Computer Communications 48 (2014) 1–4

Contents lists available at ScienceDirect

Computer Communications

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

Editorial

Opportunistic networks

1. Introduction

The present issue of *Computer Communications* is dedicated to opportunistic networks (OppNets), which are an instance of the delay tolerant networking (DTN) paradigm. Opportunistic networks have emerged as one of the most interesting evolutions of legacy Mobile Ad Hoc Networks (MANETs). In MANETs a continuous end-to-end path had to be established before a message was exchanged, meaning that the sender and the receiver had to stay simultaneously connected to a common network. Unfortunately, in real mobile ad hoc networks, due to node mobility, devices that are turned off or run out of battery and the intrinsic wireless link instability, the connectivity is such that an end-to-end path between message source and destination might never exist. In order to address this challenging scenario, OppNets turn the obstacle, i.e., mobility, into an opportunity by allowing nodes to carry the messages with them while they move, until a next hop deemed suitable is encountered. This is the new *store, carry, and forward* paradigm. Opportunistic networks are sometimes also referred to as Pocket Switched Networks, hinting at the fact the user devices act as both routers and end users of the system.

Most of the research in the area has focused on human-centric OppNets, i.e., on networks formed by thin devices (e.g., smartphones) carried by the users. Other possibilities are represented by vehicular ad hoc networks (VANETs) and *hybrid* networks. The former are networks constituted by vehicles equipped with wireless network interfaces. Due to the high mobility present in these networks, many opportunistic solutions work very well also in this environment. As far as the latter are concerned, they consider the possibility of extending and complementing OppNets with a fixed network infrastructure such as Wi-Fi Access Points, 3G/4G cellular infrastructure or road-side units (RSU) (which may support connectivity amongst vehicles).

Several challenging issues must be addressed in order to deploy opportunistic networks in real environments, and they are summarised in the research areas in Fig. 1. In the following, we will provide a brief overview of the main research directions in each of them.

Mobility and sociality. Connectivity is supported by communication technologies allowing for direct communications between devices, of which Bluetooth and WiFi are the most popular solutions. Communication channels are established when an encounter occurs between two nodes, i.e., when they come into reciprocal radio range. As nodes are sparse in the system, encounters are sporadic and depend on the mobility pattern of the nodes. Research aimed at understanding and modelling human mobility has thriven in the recent years. The importance of mobility in opportunistic networks is twofold. On the one hand, understanding mobility is essential to identify those features that may affect the performance of opportunistic data delivery schemes. For example, a crucial role is played by the inter-contact times between nodes, i.e., by the time elapsed between consecutive encounters for a certain pair of nodes. In fact, these time intervals are the main component of the delay accumulated by messages and uncovering their features from traces of real mobility is key to investigate the environment in which data delivery protocols operate. Understanding mobility is also essential for evaluating the performance of protocols for opportunistic networks under realistic conditions. To this aim, the features of mobility are to be embedded into a synthetic mobility model that will generate movements to be fed to simulators. For example, many attempts have been performed at capturing into a synthetic model those aspects that drive human mobility in real life, such as user interests and social relationships. At the state-of-the-art, several models have been proposed, capturing different characteristics of node behaviour in different kinds of OppNets. Yet, much remains to be done, in particular as far as the inter-correlations are concerned among the different factors determining the human decisions driving displacements.

Communication support. In opportunistic networks communication takes place through mechanisms able to single out the subset of encounters suitable to drive data to their destinations. The solutions proposed in the literature may be classified according to two main paradigms, namely, people-centric and data-centric. The people-centric approach is typical of **data forwarding** (“User A wants to communicate with user B”), in which the two end points of the communication address their reciprocal identities explicitly. Group communications (e.g., similar to anycast or multicast) are also considered by some proposals. Vice versa, in the data-centric approach (which can be framed within the popular Content Centric Networking idea) it is not the identities of the end points that matters but the semantic of the content itself. So, content is produced on the fly by users and is requested by other users based on the interest they have in these data. This is the perspective of **content diffusion**. Both families of data exchange policies may be affected by the mechanisms adopted for both the management of limited message buffers and cache replacement.

From the research standpoint, these are the most investigated topics. Data forwarding schemes can be classified into the two big categories of social-oblivious and social-aware schemes (also known as randomised vs. utility-based schemes), based on the amount of information they exploit for taking forwarding decisions. In social-oblivious protocols, a certain number of message replicas (possibly, infinite) is randomly diffused in the environment, in the hope that one of the replica owners runs into the destination. The performance of these solutions usually improves with the increasing number of replicas. By contrast, in social-aware

http://dx.doi.org/10.1016/j.comcom.2014.04.007

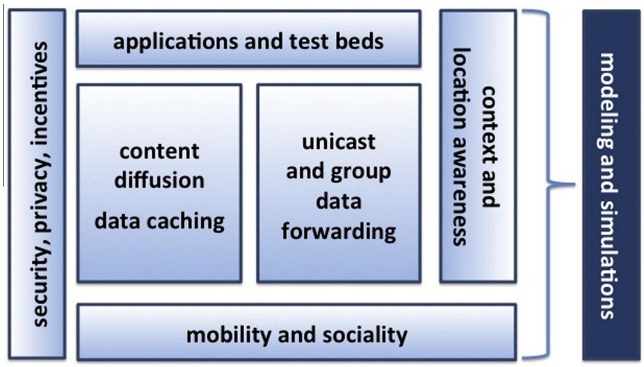

Fig. 1. Overview of the research issues in the opportunistic networking field.

protocols, nodes try to estimate the different probabilities other nodes have of encountering the destination of a buffered message, so as to relay it to the most promising next hop in terms of probability of successful delivery. The estimate is usually inferred from the observation of the past encounter patterns, under the assumption that people show movement habits that somehow repeat over time. Social-aware protocols are typically more accurate in reaching the destination, but at the price of storing a possibly large amount of contextual information.

The intrinsically human-centric nature of opportunistic networking embraces content-centric aspects when it comes to content diffusion. The social dimension of users is still relevant but other aspects are to be leveraged for effective content dissemination. The simplistic approach is to flood the network with data items. Smarter strategies can be envisioned considering where the content is generated and where the users interested in such content are located. Conceptually, content distribution can be seen as a variation of the publish/subscribe paradigm, and some approaches have tried to treat it analogously. Others have focused on the definition of some heuristics or global optimisation strategies for the distribution policy.

Applications and test beds. Several applications have been devised for opportunistic networks. Amongst the earliest, there is the support to connectivity (*i*) in case of emergency in disaster area where the fixed infrastructure has been destroyed, (*ii*) in rural areas and scarcely developed countries where the deployment of a fixed network infrastructure is not economically convenient and (*iii*) in mobile battlefield scenarios. The recent technological innovations have brought to everyone the possibility of carrying in one's pocket smartphones equipped with more memory, computation and networking capabilities than the first personal computers available on the market. As a consequence, several more applications appear of interest. Amongst the most relevant ones, we may cite:

- social-based applications: mobile social networking, content sharing, social discovery, question & answering, for the support to interactions among neighbour users with social relations or common interests;
- pervasive and urban sensing: smartphones are equipped with several sensors (camera, accelerometer, GPS), which may be fruitfully used to monitor what is going on in the user surroundings and to collect information from other devices in the environment, either held by other users or embedded in objects (Internet of Things);
- opportunistic computing: opportunistic sharing of resources and services between devices in order to provide a platform for the execution of distributed computing tasks;
- offloading of the cellular networks: the wireless technologies usable to implement OppNets are free of license, drain less battery energy than current 3G/4G technologies, and provide a significant amount of bandwidth – mostly unused currently – which could be exploited when and where the cellular infrastructures are unavailable, congested, or too expensive.

In order to better understand how people might use OppNets – so as to design communication mechanisms targeted to their needs – some prototypal implementations have been developed, which provided useful insights about users behaviour and interactions.

Context and location awareness. Context learning and management consists in the acquisition and update of a large amount of information regarding the environment the users are immersed in. This information might be, e.g., the frequency at which other nodes are encountered, the strength of the social relationships that exist between users, the places regularly visited, the type of content the encountered nodes are interested in, etc. This plethora of information is at the basis of some of the most interesting operational modes in OppNets. This, and the possibility of determining the current device position, might be leveraged to filter the data available in other users' and environmental devices so as to customise the services and content supplied by the opportunistic network to the user. The analysis of this aspect is useful for the design of both applications and data diffusion/forwarding mechanisms.

Security, privacy, incentives. Security in opportunistic networks encompasses privacy, confidentiality and trust and cooperation enforcement. In opportunistic networks, nodes make forwarding decisions based on the content of the packet and/or on the context. As a result of confidentiality and privacy requirements, such information has to be encrypted. Therefore, the big challenge is to solve the conflict between encryption and opportunistic forwarding by allowing networking mechanisms to operate on encrypted data without decrypting them. Another critical aspect in opportunistic networks is the lack of infrastructure. Nodes form a temporary network without the help of any security infrastructure and without any a priori trust relationship. The lack of security infrastructure and scarcity of resources would inherently foster nodes to selfishly behave. Inducing cooperation between nodes can be based on some rewarding and/or reputation mechanisms and on the use of some additional contextual information such as the social contacts (friends) of communicating nodes.

Modelling and simulation. Opportunistic networks are not yet commonly available outside the research environment. Any experiment able to shed light on what they would be used for, and how they should operate, would help research. At the state-of-the-art, though, the testbeds deployed are few and small-scale, hence they are not sufficient to draw general insights on the aspects discussed above. In order to address this issue, researcher have relied on analytical models and simulation tools for investigating the characteristics and performance of OppNets protocols. Both models and simulators allow to advance our knowledge on OppNets behaviour, to design and test viable solutions also in the absence of real prototypes, so as to make opportunistic networking working and available in a, hopefully, near future.

2. Content of the special issue

This special issue comprises 13 state-of-the-art papers, that have been selected out of 70 submitted contributions after a rigorous review process, which entailed two rounds of reviews from invited experts and the guest editors. We believe the selected papers provide a faithful representation of current hot topics and cutting edge research directions in the field of opportunistic networking and will be of great use to those who are carrying out research in the area.

The first paper [1] provides a survey of the evolution of opportunistic networks in the last decade. It categorises the existing opportunistic network scenarios and presents some of the already deployed applications. The paper also focuses on forwarding protocols and discusses the simulators and tools used in their evaluations.

The special issue includes a large group of papers focused on forwarding issues in opportunistic networks, from different perspectives. There are three algorithmic papers that propose and evaluate new forwarding schemes for opportunistic networks. In [2] the authors introduce GAR, a group-aware forwarding scheme for cooperatively transferring messages in an opportunistic network. Alongside the forwarding strategy, this work also introduces a buffer management strategy in which the message dropping priorities are chosen so as to minimise the loss in delivery probability. In [3] a privacy-aware geographic routing protocol is proposed, which leverages self-determined location profiles of smartphone movements in order to predict future locations while at the same time minimising the exposure of sensitive information during message exchange. Finally, [4] describes a solution for hybrid opportunistic networks, i.e., opportunistic networks that are able to integrate and explore the infrastructure, if available. The proposed HRS system does not rely on central servers and is able to accommodate a large set of state-of-the-art forwarding protocols and make them able to route messages towards the infrastructure and across the infrastructure.

The special issue also comprises three papers that aim to model the performance of data delivery at different levels. In [5], an analytical model for the delay and the number of hops that encompasses both social-aware and social-oblivious single-copy forwarding protocols, as well as different hypotheses for user contact dynamics is discussed. Specifically, exponential, Pareto, and hyper-exponential intercontact times are accommodated by the proposed analytical framework. In [6], an analytical framework for analysing data delivery in cases in which the level of cooperation (i.e., the selfishness of nodes) is related to the social ties they share or to their mobility patterns is discussed. The important metrics considered are the message delivery delay, the average power consumption and the message delivery probability. The authors also investigate how the performance can be improved by choosing the cooperation policy wisely. The last work in this class [7] investigates the important problem of fragmentation in opportunistic networks. The authors provide a system model for the case in which a single message is sent over a chain of links with on–off periods, mimicking the instability of real opportunistic networks. Then, the mean transmission time is computed, based on the number of links, the length of fragments and the distribution of link disruptions.

The performance of routing protocols is also studied in two other papers of this special issue, this time by means of extensive comparative simulations. In [8] practical problems in Epidemic routing are considered, specifically tackling those emerging from the use of Bloom filters and those related to congestion control and buffer management. Several versions of Epidemic implementing different solutions to these problems are then evaluated using NS3, identifying a Bloom filter implementation very effective in practical uses and also a combined congestion control mechanism that significantly improves the goodput of the network. In [9], the resilience of popular forwarding schemes is evaluated with respect to a set of challenges to their normal operations, namely jamming, hardware/software failures, and free-riding nodes. This resilience is evaluated, differently from the other contributions available in the literature, in terms of metric envelopes, which identify the best and worst case response of a metric.

Content dissemination in opportunistic networks is studied in [10]. Specifically, the authors propose a content-sharing system implementing a ranked search used to decide what content to exchange and in what order. The search matches the content stored locally on a device against the interests of the other users that the node has collected. Also an optional content delegation mechanism is implemented that allows to altruistically disseminate a limited amount of items based on the interests of third-parties nodes. The proposed system is evaluated through a real world experiment with mobile phones running a picture sharing application.

Real implementation issues faced in a remote village scenario are discussed in [11]. Within the N4C project, field tests have been carried out to develop and test a DTN system in a challenged scenario. One of the target areas was the Padjelanta national park in Sweden, whose population is primarily the nomadic Saami reindeer herding families who live there during the summer season. A DTN system was deployed there, providing the services of email, podcast, web caching and messaging.

Finally, the special issue also includes two papers that consider instances of the opportunistic paradigm applied to vehicular ad hoc networks (VANETs). Within this framework, the work in [12] guides us through the available solutions for routing messages in opportunistic VANETs. Instead, [13] focuses on a specific application of VANETs, an opportunistic parking assistance system, in which nodes opportunistically collect and share information on the location and availability of parking lots, and investigate the impact of misbehaving nodes, which can defer from sharing information or even forge the information they share in order to gain a competitive advantage.

Acknowledgements

To conclude, we would like to express our gratitude to all the authors who have contributed to this special issue by submitting their work, and to all invited reviewers for their invaluable feedback and responsiveness under tight deadlines, which have contributed to ensuring the highest possible quality for this special issue. A special thanks also to Dr. Marco Conti, Editor-in-Chief of Computer Communications, for his continual support and suggestions at all the stages of this special issue. Our most sincere appreciation also goes to the Elsevier's staff for their invaluable cooperation.

References

[1] V. Mota, F.D. Cunha, D.F. Macedo, J.-M.S. Nogueira, A.A. Loureiro, Opportunistic networks: a survey, models and tools, Comp. Commun. 48 (2014) 5–19.
[2] H. Chen, W. Lou, Gar: group aware cooperative routing protocol for resource-constraint opportunistic networks, Comp. Commun. 48 (2014) 20–29.
[3] A.J. Aviv, M. Blaze, M. Sherr, J.M. Smith, Privacy-aware message exchanges for humanets, Comp. Commun. 48 (2014) 30–43.
[4] C.P. Mayer, O.P. Waldhorst, Routing in hybrid delay tolerant networks, Comp. Commun. 48 (2014) 44–55.
[5] C. Boldrini, M. Conti, A. Passarella, Performance modelling of opportunistic forwarding under heterogenous mobility, Comp. Commun. 48 (2014) 56–70.
[6] P. Sermpezis, T. Spyropoulos, Understanding the effects of social selfishness on the performance of heterogeneous opportunistic networks, Comp. Commun. 48 (2014) 71–83.
[7] P. Ginzboorg, V. Niemi, J. Ott, Message fragmentation for a chain of disrupted links, Comp. Commun. 48 (2014) 84–97.
[8] A. Marandi, M.F. Imani, K. Salamatian, Practical bloom filter based epidemic forwarding and congestion control in dtns: a comparative analysis, Comp. Commun. 48 (2014) 98–110.
[9] F. Bjurefors, M. Karaliopoulos, C. Rohner, P. Smith, G. Theodoropoulos, P. Gunningberg, Resilience and opportunistic forwarding: beyond average value analysis, Comp. Commun. 48 (2014) 111–120.
[10] E. Nordström, C. Rohner, P. Gunningberg, Haggle: opportunistic mobile content sharing using search, Comp. Commun. 48 (2014) 121–132.
[11] S. Grasic, A. Lindgren, Revisiting a remote village scenario and its dtn routing objective, Comp. Commun. 48 (2014) 133–140.
[12] N. Benamar, K.D. Singh, M. Benamar, D.E. Ouadghiri, J.-M. Bonnin, Routing protocols in vehicular delay-tolerant networks: a comprehensive survey, Comp. Commun. 48 (2014) 141–158.

[13] E. Kokolaki, M. Karaliopoulos, G. Kollias, M. Papadaki, I. Stavrakakis, Vulnerability of opportunistic parking assistance systems to vehicular node selfishness, Comp. Commun. 48 (2014) 159–170.

C. Boldrini
Istituto di Informatica e Telematica, CNR, Pisa, Italy
E-mail address: chiara.boldrini@iit.cnr.it

K. Lee
School of ECE,
UNIST (Ulsan National Institute of Science and Technology),
Ulsan, Republic of Korea
E-mail addresses: khlee@unist.ac.kr

M. Önen
EURECOM, Sophia-Antipolis, France
E-mail addresses: melek.onen@eurecom.fr

J. Ott
School of Electrical Engineering, Aalto University, Finland
E-mail addresses: jo@netlab.tkk.fi

E. Pagani
Computer Science Dept., Università degli Studi di Milano, Milano, Italy
E-mail addresses: pagani@di.unimi.it

Available online 19 April 2014