or a *match* occurs (3). The peer with the match sends a message to the requesting peer which identifies the source peer