# PodNetSec: Secure Opportunistic Content Dissemination

Sacha Trifunovic, Bernhard Distl, and Franck Legendre
ETH Zurich, Switzerland

Carlos Anastasiades
University of Bern, Switzerland

**PodNet:** PodNet[1] [1] (Fig. 1(a)) targets mobile content distribution by extending the traditional podcasting concept to opportunistic peer-to-peer content delivery among users via IEEE 802.11 wireless communications in ad hoc mode. Content is organized as *episodes* in *channels*, which users can subscribe to and download content once a peer within range holds new episodes. Information thus spreads from user to user in an epidemic fashion making use of mobility.

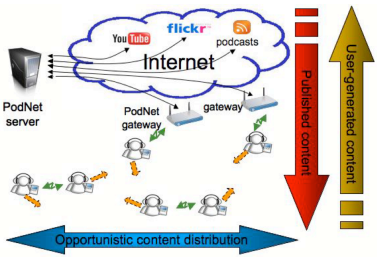
In the initial version of PodNet, content publication was done anonymously, making it an ideal platform for spreading spam and illegal content. With PodNetSec three channel types are introduced, namely *open*, *restricted*, and *closed*. Closed channels allow private and encrypted dissemination of content in a limited group e.g., for friends to share photos. Restricted channels only allow authorized users to publish content but everybody to consume it, thus basically supporting official podcasters (e.g., BBC). Open channels allow every user to consume as well as create new content. Although useful for applications such as discussion forums, or video sharing (e.g., YouTube), it may serve as an easy platform to spread spam and objectionable content. Anti-Spam control mechanisms are thus required.

**PodNetSec - Integrated Security Framework:** PodNetSec implements mechanisms – leveraging real-world social networks and communities – to prevent the dissemination of spam and illegal content in open channels. A two-level rating system as well as social trust metrics based on friend ties and local communities, are introduced and serve as input of a reactive as well as a proactive spam control mechanism.

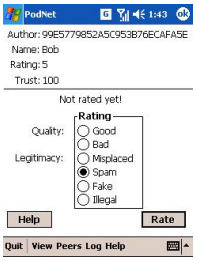
We introduce the notion of a user through self-created credentials (public/private key) [2]. These guarantee the inimitability of an identity and provide authentication of already known users, non-repudiation, and integrity without the support of a central authority (CA). As these cannot prevent users from generating multiple identities and launching Sybil attacks [3], we minimize their effect by establishing trust in genuine identities. This is based on their social ties demonstrated by a secure pairing process [4] or on their familiarity and similarity (community) in the underlying mobility graph [5].

A two level rating system is introduced to allow for content to be rated and author's to build up a reputation (based on teir publications). It allows to rate, first, the legitimacy and, second, the quality of the content.

[1] `http://podnet.ee.ethz.ch`




(a) The PodNet Architecture.




(b) PodNetSec Rating Interface.

**Figure 1: PodNet Architecture and Software.**

Ratings are then shared among users for a more accurate and faster creation of the reputation. The received ratings are weighted by the raters trust value in order to cope with liars. Whenever content is legitimate, a user may assess their satisfaction with it, in order to tune future download selection to their taste. Otherwise, a user can declare content as spam or illegal (Fig. 1(b)).

The spam control mechanism relies on the outcome of the reputation system. It blacklists any non-legitimate content (reactive) and enslaves the publication rate of an author to the consumers satisfaction and trust in the author (proactive). This avoids flooding of unwanted content and serves as an incentive to rate to improve the quality of one's usage experience.

**Demo setup:** PodNetSec is implemented and successfully tested on both Windows Mobile 2003 and Windows Mobile 6. We will demonstrate the use of the three channels types and in particular the open mode to disseminate conference related information such as proceedings and conference daily news such pictures and videos of presentations, posters and demos. We will act as spammers demonstrating our anti-spam mechanisms. Mobisys participant will be able to borrow a few devices and install our software on their mobile.

## 1. REFERENCES

[1] G. Karlsson, V. Lenders, and M. May. Delay-Tolerant Broadcasting. *IEEE Trans. on Broadcasting*, 51, 2007.
[2] G. Montenegro and C. Castelluccia. Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Addresses. In *NDSS*, 2002.
[3] J. R. Douceur. The Sybil Attack. In *IPTPS*, 2002.
[4] S. Capkun, J. P. Hubaux, and L. Buttyan. Mobility helps Peer-to-Peer Security. *IEEE TMC*, 5, 2006.
[5] S. Trifunovic, C. Anastasiades, and F. Legendre. Social Trust in Opportunistic Networks. In *NetSciCom*, 2010.