Spontaneous smartphone networks as a user-centric solution for the future internet

Gianluca Aloi, Marco Di Felice, Valeria Loscrì, Pasquale Pace, Giuseppe Ruggeri

▶ **To cite this version:**

Gianluca Aloi, Marco Di Felice, Valeria Loscrì, Pasquale Pace, Giuseppe Ruggeri. Spontaneous smartphone networks as a user-centric solution for the future internet. IEEE Communications Magazine, 2014, 52 (12), pp.26 - 33. 10.1109/MCOM.2014.6979948 . hal-01077445

HAL Id: hal-01077445
https://inria.hal.science/hal-01077445

Submitted on 14 Jan 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

SPONTANEOUS SMARTPHONE NETWORKS AS USER-CENTRIC SOLUTION FOR THE FUTURE INTERNET

Gianluca Aloi[1], Marco Di Felice[2], Valeria Loscrì[3], Pasquale Pace[1], Giuseppe Ruggeri[4]

(1) DIMES - University of Calabria, Italy, {aloi, ppace}@dimes.unical.it

(2) DISI - University of Bologna, Italy, {difelice}@cs.unibo.it

(3) INRIA Lille - Nord Europe, France, {valeria.loscri}@inria.fr

(4) DIIES - University "Mediterranea" of Reggio Calabria, Italy, {giuseppe.ruggeri}@unirc.it

ABSTRACT

In this paper we focus on a special case of User-Centric Networks (UCNs), named Spontaneous Smartphones-based Networks (SSNs), where the role of the end-user devices is played by smartphones that are, *"evolutionary"* and more active in supporting communication services. SSNs present key features like spontaneity in the creation of the network and redefinition of the devices' role in order to make them continuously adaptive to both network and users requirements. This work is devoted to identify the potential advantages of SSNs, by also providing a clear definition of the challenges and the issues that need to be faced in order to make this emerging paradigm effective and practically deployable.

1. INTRODUCTION

Nowadays, *Spontaneous Smartphone Network* (SSN) is emerging as a potential new communication paradigm, characterized by the fact that the access network has a strong self-organizing nature and it is primarily made up of users' owned devices. These latter can also act as routers by actively cooperating to forward data on multi-hop paths. SSNs can be considered a special case of User-Centric Networks (UCNs) made up only by users' devices.

This new approach of network deployment undoubtedly offers great advantages in terms of *(i)* lower costs required to set up the network access, *(ii)* reduced or no maintenance at all for network management, and *(iii)* possibility to set-up a network even on scenarios where the infrastructure is poorly available (*i.e.,* disaster scenarios, rural areas, least developed countries, etc.). Despite the enormous potentials of SSN the multi-hop communication between smartphones, or similar devices (*e.g.,* phablet, tablet), is still not an affirmed paradigm and self-organized SSNs are a challenge [1]. Usually, the network creation and management requires a massive intervention from the users that, however, would prefer being agnostic about technological issues. This requirement constitutes a unique

issue of SSNs compared to traditional self-organizing systems and generic multi-hop ad hoc networks. Hence, a framework able to limit the human intervention, with the aim of making the network management *as much spontaneous as possible,* is mandatory for the success of the SSN paradigm.

In this work, we present and discuss results of a novel framework, named STEM-Net [2] and specifically adapted to SSNs, in order to provide two main enabling features for users' devices: *(i)* network self-configuration and, *(ii)* evolvability, *i.e.,* the capacity of continuously adapting to the needs of both user and network. Through STEM-Net, a smartphone can switch between different roles. It can produce/receive data, it can forward the traffic of other terminals through multi-hop communications or it can provide the access to global network resources to other terminals, but above all, it can *autonomously* assume the most suitable role without any user intervention.

The main contributions of the paper are: *(i)* to specify advantages and issues of SSNs by identifying strategic scenarios and use cases on which SSNs can be utilized, *(ii*) to review the enabling technologies of SSNs, by also pointing out limitations of existing software frameworks in terms of self-organizing deployments, and, finally, *(iii)* to describe how the application of the STEM-Net framework can solve such issues, by also presenting a proof of concept implementation on real smartphones.

2. USE CASES AND SCENARIOS

In this section, we propose few communication scenarios (depicted in Figure 1) well suited for SSNs to motivate the need of a new and flexible system architecture for network creation and management.

Pervasive wireless Internet access: SSNs can be used to deploy a fully pervasive and infrastructure free Internet access by naturally extending the coverage of wide areas. This goal could be easily achieved because of the huge amount and density of smartphones located in all daily life environments. As a result, a pervasive scenario can be implemented by adding self-configuration capabilities to smartphones, making them able to cooperate with the aim of sharing the access to global resources.

Emergency and post-disaster recovery: When natural catastrophes disrupt traditional network infrastructures, SSNs can help both survivals and rescue teams. The survivors, by using their mobile phones and the scarce communication resources still available, can share updates, post photos, and upload videos on social media sites. We are confident that in the long run emergency services,

spontaneous smartphones-based networks will complement the safety networks (prospectively based on LTE) in place for officials only such as police and fire brigade.

Large crowd gathering places: When special events (*e.g.*, concerts, trade fairs, Olympic games) involve huge numbers of people with risks of overloading the communication infrastructure, SSNs can be used to offload mobile data traffic from cellular networks. As an example, cooperative smartphones can wisely forward user's data "*hop-by-hop*" to the nearest Wi-Fi access point so that the amount of offloaded data can further increase.

Figure 1. Use cases and communication scenario.

3. Enabling Technologies

In this Section, we provide a quick review of existing hardware and software technologies that might support the implementation of SSNs on today's smartphones.

3.1 Communication Technologies

Communication among smartphones can be supported by a plethora of short/medium range communication interfaces and technologies; in the following, we review the main features of existent or emerging wireless communication technologies available on today's smartphones, in order to discover the more suitable (if any) for the deployment of SSNs.

Bluetooth offers a short communication range and a rate that ranges from 1.2Mb/s in the early releases (version 1.2) to a maximum of 24Mb/s in the latest releases (version 4). Bluetooth requires a significant involvement by the user, since the interface should be activated, the recipient device should be discovered and the content to be sent should be manually specified. The poor communication performance, the annoying procedures and the users' reluctance hindered the diffusion of Bluetooth-based SSNs.

Near Field Communication (NFC) technologies have been successfully proposed to support content sharing between smartphones. The very short communication range (in the order of few cm) provides a natural protection against malware diffusion. However, such strength is also a limitation, since the

utilization of NFC-based SSNs is limited to few specific scenarios such as “Delay Tolerant” content sharing, in addition to the need of involving the user supervision and management.

Recent smartphones are equipped with IEEE 802.11 interface (Wi-Fi) supporting high transmission rate up to 600Mb/s (IEEE 802.11n). However, most of existing Mobile Operating Systems (MOSs) do not allow to configure the Wi-Fi interface in Ad Hoc mode, unless breaking some safety procedures and creating a super-user account, which is quite far to be practical for common users. Hence direct communication between smartphones are practically not feasible.

Wi-Fi Direct has been recently standardized to allow communication between enabled devices without any infrastructure. The devices activate a negotiation procedure at their first connection to determine which one shall act as an access point, while the other devices can connect to it by using, de facto, the Wi-Fi Infrastructured mode. However, despite the benefits in terms of increased security compared to the Ad Hoc mode, Wi-Fi Direct causes an unfair workload distribution since the smartphones acting as access points will consume more resources. Furthermore, Wi-Fi Direct does not supports multi-hop communication and, consequently, communications are limited to terminals within reciprocal communication range.

A further opportunity to support SSNs is given by LTE and also HSDPA/HSUPA. Even if these technologies are mainly conceived to provide the devices connectivity toward a network infrastructure, it is expected that LTE in 3GPP Release 12 will support the so called *Device to Device (D2D)* communications mostly based on local, opportunistic and single hop data exchange.

In Table 1, we briefly report the main characteristics of the wireless technologies discussed so far.

Table 1. Enabling technologies for SSNs.

3.2 SOFTWARE SUPPORT

While the characteristics of communication at the lower layers (MAC/PHY) depend on the wireless technology in use, the network functionalities are provided by the MOS. Two main functionalities are fundamental to implement a SSN: the possibility to turn a smartphone into a network gateway, and the

routing capabilities. Nowadays, most of the MOSs (*i.e.,* Android, IOS, Windows Phone) make available *"tethering"* modules, which enable a smartphone to provide mobile Internet connectivity through its short-range wireless interfaces (*e.g.,* Wi-Fi, Bluetooth). However, the enabling/disabling of tethering modules must be performed manually by the user. Routing capabilities on Wi-Fi networks are not provided by most popular MOSs for security reasons, even if the NIC (Network Interface Card) usually supports Ad Hoc communication mode. Existing software can be categorized into two approaches [3], respectively DTN-based [4] or MANET-based [5][6]. The first approach allows facing the problem of intermittent connectivity caused by end-user mobility, although it poses severe challenges in terms of performance and battery consumption [4]. The second approach relies on traditional routing protocols used over generic MANET; we cite experimental studies of multi-hop SSNs using OLSR [2] and AODV [5] protocols. Since most of the MOSs do not allow intercepting IP packets or modifying the routing tables at the kernel layer, these implementations run in user space [5], thus introducing additional overhead in terms of power consumption and data transfer. At the same time, since the routing policy is performed on the basis of the route length only, energy consumption can be unbalanced or lead to suboptimal SSN performance.

3.3 CHALLENGES IN THE IMPLEMENTATION OF SSNS

From all the argumentations reported above we argue that the main challenge to the implementation of SSNs is constituted by the lack of adequate software support for network creation and management. In this paper we focus on three limitations of existing software architectures:

1. *No autonomous device configuration capabilities*. In most of today's smartphone, configuration and set-up of network functionalities must be carried out by users manually, like pairing operations with other devices/networks, network formation, adjustment of transmitting parameters. This approach is not scalable and then it is not suitable for scalable deployments (*e.g.,* the pervasive access scenario) or dynamic environments (*e.g.,* the emergency scenario).

2. *No cooperative network management capabilities*. Although computational and communicational capabilities of smartphones are continuously improving, their performance are still not comparable with those of dedicated network equipments. For instance, in [1], the authors have compared the performance of a SO-HO Wi-Fi network router to a smartphone provided with mesh routing capabilities, and have found that in this latter case

power consumption constitutes a severe concern, since look-up operations are highly demanding for the smartphone's CPU. Vice versa, energy efficiency of the single device can be improved when smartphones cooperate to share the effort of network management, by dynamically deciding the role to act (*e.g.,* router/gateway) on the basis of their actual resources.

3. *No network self-organization capabilities.* SSNs are intrinsically dynamic environments, due to the end-users' mobility and to the variable traffic loads produced by the mobile applications. Self-organizing principles are required to manage the network and guarantee continuity of service in front of dynamic and unforeseen events. Moreover, in several scenarios (*e.g.,* the post-disaster recovery), the goal of the SSN becomes to maximize the operativeness of the network, considered as a single entity, rather than the performance of a single component. Achieving such distributed intelligence requires cooperation, autonomous sensing, and decision making capabilities, which of course cannot be managed in case of human control.

4. STEM-NET: A FRAMEWORK TO SUPPORT THE IMPLEMENTATION OF SSNS

In this section we describe the STEM-Net framework, originally introduced in [2] for a Smart Cities environment, and we show how STEM-Net paradigm can overcome the previous challenges becoming a viable and effective solution also in the SSN context.

The logical architecture of a generic end-user smartphone is illustrated in Figure 2. We refer to the "*stemness*" property of a smartphone as the ability to perform a protocol reconfiguration achieved throughout the combination of built-in features and algorithmic solutions. From here on, we use the term Stem-Phone to indicate this novel family of software enhanced smartphones. We further note that in our view, Stem-Phones may be a limited fraction of the existing smartphones but they can still provide useful services to the neighboring legacy phones.

Each Stem-Phone, participating to the SSN setup, can play a given set of roles according to the network capabilities/functionalities supported by the specific device. The basic set of roles of each Stem-Phone include the ability *(i)* to produce/receive data, *(ii)* to forward the traffic of other terminals and *(iii)* to act as a gateway providing access to global network resources to other terminals. The set of roles played by each Stem-Phone can vary in accordance of its own built-in characteristics (*i.e.,* hardware features or physical constraints). For example, the gateway role could require the simultaneous use of

different communication technologies to connect other nodes (*e.g.,* Wi-Fi Direct, Bluetooth) and to access to global network resources (*e.g.,* LTE, HSDPA). In addition, a Stem-Phone could also play new roles that can be dynamically configured and "learnt" from other Stem-Phones by relying on cooperation with them. This might be the case, for instance, of a Stem-Phone that upgrades its software, downloaded from its neighbors, in order to gain the ability to serve as an access point. Moreover, each role is mapped to a specific network configuration and it is foreseen the possibility for a Stem-Phone to change its configuration over time for self-optimization purposes. This might be the case, for instance, of a Stem-Phone configured as a Wi-Fi router that dynamically adjusts its transmitting power level based on measured interference conditions.

Figure 2. The generic architecture of a Stem-Phone.

4.1 STEM-NET FOR SSNS: THE GATEWAY ELECTION CASE

In this section we show how the STEM-Net framework can be usefully applied to handle autonomous configuration tasks by focusing on a basic SSN issue: the dynamic gateway election.

Let us consider a set of smartphones that cooperate to build a SSN. Without loss of generality, we suppose that the multi-hop communication is supported by following the approach proposed in [1]. Wi-Fi cards are configured in Ad Hoc Mode and the OLSR protocol is deployed. Some of the smartphones should be elected to play the role of Gateway that consists in forwarding the packets coming from the SSN on the Wi-Fi interface toward the Internet backbone by using the 3G interface. This role requires the fulfillment of several requirements: *i)* acting as gateway implies an high power consumption, therefore the gateway should be chosen among those Stem-Phones with a sufficient residual energy, *ii)* the connection between the gateway and the cellular backbone should offer an adequate throughput to sustain the traffic generated in the SSN, *iii)* since the throughput on Wi-Fi multi-hop communication roughly decreases with the number of hops, the gateway should be located in a central position with respect to the other terminals in the SSN and finally, *iv)* the Wi-Fi network nearby the gateway should be as uncongested as possible.

To address this problem, a simple but effective spontaneous gateway election procedure has been proposed in [7]. Since we only aim at showing how this election procedure is functional to SSNs, we briefly summarize our strategy in the following by referring the reader to the work in [7] for further details. Once a SSN is created, a gateway is randomly selected; after this initialization phase, the gateway role is passed to the most suitable node by following a "*stimulus-response*" model. Each node

monitors the following parameters: *i)* its own residual energy, *ii)* the congestion level experienced at the Wi-Fi interface, and *iii)* the average distance from other nodes in the SSN. The gateway g also computes the congestion experienced at the Cellular interface. All the monitored parameters are periodically exchanged between the nodes. The exact computation of the relevant parameters are given in Table 2.

The node acting as gateway constantly evaluates its attitude to keep its role and quantifies it through a specific metric called *Stimulus Metric* (*SM*) [7]:

$$SM(g) = G(residual\ energy,\ \ congestion\ on\ cellular\ interface)$$

Here, *G* represents a suitable function that is given in Table 2. Periodically, the gateway in charge broadcasts its *SM* value by starting a "*gateway handover procedure*"; upon receiving a *SM* message, each Stem-Phone i evaluates its capability to take over the gateway role and summarizes it in a new metric called *Threshold Metric (TM)* defined as follows [7]:

$$TM(i) = F\ (residual\ energy,\ \ congestion\ on\ WiFi\ interface,\ \ average\ distance\ from\ neighbours)$$

Here, F is a suitable function that is given in Table 2. If the stimulus $SM(g)$ perceived by a node i exceeds its threshold $TM(i)$, the node i assumes the role of gateway and announces its decision to the SSN.

Table 2. Parameters estimation and Stimulus-Threshold computation.

We would like to remark here that the described gateway election procedure can be easily supported by the proposed Stem-Phone architecture (Fig. 2); in particular, the *Context Manager* estimates the most *Relevant Parameters (RP)* (residual energy, congestion on Wi-Fi and Cellular interfaces, average distance), the *Cooperation Manager* takes care of the *RP* exchanges between smartphones, the *Knowledge Database* stores the *RP* both concerning the smartphone itself and neighboring ones. The *Policy Manager* translates the user preferences such as his/her reluctance to share the residual charge and their acceptable performance. Finally the *Control & Decision Brain* computes the metrics: $SM(g)$, $TM(i)$ and takes decisions.

4.2 A PROOF OF CONCEPT IMPLEMENTATION

The effectiveness of the gateway election has been already shown in [7]. Here, we are interested in providing some brief guidelines on the feasible implementation of the election process on commonly available smartphones. As hardware platform we used a Samsung Galaxy S model, which can be considered as representative of a wide range of user devices on the market.

On top of the hardware platforms we have developed a software suite, which implements the gateway election procedure as described in the former section. The software suite includes two classes of programs that implement: *i)* the basic communication functions, and *ii)* the components of the Stem-Phone architecture. The basic communication over multi-hop paths is supported by using the *OLSR daemon* (www.olsr.org).

The components of the Stem-Phone architecture have been implemented as follows:

- The *Context Manager* consists of a series of self-developed scripts that also leverage some routines offered by the Android operating system. Specifically Table 2 summarizes how *RP* is computed.
- *Cooperation Manager* has been developed by extending the OLSR protocol with two custom message types: *i)* `STEM HELLO MESSAGE` to disseminate *RP* computed by each Stem-Phone, *ii)* `STEM GATEWAY MESSAGE` to start a gateway election procedure.
- The *Knowledge Database* is implemented through a set of files in *~/proc/Stem/* directory. Specifically a file named *~/proc/Stem/context.local* stores the information relevant for the node itself, while the file *~/proc/Stem/context.extra* is filled with the information received by surrounding nodes.
- The *Control & Decision Brain* functionalities have been supported by implementing a dedicated *C* program which, starting from the information stored in the *Knowledge Database*, computes and compares *Stimulus* and *Threshold* according to the formerly described algorithm.

The realized prototypes have been tested in the deployment shown in Figure 3 where three Stem-Phones constitute a small SSN. One of the three Phones (Phone A) is unable to directly transmit data to the 3G network. This condition has been forced by instructing the Android OS to disable data communication through the 3G interface. Hence, Phone A should necessarily forward its data to one of the other two Phones (B or C) that instead have their 3G connection active. Data produced by Phone A towards Internet consists of a constant bit rate flow of 350kb/s, generated by using a custom software.

Figure 3. The test-bed set up.

To control the residual charge available to Phones B and C, their battery has been replaced with a wooden one and the phones have been powered through a tunable power supplier. Commonly available phones estimate the State of Charge (SOC) of their battery by probing the voltage provided by this latter. Thus, in our set-up we forced the phones to change their estimation of the residual charge by varying the voltage value throughout a tunable power supplier. In our test campaign the voltage provided to Phone C has been kept constant to 3.7 V to emulate a residual battery charge of about 50% of the nominal value; on the contrary, the voltage provided to Phone B has been varied in [3.2V-4.2V] to emulate the residual amount of charge showed in figure 4.

Three different approaches for the gateway election have been evaluated:

1. Phone B is manually selected. This approach is equivalent to tethering operation, which is the only solution commercially available today.
2. OLSR is installed on all the phones. In particular, Phone B and Phone C are configured as potential gateways and the choice of which one to select is left to the routing protocol. This case represents what can be obtained through the framework presented in [1] or by using similar MANET-based approaches.
3. The STEM-Net architecture is deployed on the Phones, through the software modules formerly described in Section 4.1.

Figure 4 reports the throughput achieved by Phone A when varying the gateway selection method and the residual charge at phones B and C. The worst performance is achieved when the gateway is manually chosen. In this case, as soon as the residual charge at Phone B approaches zero, this latter switches off its communication interfaces and stops forwarding data coming from Phone A, hence the communication is interrupted.

The performance improves when the choice of the gateway is carried out by using OLSR. In this case Phone B is selected as gateway as long as its available charge goes to zero. At this instant, the communication path is broken and OLSR looks for a new available gateway. After about 10 seconds Phone C is selected as new gateway. This behavior constitutes an improvement compared to the first case (manual selection) nonetheless it presents some drawbacks: (*i)* it leads to an uneven power

consumption between the available gateways, (*ii)* the search for a new gateway is started only after Phone B became inoperative and following this late reaction a service disruption of about (10s) is experienced, (*iii)* the owner of Phone B may be annoyed to have his/her phone inoperative due to the lack of charge.

In the STEM-Net framework the gateway election procedure is carried out considering also the residual charge, so the role of the gateway is always assumed by the node having the maximum residual charge. As soon as the residual charge of Phone B falls below that of Phone C, the role of gateway is passed from the former to the latter. Since the change of role is done while Phone B is still operative, the handover procedures are much faster compared to the OLSR case. Finally the STEM-Net approach does not starve Phone B, hence it provides a better experience to the end-user.

Figure 4. Throughput experienced by Phone A using different residual charge for both Phones B and C.

This simple experiment confirms the viability and effectiveness of the STEM-Net framework on commonly available devices and it paves the way for additional experimentations for upcoming SSNs.

5. Lessons Learned And Open Issues

Based on the experimental results, we can conclude that STEM-Net represents a viable solution to face the challenges on SSNs implementation introduced in Section 3.3. Indeed, cooperative network management policies can be implemented in a straight-forward way through the concepts of "roles" and node mutation (point two of Section 3.3), while network adaptiveness and distributed self-organization capabilities (point three of Section 3.3) can be achieved through the proper modeling of *stimulus/threshold* functions, that are intrinsically scenario-dependent. However, several practical issues regarding autonomous device configuration capabilities (point one of Section 3.3), have emerged from the test-bed implementation, based on which we can argue that a completely user-agnostic SSN deployment model might not be 100% feasible on today's smartphones. Skipping the technical details, most of such issues derive by the poor support provided by the MOS at the APIs level, so that several low-level network functionalities (*e.g.,* multi-hop routing) cannot be implemented without breaking some safety mechanisms of the original software equipment, which is clearly not a solution.

Finally, we conclude the paper by highlighting the existence of additional open issues that need to be addressed for practical deployments of SSNs. Security is a major concern while designing and developing spontaneous network based on mobile devices [8]. A secure self-configured protocol is required for user authentication, validation and data transfer. Moreover, novel and robust reputation mechanisms are required to identify user misbehavior within different communities [9]. Connected to the security issues, novel cooperation models and utility functions have to be designed to encourage users to share their resources with the certainty of obtaining future benefits [10]. In this context, smart mechanisms based on local pricing strategies could be used to control and prevent network congestion by prolonging the overall lifetime of the SSN, considered again as a single entity. We plan to address these open issues as future works.

6. CONCLUSION

In this paper we have investigated the potential of Smartphone Spontaneous Networks (SSNs), by analyzing the main issues and challenges from the perspective of minimizing users' involvements for network set-up and maintenance. We believe that the implementation of an actual network "*spontaneity*" model, based on "*software*" intelligence local at each smartphone, could favor the diffusion of SSNs. To this purpose, we have introduced the STEM-Net framework, and presented results of a small-scale test-bed in which gateway nodes are dynamically selected.

REFERENCES

[1] A. Iera, A. Molinaro, S.Y. Paratore, G. Ruggeri, A. Zurzolo, "Making a meshrouter/gateway from a smartphone: Is that a practical solution?" *Ad Hoc Networks*, Vol. 9, Issue 8, pp. 1414–1429, 2011.

[2] G. Aloi, L. Bedogni, M. Di Felice, V. Loscrì, A. Molinaro, E. Natalizio, P. Pace, G. Ruggeri, A. Trotta, N. R. Zema, "STEM-Net: an evolutionary network architecture for smart and sustainable cities," *Transactions on Emerging Telecommunications Technologies*, Special Issue: Smart Cities - Trends & Technologies Vol. 25, Issue 1, pp. 21-40, January 2014.

[3] H. Nishiyama, M. Ito, N. Kato, "Relay by Smartphone: Realizing Multi-hop Device-to-Device Communications", *IEEE Communication Magazine*, Vol. 52, Issue 4, pp. 56-63, 2014.

[4] H. Ntareme, M. Zenna, B. Pehrson, "Delay tolerant network on smartphones: applications for communication challenged areas", Proc. of ACM ExtremeCom, Galapagos Islands, Ecuador, 2011.

[5] T. Zhuang, P. Bskett, Y. Shang, "Managing Ad Hoc Networks of Smartphone", *IJIET International Journal of Information and Education Technology*, Vol. 3, Issue 5, pp. 540-546, 2013.

[6] P. Mitra, C. Poellabauer, “Emergency Response in Smartphone-based Mobile Ad Hoc Networks”, Proc. of IEEE ICC, Ottawa, Canada, 2012.

[7] M. Di Felice, L. Bedogni, A. Trotta, L. Bononi, F. Panzieri, G. Ruggeri, G. Aloi, V. Loscrì, P. Pace, “Smartphones Like Stem Cells: Cooperation and Evolution for Emergency Communication in Post-Disaster Scenarios”, in Proc. of IEEE BlackSeaCom, Batumi, Georgia, 2013.

[8] R. L. Gilaberte, J. Lloret, M. Garcia, L. P. Herrero, “A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation”, *IEEE Transactions on Parallel Distributed Systems*, Vol. 24, Issue 4, pp. 629-641, 2013.

[9] R. Sofia, P. Mendes, M.J. Damásio, S. Henriques, F. Giglietto, E. Giambitto, A. Bogliolo, “Moving towards a socially-driven internet architectural design”, *Computer Communication Review*, Vol. 42 Issue 3, 2012, pp. 39-46.

[10] P. Pace, G. Aloi, “Managing and Deploying Pervasive Wireless Internet Access through Attractive Connection Sharing and Reselling Mechanisms,” *Journal of Networks*, Vol. 8, Issue 2, pp. 351-364, 2013.

AUTHORS' BIOGRAPHIES

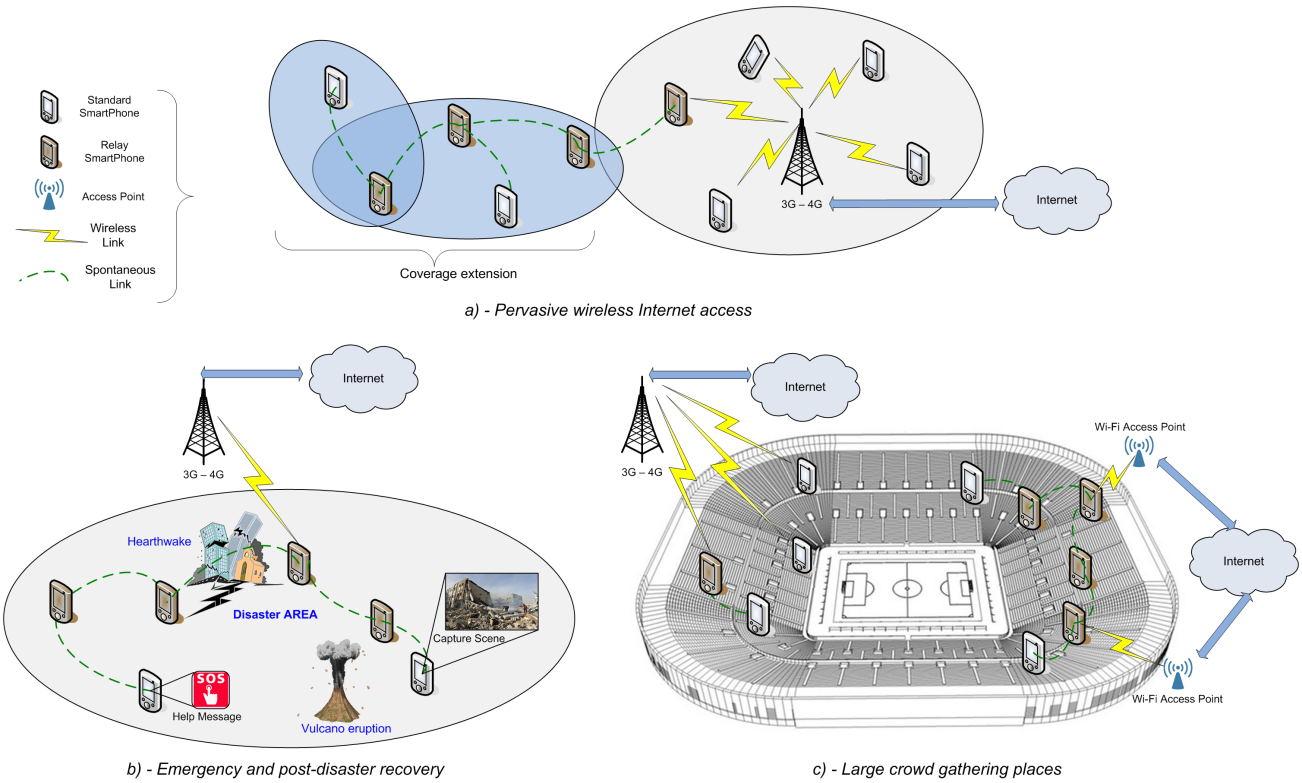
Gianluca Aloi [S'99-M'02] (aloi@dimes.unical.it) received his M.S. degree in Computer Science in 1999 and his Ph.D. degree in Systems Engineering and Computer Science in 2003. He joined the University of Calabria in 2004 where, currently, he is Assistant Professor at the Department of Informatics, Modeling, Electronics and Systems (DIMES). His research interests include spontaneous and reconfigurable wireless networks, cognitive networks, resource provisioning and sharing, software defined radio systems, localization systems and satellite communications.

Marco Di Felice received the Ph.D degree in Computer Science in 2008 from the University of Bologna, Italy. In 2008 and 2010, he was a visiting researcher at the Georgia Institute of Technology (Atlanta, USA) and at the Northeastern University (Boston, USA). Since April 2012, he is an Assistant Professor in Computer Science at the University of Bologna, Italy. He authored more than sixty papers on wireless and mobile systems and applications.

Valeria Loscrì is a permanent researcher at Inria Lille – Nord Europe (FUN Team) since October 2013. She got her Master degree in Computer Science and PhD in Systems Engineering and Computer Science in 2003 and 2007 respectively, at University of Calabria (Italy). In 2006 she was visiting research at Rice University (Houston). She authored more than 60 publications in journal, conferences, workshops and book chapters. Her research interests focus on, self-organizing systems, robotics - networks, nanocommunications.

Pasquale Pace [S'02-M'05] (ppace@dimes.unical.it) received the PhD in Information Engineering in 2005 from the UNICAL, Italy. In 2005 and 2006, he was a visiting researcher at the CCSR (Surrey – UK) and at the Georgia Institute of Technology (Atlanta, USA). He is currently an Assistant Professor in Telecommunications at the UNICAL. He authored more than sixty papers in international publications. His research interests include Cognitive networks, Sensor and Self-organized networks, Cost and Business models for resource sharing.

Giuseppe Ruggeri. (giuseppe.ruggeri@unirc.it) received the master degree in electronics engineering in 1998 From University of Catania ,Italy. In 2002 he received the Ph.D. in electronics, computer science and telecommunications engineering from University of Palermo (Italy). He is currently Assistant Professor at the Department of ICT, Infrastructures, and Sustainable Energy (DIIES) at the University "Mediterranea" of Reggio Calabria (Italy). His research interests focus on wireless networking, Self Organizing Networks, and Information Centric Networking (ICN).



a) - Pervasive wireless Internet access

b) - Emergency and post-disaster recovery

c) - Large crowd gathering places

Figure 1. Use cases and communication scenario.

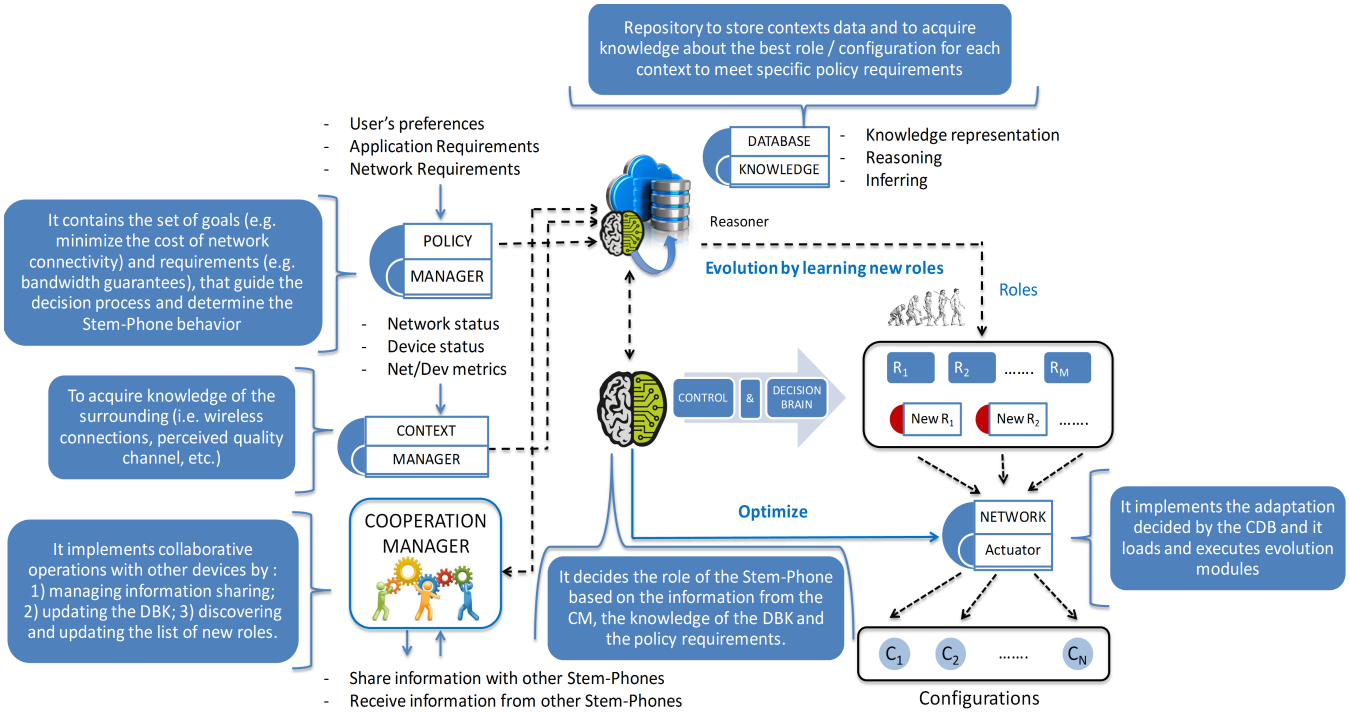


Figure 2. The generic architecture of a Stem-Phone.

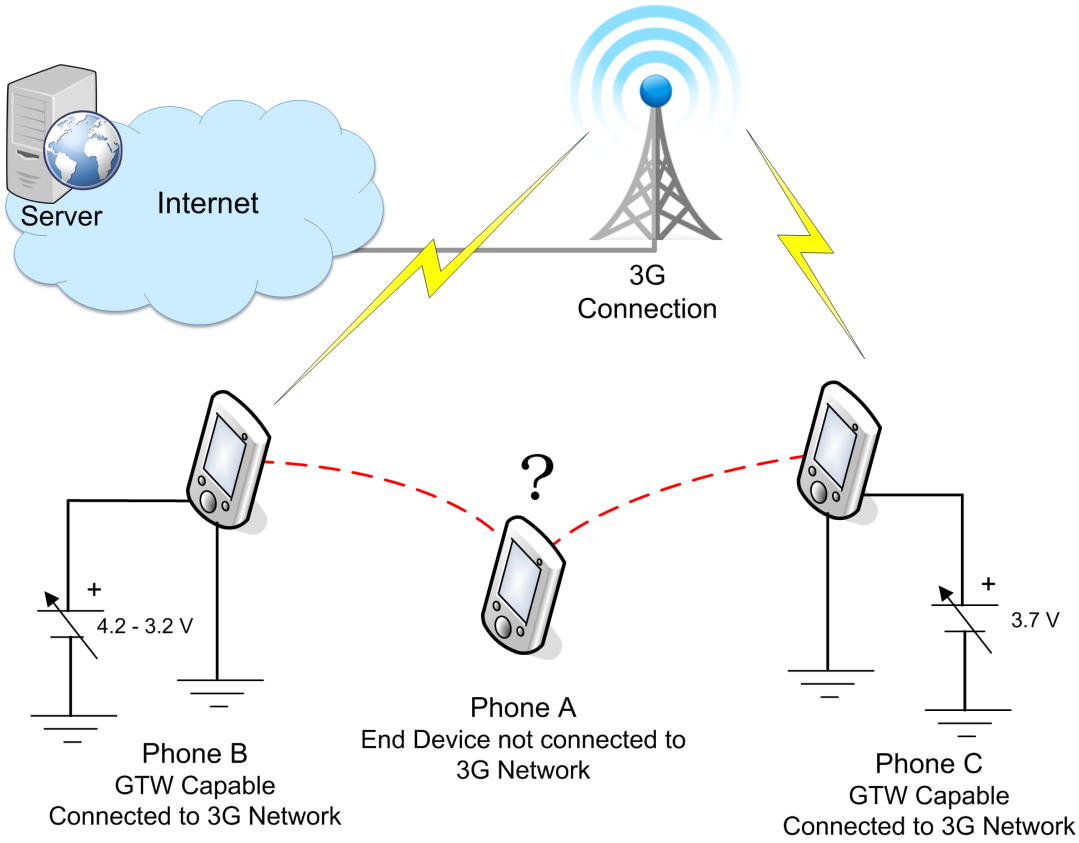


Figure 3. The test-bed set up.

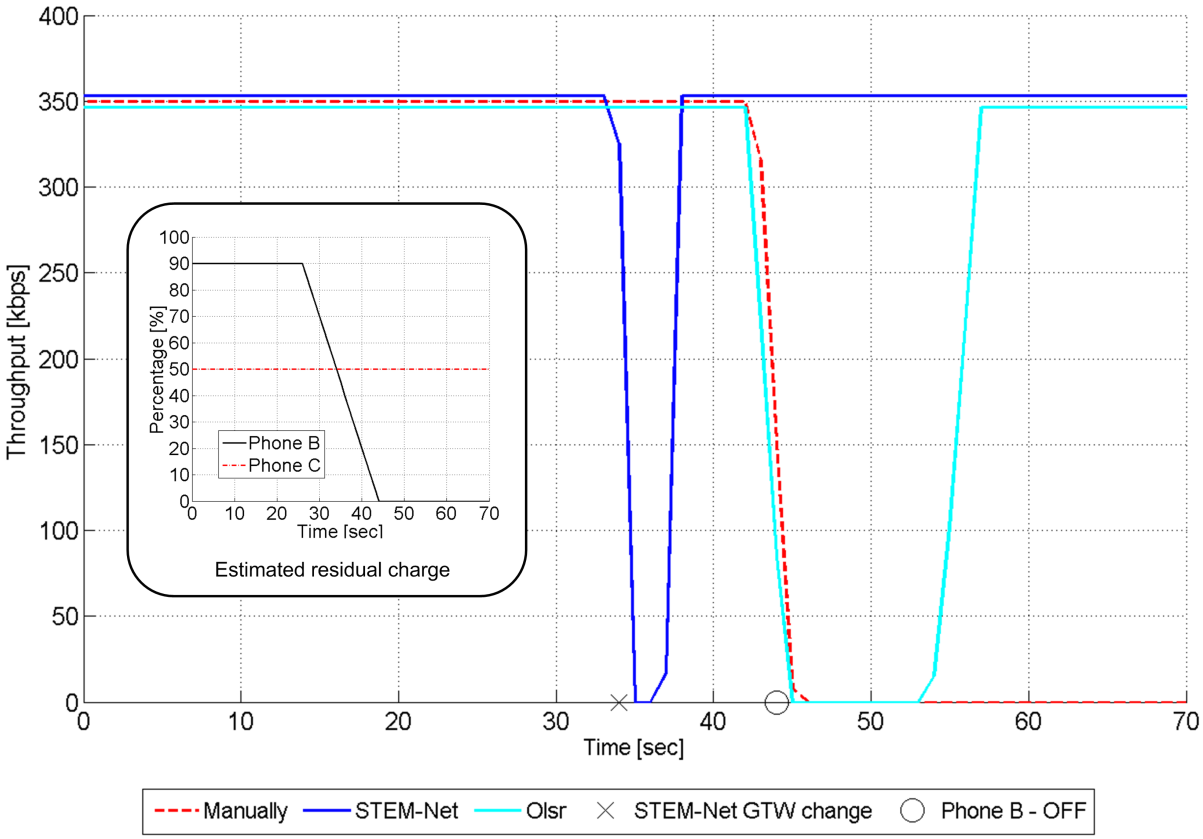


Figure 4. Throughput experienced by Phone A using different residual charge for both Phones B and C.

		Network mode	User's involvement in configuration	Data rate	Communication range	Energy consumption	Number of devices	Multi-hop
Technologies	Bluetooth	Infrastructure-less	High	Medium (up to 24Mb/s)	Low ~100m	Low	Few	Yes
	NFC	Infrastructure-less	Low	Low (up to 424Kb/s)	Very low (up to 20cm)	Low	Few	No
	Wi-Fi	Infrastructured	Low	High (Up to 600Mb/s for 802.11n with MIMO support)	Medium ~250m outdoor	High	Many	Yes
		Infrastructure-less "Ad hoc mode"	High				Few	Yes
		Infrastructure-less "Direct mode"	Low				Few	No
	HSDPA HSUPA	Infrastructured	Low	Medium (up to 42,3 Mbit/s)	High tens of Kilometers	High	Many	No
	LTE	Infrastructured (maybe also Infrastructure-less in Release 12 - D2D)	Low	High (Up to 500Mb/s in the *Advanced* version)	High tens of Kilometers	High	Many	No

Table 1. Enabling technologies for SSNs.

Section A		
Relevant Parameters Estimation	**Parameters**	**Computation Method**
	$E(i)$: Residual Energy at node i	Each operating system offers specific routines
	$C_{cell}(i)$: Congestion on the cellular interface of node *i*	The interface driver offers an estimation of total transmitted TX_{Cell}, received RX_{Cell}, dropped $DROP_{Cell}$ and corrupted ERR_{Cell} packets: $C_{cell} = \frac{DROP_{cell} + ERR_{cell}}{TX_{cell} + RX_{cell}}$
	$C_{Wi-Fi}(i)$: Congestion on the Wi-Fi interface of node *i*	The interface driver offers an estimation of total transmitted TX_{WiFi}, received RX_{WiFi}, dropped $DROP_{WiFi}$ and corrupted ERR_{WiFi} packets: $C_{WiFi} = \frac{DROP_{WiFi} + ERR_{WiFi}}{TX_{WiFi} + RX_{WiFi}}$
	$D(i)$: Average distance from neighbors of node *i*	The OLSR routing tables include the hop distance from other nodes in the SSN. $D(i)$ is the average of those hop distances.
Section B		
Stimulus and Threshold computation	**Functions**	**Computation Method**
	$G(\dots)$ Stimulus at node *g*	$SM(g) = \alpha(1 - E(g)) + \beta(C_{cell}(g))$ where the smoothing factors α and β are chosen to respect the relation $\alpha + \beta = 1$
	$F(\dots)$ Threshold at node *i*	$TM(i) = 1 - [\gamma \frac{E(i)}{E_{max}} + \delta\left(1 - \frac{C_{WiFi}(i)}{C_{WiFi}^{max}}\right) + \varphi\left(1 - \frac{D(i)}{D_{max}}\right)]$ where the smoothing factors γ, δ, and φ are chosen to respect the relation $\gamma + \delta + \varphi = 1$

Table 2. Parameters estimation and Stimulus-Threshold computation.