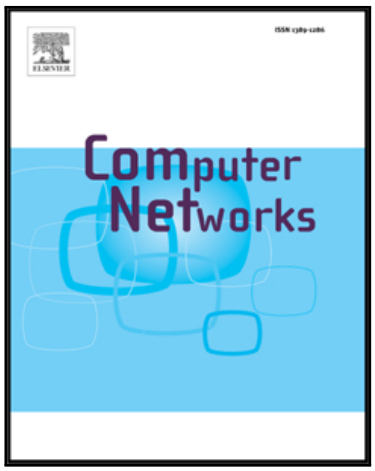

A Novel Security-Centric Framework for D2D Connectivity Based on Spatial and Social Proximity

Aleksandr Ometov, Antonino Orsino, Leonardo Militano,
Giuseppe Araniti, Dmitri Moltchanov, Sergey Andreev

PII: S1389-1286(16)30085-8
DOI: 10.1016/j.comnet.2016.03.013
Reference: COMPNW 5853

To appear in: *Computer Networks*

Received date: 28 August 2015
Revised date: 25 March 2016
Accepted date: 26 March 2016

Please cite this article as: Aleksandr Ometov, Antonino Orsino, Leonardo Militano, Giuseppe Araniti, Dmitri Moltchanov, Sergey Andreev, A Novel Security-Centric Framework for D2D Connectivity Based on Spatial and Social Proximity, *Computer Networks* (2016), doi: 10.1016/j.comnet.2016.03.013

A Novel Security-Centric Framework for D2D Connectivity Based on Spatial and Social Proximity

Aleksandr Ometov[a,c,*], Antonino Orsino[b], Leonardo Militano[b], Giuseppe Araniti[b], Dmitri Moltchanov[a], Sergey Andreev[a]

[a] *Tampere Univesity of Technology, Tampere, Finland*
[b] *University Mediterranea of Reggio Calabria, Italy*
[c] *Saint Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University), St.Petersburg, Russia*

Abstract

Device-to-device (D2D) communication is one of the most promising innovations in the next-generation wireless ecosystem, which improves the degrees of spatial reuse and creates novel social opportunities for users in proximity. As standardization behind network-assisted D2D technology takes shape, it becomes clear that security of direct connectivity is one of the key concerns on the way to its ultimate user adoption. This is especially true when a personal user cluster (that is, a smartphone and associated wearable devices) does not have a reliable connection to the cellular infrastructure. In this paper, we propose a novel framework that embraces security of geographically proximate user clusters. More specifically, we employ game-theoretic mechanisms for appropriate user clustering taking into account both spatial and social notions of proximity. Further, our information security procedures implemented on top of this clustering scheme enable continuous support for secure direct communication even in case of unreliable/unavailable cellular connectivity. Explicitly incorporating the effects of user mobility, we numerically evaluate the proposed framework by confirming that it has the potential to substantially improve the resulting system-wide performance.

1. Introduction and motivation

The numbers of devices connected to contemporary cellular networks have been increasing dramatically over the last decade [1]. Tothis end, the traffic load has also been growing tremendously, where the mobile data per smartphone and tablet is expected to reach 5 GB and 17 GB per month, respectively [2]. In addition to conventional human-generated data, a plethora of the Internet of

*Corresponding author at: Department of Electronics and Communications Engineering, Tampere University of Technology, Tampere, Finland, FI-33720. Tel.: +358 44 9714624
Email address: aleksandr.ometov@tut.fi (Aleksandr Ometov)