 DOI 10.1109/TNSM.2018.2885043. Published by: IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT 

# Using an IoT Platform for Trustworthy D2D Communications in a Real Indoor Environment

M. Nitti*, V. Popescu**, M. Fadda*
*Department of Electrical and Electronic Engineering - University of Cagliari - Italy
National Telecommunication Inter University Consortium - Research Unit of Cagliari - Italy
{michele.nitti, mauro.fadda}@diee.unica.it
**Department of Electronics and Computers - Transilvania University of Brasov - Romania
vlad.popescu@unitbv.ro

***Abstract*—The constantly increasing need for data exchange among various types of devices, mobile and fixed, is one of the main characteristics of the technological development in the last few years. Within this context, the possibility to deliver content to more devices into the same domestic environment is very interesting for both consumers and service providers.**

**The main hurdle for the Device to Device (D2D) communications is the available bandwidth and implicitly the used radio technology and frequency range. From this point of view, the so called TV White Spaces (TVWS) are an ideal candidate for short range communications, but have the problem of the interference management with the licensed services already operating there. This problem can be alleviated by using cooperative, distributed spectrum sensing techniques. This paper proposes an innovative approach for D2D communications in a real indoor environment, based on a Social Internet of Things (SIoT) architecture able to involve all participating objects in a twofold procedure, gathering both spectrum sensing and Quality of Service (QoS) data and weighting the received information using a novel trustworthiness algorithm. The algorithm, together with the entire SIoT architecture, have been implemented and extensively tested in a real indoor environment.**

***Index Terms*—Social Internet of Things, Trustworthiness, Cognitive Radio, Device to Device, Spectrum Management, Real Platform.**

## I. Introduction

Third and Fourth Generation wireless technologies (i.e., 3G and 4G) were mainly driven by demand for data services over the Internet. Instead, when the academic and industry communities started thinking about a new technology (i.e., Fifth Generation - 5G), they were pushed by the possibility to focus on new emerging traffic types and data services, characterized by different requirements and global issues to be solved, with capacity increasing up to 1000 times in the next decade expected to come from the network side [1]. The trend in future mobile networks has shown a different pattern from that of existing networks, because the main objective has changed from enabling users to connect wirelessly to the Internet for enabling massive numbers of users and objects to seamlessly connect in smart cities (i.e., Internet of Things - IoT) by 2020 and beyond.

The International Telecommunication Union (ITU) International Mobile Telecommunications (IMT)-2020 Focus Group was established in May 2015 to analyze in future networks the coexistence of emerging 5G technologies as a preliminary study into the networking innovations required to support the development of 5G systems; it individuated peak data rate, user experienced data rate, latency, mobility, connection density, energy efficiency, spectrum efficiency, and area traffic capacity as key performance metrics [2].

Considering the spectrum use, frequencies below 6 GHz were considered suitable for macro coverage (i.e., with a radius up to 2 km). For frequencies up to 30 GHz, it is not clear yet the effective use of this band, but about 2.5 GHz could be made available for microcoverage (i.e., within a 50 - 100 m radius). Frequencies from 30 to 90 GHz (i.e., visible light) were considered suitable for fronthauling and backhauling as well as local deployments (i.e., within a 10 m radius). In this range, about 40 GHz could be allocated for massive machine communications [3].

The ability of Device to Device (D2D) communications to share their radio access connection, started to be considered as a possible solution due to the possibility to reduce the cost of local service provision and to supply the increase of networks density [4], changing accordingly with the trend in the telecommunications market [5]. For example, the 3rd Generation Partnership Project (3GPP) introduced in Rel-12 improvements in the Long Term Evolution (LTE) standard, allowing D2D and machine to machine (M2M) communications, reducing costs, and supporting direct communication between close User Equipments (UEs) and indoor positioning enhancements [6].

Other approaches for short-range high speed D2D communications are for example WiFi Direct and Bluetooth 5.0 [7], with transfer rates varying from 25 to 250 Mbps. The drawback of these specific solutions is the use of the overcrowded ISM band that can lead to severe performance losses. A new adaptive access network selection algorithm over heterogeneous wireless networks was proposed in [8].

Opposed to the classic approaches based on the ISM bands, in this paper we make use of the unlicensed TVWS for D2D communications. The TVWS refers, as the name suggests, to the TV channels not used in a particular location and at a particular moment of time by any TV broadcasting services. The communication in the TVWS is based on respecting the interference constraint, imposed to protect the normal operation of licensed TV broadcast services. Various studies on the use of TVWS [9] [10] [11] have identified the joint use of geo-

location databases (GLDBs) and local detection techniques (i.e., spectrum sensing) to exploit the TVWS [12]. The GLDBs contain a list of free Digital Terrestrial Television (DTT) channels for a certain location, together with the allowable maximum radiated power for transmitting without harmful interference to DTT users. Spectrum sensing procedures, on the other side, are focused on the continuous, on-site survey of the TVWS occupation, which can be also cooperative and multi-band. The main hurdle of spectrum sensing technologies is the temporal and spatial accuracy, which can be improved, especially in crowded and dynamic scenarios, through the cooperation of sensing devices. It is therefore important to have other solutions where even devices that are not directly involved in the usage of the TVWS still contribute to the sensing procedures for the benefit of the communities of devices they belong to.

The concept of heterogeneous and pervasive objects, which collaborate to reach a common goal, is the basis behind the IoT vision. One of the main advantages of such a vision is the possibility to obtain reliable information by the other members so not to suffer from attacks and malfunctions [13]; the trust management [14] is of particular importance in our scenario, where secondary users (SUs), that is unlicensed users, have to ensure that they will not cause any interference for authorized services operating in the same or in adjacent bands.

Recently, the idea of things involved into the network together with people led to the Social IoT (SIoT) concept [15], where objects are able to establish social relationships autonomously following the rules set by their owners. The resulting social network of objects is able to deliver a faster service and information discovery, by navigating a social network of "friend" objects and also to perform a more reliable management of the received information [16].

Considering, for example, a typical home environment, it is possible to find several heterogeneous devices such as communication devices, electrical appliances, safety systems, air conditioning, smart TVs, and so on. Based on the aforementioned SIoT paradigm, all these objects create their own social relations, which are used to exchange the collected data from the environment over the Internet, even if they are not directly interested in the collected resource itself. Specifically, the usage of the SIoT paradigm would deliver a complete and trustable vision of the spectrum usage, decoupling the spectrum sensing operation from the proper transmission, and improving significantly the sensing accuracy as a whole [17].

In a home environment where lots of devices are interested in exploiting spectrum opportunities [18], several nodes trying to simultaneously communicate in the same channel could affect primary transmissions in the adjacent channels. The effective monitoring over this spectrum sharing is mainly conditioned by the spectrum view that needs to be highly reliable. This is a typical scenario where a trustworthiness algorithm could sensibly improve the management of the spectrum use also protecting primary transmissions.

In [12], the authors proposed the utilization of the SIoT paradigm for the sensing of the channel status to improve the use of the TVWS. This paper extends the previous work by:

- proposing a real system for D2D communications in an indoor scenario;
- introducing, as innovative contribution, the capacity to involve all objects in sensing and feedback procedures, in order to guarantee trustworthy transmissions in the TVWS, and implicitly not disturbing active communications of the primary users in the adjacent TV channels;
- presenting for the first time, as main contribution, the implementation of a distributed sensing procedure and a Quality of Service (QoS) evaluation procedure, both coordinated by a control logic based on a trustworthiness algorithm.

In [19], an experimental study for near real-time spectrum sensing and opportunistic spectrum access in database-driven cognitive radio networks (i.e., nROAR) using USRP boards was presented, missing the possibility to evaluate the channels during secondary transmissions. The QoS evaluation procedure is crucial for the assessment of the communication channels chosen by the spectrum sensing procedure, both for the QoS of the actual broadcasting channel, as for the protection of the adjacent channels in case they are occupied by primary licensed users (PUs). By implementing the QoS evaluation procedure, the reliability of D2D communications, in terms of the protection of PUs is expected to be significantly improved.

The paper is organized as follows: section II introduces the needed background related to TVWS and thr SIoT paradigm also presenting the used architecture; section III illustrates the real scenario used for developing the proposed system, which is described in detail in section IV. The setup for the experiments and their evaluation are described in section V. Finally, section VI draws the conclusions and introduces the future work to be done.

## II. Background

### A. TVWS

As explained in the introduction, the term TVWS addresses the TV channels not used at a specific time and place by any broadcasting TV services. TVWS are also known as digital dividend, emerged after the transition from analog to digital TV broadcasting. After this transition, large ranges of the UHF radio frequency spectrum (e.g., 512-608 MHz and 614-698 MHz in USA, 470-550 MHz and 614-848 MHz in UK and EU) have been released for unlicensed devices use. The frequency range of the TVWS in the UHF spectrum has good propagation and building penetration characteristics, making these frequencies adequate especially for indoor applications. However, the use of TVWS implies various constraints. First of all, the interference constraint, imposed to protect the normal operation of licensed Digital Terrestrial Television (DTT) services, should be met: in the TVWS all new users are unlicensed, SUs constrained to detect and avoid PUs by adjusting functional parameters such as carrier frequency, transmission power, and modulation type.

In the UK, the Independent regulator and competition authority for the UK communications industries (OfCom) presented a document [20] after the decision to allow a new wireless technology access to the unused parts of the radio

spectrum in the 470 to 790 MHz frequency band, presenting a white spaces device able to share this band with the existing uses, DTT, including local TV, Program Making and Special Events (PMSE), and wireless microphone users. From the standardization point of view, there is already a first full Cognitive Radio (CR) standard, the IEEE 802.22 Wireless Regional Area Network (WRAN), developed to exploit the TVWS bands to assure broadband access for remote and rural areas. WRAN devices are designed to operate in the frequency range 54 - 862 MHz alongside DTT transmissions. Also here, the combination of GL-DBs and spectrum sensing methods are used to enhance its operation [21]. The current version of the standard, IEEE 802.22b-2015 [22] is designed to double the throughput of devices based on the original IEEE 802.22 standard. The new amendment is intended also to serve more users per base station and enable relay capability for machine-to-machine (M2M) and IoT use cases.

Other standardization organizations, such as the ETSI [23] and the ITU [2] are using the same concepts as part of their new regulations on CR and devices operating in the TVWS. The authors also conducted various studies on compatibility between PUs and SUs in the TVWS context [9], confirming the feasibility of this type of D2D communication.

### B. SIoT Paradigm

The idea to use social networking notions within the IoT to allow objects to autonomously establish social relationships is recently gaining fast popularity. The driving motivation is that a social-oriented approach is expected to support the discovery, selection, and composition of services and information provided by distributed objects and networks [24], [25] and [26]. In this paper, we refer to the SIoT model proposed in [15], where a set of forms of socialization among objects exists and the relationship between objects can be defined as:

- *parental object relationship* (POR) among similar objects built in the same period by the same manufacturer where the role of family is played by the production batch;
- *co-location or co-work object relationship* (C-LOR and C-WOR) like humans do when they share personal (e.g., cohabitation) or public (e.g., work) experiences;
- *ownership object relationship* (OOR) for objects owned by the same user;
- *social object relationship* (SOR) when objects come into contact, sporadically or continuously, due to relations among their owners (e.g., devices/sensors belonging to friends).

All these kinds of relationships are created and updated within the SIoT platform taking into account the object's features (i.e., brand, type, computational capabilities, characteristics, etc.) and social life, that is related to their meeting other objects [27]. The resulting network and relationships can be managed thanks to the SIoT architecture, made up of four main components [15]. The *relationship management* introduces into the SIoT the intelligence that allows objects to create, manage, and even terminate a relation. This component is implemented in the Cloud, in the object gateways, and in the objects themselves when capable of implementing the relevant

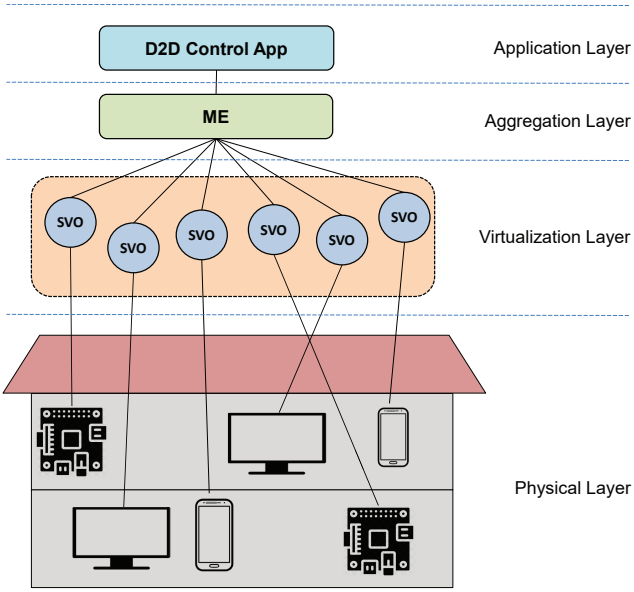


Fig. 1. SIoT Architecture

logic. Clearly, the configuration of these functions is controlled by the object owner, furthermore the resulting links could be asymmetrical. The *service discovery* component has the ability to search for the objects that can provide a required service by crawling the social network. The third component, the *service composition*, allows interaction among objects and enable to compose complex applications from atomic services. Finally, the *trustworthiness management* aims at understanding how the information provided by other members has to be processed, so to obtain a reliable system. This last component has been the topic for several recent works, such as [28], since the integration of social concepts in the management of trust can help to foster the reliability of the resulting algorithms.

In this work, the authors leverage on a cloud-based SIoT platform, named Lysis [29], to implement the proposed system. The main functionalities of the Lysis platform are shortly described in the following subsection.

### C. SIoT Architecture

The Lysis platform foresees a four layer architecture, as depicted in Figure 1:

1 **Physical Layer** includes Real World Objects (RWOs), i.e. every object which is capable of sensing the physical environment and send the acquired information to the Internet.
2 **Virtualization Layer** creates a digital counterpart of the RWOs; in order to differentiate among the different topologies of real entities, this layer offers several templates, i.e. semantic descriptions of the related RWO, which describes its capabilities and resources. The result is the Social Virtual Object (SVO), typically equipped with two interfaces that allow for a standardized communication procedure between the aggregation level and the physical devices. In particular, between a RWO and its SVO there exists a Hardware Abstraction Layer, which is in charge to create a secure

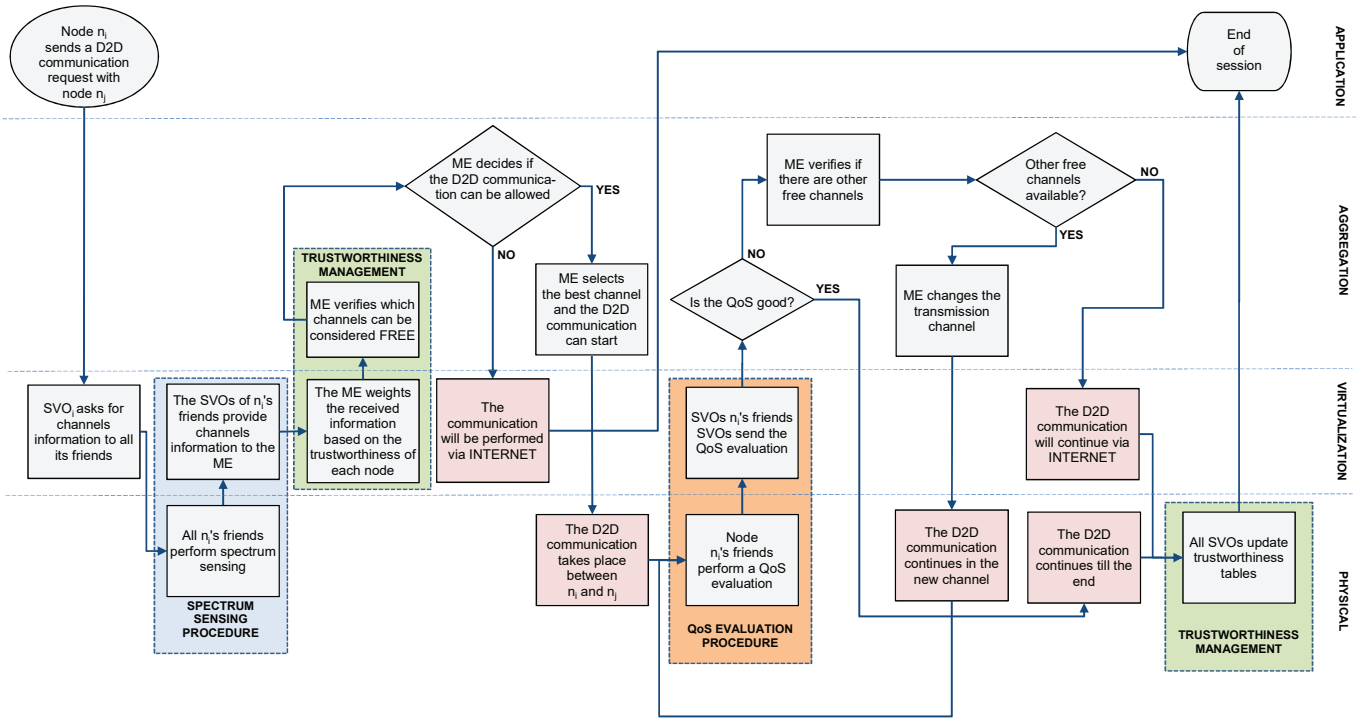


Fig. 2. Flow chart of the system

point-to-point communication (encrypted). A social identity is added to this virtual counterparts on the Lysis platform. The components depicted in the previous Section are implemented in this layer, so that all the social relations and the related functionalities are developed and maintained here.

3 **Aggregation Layer** combines information from multiple SVOs on the basis of patterns to ensure a high re-usability level. The Micro Engine (ME) is a mash-up of one or more SVOs and other MEs, responsible for getting and processing data from SVOs into high-level services requested by applications at the higher level.

4 **Application Layer** is in charge of final processing and presentation. Deployment and execution of applications makes use of one or more MEs.

## III. Real Scenario

This paper proposes a real system for D2D communications in an indoor scenario. The innovative part stands in involving all objects in sensing and feedback procedures to allow trustworthy transmissions using TVWS, not disturbing active communications in adjacent TV channels. Nowadays, a typical home environment is populated by several heterogeneous devices such as electrical appliances, safety systems, air conditioning, smart TVs, communication devices, and so on: let us call the set of devices in the smart home as $\mathcal{N} = \{n_1, ..., n_i, ...n_M\}$. Every device can sense and collect information regarding the environment, even if not directly interested in using the data; through the Internet, this information is made available to potentially every other object. The social network created by these devices can be described by an undirected graph $\mathcal{G} = \{\mathcal{N}, \mathcal{E}\}$, where $\mathcal{E} \subseteq \{\mathcal{N} \times \mathcal{N}\}$ is the set of edges, each representing a social relation between a couple of nodes. Let the set of friends of a node $n_i$ be expressed as $\mathcal{N}_i = \{n_k \in \mathcal{N} : n_i, n_k \in \mathcal{E}\}$, and the set of common friends between $n_i$ and $n_j$ as $\mathcal{K}_{ij} = \left\{n_k \in \mathcal{N} : n_k \in \mathcal{N}_i \cup \mathcal{N}_j\right\}$. Each node $n_i$ computes the trustworthiness of its $\mathcal{N}_i$ friends on the basis of its own experience and on the basis of that of its friends; we refer to this trustworthiness with $T_{ij}$, i.e. the trustworthiness of node $n_j$ seen by node $n_i$. The details on how $T_{ij}$ is computed are explained in Section IV-C.

In our scenario, we are considering the spectrum as the resource to be monitored, so let $C = \{c_1, ..., c_x, ...c_{20}\}$ be the set of possible channels. We considered only the upper part of the DTT spectrum from 702 MHz to 862 MHz, that is from channel 50 (i.e., 706 MHz) to channel 69 (i.e., 858 MHz). This choice is justified in order to make the scenario feasible for the use of mobile devices, such as smart-phones and tablets, with antennas that can operate in those frequency ranges. The goal of our paper is to obtain a complete and trustable vision of the spectrum usage thanks to the SIoT paradigm, by decoupling the functions of sensing the spectrum and transmission. The spectrum sensing cooperative methods currently implemented do not perform a control procedure on the effective transmission once started [30], and are therefore not able to identify malicious nodes that could affect the channel selection, also considering the limited number of devices involved in the procedure.

The proposed architecture comes in support for additional short-range services between devices in an indoor scenario, involving all enabled objects in a twofold procedure: a distributed social sensing procedure and a QoS evaluation procedure. Theoretically, as explained before, in a certain geo-

graphical area, the frequencies dedicated to DTT broadcasting are characterized by a static occupational status considering primary transmissions. When secondary transmissions share the free channels in the TV band, this condition changes. The proposed method helps to individuate changes in the spectrum before allowing a new communication.

As depicted in Figure 1, each device is associate with a virtual counterpart (i.e., SVO) on the Lysis platform. Whenever a device senses the spectrum, it sends that information to its virtual counterpart, so that if an object needs spectrum information for a D2D communication, it can query its social network and access its friends data. This means that information among friends are exchanged at the Virtualization Layer, i.e. among the Web Services used to implement the SVOs on the Cloud, which could be also running on the same physical machine.

The whole process starts whenever an application installed on a physical node, let us suppose node $n_i$, needs to transmit for example video content to another node $n_j$. Figure 2 illustrates the steps of the overall process. The proposed system makes use of the friends of $n_i$, i.e. the nodes in $\mathcal{N}_i$, to help the user to individuate if there is any channel available (i.e., TVWS) and authorizes the corresponding device to transmit (i.e., secondary transmission). In order to find any white spaces, the SVO of $n_i$ crawls its social network, to obtain the spectrum sensing measures data. Each node $n_k$ in $\mathcal{N}_i$ senses the spectrum and sends the information regarding the perceived received power, $P_k^R$, for each channel to its corresponding SVO; the SVO of node $n_i$ has to weight all the received information considering the trustworthiness computed by node $n_i$ towards all of its friends, namely $T_{ik}$, that provided the data in order to reduce the uncertainty of the data received and send them to the ME, which will elaborate all the information and will evaluate the availability of , based on the combined received power $P^R$. In order to minimize the possibility of interference with the PUs for newly joined devices, which only have few friends, every node has always at least one friend, the Geo Location Data Base (GL-DB). The GL-DB provides the initial TVWS availability for a certain geographical area [31] with initial trust equals to 1, which then varies according to the feedback provided by the other nodes. Using all the received information, the ME is able to have a clear view of the available channels. Based on this view, the ME has to decide whether to use Internet communications to deliver the service or D2D communications. It has to be taken into account that, in our proposed algorithm, multiple communications can occur at the same time, e.g. in the rooftop and in the basement, if the ME concludes that the same channel can be used by more than two nodes, based on the spectrum sensing procedure presented in the next Section.

If the ME approves the D2D communication, it has to select the channels for the transmission and communicates the resulting spectrum holes to node $n_i$, so that it can start to video broadcast its contents towards node $n_j$. At the same time, every node in $\mathcal{N}_i$, i.e. all the friends of $n_i$, which are in the communication range of the transmission, verifies, in terms of quality of service (QoS), that the transmission is not interfering with potential primary transmissions (i.e., PUs) operating in next adjacent channels. In particular, $n_i$'s friends sense the channel and the two channels adjacent to the selected one so that they can provide an immediate feedback about the quality of the transmission. If the transmission is not disturbing the PUs, node $n_i$ and $n_j$ can continue to communicate. However, if an interference with the primary user is detected, the nodes in $\mathcal{N}_i$ can inform the SIoT and the transmission is immediately suspended. In this case, the ME checks for other available channels and, if any, changes the transmission channel. If this happens, the D2D communication between node $n_i$ and node $n_j$ can continue in the new channel, while all the friends of $n_i$ start to sense the new channel in order to evaluate the QoS.

When the transmission is over, on a TVWS available channel or through the Internet, the trustworthiness values are updated. In particular, node $n_i$ will assign a feedback to all of its friends that provided information about the channel and update their trustworthiness values based on this feedback.

If any external causes force the D2D communication to end, such as for example an user forcefully interrupting it, or one of the devices running out of battery, than the session ends immediately without updating the trustworthiness values since there are no means to evaluate the received channel information.

## IV. System Design

In the next three sub-sections the spectrum sensing procedure (subsection IV-A), the QoS evaluation procedure (subsection IV-B), and the trustworthiness management algorithm (subsection IV-C) are presented and described.

### A. Spectrum Sensing Procedure

In [12], we presented a preliminary study, which introduces a new method able to involve all sensing-enabled objects in a distributed sensing procedure. In particular, we implemented a python software to provide each desired device (e.g., smart TVs) with sensing capabilities in the VHF/UHF bands. Energy detection measurements in the 8 MHz channel are carried out over the entire Italian DVB-T spectrum. For each channel, five consecutive measurements are performed each 0.2 seconds and the results are averaged over time.

Figure 3 shows an overview of the spectrum sensing measurements over the channels of interest (i.e., 50 to 68) obtained from different devices in an indoor environment. In order to facilitate the comprehension, we differentiated the nodes considering their location (i.e., from the basement to the rooftop of an hypothetical building). As it can be seen, devices can sense very different channel conditions, depending on their position.

Then, each SVO sends this information to the SVO requesting them, that, based on its trustworthiness knowledge, is able to weight the received data and compute the resulting received power as follows:

$$P^R = \sum_{k=1}^{|\mathcal{N}_i|} T_{ik} P_k^R \Big/ \sum_{k=1}^{|\mathcal{N}_i|} T_{ik} \tag{1}$$

The SVO forwards the combined received power, shown by the black line in Figure 3, to the ME in order to take

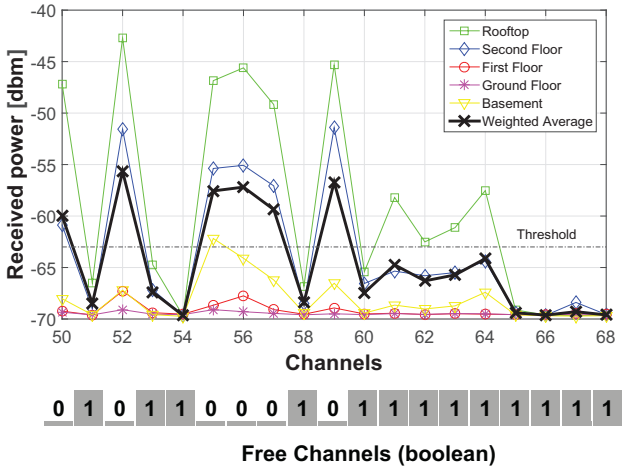


Fig. 3. Channel power sensed by each node and free channel decision

TABLE I
TRUSTWORTHINESS VALUES USED AS WEIGHTS

| Raspberry Location | Trust Value |
|---|---|
| **Rooftop** | 0.85 |
| **First Floor** | 0.7 |
| **Ground Floor** | 0.5 |
| **Basement** | 0.3 |
| **Outdoor** | 0.35 |

a decision on the availability of free channels. The ME will consider the channels as free for transmission, if the combined received power from all $n_i$'s friends is lower than a threshold, which is set to -63 dBm, based on the work in [32]. The lower part of Figure 3 shows also the channels which are labeled as free, based on the weighted signal strength compared to the previously cited threshold.

Based on the used threshold, it is then possible to define the occupational status of channel $c_x$ perceived by the generic friend $n_k$. We indicate such a status by the matrix $\boldsymbol{S} = [s_{kx}]$ where the generic element $s_{kx}$ is equal to 1 if the node $n_k$ senses the channel $c_x$ as available, i.e. with a received power lower than the threshold, and 0 otherwise.

It has to be taken into account that the weights used to compute the combined received power correspond to the trustworthiness of each device. The weights considered in Figure 3 are obtained considering the spectrum sensing measurements campaign presented in [12], which is reported in Table I, and are static, since in that paper the trustworthiness was intended as the capacity of a node to sense correctly the spectrum based on its position. In this paper, we consider the trustworthiness as the willingness of a node in providing reliable information, and then proposed a dynamic algorithm to compute it based on a feedback system.

### B. QoS Evaluation Procedure

An important step in the spectrum sensing procedure is to determine which collected information is trustworthy. To this, we make use of a feedback system that allows a node $n_i$ to provide an evaluation of the service, in our case the spectrum sensing, it has received by the providers, i.e. by its friends. The service received is represented by the occupational status of the channel $\boldsymbol{S}$.

However, an element which is frequently missing in trustworthiness algorithms is how the feedback can be practically generated [33]. Indeed, when an object receives the requested service, it needs to evaluate if the service is consistent with its query and rate it. In this work, each physical device friend of the transmitter and in the transmission range of the D2D communication (i.e., the communication allowed by the ME after the sensing procedure) will be able to evaluate if that transmission is causing interference to PUs in co- and adjacent channels. This evaluation translates into a QoS evaluation based on the levels of accuracy in terms of signal to interference and noise ratio (SINR) detected.

The demodulated, equalized, and sampled IQ constellation of the primary received signal, if present, in the adjacent channels (upper and lower) is used to evaluate the presence of harmful interference. For a good quality signal, the IQ data points are close to the ideal location, but as the signal is degraded by noise or other interference, the distance from the ideal point increases leading to a corresponding growth in symbol errors as more data points stray over the inter-symbol decision boundaries. The spread in the received data points can be seen as a signal quality indicator. Starting from these considerations, we carried out preliminary performance evaluations stressing the quality of the DTT received signals in order to individuate when the quality of images started to degrade (i.e., picture failure point - PFP) [34] due to adjacent channel interferences. By using this method, each node involved in the QoS evaluation procedure can evaluate the possible degradation in the quality of the signals received on the channels adjacent to the one used for secondary transmission due to the presence of an interfering adjacent communication.

The QoS is evaluated by all the nodes in the first adjacent channels (i.e., upper and lower), namely $c_{x+1}$ and $c_{x-1}$, as in the $\mathcal{N}_i$, i.e., $c_x$ by the interested receiving node. We indicate as $Q_k^{ij}$, the QoS evaluated by the generic friend $n_k$ regarding the transmission between $n_i$ and $n_j$, which is computed as follows:

$$Q_k^{ij} = Q_{k,x-1}^{ij} \wedge Q_{k,x}^{ij} \wedge Q_{k,x+1}^{ij} \tag{2}$$

where $Q_{k,x-1}^{ij}$, $Q_{k,x}^{ij}$, and $Q_{k,x+1}^{ij}$ are the QoS results considering channels $c_{x+1}$, $c_x$ and $c_{x-1}$ respectively, expressed as boolean values: a true value (i.e., 1) means the QoS is good and the primary transmission is not interfered; on the contrary, a false value (i.e., 0) indicates a wrong selection of the channel. $Q_k^{ij}$ is the logic *and* product of all these contributions and if its value is true indicates the primary transmission is not disturbed both in the co- and adjacent channels.

All the QoS evaluations from the nodes in $\mathcal{N}_i$ are sent to the ME, which will compute the global QoS, considering their trustworthiness level as seen by node $n_i$, based on the following formula:

TABLE II
$f_{ik}^m$, $s_{kx}$ AND $Q^{ij}$ DEPENDENCY

| $f_{ik}^m$ | $s_{kx}$ | $Q^{ij}$ |
|---|---|---|
| **1** | 0 | 0 |
| **0.4** | 0 | 1 |
| **0** | 1 | 0 |
| **1** | 1 | 1 |

TABLE III
TRUSTWORTHINESS TABLE OF EACH SVO

| | **feedback** | | | | |
|---|---|---|---|---|---|
| | $f^1$ | $f^2$ | **...** | $f^m$ | **...** |
| **List of Friends** | | | | | |

$$QoS = \sum_{k=1}^{|\mathcal{N}_i|} \left( Q_k^{ij} - (\neg Q_k^{ij}) \right) T_{ik} \tag{3}$$

The computed QoS is then used by the ME to balance the good and bad QoS evaluations and decide if the communication between $n_i$ and $n_j$ is interfering with a PU as follows:

$$Q^{ij} = \begin{cases} 1 & \text{if } QoS > 0 \\ 0 & \text{if } QoS \leq 0 \end{cases} \tag{4}$$

It has to be noted that even when the good and bad evaluations regarding the QoS match, i.e. $QoS = 0$, the ME decides to stop the communication as a conservative decision, in order to not risk any interference with a PU.

At the end of each D2D communication $m$, $n_i$ assigns a feedback $f_{ik}^m$ to the information received by its friends regarding the occupational status of channels, by crosschecking their sensing measures with the QoS evaluated by the ME. According to Table II, if the QoS is concordant with the sensed channel status, i.e. the channel was sensed as free and no interference is detected or the channel was sensed as busy and it was occupied by a PU, the friend receives a positive feedback; if the QoS is discordant, the feedback is negative: in this case, we decided to punish more the nodes that try to create collisions with a PU by giving a free light on the channel status.

### C. Trustworthiness Management Algorithm

Our algorithm is designed to allow each node to have its own view of the network; this approach is useful to avoid a single point of failure and infringement of the values of trustworthiness. Each SVO stores and manages the feedback needed to calculate the trustworthiness level regarding its friends in a table similar to the one shown in Table III, where the feedback is organized from the most recent transaction, i.e. $m$ indexes from the latest transaction ($m = 1$) to the oldest one.

To evaluate the trustworthiness, the authors are proposing a new algorithm, entirely implemented in Python. Five parameters have been considered [35]:

- **Trust composition** represents which components need to be considered when computing trust;
- **Trust propagation** refers to how the peers exchange their trust evidence;
- **Trust aggregation** represents the technique used to aggregate trust values;
- **Trust update** concerns the mechanism for updating the trust values;
- **Trust formation** represents how all the factors can combine together to the formation of the overall trust value.

To compose the trustworthiness of each node, we make use of two different parameters: the first one is based on the service provided by the nodes, i.e. the channel availability, and is evaluated through the feedback system shown in the previous Section, while the other one comes from the social trust derived by the social network among nodes. Thanks to the feedback system, any node can make use of its past experience and have a historical view of its last transactions with its friends. Considering a couple of nodes $n_i$ and $n_j$, the experience of node $n_i$ towards node $n_j$, expressed as $E_{ij}$, can be measured as:

$$E_{ij} = \delta E_{ij}^{srt} + (1 - \delta) E_{ij}^{lng} \tag{5}$$

where $E_{ij}^{srt}$ is the short-term experience and $E_{ij}^{lng}$ is the long-term experience, which are weighted differently based on $\delta$, an input parameter of the algorithm.

The short and long experience are calculated as follows:

$$E_{ij}^{srt} = \sum_{m=1}^{W^{srt}} f_{ij}^m \Big/ W^{srt} \tag{6}$$

$$E_{ij}^{lng} = \sum_{m=1}^{W^{lng}} f_{ij}^m \Big/ W^{lng} \tag{7}$$

where $W^{srt}$ and $W^{lng}$ are two temporal windows, which are useful to evaluate malicious nodes with a dynamic behavior, where their reputation oscillates between good and bad. Even if it is important to take into account as many feedback as possible, the accumulated experience is not able to quickly react to behavioral changes, so a shorter temporal window is needed to identify them. The value of the $\delta$ parameter will help the system to adjust the importance of the two experiences.

However, the reliability of collected data will also depend on the profile $P$ of the object providing the channel information, intended as the combination of its accuracy and its position. The accuracy of the object depends on its ability to sense even low-level signals and is actually its noise floor, varying from -60 dBm to -100 dBm. For example, the noise floor of a low-cost DTT tuner dongle is around -60 dBm, while a professional vector signal analyzer has a noise floor of -100 dBm, both values referring to a 8 MHz resolution bandwidth. For the sake of simplicity, in this work we only consider static objects, therefore the values associated with the profile $P$ of the objects were obtained by using the results of two previous studies [32] concerning the evaluation of the hidden node margin for TVWS. The obtained profile values are shown in Table IV.

TABLE IV
TABULATED VALUES FOR OBJECT PROFILE

| | Position (Floor) | | | | |
|---|---|---|---|---|---|
| **Accuracy** | **B** | **G** | **1** | **2** | **R** |
| **-100 dBm** | 0.4 | 0.6 | 0.8 | 1 | 1 |
| **-90 dBm** | 0.3 | 0.5 | 0.7 | 0.9 | 1 |
| **-80 dBm** | 0.2 | 0.4 | 0.6 | 0.8 | 0.9 |
| **-70 dBm** | 0.1 | 0.3 | 0.5 | 0.7 | 0.8 |
| **-60 dBm** | 0 | 0.2 | 0.4 | 0.6 | 0.7 |

TABLE V
TYPE OF FRIENDSHIP VALUES

| **TYPE** | | **F** |
|---|---|---|
| Owner Object Relationship | OOR | 1 |
| Co-Location Object Relationship | CLOR | 0.8 |
| Co-Work Object Relationship | CWOR | 0.8 |
| Social Object Relationship | SOR | 0.6 |
| Parental Object Relationship | POR | 0.5 |

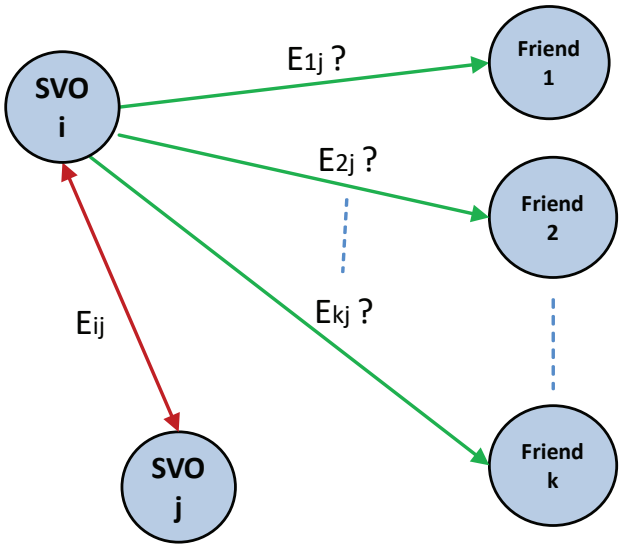


Fig. 4. Request for friends experiences

The trust value that evaluates the quality of the service provided by node $n_j$ as seen by node $n_i$ can be calculated as a combination between the profile of $n_j$ and the past experiences between the two nodes, as follows:

$$T_{ij}^{Q} = P_j * E_{ij} \tag{8}$$

The social component is calculated considering the main features of a social network among objects [33]: the centrality of the nodes and the type of friendship that connects two devices $n_i$ and $n_j$.

Centrality, expressed as $C_{ij}$, represents of how much one node ($n_j$) is central in the local network of another node ($n_i$) and not how much it is considered central for the entire network. This subjective view of the centrality helps to avoid malicious nodes which build up a lot of relations to have high values of centrality for the entire network; moreover, if two nodes share a lot of friends, it means they have similar means to evaluate the creation of a friendship. We compute centrality on the basis of the common friends $\mathcal{K}_{ij}$ among the two nodes, with respect to the total number of friendships of object $n_i$, namely $\mathcal{N}_i$.

$$C_{ij} = |\mathcal{K}_{ij}| \Big/ (|\mathcal{N}_i| - 1) \tag{9}$$

The type of friendship, indicated as $F_{ij}$, between nodes $n_i$ and $n_j$ represents an unique characteristic of the SIoT, which is used to either mitigate or enhance the information provided by a friend. Based on [33], we have assigned different values to $F_{ij}$ on the basis of the relation that connects $n_i$ and $n_j$ (see Table V).

The trust value deriving from the social parameters is then obtained as:

$$T_{ij}^{S} = F_{ij} * C_{ij} \tag{10}$$

Finally, the trust composition value can be measured as:

$$T_{ij}^{Q+S} = \alpha T_{ij}^{Q} + (1-\alpha) T_{ij}^{S} \tag{11}$$

where $\alpha$ is a parameter of the algorithm that can be set to add relevance to the first or second trust parameter, usually depending on the type of issue that needs to be solved.

To evaluate another object, a node does not rely only on its own information, but queries its social network for recommendation. Trust then propagates in a distributed approach, whereby a node $n_i$ asks to its $\mathcal{N}_i$ friends about their past experiences with the node $n_j$ and weights the recommendation from the common friends $\mathcal{K}_{ij}$ using its trust composition towards them, as in Figure 4. Even if node $n_i$ relies on its friends to compute the trustworthiness, our approach can still be considered subjective since even this information is weighted based on the node $n_i$'s own experience. The trust obtained by other friends is computed as follows:

$$T_{ij}^{I} = \sum_{k=1}^{|\mathcal{K}_{ij}|} \left( T_{ik}^{Q+S} * E_{kj} \right) \Big/ \sum_{k=1}^{|\mathcal{K}_{ij}|} T_{ik}^{Q+S} \tag{12}$$

Finally, the node aggregates both its own computed trust and the recommendation received by its friends as

$$T_{ij} = \beta T_{ij}^{Q+S} + (1-\beta) T_{ij}^{I} \tag{13}$$

where $\beta$ is a parameter of the algorithm that can be set to add relevance to the composition or propagation parameter. Also in this case, it depends on the type of issue that needs to be solved.

After each D2D communication, a new feedback is released to all the friends providing channel information, and node $n_i$ can add new entries to its trustworthiness table and update all the related trust values to take into account the new experience.

## V. Experimental evaluation

This Section analyses the performance of the proposed system through a real-world implementation. The first subsection describes the setup for our experiments, while the second show the obtained results.

### A. Set-Up fon an indoor environment

To evaluate the feasibility and performance of the proposed system, a real indoor environment has been reproduced. To simplify the scenario, concurrent service requests and simultaneous D2D communications are not considered.

The measurements were performed inside the Department of Electric and Electronic Engineering (DIEE) located in Cagliari, Italy, using the 702-858 MHz frequency range (i.e., upper part of the Italian DTT spectrum). The indoor environment, where the measurements were performed, has some peculiar characteristics: the height of the ceiling (6 m) is bigger than for normal residential environments and the thickness of the walls (1 m) is also at least three times bigger than usual internal walls. For these reasons, the propagation characteristics for the test environment can be considered implicitly worse than for a residential environment. A total of 10 devices were used for our setup, namely 10 Raspberry Pi 3 platforms, which were placed at five different floors of the indoor environment, from the highest (i.e., rooftop) to the lowest (i.e., 6 meters under the ground level) position of the considered building. All the Raspberry Pi platforms were connected to the Lysis platform and then to their SVOs through a WiFi connection.

For the performed tests, the Raspberry Pi platforms (i.e., the nodes of the system), were connected via their USB Ports to Realtek DTT TV tuner dongles based on the RTL2832U chipset. Each node runs a python software enabling the use of the DTT dongles as wideband radio scanners performing energy detection measurements over 8 MHz channel. The same dongles were programmed to decode the DTT signal on specific channels and in order to evaluate the interference level caused by opportunistic transmissions to adjacent communications. Specifically, the standard Linux DVB library was used to decode the DTT signals, using a Python-based binding implemented on the Raspbian distribution. Upon decoding the DTT MPEG transport stream (TS) of the first channel of the multiplex, the following parameters are evaluated: signal strength, signal-to-noise ratio, and packet errors. These three parameters are combined into one single threshold using an experimental procedure that monitored the quasi-error-free (QEF) quality target [9] of the DVB reception in a test environment where the signal strength and the amount of noise were gradually varied.

In order to register the node RWO to the Lysis platform and let them communicate with the corresponding SVOs, we created a new template, in Python, which is in charge to collect all the sensing information provided by the nodes, the QoS evaluations regarding the channel. The trustworthiness algorithm was implemented as a Python software running on a local server.

Once all the nodes are registered on Lysis, they start to create their own relations: the nodes located on the same floor create a C-LOR except for the ones in the basement, which we simulate as a working place and hence they create a C-WOR. In order to create the other relations, we suppose that the nodes on the second and third floor belong to the same user so these four platforms form OORs. We suppose that some of the nodes belong also to different manufacturers so that even POR can be established among them. Finally, we also consider the social relations of the owners of some of the nodes in order to create SOR. The resulting social network of the entire setup is shown in Figure 5.

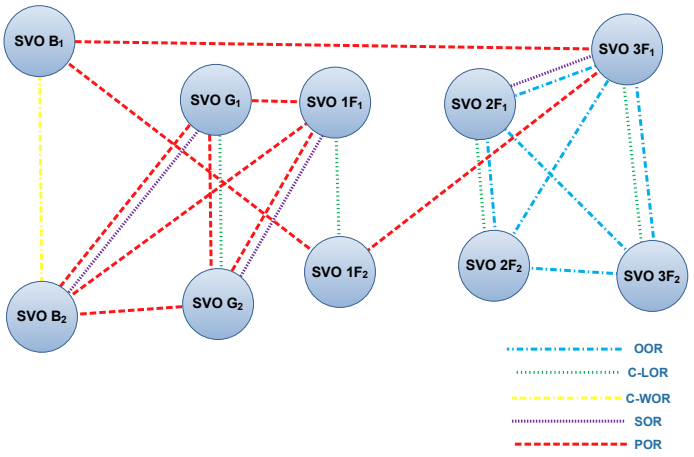


Fig. 5. Resulting social network of our setup

At the aggregation layer, we implemented a ME in Python, which is responsible to mash-up the information from the different SVOs and take decisions; in particular it has to select the channel (if available) for the D2D communication and to check the TVWS list for a different channel if the QoS procedure highlights an error.

The registration of the nodes on the Lysis platform is initiated by the nodes that are aware of the IP and port address of the ME which is pre-coded in their installed Python templates. The bidirectional information exchange between the RWOs and the ME is done in all phases of the communication with HTTP GET and POST methods. A HTTP server was implemented on the nodes using the Django framework.

The transmission of the video content is implemented using the same computational platform of the nodes connected via the Ethernet port to a USRP2920 Software Defined Radio (SDR) platform. A GNU Radio software running on the node is sending the DVB-T compliant MPEG Transport Stream (TS) to the SDR which then modulates the stream on the specific channel chosen by the ME.

### B. Analysis of performance

Among the 10 nodes, we implemented a malicious behavior, i.e. a behavior corresponding to a node who cheats whenever it has the possibility to do so in order to disrupt the benefit of the network.

Each transaction starts by selecting a node that triggers an application request to transmit some data to another random node and ends whenever the communication is completed. A transaction is considered successful whenever the ME decides

TABLE VI
MEASUREMENT PARAMETERS

| EXPERIMENT | Malicious Nodes | $\beta$ | $\alpha$ | Intelligence | $\delta$ |
|---|---|---|---|---|---|
| $\beta$ **variation** | 3 | 0.2-0.4-0.6-0.8 | 0.75 | N | 0.5 |
| **Malicious Nodes** | 1 to 5 | 0.8 | 0.75 | N | 0.5 |
| $\alpha$ **variation** | 3 | 0.8 | 0-0.25-0.5-0.75-1 | Y | 0.5 |
| $\delta$ **variation** | 3 | 0.8 | 0.75 | N | 0.25-0.5-0.75-1 |

to allow a D2D communication, i.e. the spectrum sensing procedure indicates the channel availability, and the QoS evaluation shows no interferences with a PU, i.e. the D2D communication can continue till all the data are transmitted. If for any reason, the communication is performed via Internet or the ME has to change the transmission channel, then the transaction is considered as failed, since the trustworthiness algorithm has not been able to isolate the information provided by malicious nodes.

The malicious nodes can be one of the requester's friends and they will provide false information regarding the channel and/or the QoS evaluation. Malicious nodes' behavior can be classified in two types: the first one will act maliciously with everyone, while the other type will implement an intelligent behavior and only acts maliciously with objects that it meets occasionally or it has never met, i.e. with nodes it has weak relations (PORs and SORs), and behaves benevolent with the others. Table VI summarizes the main parameters considered during the performed test.

As preliminary evaluation, the time interval between the start of a D2D communication and its interruption after QoS evaluation procedure is considered. The time to obligatory cease a secondary transmission is not fixed and can vary with a determined standard or the regulations adopted in a certain country. For example, the IEEE 802.22 Wireless Regional Area Network (WRAN) standard [22] introduces a parameter named "channel move time", indicating the time taken by a WRAN system to cease all interfering transmissions on the current channel immediately after detection, that is equal to 2 seconds. Instead, considering Ofcom indications [20], its maximum value is set to 5 seconds. During the implementation of our system, we decided to consider the worst case, that, for the best of our knowledge, is 2 seconds. For this reason, all the software procedures that control the transmission/reception operations and data processing between SVO and ME were implemented and optimized in order to have a maximum latency of 2 s.

Since the goal is to monitor the interruption time needed to stop a D2D communication, we do not consider any malicious nodes. We then allow two nodes to communicate and allow the transmitter's friends to evaluate the QoS. When the D2D communication starts, we add an external disturbing signal, acting as a PU and monitor the time needed for the transmitter to receive a notification from the ME to stop or change the channel. We performed 30 consecutive disturbed communications and show the obtained results in Figure 6. As can be deduced, the time intercurring from when the communication starts to its forced interruption never exceeds

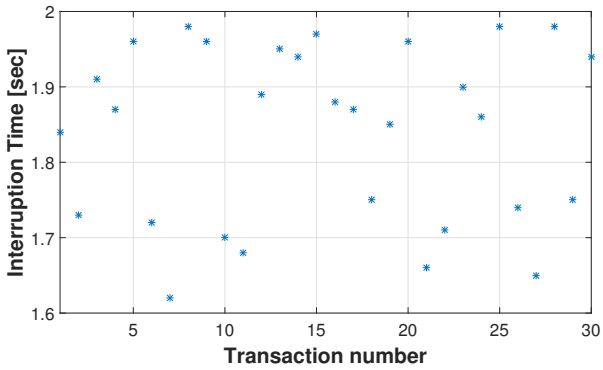


Fig. 6. Interruption time variation

2 seconds, as initially stated, with an average value of 1.84 seconds.

Subsequently we tested the proposed trustworthiness algorithm. As the radio situation is considered as static in our test environment, i.e. we know the spectrum is free from channel 60 to channel 69, and we implemented only one transmission at a time, in order to test the trustworthiness algorithm and to shorten the experimental time, we considered that every SVO already has information regarding the channel status and the QoS evaluation and that it provides them correctly based on its behavior (malicious or not).

The first set of experiments was intended to analyze the impact on the trust of the $\beta$ parameter, i.e. the importance of the experience accumulated by a node itself w.r.t. the feedback obtained from its friends. Figure 7 shows the success rate when the malicious nodes do not present any intelligent capability, hence they behave maliciously with everyone.

We can observe how, when the accumulated experience for a single node is low, i.e. there are few transactions, it is important to take into account the opinion of the friends, in order to faster isolate the malicious nodes and to obtain a better success rate. However, when a node is able to accumulate enough experience, then trusting its own experience helps to avoid the scenario where malicious nodes are camouflaged as friends. Regarding the value of $\beta$, the algorithm is able to isolate the malicious nodes (success rate equals to $99,9\%$).

Then, we tested the reaction of the system to the presence of malicious nodes trying to corrupt spectrum occupancy information. Figure 8 depicts the success rate, as a function of the transaction number when varying the percentage of the malicious nodes. It can be noted how our system is able to converge even with 70% of malicious nodes, since every

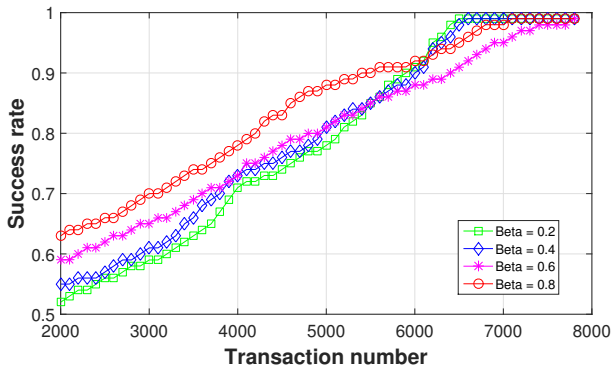


Fig. 7. Transaction success rate variation considering different values of $\beta$ parameter in presence of three malicious nodes

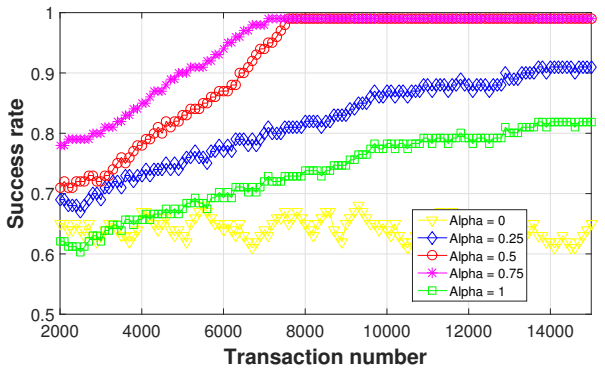


Fig. 9. Transaction success rate variation considering different values of $\alpha$ parameter in presence of an intelligent malicious node

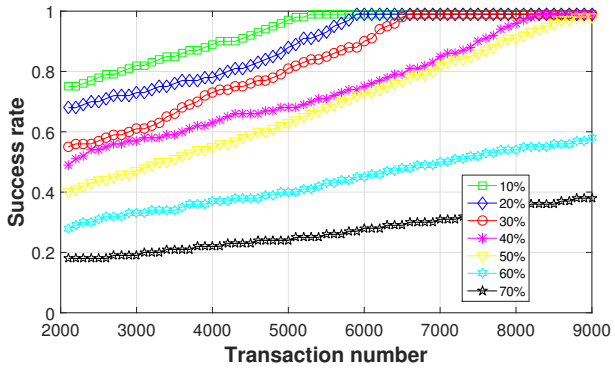


Fig. 8. Transaction success rate variation in presence of malicious nodes

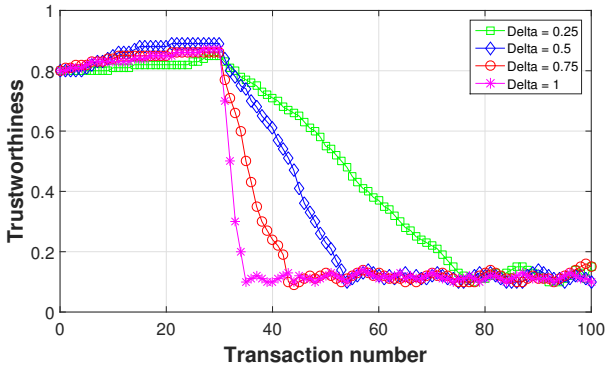


Fig. 10. Trustworthiness variation considering different values of $\delta$ parameter monitoring a node that become malicious

node has its own vision of the network based on its own experience regarding the target node and its friends. However, the time needed to converge is longer, since there is the need to accumulate more feedback to cope with the false information received by the malicious nodes and to isolate them.

Successively, we investigated the behavior of the algorithm when facing an intelligent malicious node, adapting its behavior based on the node it is interacting with. The results are shown in Figure 9, when varying the $\alpha$ parameter: this parameter is necessary in order to weight differently the contribution received from the feedback system and the ones derived from the social network. It can be easily noticed that considering only one contribution is not enough to isolate the malicious nodes: the social trust oscillates around a regime value of around 0.65, while the feedback system can achieve only an 80% success rate. However, by composing these two parameters, it is possible to make the algorithm converge even with intelligent malicious nodes after 7000 transactions.

The focus of the last set of experiments was set on the analysis of the importance of the $\delta$ constant, i.e. how the proposed algorithm reacts to a node that, after building up its trustworthiness, starts to behave maliciously. Figure 10 shows the computed trust values in this scenario: it can be seen that the algorithm is able to quickly adapt to the change in the node behavior. In particular, when only the short-term experience is considered, i.e. $\delta$ equals to 1, the algorithm adapts in only 5 transactions. However, the long-term experience is still needed to mediate any possible unintentionally wrong evaluation from friends.

## VI. Conclusions and Future Work

This paper proposes an innovative approach for D2D communications in a real indoor environment, based on a SIoT architecture able to involve all participating objects in a twofold procedure, gathering both spectrum sensing and Quality of Service (QoS) data and weighting the received information using a novel trustworthiness algorithm. The algorithm and the entire SIoT architecture have been implemented and extensively tested in a real indoor environment, taking into consideration various device classes, indoor locations and relationships between the involved nodes. The spectrum sensing and the evaluation of the QoS was implemented using Raspberry Pi computational platforms equipped with USB DTT dongles for which a specific software was written allowing them to gather the spectral data and to monitor periodically the quality of the received DTT signal.

The stability of the entire system was tested also in the presence of malicious nodes sending wrong informations, confirming the reliability of the algorithm, both for short and long term evaluation.

As for the future work, our intention is to evaluate the proposed system performance in other real scenarios. One of

these will be an outdoor smart city scenario characterized by the presence of vehicular and pedestrian users interested in sharing services and resources.

## Acknowledgements

This work was partially supported by Italian Ministry of University and Research (MIUR), within the Smart Cities framework (Project CagliariPort2020, ID: SCN_00281 and Project Cagliari2020, ID: PON04a2_00381) and by a grant of the Romanian Ministry of National Education and Scientific Research, RDI Programe for Space Technology and Advanced Research - STAR, project number STAR CTR 147.

## References

[1] Q. Li, A. Papathanassiou, and W. G., "5g network capacity: key elements and technologies," *Vehicular Technology Magazine, IEEE*, vol. 9, pp. 71–78, March 2014.

[2] ITU, "Itu towards imt for 2020 and beyond," *Online: https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx*, 2015.

[3] D. Soldani and A. Manzalini, "Horizon 2020 and beyond: On the 5g operating system for a true digital society," *Vehicular Technology Magazine, IEEE*, vol. 10, pp. 32–42, March 2015.

[4] J. Montalban, P. Scopelliti, M. Fadda, E. Iradier, A. Desogus, C., M. P., and G. M., Araniti, "Multimedia multicast services in 5g networks: Subgrouping and non-orthogonal multiple access techniques," *IEEE Communications Magazine*, vol. 56, no. 3, pp. 96–103, 2018.

[5] M. Tehrani, M. Uysal, and H. Yanikomeroglu, "Device-to-device communication in 5g cellular networks: Challenges, solutions, and future directions," *Communication Magazine, IEEE*, vol. 52, pp. 86–92, May 2014.

[6] 3GPP, "3rd generation partnership project; technical specification group services and system aspects; study on architecture enhancements to support proximity-based services (prose) (release 12)," *3GPP TR 23.703 V12.0.0 (2014-02)*, Feb 2017.

[7] U. N. Kar and D. KumarSanyal, "An overview of device-to-device communication in cellular networks," *ICT Express on Science Direct*, Oct 2017.

[8] M. Anedda, G. Muntean, and M. Murroni, "Adaptive real-time multi-user access network selection algorithm for load-balancing over heterogeneous wireless networks," *IEEE International Symposium on Broadband Multimedia Systems and Broadcasting*, July 2016.

[9] M. Fadda, M. Murroni, and V. Popescu, "A cognitive radio indoor hdtv multi-vision system in the tv white spaces," *IEEE Transactions on Consumer Electronics*, vol. 58, no. 2, pp. 302–310, 2012.

[10] S. Mo, H. Gregory, and L. Chenyang, "Real-world empirical studies on multi-channel reliability and spectrum usage for home-area sensor networks," *IEEE Transactions on Network and Service Management*, vol. 10, no. 1, pp. 56 – 69, 2013.

[11] T. Daphne, C. Marinos, C. Stuart, and P. George, "Adaptive resource management and control in software defined networks," *IEEE Transactions on Network and Service Management*, vol. 12, no. 1, pp. 18 – 33, 2015.

[12] M. Fadda, M. Nitti, V. Pilloni, V. Popescu, and M. Alexandru, "Distributed spectrum sensing for indoor broadcasting services using an iot platform," *IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, 2017.

[13] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for internet of things," *Journal of network and computer applications*, vol. 42, pp. 120–134, 2014.

[14] F. Bao, R. Chen, M. Chang, and J.-H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," *IEEE transactions on network and service management*, vol. 9, no. 2, pp. 169–183, 2012.

[15] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," *Computer Networks*, vol. 56, no. 16, pp. 3594–3608, 2012.

[16] R. Chen, F. Bao, and J. Guo, "Trust-based service management for social internet of things systems," *IEEE transactions on dependable and secure computing*, vol. 13, no. 6, pp. 684–696, 2016.

[17] M. Nitti, M. Murroni, M. Fadda, and L. Atzori, "Exploiting social internet of things features in cognitive radio," *IEEE Access*, vol. 4, no. 7801922, pp. 9204–9212, 2016.

[18] L. Jalal, M. Anedda, V. Popescu, and M. Murroni, "Qoe assessment for iot-based multi sensorial media broadcasting," *IEEE Transactions on Broadcasting*, vol. 64, no. 2, pp. 552–560, 2018.

[19] R. D. B., B. Chandra, and G. Sean, "nroar: Near real-time opportunistic spectrum access and management in cloud-based database-driven cognitive radio networks," *IEEE Transactions on Network and Service Management*, vol. 14, no. 3, pp. 745 – 755, 2017.

[20] Ofcom, "Ofcom: Implementing tv white spaces," *Online: https://www.ofcom.org.uk/__data/assets/pdf_file/0034/68668/tvws-statement.pdf*, Feb 2015.

[21] I. . WG, "Part 22: Cognitive wireless ran medium access control (mac) and physical layer (phy) specifications: Policies and procedures for operation in the tv bands. ieee standard for information technology - telecommunications and information exchange between systems wireless regional area networks (wran) - specific requirements," *IEEE Std 802.22-2011*, 2011.

[22] I. 802.22b WG, "Ieee std 802.22b-2015 (amendment to ieee std 802.22-2011 as amended by ieee std 802.22a-2014) - ieee standard for information technology–telecommunications and information exchange between systems - wireless regional area networks (wran)–specific requirements - part 22: Cognitive wireless ran medium access control (mac) and physical layer (phy) specifications:policies and procedures for operation in the tv bands - amendment 2: Enhancement for broadband services and monitoring applications," *IEEE Std 802.22b-2015*, 2015.

[23] ETSI, "Etsi en 301 598 v1.1.1," in *White Space Devices (WSD); Wireless Access Systems Operating in the 470 MHz to 790 MHz TV broadcast band. Harmonized EN Covering the Essential Requirements of Article 3.2 of the RTTE Directive*, ETSI, 2014.

[24] A. Ortiz, D. Hussein, S. Park, S. Han, and N. Crespi, "The cluster between internet of things and social networks: Review and research challenges," *Internet of Things Journal, IEEE*, vol. 1, pp. 206–215, June 2014.

[25] P. Mendes, "Social-driven internet of connected objects," in *Proc. of the Interconn. Smart Objects with the Internet Workshop*, 2011.

[26] V. Pilloni, L. Atzori, and M. Mallus, "Dynamic involvement of real world objects in the iot: A consensus-based cooperation approach," *Sensors*, vol. 17, no. 3, p. 484, 2017.

[27] L. Militano, M. Nitti, L. Atzori, and A. Iera, "Enhancing the navigability in a social network of smart objects: A shapley-value based approach," *Computer Networks*, vol. 103, pp. 1–14, 2016.

[28] E. K. Wang, Y. Li, Y. Ye, S.-M. Yiu, and L. C. Hui, "A dynamic trust framework for opportunistic mobile social networks," *IEEE Transactions on Network and Service Management*, vol. 15, no. 1, pp. 319–329, 2018.

[29] R. Girau, S. Martis, and L. Atzori, "A cloud-based platform of the social internet of things," in *EAI International Conference on Cyber Physical Systems, IoT and Sensors Networks*, IET, 2015.

[30] V. Pilloni, P. Navaratnam, S. Vural, L. Atzori, and R. Tafazolli, "Co-operative task assignment for distributed deployment of applications in wsns," in *Communications (ICC), 2013 IEEE International Conference on*, pp. 2229–2234, IEEE, 2013.

[31] S. W. Oh, Y. Ma, M. Tao, and E. Peh, "Tv white space:the first step towards better utilization of frequency spectrum," *Wiley-IEEE Press*, 2017.

[32] P. Angueira, M. Fadda, J. Morgade, M. Murroni, and V. Popescu, "Field measurements for practical unlicensed communication in the uhf band," *Telecommunication System*, vol. 61, no. 3, pp. 443–449, 2016.

[33] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social internet of things," *Knowledge and Data Engineering, IEEE Transactions on*, vol. 26, pp. 1253–1266, May 2014.

[34] ITU, "Recommendation itu-r bt. 1368-12," in *Planning criteria, including protection ratios, for digital terrestrial television services in the VHF/UHF bands*, ITU, 2015.

[35] J. Guo and R. Chen, "A classification of trust computation models for service-oriented internet of things systems," pp. 324–331, IEEE, 2015.

**Michele Nitti** received a M.Sc. degree in Telecommunication Engineering with full marks in 2009. In 2014, he was awarded with the Ph.D. degree in Electronic and Computer Engineering with Doctor Europaeus mention. He has been technical program co-chair for the IEEE International Symposium on Broadband Multimedia Systems and Broadcasting 2017 and he is actually a member of the editorial board for the Computer Networks Journal. He is currently Assistant Professor since 2015 at the University of Cagliari. His main research interests are on Internet of Things (IoT), particularly on the creation of a network infrastructure to allow the objects to organize themselves according to a social structure in Smart City scenarios.

**Vlad Popescu** Vlad Popescu received the M.Sc. degree in electronics and computer engineering and the Ph.D. degree in telecommunications from the Transilvania University of Brasov, Romania, in 1999 and 2006, respectively. In 2000, he was with the University of Malm, Sweden, specializing in multimedia applications for four months. From 2001 to 2002, he was a Research Fellow with the Technical University, Aachen, Germany, where he finished the experimental part of his Ph.D. studies on wireless communication in underground environments from 2004 to 2005. Since 2009, he has been a Visiting Professor with the Department of Electrical and Electronic Engineering, University of Cagliari, Italy. Since 2000, he is an Associate Professor with the Department of Electronics and Computers, Transilvania University of Brasov. He also collaborates close with the Department of Electrical and Electronic Engineering, University of Cagliari both on research and didactic level. His main research topics of interest are telecommunications, cognitive radio systems, multimedia applications, and data acquisition.

**Mauro Fadda** is an assistant professor in the Department of Electronic and Information Engineering of the University of Cagliari. He received a M.Sc. degree in Telecommunications Engineering from the University of Bologna in 2006 and his Ph.D. from the University of Cagliari in 2013. He was a researcher for the National Research Center in Bologna, then for the Research Center of Sardinia in Pula, for the Autonomous Region of Sardinia, and also for the Research unit of the Italian University Consortium for Telecommunications in Cagliari. His main research interest are Telecommunications, Cognitive Radio systems, mobile technologies, and broadcasting systems.