Pervasive and Mobile Computing ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

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

Fast track article

Trust and reputation management for opportunistic dissemination☆

Radu-Ioan Ciobanu, Radu-Corneliu Marin, Ciprian Dobre*, Valentin Cristea

Faculty of Automatic Control and Computers, University Politehnica of Bucharest, 313 Splaiul Independentei, Bucharest, Romania

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Opportunistic
Dissemination
Trust
Reputation

ABSTRACT

Nodes in opportunistic networks need to cooperate to disseminate data. However, employing intermediate nodes for dissemination leads to several security issues. Here, we propose an opportunistic trust and reputation mechanism entitled SAROS, which detects and avoids malicious nodes, i.e. nodes which, upon receiving messages for other interested peers, modify their content in order to spread false information. This can negatively affect the network, by polluting it with spam messages, or dropping messages of interest to the nodes in the network. By detecting and avoiding malicious nodes, SAROS is able to increase the percentage of correct messages that reach their destinations.

1. Introduction

Since opportunistic networks (ONs) are totally decentralized, nodes need to cooperate in order to successfully create a publish/subscribe environment that benefits all the nodes in the network. However, employing intermediate nodes for performing dissemination can lead to several issues. In this paper, we handle the problem of trust and reputation in opportunistic networks. Namely, we propose a trust and reputation mechanism (entitled SAROS—Socially-Aware Reputation mechanism for Opportunistic diSsemination) which has the purpose of detecting and avoiding malicious nodes. A malicious node is a member of the opportunistic network which, upon receipt of a message to be forwarded to interested nodes, modifies its content in order to spread false information. This can lead to the pollution of the ON with spam messages, and to the loss of messages of interest to the nodes in the network. By detecting and avoiding such malicious nodes, SAROS is able to increase the percentage of correct messages that reach their destinations.

SAROS is implemented as a component of Interest Spaces (presented in more detail in [1,2]), which is an interest-based data dissemination framework for opportunistic networks. It is able to disseminate data to interested nodes, by taking advantage of their context information (such as location, interests, social connections, encounter history, etc.). Its advantage is that it offers a unified interface for data dissemination in various situations.

Since opportunistic networks are decentralized and two nodes are only connected upon a contact (i.e. when they are in range), handling trust and reputation is a totally different problem than in regular peer-to-peer networks. There is no central entity that can be used as an authority regarding node reputation, and a node only has information that it has gathered itself, or that it has received from encountered nodes. However, a node cannot know how much to trust the information received from an encountered node, which may very well feed it false data. For example, a malicious node can report other malicious

☆ Supported by national project MobiWay, Project PN-II-PT-PCCA-2013-4-0321.
* Corresponding author.
E-mail addresses: radu.ciobanu@cti.pub.ro (R.-I. Ciobanu), radu.marin@cti.pub.ro (R.-C. Marin), ciprian.dobre@cs.pub.ro (C. Dobre), valentin.cristea@cs.pub.ro (V. Cristea).

http://dx.doi.org/10.1016/j.pmcj.2016.09.016
1574-1192/

nodes that it collaborates with as trustworthy nodes. Thus, a node can easily form a wrong impression (i.e. it can think that a malicious node is trustworthy) by believing the information provided by malicious nodes, especially if it encounters them often.

However, this is where the advantage of opportunistic networks is shown. Since opportunistic networks are formed of mobile devices, mobility can also act as a benefit. For example, it is much more difficult for a malicious node to follow a "victim" node around to feed it false information than it is for nodes in a regular peer-to-peer network to flood the victim with false information whenever they want. Moreover, opportunistic nodes are generally mobile devices such as smartphones that belong to humans, so interactions are governed by social connections and user mobility. This means that a large part of the encountered nodes are familiar, and most of them are even connected through an online social network. Since connecting on such a social network requires that the nodes know (and implicitly trust, to an extent) each other in real-life, this information can be used to assign pre-set trust values to connected nodes.

In order to have an informed view of the entire network (or as much of it as possible), nodes have to collect data about the behavior of relay nodes, as well as regarding the opinions of other nodes about them. Since an opportunistic node cannot know on the spot whether another node it has relayed its message to actually delivers it to the intended destinations, a different means of confirmation should be employed. Other solutions employ feedback messages that are spread in the network upon a successful delivery. However, such messages tend to flood the network, so a better means might be to employ gossiping. Thus, when a successful delivery occurs, a node can increase its opinion regarding the relay node (or nodes), and gossip this information to other nodes in the network. This way, information is spread through the entire network, and more and more nodes get to see the bigger picture.

Another problem regarding opportunistic networks is that nodes do not have a direct method of deciding whether a received message has not changed during its life in the network (since it may pass through many hops until its destination, some of which can be malicious). Means of encrypting messages have been proposed [3], but they are based on nodes establishing a key in an offline manner, prior to getting on the network, which is not always feasible. Nodes can sign messages with a certificate, but the problem is that there is no central trusted entity that is able to generate and confirm the authenticity of these certificates.

We consider that SAROS is the first opportunistic trust solution that has detection mechanisms for messages that have been tampered with, while also using social information to pre-establish trust. Other social-based solutions simply use social relationships to decide whether a node is trustworthy, without actually analyzing the content carried by that node, while also not giving a chance for delivery to nodes that are not socially connected (which can lead to missing some valid data exchange opportunities). SAROS takes advantage of the inherent design of opportunistic networks to receive a message on multiple paths and decide its correctness.

The rest of this paper is structured as follows. Section 2 presents the state of the art in the area of trust and reputation management for mobile networks. Then, in Section 3 we present an overview of the Interest Spaces framework, discussing its architecture and the composing layers. In Section 4, we propose and present SAROS, and in Section 5 we perform an experimental evaluation of the proposed solution for multiple scenarios. Finally, in Section 6, we present our conclusions.

2. State of the art

A very thorough survey of security and trust management in ONs is presented in [3]. Among a multitude of security and privacy-related issues, the authors also tackle the problem of managing trust in opportunistic networks, in terms of having confidence that a node that is relayed a message will successfully deliver it towards the intended destination. The authors present existing trust solutions for mobile networks, and split them into several categories, depending on the type of trust establishment: reputation-based trust [4,5], social trust [6,7], environmental trust [8], and data-centric trust [9,10].

EigenTrust [11] is a trust and reputation system where nodes compute and use global trust values for choosing the peers they download data from, in order to avoid and isolate malicious nodes. EigenTrust nodes compute local trust values for their peers based on their transaction history. In order to decide if a node is to be trusted, EigenTrust computes a global trust value for that node, obtained from the local trust values assigned by other peers to that node, weighted by the global reputations of the assigning peers. The authors also introduce the notion of pre-trusted peers, which are the first nodes queried regarding peer reputations, and they are also automatically trusted.

Similarly to EigenTrust, PowerTrust [12] is a reputation system for P2P networks that builds a trust overlay network to model the trust relationship between peers, and is based on the observation that user feedback can be approximated by a power-law distribution. It dynamically selects a small number of power nodes (which have the highest reputations) by using a distributed ranking mechanism. These power nodes are chosen dynamically and constantly updated, so PowerTrust is more robust than EigenTrust towards popular nodes leaving the network or getting infected. Our solution uses some ideas from EigenTrust and PowerTrust. Namely, nodes compute local trust values based on their own experiences with other nodes, but also use gossiping to find out other peers' opinions of interacting nodes, which are used to compute global trust values for a more informed decision. It also uses pre-trusted peers, which are different from node to node, being chosen from the node's social connections.

In [13], the authors propose an ontology-based trust model, where the network nodes' behavior is analyzed based on direct and indirect reputation. It takes advantage of a reputation system to support the decisions that must be made by users when they have to choose whether or not to trust another user during opportunistic encounters. In this situation,

Please cite this article in press as: R.-I. Ciobanu, et al., Trust and reputation management for opportunistic dissemination, Pervasive and Mobile Computing (2016), http://dx.doi.org/10.1016/j.pmcj.2016.09.016