The International Journal of Parallel, Emergent and Distributed Systems
Vol. 00, No. 00, Month 2011, 1–28

RESEARCH ARTICLE

Opportunistic Forwarding for User-Provided Networks

Efthymios Koutsogiannis[a], Lefteris Mamatas[b]* and Vassilis Tsaoussidis[a]

[a]*Democritus University of Thrace, Department of Electrical and Computer Engineering, Building A, Panepistimioupoli Xanthis, Kimmeria, 67100 Xanthi, Greece*; [b]*University of Macedonia, Department of Applied Informatics, 156 Egnatia Street, 546 36 Thessaloniki, Greece*

(*v1.0 released January 2017*)

We study opportunistic forwarding in a community-based networking paradigm where mobile users and shared access points (SAPs) collectively provide Internet access to users (mobile or not), including those in areas where other connectivity options are not available. Our approach is based on an efficient interoperation of two challenging network types: the opportunistic and the user-provided networks (UPNs). This requires a re-evaluation of the existing assumptions regarding inter-contact patterns and their alignment to this hybrid environment. We confirm our arguments with numerical results from a stochastic model as well as experimental scenarios with realistic parameters using the ONE simulator. Our experiments are based on a reference routing algorithm we designed and implemented that extends the spray 'n focus protocol and exhibits the following characteristics: (i) is oriented to this integrated environment; (ii) employs delay-tolerant networking (DTN) technologies along with contact prediction; and (iii) is independent of the deployed UPN approach. According our results, the proposed methodological approach achieves lower communication overhead, latency and storage requirements compared to representative opportunistic routing algorithms.

Keywords: User-Provided Networks; Delay-Tolerant Networks; Opportunistic Communications; Contact Prediction

1. Introduction

There is a recent trend in the networking research that brings together mobile and fixed infrastructure resources, such as the Mobile Edge and Fog Computing [43], [4]. Its main goal is a fruitful inter-operation between both sides of the network edge, supporting novel applications and services for heterogeneous wireless/mobile networks, including 5G, WiFi, wireless sensor networks and Internet of things (IoTs) deployments. Such approaches can enable localized applications operating at very low time-scales, e.g., virtual servers hosted in nearby cloud environments can provide services to the mobile users. Furthermore, a number of research works (e.g., [33]) investigate autonomous mobile applications, where mobile users communicate between each other and the local infrastructure through short-range wireless communications, e.g., WiFi, near field communication (NFC), Bluetooth and WiFi Direct. Example applications are for local information search, car pooling and healthcare [33], [38].

---

*Corresponding author. Email: emamatas@uom.edu.gr

ISSN: 1744-5760 print/ISSN 1744-5779 online

DOI: 10.1080/17445760.YYYY.CATSid
http://www.informaworld.com

In this context, we argue that community supported networks can be seen as a main enabler for such capabilities, increasing the connectivity options and improving performance of mobile users. Users can be organized in communities, forming a shared network access infrastructure. For example, home-users could be sharing their Internet connection with other users passing by their area, in exchange for their own Internet access at times they are out of home. Such user-provided networks (UPNs) (e.g., [50], [2] - [7]) have been proposed as an efficient way to exploit the available network resources that are either unused or underutilized, thus improving network coverage even without additional network equipment. In support to the above arguments, paper [37] investigates the relation between UPN proposals and equivalent competing wireless network access technologies (e.g., cellular networks).

The earlier UPN proposals (e.g., studies, implemented approaches or network access sharing incentive mechanisms) consider home-users as potential mini-providers and focus on the infrastructure side of the solutions (e.g., FON [2], OpenSpark [6] and WiFi.com [7]). Recently a new generation of UPN approaches appeared (e.g., [24], [40]) which implement multi-hop routing among the wireless links [45], increasing furthermore the Internet access area and improving the quality of service (QoS). Other researchers propose network protocols focusing on the efficient sharing of network resources between the home- and the guest-users. For example, in our previous studies [44], [36], [31], we proposed service differentiation and load balancing mechanisms guaranteeing that home- or office-users only offer their unused resources to mobile devices in the area.

In the current work, we investigate a relevant communication environment that goes one step further, considering mobile users as Internet gateways through handling the associated intermittent connectivity. We assume a coexistence of several networks or technologies with a wide-range of characteristics (Wi-Fi, wired Internet, plethora of mobile devices - phones, PDAs, laptops, etc.). Such environments are bridging the connectivity gaps between distant user-provided WiFi access points (APs). They have a self-evident opportunistic nature, since connectivity is both intermittent and unscheduled. The delay-tolerant networking (DTN) [17] paradigm has been proposed for networks with similar challenging communication conditions (e.g., with frequent link disruptions). However, we consider here the delay-tolerant networks (DTNs) as extensions of the Internet, rather than as independent networks, i.e., we are handling the relevant heterogeneity aspects.

In such a hybrid environment, advanced data storing at mobile users and shared access points (SAPs) is a main an enabling technology, i.e., the store-carry-and-forward paradigm, which adds storage in the routing parameters and relies on the movement of the mobile users to exploit even the slightest communication opportunity. We argue that a routing strategy should exploit dynamically: i) mobility, in order to increase the potential on data communication; ii) operational capacity of participating nodes, including energy and storage; and iii) fixed infrastructure, in order to alleviate the communication burden of mobile nodes. Hence, such strategy should combine various distinct tactics that are adaptable to the network conditions.

More specifically, there have been several protocol mechanisms that attempt to reduce redundant transmissions and increase the performance of mobile nodes (e.g., those described in section 2). Given the resource-constraints of mobile devices, it is crucial to minimize the requirements in both hardware (i.e., GPS, battery) and software resources (i.e., memory, CPU usage). Here, we focus on the contact prediction mechanisms, not only between mobiles but also between mobiles and the infrastructure. We assume that intermittent connectivity can appear both in the wireless links between the mobile nodes and at the access point level (e.g., users may occasionally enable or disable sharing). Mobile nodes can predict future contacts and further estimate which node is more suitable to forward the data to the Internet. Under certain conditions, inter-contact times can be utilized as a means to estimate with notable accuracy the network topology.

To demonstrate the potential of our approach, we introduce a reference opportunistic routing protocol that employs contact forecasting and is suitable for any UPN cooperative networking scheme, as long as the WiFi access points and the mobile nodes incorporate data storage. Future contact prediction in this hybrid environment is achieved via storing history of encounters and performing curve fitting of inter-contact times distribution. Our routing mechanism adopts the limited data replication features of the *Spray & Focus* [52] protocol (i.e., discussed in Section 2) to exploit node mobility and reduce the imposed overhead. We evaluate our proposal against a number of popular protocols in realistic scenarios. Our results show that our protocol outperforms the aforementioned protocols with regard to imposed overhead, latency and data buffering time.

Our proposal could work in other access network infrastructures as well (e.g., networks of hotspots or infostations). Such facilities may benefit from mobile network extensions, e.g., the shared wireless infostation model (SWIM) solution brings together the infostation concept with the ad hoc networks [49]. Here, we selected to focus on the user-provided networks, since they constitute a challenging representative.

We summarize the main contributions of this paper below:

- We present the studied network environment and the relevant routing issues, i.e., a User-Provided Network utilizing both Shared Access Points (SAPs) and mobile users that are collectively providing Internet access through mitigating the intermittent connectivity issues.
- We analyze the main characteristics of this hybrid network environment with a continuous-time Markov chain based theoretical analysis, such as the impact of the community-based infrastructure on the mobile communication and the trade-off between forwarding data or storing them for another upcoming communication opportunity.
- We revisit existing assumptions and analysis related to the inter-contact patterns and propose particular adjustments towards manifesting improved forecasting accuracy for such hybrid infrastructures.
- We integrate our findings into a reference protocol and compare it with other representative opportunistic protocols by conducting simulations with realistic parameters (e.g., using real city maps and locations of SAPs).
- We define the next steps to improve our proposal furthermore, including the relevant security / privacy issues and incentive mechanisms motivating users to participate in such community-based schemes.

In section 2, we discuss the studied context, its associated characteristics and contrast the related studies and mechanisms to our proposal. In section 3 we provide a theoretical analysis regarding the impact of different routing strategies in terms of efficient Internet access through SAPs. In section 4, we elaborate on the inter-contact times distribution as an important routing factor and detail our proposed mechanism. The experimental evaluation lies in section 5. We present our next steps along with important aspects such as security, privacy and incentive mechanisms and conclude this paper in sections 6 and 7, respectively.

2. Studied Context and Related Works

Ubiquitous connectivity constitutes a modern necessity, particularly in metropolitan areas, which due to the recent advances in technology and user habits (e.g., novel telecommunication systems, improved power consumption of mobile devices, crowded areas with mobile users) can be covered at a great extend. In this context, user-provided networks have been proposed [50] as an umbrella framework for broadband access sharing. This networking scheme is based on Wi-Fi access sharing by home-users that are willing to dispense a portion of their bandwidth in order to enhance mobile connectivity. Existing UPN approaches with a wide adoption, such as the FON [2], the OpenSpark Community [6] and the WiFi.com [7], demonstrate that commercial deployment of such initiatives is indeed possible. The new generation of UPN solutions bring together community-based network access sharing schemes with wireless and mobile networks. For example, the ad hoc paradigm is adopted from the Athens wireless metropolitan network (AWMN) [1] and the Lancaster University [24], where mobile nodes implement multi-hop communication to increase the network access area.

Most existing relevant proposals, with the exception of [40], [45], [28], do not consider the opportunistic nature of the guest-users, often moving between different access points and thus facing intermittent connectivity. We note that intermittent connectivity, at a different time-scale, is often characterizing home access points also, since it is not expected a 24-7 operation from a community-operated access point. For example, in UPN approaches without credit-based mechanisms (e.g., the Whisher solution acquired by WiFi.com [7]) a user can register to participate but occasionally turn off his access point when he is not using it [58]. The Bytewalla proposal [40] uses opportunistic networking technologies but to implement a data-mule paradigm (i.e., assuming mobile users are carrying data over long distances). The work in [45] introduces the Delay Tolerant Reinforcement-Based (DTRB) routing solution and the Messages on oFfer incentive mechanism, while investigating the tethering-based UPN approach (i.e., mobile users act as Internet access networks, assuming no fixed Internet access infrastructure). DTRB uses Multi-Agent Reinforcement Learning (MARL) techniques to detect available routes and deliver the messages producing a best reward.

Here, we suggest that any cooperative networking scheme using access points and mobile devices with integrated storage capabilities could potentially offer improved connectivity to mobile users. In [28], we evaluated the impact of such scheme, showing a significant improvement on the communication of mobile devices with the Internet in terms of delivery ratio, overhead and delay. In practice, we evaluated the suitability of state-of-the-art DTN routing protocols for this mixed environment, such as *Epidemic* [54], *Spray & Focus* [52] and *MaxProp* [12].

Epidemic routing [54] is using flooding to replicate and transmit messages to new contacts without a message copy, which can be controllable to reduce communication overhead. Two important but similar protocols, namely the *Spray and Wait* [51] and *Spray and Focus* [52], are using the packet replication technique. The protocols share common functionality regarding the "Spraying" phase, where a predetermined number of a packet's copies is being transmitted to different relays. Moreover, in "Wait" phase each of the relays caries its copy until it encounters the destination directly. On the contrary, in "Focus" phase when a relay has a single copy available, it will forward the copy to another relay based on a single-copy utility function, using timers and history of encounters.

There is a number of probabilistic opportunistic routing approaches, such as *MaxProp* [12] and *PRoPHET* [34]. The *MaxProp* algorithm prioritizes the schedule of packets to be transmitted and dropped, based on historical data and several complementary mechanisms. It implements flooding until the discovery of a contact. Then, all messages not directed to the particular contact will be replicated and transmitted. The protocol implements an intelligent approach to rank the messages to be transmitted and those that will be dropped. Practically. *MaxProp* uses an ordered-queue based on each message destinations, ordered by an estimated likelihood of an existing future path to that destination. The *PRoPHET* protocol exploits the non-randomness of real-world encounters by maintaining a set of probabilities for successful delivery to known destinations and replicating messages to nodes that have a better probability to deliver them.

We note that existing state-of-the-art DTN routing protocols are not the ideal solutions for the studied hybrid network environment, i.e., they are designed for homogeneous opportunistic environments and are not considering the surrounding fixed infrastructure that can assist the communication. For example, an efficient DTN routing protocol could allocate functionality and offload resources to the infrastructure networks. This allows for significant resource saving, e.g., in terms of energy and storage. In addition, wired connectivity between SAPs ensures instant communication and data dissemination, when necessary. In [28], we justified experimentally the need for a hybrid opportunistic protocol, employing strategies adapted to the nature of the communicating node (i.e., whether it is fixed or mobile). The same argument is confirmed from our theoretical analysis in the following section.

A similar approach have been followed for other mixed networking environments. For example, paper [59] proposes a hybrid framework that integrates DTN with IoT communications and solution [20] brings together IoTs with infrastructure networks in a Fog Computing context. Regarding hybrid VANET environments, the research work [47] proposes a hybrid extension of *MaxProp* protocol and proposal [57] groups nodes based on their contact characteristics in order to apply different routing strategies per group. A hybrid routing approach to a disaster scenario is presented in [21]. It considers both fixed nodes (e.g., throw boxes) and mobile nodes (e.g., mobile relief workers). In paper [56], the authors propose a Hybrid DTN-MANET routing protocol which applies DTN strategies between disjoint groups of nodes and MANET routing within these groups. Another protocol bringing together DTNs with MANETs is *OLSR-OPP* [10], which is an opportunistic extension of the *Optimised Link-State Routing (OLSR)* [16] protocol. The idea is to combine the efficiency of the OLSR-based MANETs with the flexibility of the store-and-forward concept of DTNs.

Other relevant opportunistic routing protocols do not consider hybrid environments rather than hybrid networking conditions. For example, the routing algorithm *HMCR* [55] has been proposed for space environments. *HMCR* uses a multiple copy routing algorithm that combines contact graph and delivery probability metrics to make forwarding decisions. Approach [25] combines the *Spray-and-Wait* with the *PRoPHET* routing protocols with the aim to intelligently route sufficient number of message copies in the network. The hybrid routing protocol, presented in [9], is adaptively switching between cooperative forwarding and reactive store-carry-forward routing.

In this paper, we elaborate on the need for hybrid opportunistic routing strategies bespoke for the studied environment using a theoretical analysis. Additionally, we propose a relevant protocol that employs prediction of contact opportunities. Knowledge about future contacts allows mobile devices to take the most appropriate decisions regarding information forwarding or even energy-saving strategies (e.g., to suspend the network subsystem whenever there is no connection). For example, an efficient routing algorithm could predict the next contact using an estimation of the inter-contact times distribution. The latter characterizes the time gaps separating two contacts between the same pair of nodes and derives at each node from the history of encounters.

Some years ago, the aggregated inter-contact time (AIT) distribution (i.e., for the system) was wrongly assumed to be similar to the individual node pairs inter-contact time (IPIT) distributions [39]. We note that the distribution type may change under certain conditions. From the theoretical view-point, the aggregated inter-contact time distribution can be represented as a mixture of individual node pairs' distributions [42]. Consequently, different parameters into the mixing distributions result into different aggregated distributions, ranging from exponential to heavy-tail distributions. This is also validated in a number of research papers that analyze measurements in real experiments:

- In [14], the authors suggest that at shorter time-scales (range of [10 minutes; 1 day]) both IT/AIT are characterized by a power law and for longer time-scales (range of days) the distribution changes, usually to exponential. This is confirmed from a wide-range of results from real experiments, e.g., three access point-based data sets and five direct-contact data sets. It is intuitively suggested that this allegation is associated with the probability of a user to revisit the same place, i.e., the half of day time-period may be associated to the end of working day.
- In [42], the AIT is associated with each IPIT. That said, in heterogeneous networks the type of the aggregating distributions defines the form of the aggregated distribution. Thus, focus should be given on the IPIT and the heterogeneity of individual pairs' contact patterns, rather than on the AIT statistics, which are not representative of network properties. Moreover, authors present examples with different sets of distributions.
- In [13], inter-meeting time distribution change from power law to exponential is related to the geometry of the topology (i.e., the diameter D of the network domain) and the correlation in mobility patterns. More specifically, the authors prove that stronger correlation in mobility patterns results in non-exponential beginning of inter-meeting time. In addition, contact-based metrics such as inter-meeting time, contact time and inter-any-contact time proved to have the invariance property; more specifically, the mean of these metrics is independent of the degree of correlation.

In the current work, we attempt to re-evaluate these assumptions in the context of our environment, which has particular requirements. For example, our reference protocol uses a contact prediction method that estimates the distribution of inter-contact times of each node with every SAP, thus it is neither aggregated nor individual pair as in previous references, but rather an intermediate approach since every SAP is considered as the same single node. Curve fitting is used in order to determine the properties of the distribution, based on the history of previous encounters and other practical constraints (e.g., considering realistic time-scales).

In the next section, we present a theoretical analysis that investigates: (i) opportunistic routing mechanisms that exploit the characteristics of the studied environment, and (ii) the involved performance trade-offs.

3. Theoretical Analysis

In order to investigate basic characteristics of the integrated UPN and DTN context and relevant routing strategies, we approach stochastically a scenario that mixes mobile with infrastructure nodes (i.e., SAPs). The nodes forward data using well-established opportunistic routing algorithms, i.e., the first-contact (i.e., passing the data to the first node it contacts), direct-contact (i.e., passing the message to the destination only) and epidemic (i.e., using flooding). These algorithms are contrasted to a hybrid approach to the epidemic protocol that adapts its behavior to the node type (i.e., whether it is fixed or mobile).

Our stochastic model of choice is the Continuous-time Markov Chain (CTMC). This particular model allowed us to model state-change durations (i.e., in our case the inter-contact times) with exponential distributions and continuous time-steps. The choice of exponential distribution matches the behavior of the RandomWay-Point mobility model. Discussions on which theoretical distributions fit the inter-contact time distributions better can be found in sections 2 and 4. States are discrete and reflect the set of nodes hosting a file (i.e., to be transmitted to the Internet). For example, in a scenario with 4 mobile nodes and 1 SAP: the finite set of states S = $\{s_0, s_1, s_2, s_3, s_4, s_5\}$ and the mapping between states and physical nodes-cases are L(s_0) = {mobile 1}, L(s_1) = {mobile 2}, L(s_2) = {mobile 3}, L(s_3) = {mobile 4}, L(s_4) = {SAP 1}, L(s_5) = {Forwarded to the Internet}.

The initial state (i.e., s_{init}) can be equal to $s_0 = 10000$, which means the first mobile user initially hosts a file for transmission. In the first state change, assuming a contact of the first user with the second, the file could be forwarded to the latter node. This associates with a state change from s_0 to $s_1 = 01000$. In this example, we assume the mobile nodes incorporate the first contact routing algorithm. Algorithms such as epidemic use data redundancy and require even more states. For example, state 11100 means the first three nodes host the file. The end state is reached when the file is forwarded to the Internet. This scenario is characterized by the Markov property, since a state-change is based on the previous step only, i.e., transmission could start from any node so any state could characterize the initial condition.

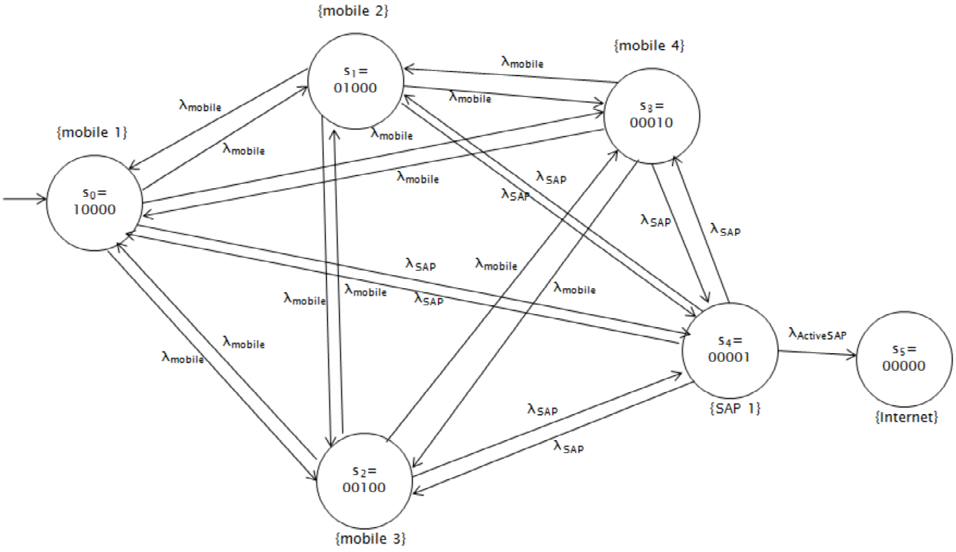


Figure 1. Markov state diagram of the direct contact routing algorithm

The proposed model is based on the following assumptions. We assume a total number of nodes *N*, i.e., *m* mobile nodes and *N-m* SAPs. Due to the ergodic properties of the scenario, a small number of nodes (i.e., N=5) deemed appropriate for the present study, while exhibiting acceptable complexity. Additional assumptions follow:

- SAPs may be active or inactive, i.e., a user may periodically disable sharing, when he requires more bandwidth.
- Mobile nodes are moving in accordance with the RandomWayPoint mobility model.
- The first mobile node hosts initially the data to be forwarded to the Internet (i.e., to an active SAP).

In figure 1, we present the Markov state diagram of the direct contact routing algorithm in a scenario with 4 mobile nodes and 1 SAP.

Below, we define the different exponential rates λ, representing the time between consecutive state changes. Since the mobile nodes are moving according the RandomWayPoint mobility model and based on the analysis in [8], we assume the inter-contact time between mobile nodes is characterized by an exponential distribution with rate λ_{mobile} and is independent from the spatial distribution of the mobile nodes:

$$\lambda_{mobile} = \frac{8r\rho\bar{\upsilon}}{\pi A^2} \tag{1}$$

where r is the radius of the node radio range, ρ is a fixed parameter with the value 1.3683, $\bar{\upsilon}$ is the expected mobile node speed and A the size of the assumed two-dimensional square area the node is moving.

The inter-contact time between the mobile nodes and SAPs is also characterized by an exponential distribution with a rate that depends on the SAPs' positions:

$$\lambda_{SAP} = 2r\bar{\upsilon}f(x,y) \tag{2}$$

where r and $\bar{\upsilon}$ parameters defined as above and $f(x,y)$ the PDF of node distribution at position (x,y).

For the RandomWayPoint mobility model, the spatial distribution of the mobile nodes can be captured by the function [11]:

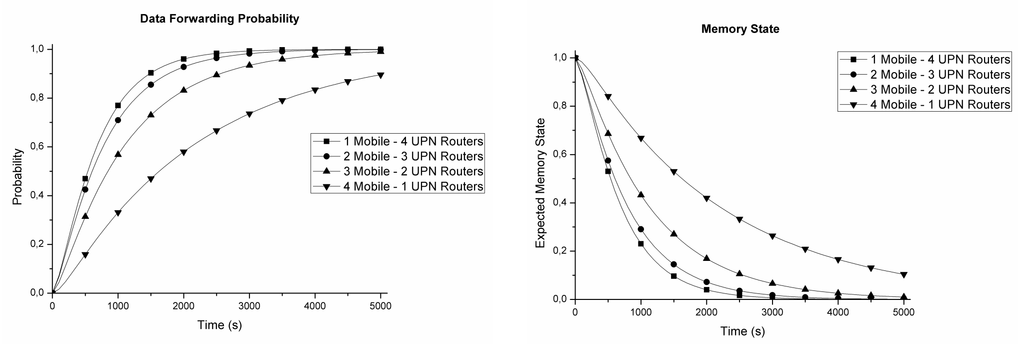
$$f_{XY}(x,y) \approx \frac{36}{\alpha^2}(x^2 - \frac{\alpha^2}{4})(y^2 - \frac{\alpha^2}{4}) \tag{3}$$

where α parameter defines the node movement limits (i.e., $-a/2 \leq x \leq a/2$ and $-a/2 \leq y \leq a/2$) and x,y the node coordinates.

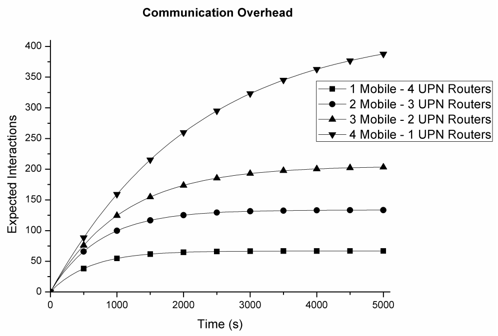
The PDF of a SAP's operation (active or inactive) could be matched from an exponential distribution with a relative high rate change $\lambda_{activeSAP}$, in order to reflect average surfing-time (e.g., a few hours per day).

Using the above model, we implemented four different routing algorithms:

- **First contact:** The sender passes the data to the first contact it meets.
- **Direct contact:** The sender forwards the data to the destination only.
- **Epidemic:** Every node in-contact with the sender receives a copy of the data (flooding).
- **Epidemic in SAPs:** Only the SAPs (even inactive) receive a copy of the data.



(a) Data forwarding probability (b) Memory state



(c) Communication overhead

Figure 2. Impact of the fixed nodes number on the performance of the first contact routing algorithm

We analyzed the proposed model and implemented routing mechanisms with the PRISM probabilistic model checker [29], using sets of parameter matching particular theoretical scenarios. The results follow.

3.1 Impact of Infrastructure on Mobile Communication

In the first scenario, we evaluate the impact of the number of fixed infrastructure nodes on the performance of the first contact routing algorithm. This is a simple scalability test of the deployed infrastructure, demonstrating also how beneficial it is for the mobile devices. We range the number of SAPs from 4 to 1 and the number of mobiles from 4 to 1, respectively.

In figure 2(a), it is evident that a large number of SAPs implies more Internet forwarding opportunities. This reflects on less memory state for the routing algorithm (figure 2(b)). This is not unreasonable, since the algorithm frees-up state, because the transmission is finished sooner. Through this simple example, we demonstrate how beneficial the infrastructure can be for the communication performance of the mobile users.

Contrasting figures 2(a) and 2(c) for the case of 1 mobile and 1 SAP it becomes evident that a larger number of interactions may not lead to better forwarding opportunities. In general, the total number of interactions between the users increases with the number of mobiles (figure 2(c)). The first contact algorithm does not have the sophistication to decide when it is reasonable to keep the data and when to forward it, i.e., forwards data in all contact cases, therefore an accurate estimation of contact-opportunities is needed.

3.2 To Forward or to Store?

In the second scenario, using the basic opportunistic routing algorithms as a reference, we explore the trade-off between the communication cost and the memory state. Furthermore, we contrast the epidemic algorithm with its variation called hybrid epidemic that acts as:

- the epidemic algorithm in case a mobile node contacts an infrastructure node.
- the first contact algorithm in case mobile nodes contact each other.

Epidemic and *hybrid epidemic* have almost the same data forwarding probability in a scenario with 1 SAP and 4 mobiles (figure 3(a)). For the same result (i.e., the data forwarding probability), the involved trade-off between communication cost and memory state is tuned differently for the two algorithms. *Epidemic* trades communication cost (i.e., lower number of interactions) for memory state (figures 3(b), 3(c)). The hybrid epidemic is doing the opposite, having a larger number of interactions (figure 3(b)) with much less memory state (figure 3(c)). Actually, the hybrid epidemic trades state for communication cost, in the case of mobiles only (figures 3(d), 3(e)), adapting to the node's resource constraints.

For example, a tactic trading communication cost for memory state should be used from devices with energy-expensive network cards. The reverse could be used from devices with memories that consume much energy for storing or accessing data frequently. In the case of SAPs, storing redundant data is not an issue, since these devices are not battery-powered.

To summarize the above analysis:

- Infrastructure can support mobile communication. For example, mobile devices could offload storage, processing or communication cost to the infrastructure.
- A sophisticated routing algorithm that follows hybrid strategies adapted to the type of communicating node is needed. It is important for this algorithm to be able to estimate the future contact opportunities.
- The involved trade-offs should be tuned in accordance with the node requirements and capabilities.

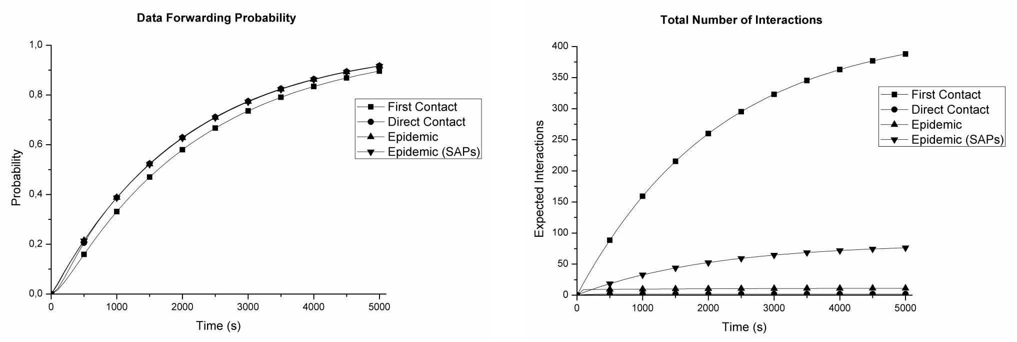
Such findings defined the requirements of our reference routing protocol and are described below.

4. Our Proposal

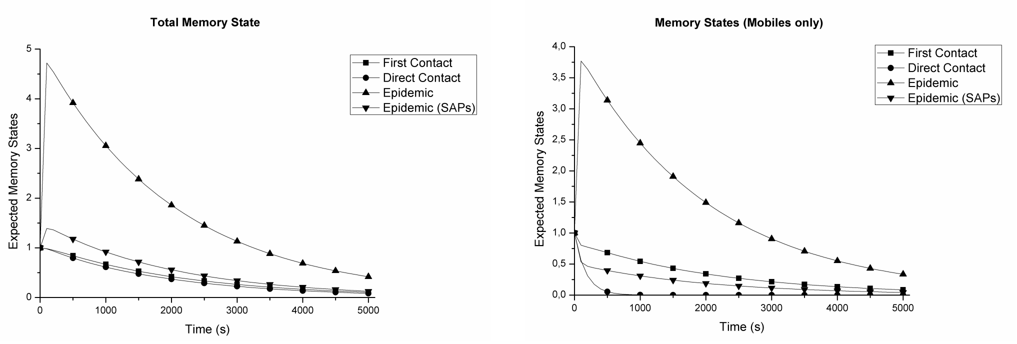
4.1 Design Considerations

The heterogeneity of the studied networking scheme provides significant advantages such as bandwidth surplus, energy and potentially storage adequacy on the wired part and mobility on the wireless. Nevertheless, energy, storage and bandwidth restrictions, along with intermittent connectivity are the main disadvantages that characterize mobile nodes. In order to exploit the benefits of the wired infrastructure, forwarding data to mobile nodes should be cautious and routing should effectively exploit shortest paths to access points and accommodate varying node density.

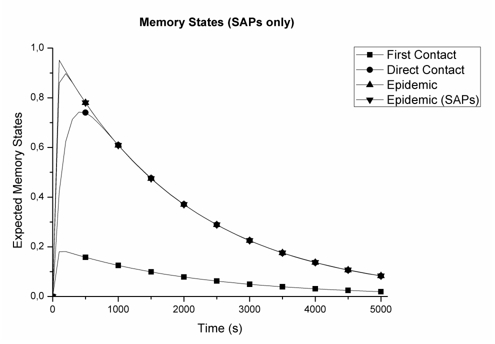
Therefore, a routing protocol should be capable of performing efficiently in sparse SAP topologies, relying on mobile nodes for delivery (operating in an opportunistic fashion). Replication-based mechanisms proved experimentally to be most efficient in the latter conditions in [28]; the theoretical analysis in [51] supports this claim further. Thus, this networking perspective could be covered by dispersing a limited



(a) Data forwarding probability (b) Total number of interactions



(c) Total memory state (d) Memory state of mobile nodes



(e) Memory state of SAPs

Figure 3. Investigating the trade-off between forwarding and storing in basic routing algorithms

number of copies to the mobile users in order to achieve high delivery probability to a distant SAP with minimal overhead.

However, in topologies where WiFi coverage is dense, redundant transmissions should be avoided and direct delivery to a SAP in the vicinity should be preferred. Hence, replication does not suffice since it can cause a significant impact on the overhead that can be avoided. Topological knowledge is a crucial factor for routing performance; especially in energy constraint networks it becomes dominant. The majority of smart phones nowadays is GPS enabled, however this is a very greedy feature regarding battery consumption. Moreover, frequent updates are necessary in order to estimate the destination of movement and acquire SAP exact positions, rendering such solution even more unsuitable. A simple and energy efficient mechanism is needed.

Nodes in urban environments may follow a movement pattern while passing by several SAPs. A node may revisit a previous SAP, but studying its history of encounters allows for a generic description of the node's likelihood to visit any SAP. We argue that connectivity probability for a mobile node could be estimated based on its previous encounters with SAPs. However, in this hybrid environment every SAP is considered to be an Internet extension, therefore one should focus on the frequency of connectivity availability to the Internet rather than on the individual point of access.

To show the potential of the proposed methodology, we designed and implemented a reference routing algorithm that relies on infrastructure in order to forward data to the final recipient (e.g., upload social network data to a server) and concurrently it exploits mobile nodes' mobility to achieve that. SAP contact prediction is a crucial part of the mechanism, thus we focused on contact prediction via inter-contact time and studied the types and characteristics of the distributions.

We elaborated on the *inter-contact* times distribution (ICD) of 50 mobile nodes in three scenarios with realistic access point topologies. London and Thessaloniki center maps were used along with shared access points, while the mobile nodes follow the map route movement model (implemented in the ONE simulator [26]) in the first two scenarios and the Random Way Point (RWP) movement model in the third. London and RWP scenarios implement the same network topology, however in RWP there are no map restrictions (e.g., roads, buildings), as opposed to London and Thessaloniki cases. More specifically, we present the ICDs in the experiments for the following groups: i) all nodes, ii) between mobiles only, iii) between mobiles and SAPs, and iv) between mobiles and any SAP.

	ICDs (i)	ICDs (ii)	ICDs (iii)	ICDs (iv)
London	Exp(0,63)	Exp(0,51)	Exp(0,86)	Exp(0,99)
Thessaloniki	Pow(0,85)	Exp(0,99)	Pow(0,96)	Exp(0,99)
RWP	Exp(0,51)	Exp(0,75)	Exp(0,55)	Exp(0,99)

Table 1. Inter-contact times distributions for 3 scenarios

Table 1 depicts the curve fitting results, namely the values of the squared correlation coefficient (r^2) and the best matching distributions for the three scenarios discussed. Compared to the other cases, using inter-contact time distribution between mobiles and any SAP in conjunction with Random Way Point model of movement, reduces significantly the possibility of heavy tail characteristics and further supports the claim that the exponential distribution is indeed suitable. The physical meaning is that it is more likely for a mobile user to meet any SAP than to meet a specific access point.

In [42] the CCDF of the aggregated inter-contact times is related to the CCDF of the inter-contact times between a pair of nodes $F_\lambda(x)$ whose rate is $f(\lambda)$ according to:

$$F(x) = \frac{1}{E[\Lambda]} \int_0^\infty \lambda f(\lambda) F_\lambda(x) d\lambda \tag{4}$$

In equation (4), λ is the inter-contact times rate of an individual pair of nodes, while the rates of individual pairs inter-contact times are distributed according to a continuous random variable Λ with density $f(\lambda)$ and $E[\Lambda]$ the expected value of Λ. Similarly to [42], we assume that $F(x)$ is the CCDF of the aggregated inter-contact times between mobile nodes and any SAP. Experimental results from Table 1, concluded that it is most likely that F(x) is exponential. Therefore since F(x) is exponential and $f(\lambda)$ is the rate density distribution[1], it is rational that the CCDF

---

[1] In our experiments, the exponential distribution matched better the rate density distributions, compared

of the inter-contact times of an individual mobile node, $F_{\lambda}(x)$, is exponential as well.

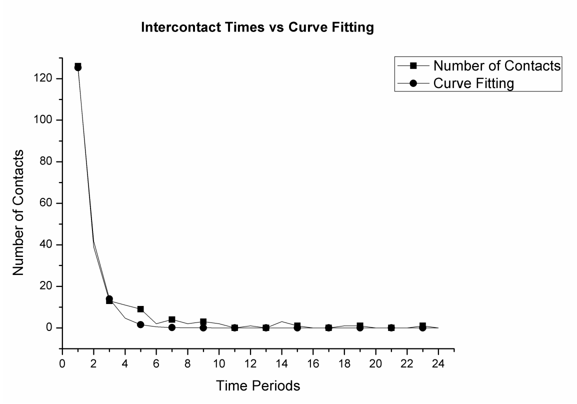


Figure 4. Intercontact times - Curve fitting comparison

In addition, Figure 4 depicts a representative example of curve fitting. The total inter-contact times of a mobile node are plotted along with the exponential distribution that is derived from the curve fitting process (the remaining values after 25 in the figure are zero). The exponential distribution ($f(x) = a * e^{b*x+c}$) matches the actual data, while r^2= 0.9915. Thus, it is reasonable to assume that in our experiments and regarding both mobility models (i.e., RWP and map-route shortest-path movement) the distribution of inter-contact times between a single mobile and any SAP matches the exponential distribution. Furthermore, the overall increased performance of the algorithm in section 5 amplifies the above claim.

As a bottom line, our routing mechanism predicts future SAP contacts by estimating inter-contact times distribution with any SAP. The latter follows the exponential distribution, hence contact prediction is feasible due to convergence. The imposed overhead comprises tracing of SAP encounters, computation of SAP encounter probability and the transmission of one packet per node encounter in addition to replication mechanism, which are justified by the significant protocol efficiency increase. This new algorithm exploits DTNs' main feature, unification of heterogeneous networking environments, in order to highlight the benefits from exploiting wired infrastructure interaction in mobile routing.

4.2 Hybrid Routing Mechanism

The algorithm should be efficient in both rural and metropolitan areas relying on mobile nodes or direct delivery to a SAP for data delivery, respectively. Therefore, its functionality comprises data replication at a first stage and regulation of forwarding at a second stage. The algorithm produces a fixed number of copies (i.e., parameter L)that disperses to neighbors according to "Spray" phase (specifically "Binary Spraying") [51] of "Spray and Focus" mechanism [52]. However, in "Regulation Phase", nodes rely on future contact prediction in order to route the single messages to SAPs. We selected the "Spray and Focus" mechanism as a basis, since it produced the best results against the state-of-the art DTN protocols we tested [28]. We used the same parameter L in both protocols. We plan to investigate other routing approaches in a future work, such as similar to the hybrid approaches dis-

---

to the theoretical distributions.

cussed in Section 2. The pseudocode of the proposed hybrid routing mechanism follows.

Hybrid Routing Mechanism's Pseudocode

"Spray Phase":

- The source node creates n message tokens for every generated message
- Every mobile node or offline SAP carrying n ($n > 1$) message tokens, forwards a message copy along with $\lfloor \frac{n}{2} \rfloor$ tokens and retains $\lceil \frac{n}{2} \rceil$ upon a contact
- A mobile node with a single token can only forward it further according to *Regulation Phase*

"Regulation Phase":

- Upon a new encounter, mobile nodes exchange the estimated number of SAPs they predict to contact
- The message is forwarded to another mobile node due to higher contact prediction, or to a SAP for delivery

In parallel, each mobile node upon a SAP contact updates its intercontact times and estimates its future SAP contacts according to the following pseudocode. Note that all SAPs are considered as simple Internet gateways and there is no topological knowledge, therefore each mobile is only concerned about the intercontact time distribution for any SAP.

SAP Contact Prediction Pseudocode

- Computes the intercontact time since last SAP encounter
- Increases by one the according intercontact time category (based on user defined granularity)
- Computes the parameters of the intercontact time distribution via curve fitting[1] for all time categories
- Estimates the number of SAP contacts in the imminent future (user defined period) by computing the integral of the distribution

Figure 5 depicts a scenario where a PDA in a rural area transfers a single copy of data to a smart phone passing by its area (step 1) during the Spray phase (PDA keeps another single copy), towards a metropolitan area. In step 2 the smart phone contacts a laptop in the vicinity. There is a single data copy, therefore according to Regulation phase the mobiles exchange contact estimation and the laptop receives the copy due to higher estimation value. In step 3, the laptop contacts the offline SAP 2 and transfers the data copy to it. SAP 2 does not have an active Internet connection ("occupied SAP"), however it communicates with online SAP 3 through WiFi. Hence the data is being delivered to SAP 3 (step 4) and along to the final recipient through the Internet. Therefore, in case of an "occupied" SAP (Internet access is prohibited to mobile nodes, however data storing is available) data can be transferred to online SAPs or mobile nodes in the vicinity, although the last copy is kept in case the SAP becomes online. Online access points deliver the data to the recipient instantly, while extra copies are being discarded.

---

[1] In our experiments, the Offset Exponential function (y = a * e^{b*x+c}) matched well the SAP intercontact times distribution, as shown in section 4.1.

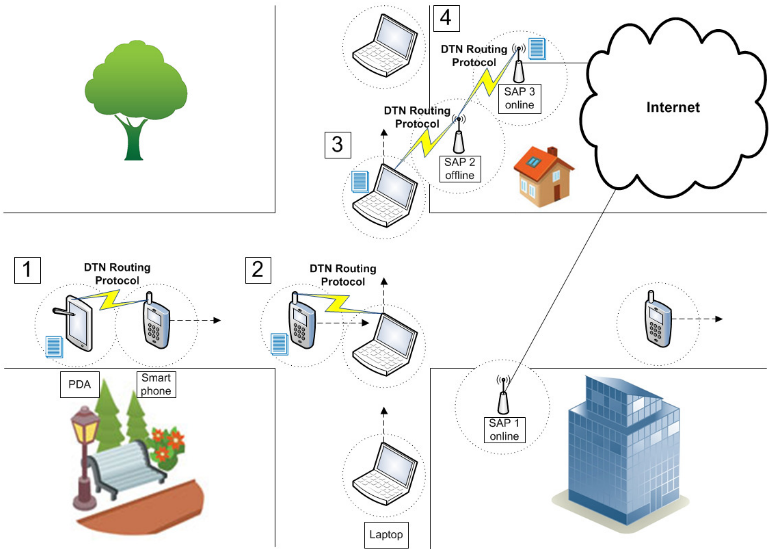


Figure 5. Protocol's functionality example-scenario

5. Experimental Evaluation

5.1 *Scenarios - Methodology*

In order to demonostrate the potential of the discussed methodological approach, we evaluate the performance of our reference routing protocol in the studied networking paradigm under realistic conditions. We simulate a geographical area of 2160m x 1600m, in the center of London. In Fig 6, the simulated area covers 349 different streets and 1876 landmarks. Based on detailed information about the specific area from [2], we have placed the exact number of FON users (i.e., 100 BTFON home-users - FON appears with the name BTFON in UK), at the corresponding coordinates. This results in a more realistic topology, since this set of users already expressed an interest to adopt a UPN-based network paradigm. We parsed the aforementioned information into ONE simulator.

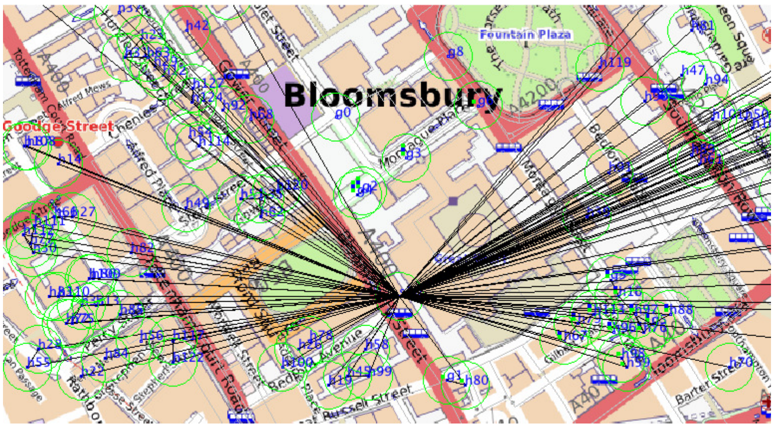


Figure 6. Simulated topology - Center of London

Furthermore, we extended the ONE simulator with better support for wired networks and two new types of nodes: (i) the home- or office-user that owns a SAP, and (ii) a server node, which hosts data for the mobile users (e.g., social profile photos). We assume that all home-users are permanently connected to a server node (e.g., a server farm) with a wireless interface too, situated in Gower Street (see Fig. 6). We designed and implemented the discussed DTN routing protocol, along with additional functionality on statistics. Several modifications were made in ONE in order to operate realistically, such as enabling deletion of duplicate, already delivered messages in SAPs for all algorithms. Moreover, it should be noted that in the current work we focus on the uplink and leave the downlink as a future work. Depending on the characteristics of the data (e.g., volume, urgency) the proposed scheme can also be applied to the downlink using the mechanism of contact prediction and message replication, in order to reach the mobile destination through intermediate mobile nodes. However, further SAP exploitation can be accomplished in order to send the data directly to the mobile recipient. Contact prediction is needed in the latter case in order to send the data through the wired infrastructure to the nearest SAP to the mobile destination and avoid intermediate mobile nodes.

Mobile nodes are moving in the area and transmit periodically data (every 60 to 80 seconds, according to a uniform distribution) to the server node, while their speed is approximately that of a pedestrian (0,5 - 1,5 m/s). Message sizes follow the uniform distribution [100kB, 200kB] (e.g., a typical social profile photo). Their movement is restricted to the streets in the map, according to the map route and shortest path algorithms, supported from the ONE simulator. Mobile nodes and SAPs are set to 30m transmission range. The upper bound in the number of mobile nodes was restricted due to simulator's memory demands.

All nodes (mobile and fixed) have storage capabilities, but infrastructure nodes, i.e., SAPs, comprise extensive storage resources. In our setup, mobile nodes and SAPs have 30MB of storage available. These are only indicative figures and serve as pointers for future settings. Without loss of generality, we assume here a particular case of UPNs, where the SAP is only available to mobile users, whenever the home-user is idle. A similar approach is presented in [28]. This practically means that when the home-user is using his Internet connection, only storage capabilities are offered to the mobile nodes within range. We assume three representative home-user profiles: (i) users that are idle for 8 hours per day only (e.g., during working hours), (ii) users that are permanently idle (e.g., they are absent), and (iii) users that are only periodically using their connection throughout the day (i.e., according to a normal probability distribution: 1-3 hours at home and 1-2 hours away). Nodes periodically transmit beacons to recognize each other's presence. Fig. 6, shows our experimental setup. The server is referenced as s-node, mobile-guests as g-nodes and home-users as h-nodes.

Since a crucial aspect is to maximize energy efficiency of the mobile nodes, a maximum data delivery ratio should be combined with minimum communication / storage overhead and latency. In this context, we measure the following:

- $OverheadRatio$, which is equal to: $\frac{PacketsRelayed - PacketsReceived}{PacketsReceived}$ and captures packet delivery ratio with respect to the number of packets relayed.
- $AverageLatency$, which captures the average packet latency that increases with the number of hops the packet crosses.
- $AverageBufferTime$, which reflects the average time the packets are buffered, in order to evaluate protocol storage efficiency.

Since we do not consider packet drops in our experiments, we omitted the delivery-ratio metric due to the space constraints.

We have evaluated how existing opportunistic routing algorithms behave in this hybrid networking scheme, where SAPs offer storage resources apart from only connectivity. We selected three representative storage-enabled algorithms, namely: *Spray and Wait* [51], *Spray and Focus* [52] and *MaxProp* [12] and compared them with a new we designed specifically for this environment. We chose the first two as the protocols with functionality closer to the proposed and the *MaxProp* as a representative probabilistic opportunistic routing protocol, used in hybrid network environments as well (e.g., in [47]). Due to space constraints, we left the more extensive comparison of the proposed work with other approaches (e.g., social-based routing or other probabilistic protocols like *PRoPHET* [34]) as a future work.

In our previous study [28], Spray And Focus was the overall outperforming algorithm. These preliminary experimental results evinced that the proposed networking scheme avails in terms of latency, buffering time and overhead ratio. Combining wireless nodes with wired infrastructure is significantly beneficial for mobile devices. Supporting this hybrid cooperating scheme by a suitable routing protocol, further enhances the mobile performance in every aspect. Thus, we integrated message replication with future contact prediction in order to design a SAP aware protocol that will perform efficiently in the proposed paradigm. This protocol discriminates mobile devices from SAPs in order to offload storage, processing and communication cost to the fixed infrastructure.

5.2 Experimental Results

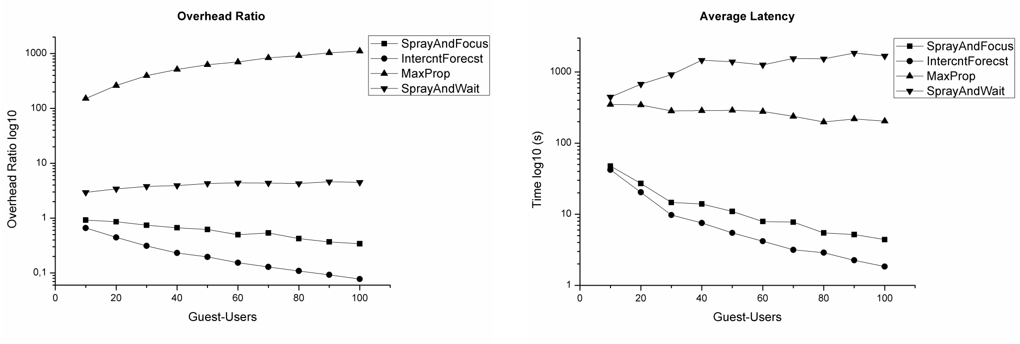
We have evaluated the proposed environment using three experimental scenarios in order to study its impact on the performance of the aforementioned algorithms. More specifically, we experimented on the impact of the topology, using a variety of mobile nodes and SAPs. In addition we conducted a scenario where SAPs follow different usage profiles in order to analyze the algorithms' performance. The exact network conditions and node movement were replicated, in order to receive comparable results.

5.2.1 Scenario 1: Impact of Guest-Users' Number

In this scenario, we compare the functionality of the four algorithms in accordance with the number of mobile users. The scalability potential of each algorithm in this extended opportunistic networking paradigm is also evaluated at this point. Theoretically, in conditions of low number of mobile nodes, the performance of the algorithms should be similar, since routing is limited. Moreover, as the number of guest-users increases the impact of routing strategy should be more obvious and the most efficient strategy would be to relay data to nodes that are most likely to visit a SAP sooner. We have used the topology of 100 SAPs constantly available and a variety of 10-100 mobile nodes.

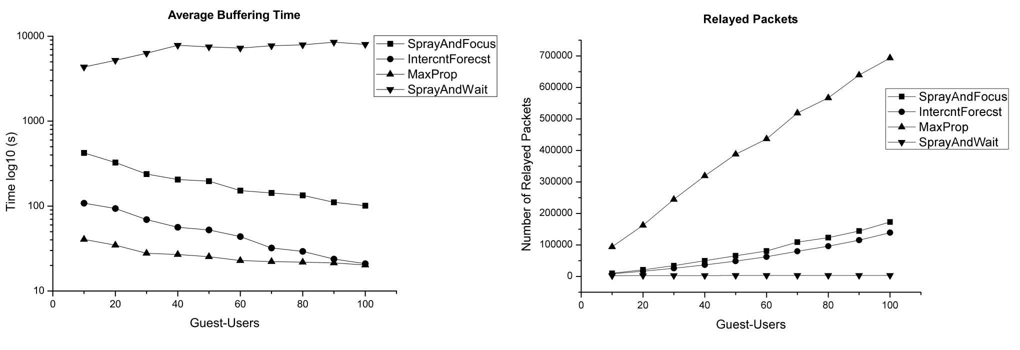
The overhead ratio of each algorithm is presented in Fig. 7(a). *MaxProp* appears to have a linear curve as mobile users increase, therefore its worst performance justifies the logarithmic scale. Replication based algorithms achieve much lower overhead ratio than *MaxProp*, while *Spray and Focus* and the proposed mechanism are favored by the increase of the guest-users and manage to reduce their overhead ratio.

Fig. 7(b) depicts algorithms' average latency on a logarithmic scale. Increasing the number of guest-users, has a negative impact on *Spray and Wait* and slightly beneficial on *MaxProp*. On the contrary the proposed algorithm along with *Spray and Focus* exploit the abundance of mobile nodes and using more sophisticated approaches achieve much lower average latencies. In addition, average buffering time is presented in Fig. 7(c). *MaxProp* appears to have the lowest buffering time due to its flooding-based nature and message removal policies. Experimental results prove that *MaxProp* removes significantly more messages at the nodes than



(a) Overhead ratio

(b) Average latency



(c) Average buffering time

(d) Relayed packets

Figure 7. Impact of the guest-users' number

the other algorithms, even though not presented here owing to space limitation. In addition, it should be noted that as the number of guest-users increases the improvement is insignificant. *Spray and Wait* appears to be the worst performing algorithm due to lack of sophistication, while the proposed algorithm achieves lower average buffering time as the number of guest-users increases. The difference in functionality is also obvious in the number of relayed packets in Fig. 7(d). *Spray and Wait* disperses all the copies during the "Spray" phase and operates as *Direct Delivery* algorithm during the "Wait" phase, therefore the increasing number of guest-users has almost none effect on its performance. On the contrary *MaxProp* appears to have a linear relation to the number of guest-users, showing inability to adapt and the worst performance as well. The proposed algorithm along with *Spray and Focus* appear to scale well with respect to the increasing number of guest-users.

In conclusion, as the number of guest-users increases, the proposed algorithm outperforms in terms of overhead ratio and average latency. In addition, it performs more efficiently than the others with regard to average buffering time and relayed packets, especially when taking into consideration that the algorithms that achieve better results have limited or inappropriate functionality (e.g., package removal). Therefore the proposed mechanism is the most efficient with respect to the increasing number of guest-users.

5.2.2 Scenario 2: Impact of Home-Users' Number

In the second scenario, the four algorithms have been evaluated with regard to home-users' number. We focus on the impact of different number of SAPs using 100 guest-users. Despite the large number of guest-users for the specific topology, it should be noted that the experimental results of *Scenario 1*, showed that the performance of the proposed algorithm converged to that of the second best algorithm so far, *Spray and Focus*, for those values (it is not clear due to the logarithm in the figures). Therefore, the impact of the proposed cooperative networking scheme on routing was evaluated under the most unfavorable conditions.

The number of SAPs varies from 0 (the server has a wireless interface also) to 100. Few home-users result solely in exchange of messages between mobile users in order to deliver data, canceling in a sense the benefits of the proposed scheme. However, as the number of SAPs increases, relaying data to mobile users should be reduced and home-users should be prioritized in routing as to deliver data to the server. Therefore the specific scenario allows studying the algorithms' functionality under highly opposite SAP density conditions.

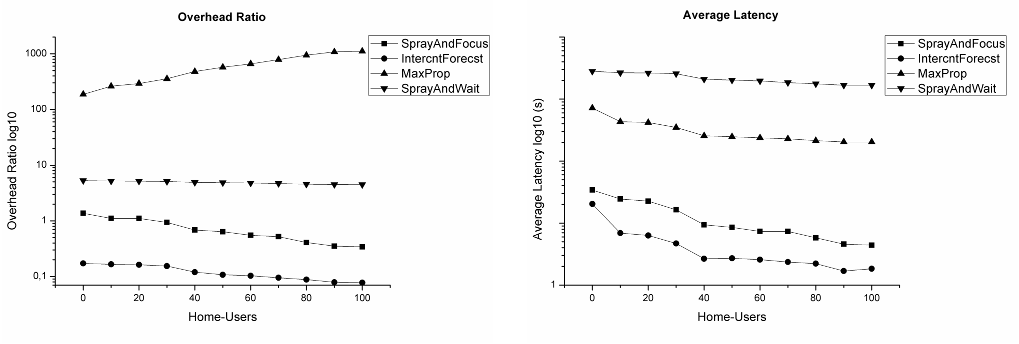
The overhead ratio achieved is depicted in Fig. 8(a). *MaxProp* is the worst performing with respect to overhead and appears to have a linear relation to the number of SAPs, therefore logarithmic scale is needed. The performance of *Spray and Wait* is slightly improved as the number of SAPs increases, whereas the proposed algorithm is outperforming and along with *Spray and Focus* take advantage of SAP density and reduce their overhead. In Fig. 8(b) the average latency verifies that mere replication and flooding-based routing are not exploiting the topological changes at the extend the others do. The difference in latency necessitates the use of logarithmic scale. Sophisticated routing policies result in more timely delivery, while as the number of SAPs increases the performance is further increased.

In addition, the average buffering time in Fig. 8(c) shows the significant difference in the functionality of the algorithms. *Spray and Wait* due to direct delivery achieves the highest average buffering time. *MaxProp* and the proposed algorithm appear to be quite similar, although the former due to removing messages and flooding them, while the latter owing to discriminating the nodes and exploiting the infrastructure. The number of relayed packages can also justify that claim in Fig. 8(d). As the number of SAPs increases *MaxProp* linearly increases the relayed packets. On the contrary the proposed algorithm manages to retain the relayed packets at the same levels both in absence and abundance of SAPs.

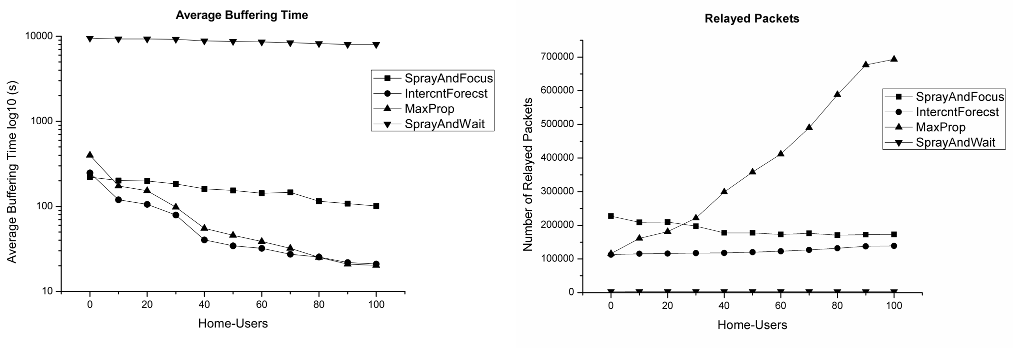
Regarding the specific scenario, the proposed algorithm is the overall most efficient. It achieves the lowest overhead ratio, average latency and buffering time at all times. Future contact prediction and forwarding policies allow it to adapt to highly opposite network conditions. It manages to cope with lack of infrastructure, based on its replication mechanism, while in cases of high network coverage it reduces redundant transmissions and buffering time based on SAP encounter forecast.

5.2.3 Scenario 3: Impact of Home-Users' Usage Profiles

In order to evaluate the proposed scheme in more complex and realistic conditions, such as in UPNs, we deploy a topology where each home-user adopts one of the three usage-profiles described in section 5.1. This scenario intends to study and compare the performance of *Spray and Focus* [52] as a representative opportunistic routing protocol with the one specifically designed for this environment, in a topology consisting of 100 home-users (due to performance convergence as in Scenario 1, even though it is not clear in these figures due to the use of logarithm) with different usage-profiles. The latter in conjunction with a variety of guest-user number, excludes the remaining algorithms due to poor adaptivity and overall reduced performance, as shown in previous scenarios. Therefore, we discriminate the cases according to home-users' percentage that follows each of the three usage profiles: A) always away, B) away for 8 hours, C) periodically away (1-3 hours at home, then 1-2 hours away). Moreover, we simulated the cases where (A, B, C) percentages are: i) (100, 0, 0), ii) (40, 20, 40), iii) (0, 0, 100), while guest-users vary (10-100).



(a) Overhead ratio (b) Average latency



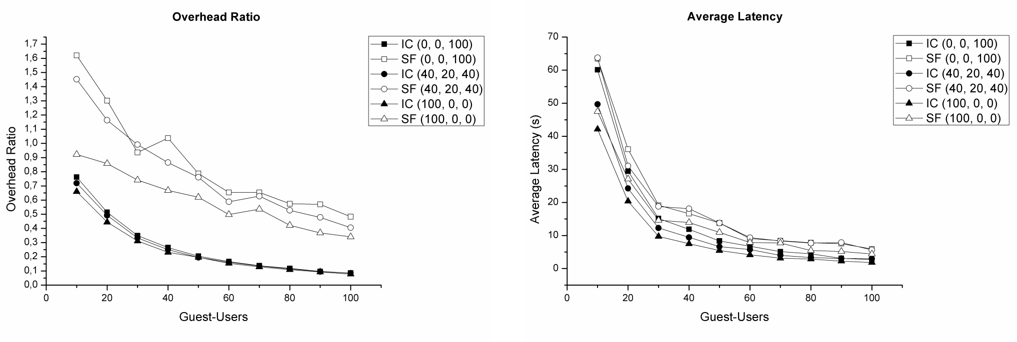
(c) Average buffering time (d) Relayed packets

Figure 8. Impact of home-users' number

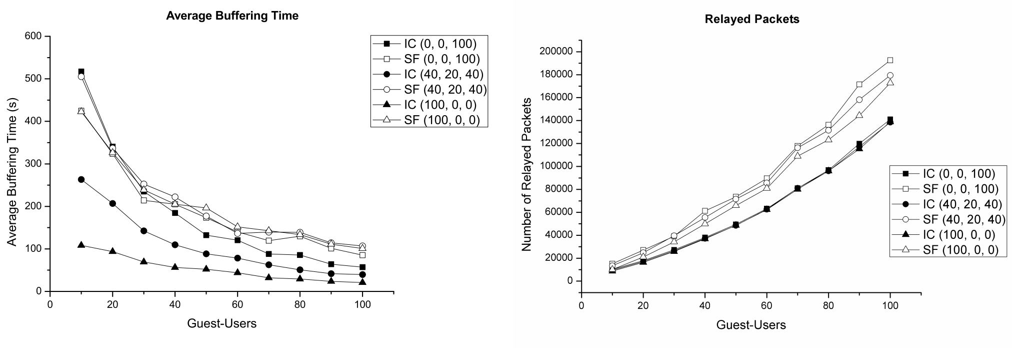
We conducted a series of experiments where increasing home-users with usage profiles (ii) and (iii), causes lack of connectivity, while increasing the number of guest-users allows for more routes and improved message delivery in terms of time. In these experiments, we observed that data remains stored at home-users available for: i) delivery to the server when connection will be up, ii) transmission to a guest-user in the vicinity, iii) transmission to a home-user in the vicinity.

The proposed algorithm achieves significantly less overhead ratio in any case as depicted in Fig. 9(a). It should be noted that *Spray and Focus* (SF) has quite different results in the two opposite cases (100% always on and respectively periodical use), while on the contrary the proposed mechanism (IC) confines the overhead ratio approximately the same. The proposed mechanism outperforms in terms of average latency, as depicted in Fig. 9(b) on a logarithmic scale. It achieves the lowest average latency in any case, while the spike in the case of (40, 20, 40) for 100 guest-users is justified by the topology and the high latency of the additional ten nodes. The average buffering time in Fig. 9(c) evinces the efficiency of the proposed algorithms regarding data storage. Comparing the corresponding curves, it is evident that even both algorithms improve as guest-user number increases, messages are buffered for much less time by the proposed algorithm than in *Spray and Focus*. Finally, in Fig. 9(d) the number of relayed packets of the proposed algorithm is constantly much lower and is kept to similar levels at any case, as opposed to the aforementioned algorithm.

Therefore, the new algorithm is most adaptive to the variation of usage profiles and guest-user increase. It outperforms *Spray and Focus* due to its sophisticated mechanisms in every metric used in this scenario. Furthermore, its main characteristics, contact prediction and message replication render it the overall most efficient protocol and highlight the significant benefit a hybrid cooperative scheme



(a) Overhead ratio (b) Average latency



(c) Average buffering time (d) Relayed packets

Figure 9. Impact of the home-users' usage profiles

can provide.

6. Open Issues

In this paper, we study a heterogeneous communication paradigm that comprises of infrastructure and mobile nodes. We consider data storing at mobile users and SAPs plus offloaded functionality to SAPs in order to improve resource efficiency. We employ inter-contact times estimation in routing and demonstrate the proposed methodology through a reference routing algorithm based on the principles of the DTN technologies. Although there is space for improvements in our routing protocol, it outperforms existing relevant mechanisms.

Further work on curve fitting methods in order to investigate the accuracy versus computing cost trade-off could improve the performance furthermore. Curve fitting requires complex computations, thus higher processing cost in order to have a precise estimation of future contacts. However, trading precision with computation by using different curve fitting or estimation method in general could result in a more energy efficient solution with little impact on routing. We justify the use of inter-contact times estimation through experimental and theoretical results. Nonetheless, the solid theoretical proof that a single node's intercontact times distribution with any SAP is exponential, remains a future work.

Message replication provides multiple paths and increases the probability of data to reach a SAP. In order to alleviate the communication overhead, the spraying phase could be redesigned in order to limit multiple transmissions based on the routing info and SAP contact estimation. Therefore, trading the communication cost with latency would increase energy efficiency in mobile devices. The main characteristic of the proposed hybrid communication scheme, offloading functionality to the SAPs, can be further enhanced as well. SAPs can be more active in routing and based on their "permanent" wired interaction they could direct network traffic and mobile nodes as well. Moreover, adding a SAP routing protocol that will handle inter-SAP communication through the wired infrastructure poses insignificant overhead in local area scale. Social-based routing approaches could be applied here efficiently, which is an aspect we plan to investigate. A more extensive comparative analysis of the proposed solution against other important opportunistic routing approaches, such as the probabilistic routing protocol using history of encounters and transitivity (PRoPHET) [34] protocol, is in our plans as well.

Beyond the improvements of the proposed routing algorithm, we work towards a complete infrastructure that provides relevant functionalities. This requires core aspects to be investigated, such as the associated security and privacy issues and the appropriate incentives for the users to participate in the bandwidth sharing scheme. The next step is to exploit the useful insight from this analysis to design security, privacy-preserving mechanisms and incentives that tackle these issues, while being adjusted to the proposed hybrid environment. An initial investigation of the above aspects follows.

6.1 Security and Privacy Challenges

Here, we investigate security and privacy issues related to the studied hybrid context that brings together UPNs with opportunistic networks. This requires a relevant analysis on both of these contexts.

On the one hand, there are the UPN-related security and privacy aspects. Paper [32] suggests a classification of the relevant WiFi sharing aspects that includes security threats, accounting risks and administrative and usability problems. In the bandwidth sharing environments, it is common to use a VPN solution that protects both the external mobile and the provided network users, using an authenticated and encrypted tunnel. For example, SWISH [32] establishes a tunnel from the provided network to the user's home network. It also provides protocol extensions for the charging of the forwarded data, while protecting privacy and preventing abuse. SWISH has been deployed at two Belgium universities and is based on a protocol (i.e., [46]) that uses cryptographic mechanisms implementing authentication between the external user, his home network and the visited network. However, VPN connections cannot protect the provided networks agains DoS attacks and blacklisting [46]. Furthermore, such operation cancels the advantages of low-latency localized services, since the communication should pass from networks further away. The mobile users may access the Internet using an untrusted access point, that in-turn could be connected to a real visited network, i.e., performing man-in-the-middle attacks to the mobile user. Such issues and solutions are thoroughly investigated in [19].

Furthermore, the WiFi access sharing solutions may request user private information (e.g., name and credit card information) either for commercial reasons or to avoid user misbehavior. In case of the latter reason, they may monitor user activities. However most users prefer to remain anonymous. Clearly, there is a trade-off here between user privacy and accountability (i.e., be able to trace a user that performed illegal activities). For example, the AP owner may eavesdrop client's traffic in order to steal sensitive information and the same issue may appear in a mobile user regarding the traffic it forwards. The public WiFi hotspots have similar security and privacy challenges.

On the other hand, the DTNs face important security and privacy challenges. In the opportunistic networks all nodes could potential forward data but some of them may be malicious. There is a number of potential issues that relate to the users privacy or network security. The research work [41] carries out extensive investigations and discusses relevant solutions for such challenging problems. The payload confidentiality issues can be handled using encryption, i.e., the sender and destination should agree on encryption keys [48]. An attacker may infer communication patterns [30], even without being able to read the message content. Anonymity and location privacy issues may be important as well, depending on the context. A relevant issue is social graph privacy, that is relevant to the social network routing protocols [27], i.e., social ties between users are considered sensitive information. In such solutions the social ties can reveal the identity and location of a user. Furthermore, a number of attacks can be associated with the opportunistic networks impacting the network performance or availability, including the black hole, the Sybil, the routing information falsification and the flooding attacks [15].

DTNs provide security functionality primarily via the Bundle Security Protocol [53], that enables data encryption at intermediate nodes. User authentication and confidentiality rely on the existence of a trusted authority or a broadcast server for key management and distribution. In order to participate in User Provided Networks, users and their SAPs need to be registered and verified. During user registration the exchange of private keys or unique identities can take place securely through the wired infrastructure. Having exchanged the private information, there are several security mechanisms that can be applied for the exchange of public information, such as Identity-Based Cryptography (IBC) [18].

The studied integrated environment has similar security and privacy issues with the above, but some of them can be tackled easier. For example, its opportunistic aspect does not require a distributed authentication mechanism, since it can benefit from a centralized authentication through the UPN network. An approach that provides communication through the guest network using an encrypted VPN but authentication through the home-network makes sense, since it can balance well the communication delay (i.e., enabling localized applications) with the security and privacy implications. This assumes environments with a minimum level of trust (e.g., an academic campus, or within a social network). In the context of this paper, security and privacy are not our main focus and deserve an independent study.

6.2 Incentives to the Mobile Users and AP owners

Last but not least, a main challenge for all community-based shared Internet schemas is to give appropriate incentives to users in order to cooperate for efficient network resource sharing [45], [22], [36]. The mobility-based approaches require incentives for both AP owners (i.e., to open up their connections) and the mobile users (i.e., to provide forwarding capabilities to the nearby mobile nodes). The resource-constraints of the mobile devices (e.g., limited energy or storage capacity) make this problem even more challenging.

Most of the approaches are credit-based, reputation-based or both. The credits could represent a virtual currency that could be exchanged for connectivity, a better service or real money, encouraging the users to volunteer. The reputation-based schemas build reputation for the better achieving users, quantifying their cooperation levels. Such users may receive a better service. A relevant issue is how to implement the service accounting. In general, the incentive schemas should charge external users and reimburse AP owners. According to [22], a flat rate accounting may permit lopsided behaviors, a bandwidth accounting comes with difficulty to measure accurately bandwidth and the time-based accounting may use heart bits. The same work introduces solutions for the latter two accounting methods. A main issue here is to adopt an incentive schema that renders UPNs more attractive than the conventional Internet access technologies.

Example incentive mechanisms for UPNs are: (i) the Less Than Best Effort approaches [36], [44], [31] that offer guest users the resources that are not utilized by the SAP users; (ii) the Messages on oFfer (MooF) [45] mechanism which is a credit-based incentive mechanism enabling device to device data exchange; (iii) the SMART [60] that is a credit-based schema assuming a central authority for virtual banking and the nodes decide to participate based on each particular reward and the requested class of service; and (iv) the Practical incentive (Pi) [35] that combines both reputation- and credit-based approaches, giving a credit when the message arrives to the destination and a better reputation even if the message does not reach the target. For example, the mobile broadband Internet access may have a diverse cost and performance, which may not be true for a WiFi connection in the area. Furthermore, the latency may be significantly lower for local services. The Open Garden [5] and the Karma [3] startups implemented two interesting mobile UPN models. The former approach exploits the diversity of user requirements and capabilities through crowd sourcing and the latter allows mobile users to become mobile WiFi hotspots, in exchange of a compensation. A categorization of the different UPN incentive models, including the mobile UPN approaches, can be found at [23].

Although our solution is independent from the deployed incentive mechanisms, as long as they consider the mobile user aspect (e.g., to motivate him/her to forward data from other users), a new variation of our protocol that supports inherently such capabilities is in our plans.

7. Conclusions

We proposed a hybrid networking paradigm in the context of UPNs that improves mobile connectivity and network performance. The DTN technology unifies transparently the mobile with the wired infrastructure and achieves efficient data storage management. We have designed a new reference routing algorithm based on message replication and encounter prediction, in order to highlight the perspective of fixed shared access network exploitation from the mobile nodes.

Our theoretical analysis evinced that in such hybrid environments data storing can occasionally be more preferable than forwarding, rendering contact prediction even more important. We elaborated on inter-contact times distribution between mobile users and SAPs and utilized curve fitting in order to route packets based on SAP encounter forecasting. We evaluated the new algorithm in conjunction with well known DTN routing algorithms in both sparse and dense coverage scenarios. In the investigated experimental scenarios, the proposed networking scheme achieved better performance compared to representative opportunistic routing algorithms, in terms of overhead, latency and buffering time.

Acknowledgement

The research leading to these results has received funding from the European Community's Seventh Framework Programme ([FP7/2007-2013, FP7-REGPOT-2010-1, SP4 Capacities, Coordination and Support Actions) under grant agreement number 264226 (project title: Space Internetworking Center-SPICE).

References

[1] Athens wireless metropolitan network (AWMN), available at: http://www.awmn.net, accessed at: 26-May-2017.

[2] FON Community, available at: http://www.fon.com, accessed at: 26-May-2017.

[3] Karma Mobility Inc, *Karma Inititiative*, available at: http://www.yourkarma.com, accessed at: 26-May-2017.

[4] *Open Fog Consortium*, available at: http://www.openfogconsortium.org, accessed at: 26-May-2017.

[5] Open Garden, *Open Garden Initiative*, available at: http://www.opengarden.com, accessed at: 26-May-2017, San Francisco, USA.

[6] OpenSpark Community, available at: https://open.sparknet.fi, accessed at: 26-May-2017.

[7] WiFi.com, available at: http://www.wifi.com, accessed at: 26-May-2017.

[8] M. Abdulla and R. Simon, *The Impact of Intercontact Time within Opportunistic Networks: Protocol Implications and Mobility Models.* Department of Computer Science, George Mason University, Fairfax, VA 22030.

[9] C.Y. Aung, I.W. Ho and P.H. Chong, *Store-Carry-Cooperative Forward Routing with Information Epidemics Control for Data Delivery in Opportunistic Networks*, IEEE Access, 2017.

[10] S.R. Azzuhri, H. Ahmad, M. Portmann, I. Ahmedy, R. Pathak, *An Efficient Hybrid MANET-DTN Routing Scheme for OLSR*, Wireless Personal Communications, 89(4), 1335-1354, 2016.

[11] C. Bettstetter, G. Resta, and P. Santi, *The Node Distribution of the Random Waypoint Mobility Model for Wireless Ad Hoc Networks.* IEEE Trans. Mobile Computing, vol. 2, no. 1, pp. 25-39, Jan.-Mar. 2003

[12] J. Burgess, B. Gallagher, D. Jensen and B.N. Levine, *MaxProp: Routing for Vehicle-Based Disruption-Tolerant Networks*, In Proc. of IEEE INFOCOM (April 2006).

[13] H. Cai and D.Y. Eun, *Toward stochastic anatomy of inter-meeting time distribution under general mobility models*, In MobiHoc '08: Proceedings of the 9th ACM international symposium on Mobile ad hoc networking and computing (2008), pp. 273-282.

[14] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass and J. Scott, *Impact of human mobility on opportunistic forwarding algorithms*, IEEE Transactions on Mobile Computing, pages 606-620, 2007.

[15] F.C. Choo, M.C. Chan, and E.C. Chang, *Robustness of DTN against routing attacks*, In 2010 Second International Conference on COMmunication Systems and NETworks (COMSNETS 2010), January 2010.

[16] T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, and L. Viennot, *Optimized link state routing protocol (OLSR)*, RFC, vol. 54, no. 2, 2003.

[17] K. Fall, *A delay-tolerant network architecture for challenged internets*, SIGCOMM'03, ACM, New York, NY, USA, 27-34.

[18] S. Farrell and V. Cahill, Delay- and Disruption-Tolerant Networking. Artech house, Boston, London, 2006.

[19] J. Ferm, *Security analysis of WLAN roaming solutions*, Master Thesis, Lunds Tekniska Hgskola, August 19, 2013.

[20] L. Gao, T.H. Luan, S. Yu, W. Zhou and B. Liu, *FogRoute: DTN-based data dissemination model in fog computing*, IEEE Internet of Things Journal, 4(1),

225-235, 2017.

[21] A.K. Gupta, I. Bhattacharya, P.S. Banerjee, J.K. Mandal and A. Mukherjee, *DirMove: direction of movement based routing in DTN architecture for post-disaster scenario*, Wireless Networks, 22(3), 723-740, 2016.

[22] H. Hongyi, *OpenWiFi: a consumer WiFi sharing system*, PhD Thesis, Massachusetts Institute of Technology, 2007.

[23] G. Iosifidis, L. Gao, J. Huang and L. Tassiulas, *Incentive mechanisms for user-provided networks*, in IEEE Communications Magazine, vol. 52, no. 9, pp. 20-27, September 2014.

[24] J. Ishmael, S. Bury, D. Pezaros, and N. Race, *Deploying Rural Community Wireless Mesh Networks*, IEEE Internet Computing, vol. 12, no. 4, pp. 2229, Jul. 2008.

[25] H. Kaur and H. Kaur, *An Enhanced Spray-Copy-Wait DTN Routing Using Optimized Delivery Predictability*, In Computer Communication, Networking and Internet Security (pp. 603-610), Springer, Singapore, 2017.

[26] A. Keränen, J. Ott and T. Kärkkäinen, *The ONE Simulator for DTN Protocol Evaluation*. SIMUTools '09, Rome, Italy (2009).

[27] A. Korolova, R. Motwani, S.U. Nabar, and Y. Xu, *Link privacy in social networks*, In 2008 IEEE 24th International Conference on Data Engineering (ICDE 2008), April 2008.

[28] E. Koutsogiannis, L. Mamatas and I. Psaras, *Storage-Enabled Access Point for Improved Mobile Performance: An Evaluation Study*, 9th International Conference on Wired/Wireless Internet Communications (WWIC 2011), Barcelona, Spain, June 15-17, 2011.

[29] M. Kwiatkowska, G. Norman, and D. Parker, *PRISM: Probabilistic Symbolic Model Checker*. In T. Field, P. Harrison, J. Bradley and U. Harder (editors) Proc. TOOLS 2002, volume 2324 of Lecture Notes in Computer Science, pages 200-204, Springer. April 2002.

[30] Z. Le, G. Vakde, and M. Wright, *PEON: privacy-enhanced opportunistic networks with applications in assistive environments*, In PETRA 09: Proceedings of the 2nd International Conference on PErvsive Technologies Related to Assistive Environments, June 2009.

[31] S.A. Lenas and V. Tsaoussidis, *Enabling free internet access at the edges of broadband connections: a hybrid packet scheduling approach*, SIGMOBILE Mobile Computing and Communications Review (MC2R), Vol. 18, Issue 1, pp.55-63, February 2014.

[32] D. Leroy, G. Detal, J. Cathalo, M. Manulis, F. Koeune, and O. Bonaventure, *SWISH: secure WiFi sharing*, Computer Networks, 55(7), 1614-1630, 2011.

[33] X. Liang, K. Zhang, X. Shen and X. Lin, *Security and privacy in mobile social networks: challenges and solutions*, IEEE Wireless Communications, vol. 21, no. 1, pp. 33-41, February 2014.

[34] A. Lindgren, A. Doria and O. Schelen, *Probabilistic Routing in Intermittently Connected Networks*, In SIGMOBILE Mobile Computing and Communication Review, v.7 n.3, July 2003.

[35] R. Lu, X. Lin, H. Zhu, X. Shen, and B. Preiss, *Pi: A practical incentive protocol for delay tolerant networks*, IEEE Transactions on Wireless Communications, vol. 9, no. 4, pp. 14831493, April 2010.

[36] L. Mamatas, I. Psaras and G. Pavlou, *Incentives and algorithms for broadband access sharing*, 1st ACM Sigcomm Workshop on Home Networks (HomeNets), New Delhi, India, August 2010.

[37] M.H. Manshaei, J. Freudiger, M. Felegyhazi, P. Marbach, and J.P. Hubaux, *On wireless social community networks*, INFOCOM, 2008.

[38] M. Motani, V. Srinivasan, and P. Nuggehalli, *Peoplenet: Engineering a Wireless Virtual Social Network*, Proc. MobiCom, 2005, pp. 243-257.

[39] A. Muhammad and R. Simon, *A Simulation Study of Common Mobility Models for Opportunistic Networks*, In 2008 41st Annual Simulation Symposium ANSS (April 2008), pp. 43-50.

[40] H. Ntareme and S. Domancich, *Security and performance aspects of bytewalla: A delay tolerant network on smartphones*, in Proceedings of the 2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications, ser. WIMOB, (2011).

[41] I. Parris, *Practical privacy and security for opportunistic networks*, PhD Thesis, University of St Andrews, 2014.

[42] A. Passarella and M. Conti, *Characterising aggregate inter-contact times in heterogeneous opportunistic networks*, NETWORKING 2011, pages 301-313, 2011.

[43] M. Patel, B. Naughton, C. Chan, N. Sprecher, S. Abeta, and A. Neal, *Mobile-Edge Computing Introductory Technical White Paper*, White Paper, Mobile-edge Computing (MEC) industry initiative, European Telecommunications Standards Institute (ETSI), September 2014.

[44] I. Psaras and L. Mamatas, *On Demand Connectivity Sharing: Queuing Management and Load Balancing for User-Provided Networks*, Computer Networks (COMNET), Elsevier Science, Special Issue on Wireless for the Future Internet, volume 55, issue 2, February 2011.

[45] V.G. Rolla and M. Curado, *Enabling wireless cooperation in user provided networks*, IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, ON, 2015, pp. 1114-1121.

[46] N. Sastry, K. Sollins, and J. Crowcroft, *Architecting citywide ubiquitous Wi-Fi access*, in: Proceedings of the HotNets-VI, 2007.

[47] S.F.A. Shah, M.H. Zafar, I. Andonovic and T. Jan, *Hybrid routing scheme for Vehicular Delay Tolerant Networks*, 8th Computer Science and Electronic Engineering (CEEC), Colchester, 2016, pp. 158-163.

[48] A. Shikfa,M. Onen, and R. Molva, *Privacy and confidentiality in context-based and epidemic forwarding*, Computer Communications, 33(13):14931504, April 2010.

[49] T. Small and Z.J. Haas, *The shared wireless infostation model: a new ad hoc networking paradigm (or where there is a whale, there is a way)*, In Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing (MobiHoc '03). ACM, New York, NY, USA, 233-244.

[50] R. Sofia and P. Mendes, *User-provided networks: consumer as provider*, IEEE Communication Magazine, 46, pages 86-91, 2008.

[51] T. Spyropoulos , K. Psounis, and C. S. Raghavendra, *Spray and wait: an efficient routing scheme for intermittently connected mobile networks*, Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking, p.252-259, August 26-26, 2005, Philadelphia, Pennsylvania, USA.

[52] T. Spyropoulos, K. Psounis and C.S. Raghavendra, *Spray and Focus: Efficient Mobility-Assisted Routing for Heterogeneous and Correlated Mobility*, Fifth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom), 79–85, White Plains, NY (19-23 March 2007).

[53] S. Symington, S. Farrell, H. Weiss and P. Lovell, *RFC 6257*, http://www.rfc-editor.org/rfc/rfc6257.txt.

[54] A. Vahdat and D. Becker, *Epidemic routing for partially connected ad hoc networks*, Technical Report CS-200006, Duke University (2000).

[55] P. Wan, S. Chen, T. Yu and Z. Hua, *A hybrid multiple copy routing algorithm*

in space delay-tolerant networks, Science China Information Sciences, 60(4), 2017.

[56] J. Whitbeck and V. Conan, *HYMAD: Hybrid DTN-MANET routing for dense and highly dynamic wireless networks*, Computer communications, 33(13), 1483-1492, 2010.

[57] Y. Xie, J. Bao, Z. Song and Y. Zhou, *A hybrid opportunistic Routing Scheme based on nodes grouping strategy for VANETs in Urban Scenarios*, 25th Wireless and Optical Communication Conference (WOCC), Chengdu, 2016, pp. 1-5.

[58] A. Xin, V. Srinivasan, and C.K. Tham, *Wi-Sh: A Simple, Robust Credit Based Wi-Fi Community Network*, INFOCOM (2009).

[59] Y. Xu, Y.V. Mahendran, and S. Radhakrishnan, *Internet of Hybrid Opportunistic Things: A novel framework for interconnecting IoTs and DTNs*, IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), San Francisco, USA, 2016.

[60] H. Zhu, X. Lin, R. Lu, Y. Fan, and X.S. Shen, *SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks*, IEEE Transactions on Vehicular Technology, vol. 58, no. 8, pp. 46284639, October 2009.