Computer Networks 70 (2014) 330–344

Contents lists available at ScienceDirect

Computer Networks

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

On the performance of secure user-centric VoIP communication

Pantelis A. Frangoudis [a,*], George C. Polyzos [b]

[a] INRIA Rennes-Bretagne Atlantique, Campus de Beaulieu, 35042 Rennes, France
[b] Mobile Multimedia Laboratory, Department of Informatics, School of Information Sciences and Technology, Athens University of Economics and Business, 11362 Athens, Greece

ARTICLE INFO

Article history:
Received 10 January 2014
Received in revised form 12 June 2014
Accepted 16 June 2014
Available online 26 June 2014

Keywords:
Wireless networking
VoIP
Virtual private networks
Network security
User-centric networking

ABSTRACT

Motivated by the increased Wi-Fi coverage in metropolitan areas and the emergence of user-centric wireless access schemes, we focus on the provision of secure, user-centric voice services and explore their potential performance-wise, by designing a VoIP communications scheme tailored to open-access wireless environments, but also with wider applicability, and experimenting with it to estimate its upper bounds on VoIP capacity, under constraints posed by user-centrism; operation at low-cost and on user-controlled equipment, minimal dependence on centralized entities, and tackling specific security challenges. We identify quality degradation factors and quantify their importance by simple analysis and experimentation, showing that typical user Wi-Fi equipment can sustain a satisfactory number of concurrent secure VoIP sessions with acceptable Quality of Experience and, at the same time, protection from malicious user activity can be offered to access providers, while a level of roaming privacy can be guaranteed.

1. Introduction

The traditional view of communications has recently been disrupted by the evident user empowerment in all aspects of the communication process. Traditionally, the operator-centric view dominated, where users had a passive role as service consumers. This view seems to change and the factors that have led to this shift are numerous.

Hand-in-hand with the revolution in current Internet usage trends, where we witness a vast increase in the volume and popularity of user-generated content, a new communication paradigm, where users have a central role, has emerged. With the advent of low-cost, ubiquitous, and easy to install and configure wireless equipment, but most importantly, protocols that operate in unlicensed spectrum, users can effectively acquire the dual role of becoming service consumers and *providers* at the same time. This fact has the potential of bringing up new disruptive technologies, where users can enjoy low-cost wireless connectivity via the infrastructure provided by a heterogeneous crowd of *micro-operators*.

In this work, building on advances in user-centric wireless access [1,2], we focus on providing user-centric voice (and multimedia) communication services in such an environment. We assume an underlying access substrate where nomadic users enjoy community-based Internet access by potentially anonymous, and most probably untrusted, Wi-Fi hotspot operators and wish to set up end-to-end multimedia communication in a user-centric way, in the sense that critical operations such as signaling and security management are carried out on user-controlled software and equipment, with minimal dependence on centralized infrastructures. It should be noted that, although our work is positioned in the context of community-based Wi-Fi access, our approach to setting up end-to-end VoIP communication is more generic and could be applied to other wireless access infrastructures as well.

* Corresponding author. Tel.: +33 299847581.
E-mail addresses: pantelis.frangoudis@inria.fr (P.A. Frangoudis), polyzos@aueb.gr (G.C. Polyzos).

http://dx.doi.org/10.1016/j.comnet.2014.06.009
1389-1286/© 2014 Elsevier B.V. All rights reserved.

We face both security and performance challenges. Trust cannot be assumed among access providers and roaming users, thus data confidentiality cannot be guaranteed. At the same time, access providers need to be protected from malicious activities on behalf of roaming users, to which they may be held legally liable. On the other hand, performance of VoIP over user-centric wireless networks is a key issue, in part due to the unpredictable nature of wireless communications, where delay sensitive applications like Internet telephony are known to suffer. Poor signal conditions, but also contention for access to the medium and interference brought by spectrum scarcity, dense and anarchic Wi-Fi deployment, and poorly-configured wireless equipment, account for that. The need for security has also an adverse effect: important space and processing overhead is imposed by mechanisms applied to protect communications. These performance penalties are intensified by the limitations and challenges of a user-centric solution; minimal dependence on centralized infrastructure and operation on low-cost, resource-constrained, user-provided equipment, i.e., embedded WLAN devices and mobile terminals.

We approach the above challenges performance-wise, by designing and experimenting with a secure voice communications scheme which makes use of tunneling technologies, and evaluating service quality adopting a Quality-of-Experience (QoE)-oriented stance. Our purpose is to estimate the maximum number of simultaneous VoIP calls of acceptable quality – as a user would perceive it – that a typical home WLAN can sustain, by measuring how the use of security mechanisms and Wi-Fi operation affect voice quality. The contributions of this work are summarized below:

- We present solutions for VoIP communication services set up in purely user-centric fashion and operating fully on user equipment, designed for, but not limited to, a user-centric/community-based wireless access environment, and also discuss various design alternatives.
- We study the tradeoff between security and performance under the constraints posed by low-end user equipment. To the best of our knowledge, we are the first to provide a *combined* study of the overheads imposed by security mechanisms both at the processing and the protocol level under the premise that both call endpoints are connected to Wi-Fi links and cryptographic operations are carried out on low-cost, off-the-shelf user equipment, thus shedding light on the practical performance limits of secure user-centric VoIP communication.

This article is structured as follows: Section 2 provides a review of the state of the art in relevant research fields. Section 3 presents a user-centric secure VoIP service designed for user-centric wireless access, but also discusses design alternatives. In Section 4 we focus on the performance evaluation of this service; we use a simple analytic model to estimate upper bounds on VoIP capacity for our tunneling-based architecture (Section 4.2), describe our experimental methodology and testbed (Section 4.3) and present performance results (Section 4.4). In Section 5 we summarize and discuss our conclusions.

2. Related work

2.1. User-centric wireless access

User-provided wireless access schemes have recently received research and commercial attention. Based on the private contributions of individuals who operate Wi-Fi equipment, architectures and systems are being proposed with the aim of building resource sharing communities to achieve wide wireless coverage [1]. In this section we overview approaches in this direction, since our design assumes that such a scheme will be used for Wi-Fi access.

Large wireless communities such as guifi.net [3] and the Athens Wireless Metropolitan Network [4], counting thousands of participants, are nowadays a reality. Various communication services, and, notably, intra-community VoIP, are run on top of them, while at the same time they act as testbeds for research and experimentation [5]. Originally, research in the area focused on the technical aspects of building wireless community networks, but attention soon shifted towards socioeconomic and incentive aspects. A critical aspect of user-provided wireless networks is to design mechanisms to encourage contribution while limiting attacks by selfish users who aim at *free riding*. In our prior work [2], we proposed a fully decentralized scheme to this end. Our multimedia communications architecture was designed with this scheme in mind.

FON [6] has followed a different architectural approach. It acts as a mediator for the development of a Wi-Fi sharing community, centrally dealing with user authentication and accounting. The role of such mediators as community providers is modeled by Biczók et al. [7,8]. They analyze their interactions with users and ISPs in global-scale wireless community networks and explore the space of available parameters (e.g., roaming cost, ISP's profit share) to determine the benefits of each player when joining the community. The authors present interesting results regarding the role of ISPs: Arguing that ISP endorsement is important for the global scaling of wireless communities, they find that depending on parameters set by the mediator, they will either fully support or abandon (i.e., prohibit Wi-Fi sharing) the community. This conclusion appears to be closely related to the terms of use adopted by ISPs regarding broadband connection sharing over Wi-Fi.

Two significant issues pertinent to wireless communities are studied by Manshaei et al. [9]. First, they study how initial community network coverage and user payoffs and fees affect the evolution of the community. Second, they focus on the competition between licensed wireless access providers and community-based ones, which is an important step towards answering whether wireless communities can be a viable alternative (or complement) to licensed cellular networks.

Ai et al. [10] focus on a critical usability aspect; their scheme only requires software updates at the client side and no firmware upgrades at the AP side. However, their design depends on a central server.

The legal aspects of user-provided wireless access should not be neglected. MacSíthigh [11] discusses how the adoption of open wireless access is hindered by a