Elsevier Editorial System(tm) for Computer Networks

Manuscript Draft

Manuscript Number:

Title: Trust-based and Social-aware Coalition Formation Game for Multihop Data Uploading in 5G Systems

Article Type: SI:Cyber-phisical MNP

Keywords: D2D; Trustworthiness; Social proximity; D2D communications; Game Theory; 5G

Corresponding Author: Dr. Giuseppe Araniti,

Corresponding Author's Institution: University Mediterranea of Reggio Calabria

First Author: Leonardo Militano

Order of Authors: Leonardo Militano ; Antonino Orsino ; Giuseppe Araniti; Michele Nitti ; Luigi Atzori; Antonio Iera

Abstract: In this paper a trust-based coalition formation game is proposed to design opportunistic hop-by-hop forwarding schemes, relying on cellular Device-to-Device (D2D) communications, to enhance content uploading services. The User Equipments (UEs) are sources of data to be uploaded to a cellular base station (eNodeB) and are assumed to be rational self-interested players as they aim at maximizing their own utility by also cooperating to opportunistically implement proximity-based data exchanges. The presence of malicious nodes in the network is a constant threat for the successful cooperation among the devices. To cope with this issue, reliability and reputation notions are considered to model the level of trust among the players. Taking inspiration from the recent Social Internet of Things (SIoT) paradigm, social-awareness of the devices is spotted as a key notion to effectively define the wished trustworthiness. The effectiveness of the proposed solution is validated through a simulative analysis showing a relevant reduction in the data loss due to malicious behavior of a subset of the involved devices. In particular, up to 86% reduction in terms of data loss is obtained with respect to the case where the proposed trust model is not implemented. Moreover, the trust-based and social-aware solution also guarantees higher gains in terms of the uploading time for the devices taking part of the cooperative D2D-based content uploading.

Trust-based and Social-aware Coalition Formation Game for Multihop Data Uploading in 5G Systems

L.Militano[a], A.Orsino[a], G.Araniti[a,*], M.Nitti[b], L.Atzori[b], A.Iera[a]

[a] *University Mediterranea of Reggio Calabria, DIIES Department, Italy*
[b] *University of Cagliari, DIEE Department, Italy*

Abstract

In this paper a trust-based coalition formation game is proposed to design opportunistic hop-by-hop forwarding schemes, relying on cellular *Device-to-Device* (D2D) communications, to enhance content uploading services. The User Equipments (UEs) are sources of data to be uploaded to a cellular base station (eNodeB) and are assumed to be *rational self-interested* players as they aim at maximizing their own utility by also cooperating to opportunistically implement proximity-based data exchanges. The presence of *malicious* nodes in the network is a constant threat for the successful cooperation among the devices. To cope with this issue, *reliability* and *reputation* notions are considered to model the level of *trust* among the players. Taking inspiration from the recent Social Internet of Things (SIoT) paradigm, *social-awareness of the devices* is spotted as a key notion to effectively define the wished trustworthiness. The effectiveness of the proposed solution is validated through a simulative analysis showing a relevant reduction in the data loss due to malicious behavior of a subset of the involved devices. In particular, up to 86% reduction in terms of data loss is obtained with respect to the case where the proposed trust model is not implemented. Moreover, the trust-based and social-aware solution also guarantees higher gains in terms of the uploading time for the devices taking part of the cooperative D2D-based content uploading.

Keywords: D2D, Trustworthiness, Social proximity, D2D communications, Game Theory, 5G

*Corresponding author. University Mediterranea of Reggio Calabria, DIIES Department, 89122 Reggio Calabria, Italy. Email: araniti@unirc.it. Phone: +3909651693420

Email addresses: leonardo.militano@unirc.it (L.Militano), antonino.orsino@unirc.it (A.Orsino), araniti@unirc.it (G.Araniti), michele.nitti@diee.unica.it (M.Nitti), l.atzori@diee.unica.it (L.Atzori), antonio.iera@unirc.it (A.Iera)

1. Introduction

Fifth generation (5G) systems are expected to introduce a revolution in the ICT domain with innovative networking features [1]. Among them, device-to-device (D2D) communications, whereby in-proximity devices communicate directly with each other to avoid routing the data paths through the network infrastructure, will play an undoubted key role [2]. The growing interest toward this technology is related to the possibilities it offers to extend the network coverage and overcome the limitations of conventional cellular systems. Among others, D2D communications, either over cellular resource or over alternative Wi-Fi/Bluetooth technologies, introduce benefits in terms of improved spectrum utilization, higher throughput, and lower energy consumption [3]. Based on these observations, a number of D2D-based applications have been investigated for future 5G wireless systems, such as mobile data offloading for proximity based applications, network coverage extension (also in case of network failure), content sharing support among UEs, etc. [4]. In this context, the reference scenario for this paper considers groups of UEs in close proximity to each other willing to upload some data to the cloud or to a central server. Typical examples for these are small-scale environments at aggregation places (e.g., a stadiums, university campuses, music events, or fairs) where UEs can exploit opportunistic data forwarding over the devices in proximity [5]. A further example is disaster scenarios where D2D relaying may be important to send out emergency messages from disconnected areas and to support information sharing among people gathered in evacuation centers [6].

In a traditional cellular system, each UE interested in uploading a content activates a unicast uplink communication to the eNodeB. In very crowded environments, where many UEs want to upload some content, the risk of spectrum crunch and poor service quality is very relevant. Moreover, a UE located far from the eNodeB could suffer from low channel quality leading to out-of-coverage situations, which, in some cases, may be of high concern (in emergency situations, for instance). These limitations are overcome by solutions that exploit the enhanced capabilities and multiple network interfaces of modern smart devices. As an example, the research activities in the field of Mobile Networking in Proximity (MNP) [7] is very active. This new paradigm complements the classic scenario by adding continuous connectivity coverage through short-range communications, based on Bluetooth and WiFi Direct, whenever a loss of connectivity is observed due to obstacles, coverage hole, or bad channel quality. Based on this paradigm, a UE that is far from the base station may establish proximity-based communications with nearby UEs that are experiencing a higher-quality in the communication link to the eNodeB. The proximity communication can be implemented over multiple cellular D2D links to set-up opportunistic hop-by-hop forwarding towards the destination. A necessary condition for such a "cooperative" relaying solution to bring benefits compared to the non cooperative case, is that the link quality of the multihop D2D topology is higher than that one of the separate links. This condition is more likely to occur in non-isotropic propagation environments with obstacles where non line of sight (NLOS) conditions

may cause partial and temporary out-of-coverage conditions [8].

A first analysis of a cooperative content uploading in LTE-A (Long Term Evolution-Advanced) scenarios has been proposed in a recent paper [9]. In this paper, we continue our research by introducing an analysis of a challenging aspect of utmost importance for an effective implementation of proximity communications, namely the need of *trustworthiness* [10], [11]. In realistic scenarios, where human interactions and human behavior is to be considered, the presence of *malicious* nodes in the network is a constant threat for a successful cooperative interaction. Indeed, in opportunistic and random communications among UEs, the end-users may not be aware of the device and end-user they are going to be connected to. Malicious nodes may decide to drop the data packets they are expected to forward without informing the interested users. To cope with these threats, objective of this paper is to model a trust-based and social-aware multihop D2D data uploading able to satisfy the rational users interested in reducing their content uploading time. To reach this goal, *reliability* and *reputation* notions will be considered to model the level of *trust* among the involved entities. By taking inspiration from recent Social Internet of Things (SIoT) models [12], in this paper we consider the sociality level of the devices to model the *reliability* of the communication [13]. The historical *reputation* of the cooperative users will also be considered to offer rational users the possibility to filter out untrusted users and avoid unsuccessful opportunistic hop-by-hop D2D interactions. The main contributions of this paper can be summarized as follows:

- We model the *trust* constraints for a successful D2D-based content uploading, where sociality among devices, as a measure of *reliability*, and historical *reputation* are included into the model;
- We define the content uploading time through a multihop D2D topology as a function of the number of UEs forming the topology and the links status;
- We define a *constrained coalition formation game* that forms the overlapping multihop D2D coalitions under the constraint of reciprocal UEs proximity for the direct links activation and a minimum *trust* level among the cooperating devices. The algorithm converges to a stable coalition structure, where all players are happy to join the formed network partition and do not have incentives to leave the coalition they are part of;
- We perform a simulative performance evaluation showing high reduction in the data loss due to malicious behavior of a subset of the involved devices. In particular, up to a 86% reduction in terms of data loss is obtained with respect to the case where the proposed trust model is not implemented. Moreover, the trust-based and social-aware solution also guarantees higher gains in terms of the uploading time for the devices taking part in the cooperative D2D-based content uploading.

The rest of the paper is organized as follows. In Section 2 we discuss the reference system and research background for multihop D2D communications in LTE-A systems. The proposed trust model and the sociality concepts are introduced in Section 3. Section 4 introduces the constrained coalitional game adopted to model the D2D topology formation. Numerical results are provided in Section 5, whereas conclusions are drawn in the last section.

2. Reference System and Research Background

We consider a single LTE-A cell with multiple UEs interested in uploading their content to the Internet. Data uploading according to the traditional *cellular-mode* is performed through the activation of separate links from each UE to the eNodeB. With the proposed *cooperative upload* instead, under the control of the eNodeB (i.e., network-assisted D2D), the UEs organize themselves to form a "logical multihop D2D topology" and cooperate in uploading the content generated by *all* of them to the eNodeB (see Fig. 1). In general, only the UEs in mutual coverage can establish direct links. In the formed cooperative topology, that we hereafter also call "coalition", the UEs located farther from the base station relay their content to a nearby UE and only the UE at the head of the topology, the so-called *gateway*, is in charge of uploading all the contents received from the other UEs to the eNodeB. The gateway is the UE with the best link quality in the coalition and it may receive, if needed, all the radio resources that would have been separately allocated by the eNodeB to the UEs in the coalition. All intermediate UEs in the topology also act as *relays* for the contents received from the upstream UEs, thus benefiting of the higher quality of the short D2D links w.r.t. the direct cellular link. Actually, when overlapping coalitions are formed, any intermediate UE can receive content from multiple branches of the resulting tree topology. Thus, in the most general configuration, each relay has one or more links active to receive data from the preceding sources in the tree topology, and one single link active to relay data (its own generated traffic and the traffic from the incoming D2D links) to the subsequent UE in the topology.

Each UE operates in half-duplex mode; thus, it either receives or transmits in a given transmission time interval. We consider a reasonable assumption for *rational* self-interested devices, that each UE uploads its own generated content first and then the content received by the preceding UEs in the topology. In particular, the transmission starts only after that the generic UE has received the whole content (in other words, UEs use the decode-and-forward relaying protocol). Devices in the same coalition may share the same resources, whereas devices in different coalitions are always allocated to orthogonal frequency resources by the scheduler at the eNodeB, so that no mutual interference is caused by different coalitions (this is a reasonable assumption, used in other works [14]). Simultaneously transmitting UEs within the same coalition can use either the same or different frequencies, based on the decision of the eNodeB according to the interference level experienced on each direct link. In particular, in this

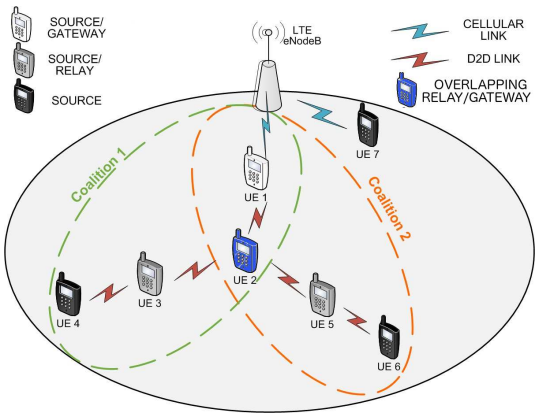


Figure 1: Multihop D2D-based coalitions in tree topology.

paper we consider the case where the same radio resources can be reused on the D2D links as they do not cause mutual interference.

The eNodeB manages the spectrum by assigning the adequate number of RBs[1] to each scheduled user and by selecting the Modulation and Coding Scheme (MCS) for each RB. Scheduling procedures are based on the *Channel Quality Indicator* (CQI) feedback, transmitted by each UE to the eNodeB over dedicated control channels. The CQI is associated to a given maximum supported MCS as specified in [15]. Thus, given a link l and the allocated RBs, the channel data rate $R_{Ch,l}$ on the wireless link l follows Shannon's capacity formula $R_{Ch,l} = Blog_2(1+\gamma_l)$, where γ_l is the signal to interference plus noise ratio (SINR) value experienced on the link and B is the available bandwidth. For a user transmission, the available bandwidth B is determined by the radio resource allocation policy. In addition, in the LTE-A system generally the channel data rate for transmitting over cellular and D2D links, i.e., $R_{Ch,m}$ and $R_{Ch,d}$ is determined as a function of the CQI values. Therefore, for a given CQI value q, the attainable data rate can be represented as a function $f(q, n_q)$[2] where n_q are the assigned RBs.

When D2D coalitions are formed in the cell, we propose that the eNodeB only assigns to the gateway of each coalition a *pool* of uplink resources that can reach up to the sum of the radio resources separately requested by the UEs in the coalition. Preliminarily, the eNodeB collects the *Channel Quality Indicators* (CQIs) from each UE relevant to the direct links with all its neighbors and the uplink. Then, the eNodeB assists the users in the cooperative coalition formation process. In the first step, the eNodeB computes the radio

[1]The RB corresponds to the smallest time frequency resource that can be allocated to a user (12 sub-carriers) in LTE. For example, a channel bandwidth of 20Mhz corresponds to 100 RB.

[2]The admissible throughput values per MCS level follow Table 7.1.7.2.1-1 in [16].

resources allocated to the UEs as if they were transmitting separately on the uplink according to the adopted scheduling policy. These resources are "virtually" allocated since UEs may form a coalition and can be used as the *pool* of resources allocated to the gateway. Based on this initial information, the eNodeB implements the coalition formation algorithm (see Section 4). As a result, stable coalitions are formed in the cell, the roles of each node in the coalition is identified, and routing path is defined. In particular, when considering a potential coalition, a step-wise decision algorithm determines the *best path* that covers all the nodes in the topology. To this aim, the eNodeB first sorts the devices in a decreasing order of uplink CQI (first those with better channel quality) and then selects the first node in the list as the *gateway* for the coalition. This is important, so that the resource pooling will produce the highest throughput toward the eNodeB for the whole multihop topology. Once the gateway is selected, the *best path* over the set of nodes is computed with focus on the D2D link qualities. We consider a simple *greedy* approach where the next hop from the gateway is selected as the one in the one-hop vicinity with the best D2D link quality. Similarly, each node in the topology will select its neighbor based on the best CQI of the direct link to the remaining nodes in the coalition. Once the coalitions are formed in the cell, the eNodeB determines the radio resources assigned to the gateway and to each D2D link and transmits all the information to the UEs so that the transmissions can start.

3. The Social-aware Trust Model for D2D-based Cooperation

In a cooperative context as the one studied in this paper, it is of utmost importance to build a trust-based interactions to guarantee reliability in the communication and limit the negative effect of typical issues such as the presence of *malicious* nodes in network [13] or *free riders* [17]. Malicious nodes may be active to manipulate the reputation of the devices through *ballot-stuffing* and *bad-mouthing attacks* to either increase its own reputation or decrease the reputation of other nodes. A free rider is a node that is taking part in a coalition to benefit from a reduced content uploading time, but is actually dropping all the incoming data from the upstreams in the cooperating topology. In this way, the node saves the energy of its battery while still benefiting from the cooperative behavior of the other nodes in the coalition. These behaviors, require solutions able to isolate the malicious nodes and build reliable reputation of the nodes.

In the past few years, with the advent of online social networks several methods to calculate trust and distrust between two persons have been proposed [10], [11] [18]. Generally, trust is defined as the quantified belief by a truster with respect to the competence, honesty, security and dependability of a trustee within a specified context [19]. When two users want to cooperate, one of them (the truster) assumes the role of a service requester and the other (the trustee) acts as the service provider. Specifically, in our cooperative coalition the node acting as relay/gateway for another node will be the trustee and the source node of the relayed data is the truster. The trustworthiness of the truster with respect to the trustee can be determined considering reliability and/or reputation. The

former is a direct measure derived by subjective observations of the truster during its interactions with the trustee; the latter is an indirect measure based on the opinions that the other actors in the community have about the trustee.

In the literature, several trust models have been proposed to represent both reliability and reputation [19]. The mechanism we propose enhances classic trust models through the exploitation of *social relationships* among the involved devices (to improve device *reliability*) and of recommendation exchange (to the purpose of reputation definition). In particular, we consider the potential of the SIoT model defined in [12], to embrace the social networking concepts and build trustworthy relationships among the devices [13]. In particular, mobility patterns and relevant context can be considered to configure the appropriate forms of socialization among the UEs. Specifically, the so-called *co-location object relationships* (C-LOR) and *co-work object relationships* (C-WOR) are established between devices in a similar manner as among humans, when they share personal (e.g., cohabitation) or public (e.g., work) experiences. Another type of relationship may be defined for the objects owned by a single user, which is named *ownership object relationship* (OOR). The parental object relationship (POR) is defined among similar devices built in the same period by the same manufacturer, where the production batch is considered a family. Finally, the social object relationship (SOR) is established when objects come into contact, sporadically or continuously, for reasons related to relations among their owners.

In this work, we propose a network-assisted model where the eNodeB serves as a trusted third party supporting the coalition formation among the interested players. To this aim, the eNodeB will store up-to-date information about the reliability, reputation and trust parameters relative to the users in the cell. In particular, we assume that the eNodeB will store a so-called *player trust matrix (PTM)* with information relevant to every couple of devices in the network. The information stored in the PTM will be used whenever a new trust-based coalition formation step is considered for cooperative content uploading by eNodeB (see details of the algorithm in Section 4). After each cooperative content uploading, the eNodeB will send an acknowledgment to the respective source nodes. Moreover, it will detect malicious behaviors in the coalitions based on data loss levels and update the reliability level of the interested players. We assume the data amount for the information exchange between source nodes and the eNodeB to be small and the data to be sent over control channels. Compared to the main content size to be uploaded by the source nodes, the control messages are very small and the corresponding transmission time and energy consumption are assumed to be negligible. Let $i \rightarrow j$ be a generic D2D link in the coalition being considered at time t during the coalition formation algorithm, where node j is expected to act as relay/gateway for the data he receives from node i (its own and the preceding nodes in the topology); we consider i, j as the truster and the trustee respectively. The parameters the eNodeB will use to determine the level of trust for the link, and contained in the PTM, are:

- *Social player reliability* ($spr_{i,j}$): is the reliability that node i assigns to player j only based on the social relationship that links the two players

and is a value in $[0, 1]$;

- *Player reliability* ($pr^t_{i,j}$): is the reliability that node i assigns to player j at time instant t. This is a subjective evaluation of the players which we consider to be influenced by the *social player reliability* and the outcome of past interactions where player j was expected to act as relay/gateway for player i. Specifically, the player reliability value is a real number ranging in $[0, 1]$ with the $0/1$ values meaning that i judges player j as completely unreliable/reliable.

- *Recommendation reliability* ($rr_{i,j}$): is the reliability that node i assigns to the recommendations provided by player j about other players in the network. Also this parameter is based on a subjective evaluation of the interested player and in our model it is influenced by the social relationship between the interested UEs. It is a real number ranging in $[0, 1]$ with the $0/1$ values meaning that i judges the recommendation received from j as completely unreliable/reliable.

- *Player reputation* ($pp^t_{i,j}$): is the reputation that player i assigns to player j for the specific service based on the recommendations provided by other players in the network at time instant t. Similar to the previous parameters, it is a real number ranging in $[0, 1]$ with the $0/1$ values meaning that the reputation assigned by i to player j based on the recommendation of the other devices is minimum/maximum.

- *Player trust* ($pt^t_{i,j}$): is the trust level that player i associates to player j at time t, which is the final parameter that determines whether player i is willing to entrust player j as relay/gateway node in a D2D-based cooperative coalition. This is a weighted combination of the reliability $pr^t_{i,j}$ and the reputation $pp^t_{i,j}$ for the player. The final player trust value is a real number ranging in $[0, 1]$ with the $0/1$ values meaning that player j is considered as completely untrusted/trusted by player i.

Player reliability. The *player reliability* is updated over time based on the past experience related to cooperative interactions where a player was expected to act as relay/gateway for the data sent by a precedent player in the formed D2D topology. To consider the past experience, we assume that for each cooperative interaction the eNodeB sends an acknowledgment to the source nodes in the coalition with information about the data being successfully received. However, based on this simple information, it is not possible for the eNodeB to determine which node in the cooperative topology has actually dropped the data. In our proposal we assume that the eNodeB will associate the outcome value δ_d to the node j that was entrusted by node i as relay/gateway forming a D2D link $i \rightarrow j$. Thus, at time $t = 0$ when no cooperation history exists, the only information the interested devices can exploit for judging the *player reliability* is *social player reliability* ($spr_{i,j}$). This is set according to predefined values as

reported in Table 1[3]. At subsequent time instants $t > 0$ the player reliability $pr^t_{i,j}$ is computed by taking into consideration the past interactions between i and j, with j acting as relay/gateway for data sent by i. We define with $\Delta^t_{i,j} = \{\delta_1, \ldots, \delta_d \ldots \delta_D\}$ the set of past interactions registered until time t, where the generic $\delta_d \in [0,1] \in \mathbb{R}$ is a value measuring the outcome of the cooperative interaction. This is equal to the total percentage of data that has been successfully forwarded by node j and reached the eNodeB. Thus, the player reliability $pr^t_{i,j}$ is computed as follows:

$$pr^t_{i,j} = \begin{cases} spr_{i,j} & t = 0 \\ \alpha \cdot spr_{i,j} + (1-\alpha) \cdot \frac{\sum_{d \in \Delta^t_{i,j}} \delta_d}{|\Delta^t_{i,j}|} & t > 0 \end{cases} \quad (1)$$

where $\alpha \in [0,1]$ is a real number used as weighting factor to give more or less importance to the initial sociality relationship between the involved nodes.

Table 1: Player and recommendation reliability values associated to the social relationship between devices.

Relationship	**Description**	**Social player reliability** ($spr_{i,j}$)	**Recomm. reliability** ($rr_{i,j}$)
Ownership object relationship (OOR)	Objects owned by the same person	1	0.9
Co-location object relationship (C-LOR)	Objects sharing personal experiences	0.8	0.6
Co-work object relationship (C-WOR)	Objects sharing public experiences	0.7	0.5
Social object relationship (SOR)	Objects in contact for owner's relations	0.6	0.5
Parental object relationship (POR)	Objects with production relations	0.5	0.4
No relationship		0.1	0.1

Player reputation. The player *reputation* is based on the opinions of the community in the network. This information stored in the PTM at the eNodeB is updated after each cooperative interaction. Let us consider a player i asking an opinion about player j and let $\mathcal{K} \subseteq \mathcal{N} \backslash \{i\}$ be the set of players which provide an opinion about player j to player i. The opinion player k will provide is its own measure of trust about player j at time instant t, i.e., $pt^t_{k,j}$. The opinion received from the other players in the network is weighted by a confidence factor the requesting player has about the received recommendation. This weighting factor is the so-called *recommendation reliability* ($rr_{i,k}$). In our model the *recommendation reliability* is set according to the social relationship between the involved devices and its value is reported in Table 1. Noteworthy, we assume that the *recommendation reliability* has a lower value w.r.t. *social player reliability* in

[3]If two communicating entities are tied by two or more types of relationships, the strongest tie with the highest factor has to be considered [13].

general. The reason for this choice is that the recommendation received by a socially related device may be influenced by the outcome of past cooperative iterations with other devices which affected the ability to provide an objective recommendation. Thus, the *player reputation* at time t is computed as follows:

$$pp_{i,j}^{t} = \frac{\sum\limits_{k \in \mathcal{K}} rr_{i,k} \cdot pt_{k,j}^{t}}{\sum\limits_{k \in \mathcal{K}} rr_{i,k}} \tag{2}$$

Player trust. Based on the notions introduced above, player i can finally determine the player trust value $pt_{i,j}^{t}$ it associates to player j at time instant t. This is a combination of the player reliability value at time t, $(pr_{i,j}^{t})$, and the player reputation $(pp_{i,j}^{t})$, suitably weighted by a real coefficient β ranging in $[0, 1] \in \mathbb{R}$:

$$pt_{i,j}^{t} = \begin{cases} 0.5 & t = 0 \\ \beta \cdot pr_{i,j}^{t} + (1 - \beta) \cdot pp_{i,j}^{t} & t > 0 \end{cases} \tag{3}$$

Note that for new coming nodes at time $t = 0$, the initial trust is set to 0.5 as suggested in [20] to contrast *whitewashing strategies* where a dishonest adviser is able to whitewash its low trustworthiness by starting a new account with the initial trustworthiness value.

4. A Constrained Coalition Formation for Trust-based Cooperation

In this section we introduce a so-called constrained coalition formation (CCF) game for the cooperative D2D content uploading. A traditional coalitional game in cost form is defined by $(\mathcal{N}, c)$ where $\mathcal{N} = \{p_1, \ldots, p_N\}$ is the set of N players and c is the cost function that models the feasible cost-value $c(S)$ for every set of players (coalition) $S \subseteq \mathcal{N}$. In particular, it is an *overlapping coalition formation game* [21] when each player is able to cooperate and join multiple coalitions. In our problem, the cost for a player p_i in coalition S is expressed in terms of uploading time needed for its own data to reach the eNodeB. With this utility, that is not transferable by definition, the studied game is a *non-transferable utility* game. In particular, for any singleton coalition $\{i\}$, the cost for player i alone is equal to the content uploading time in the cellular mode, i.e., when the UE uploads its content of size b_i over its cellular link having a data rate r_i^c: $c(\{i\}) = \frac{b_i}{r_i^c}$. For any coalition $S \subseteq N$, with cardinality $|S| > 1$, the associated cost is $c(S)$ is the data uploading time for the coalition as defined in Section 4.1. If the multihop D2D coalition cannot be formed due to coverage or trust constraints between the involved UEs, then we define: $c(S) = \sum_{i \in S} c(\{i\})$. In particular, the problem definition will lead to either a line or a tree topology for the coalitions.

We define a *collection* of coalitions $\mathcal{C}$ as the set $\mathcal{C} = \{C_1, \ldots, C_l\}$ of mutually disjoint coalitions $C_i \subset \mathcal{N}$ such that $C_i \cap C_{i'} = \emptyset$ for $i \neq i'$. If the collection

contains all players in $\mathcal{N}$, i.e., $\bigcup_{i=1}^{l} C_i = \mathcal{N}$, then the collection is a *partition* or *coalition structure (CS)*. The set of all possible *coalition structures* is identified by $\Pi(N)$. Formally we define the CCF game for the problem studied in this paper as $G =< \mathcal{N}, \mathcal{P}, \mathcal{Q}, \mathcal{Z}, c >$ where $\mathcal{N}$ is the set of UEs in the cell and $S \subseteq \mathcal{N}$ is any multihop D2D coalition, $\mathcal{P} \subseteq 2^N$ is a set of *positive constraints* such that a coalition C satisfies a constraint $P \in \mathcal{P}$ if $P \subseteq C$, $\mathcal{Q} \subseteq 2^N$ is a set of *negative constraints* such that a coalition C satisfies a constraint $Q \in \mathcal{Q}$ if $Q \nsubseteq C$, and $\mathcal{Z}$ is a set that defines the constraints on the coalitions size (*size constraints*). In our setting, the constraints for the problem are only the negative constraints deriving from a combination of *trust* and *coverage* between pairs of UEs, whereas we set $\mathcal{P} = \emptyset$, $\mathcal{Z} = \emptyset$. For the exact definition of $\mathcal{Q}$, those coalitions for which the CQI value between two consequent UEs in the corresponding topology is zero should be automatically considered as *not feasible* and thus stored in $\mathcal{Q}$. Moreover, we introduce a *feasibility threshold* FT for each coalition. It indicates the minimum value of trust for each D2D link in a coalition that allows to consider the same as a feasible coalition. We say that coalition $\mathcal{S} \subseteq \mathcal{N}$ is *not feasible* and thus included in $\mathcal{Q}$ if the resulting topology foresees at least one link $i \rightarrow j$ that does not meet the following constraint:

$$pt_{i,j} \cdot d_{i,j} \geq FT \tag{4}$$

where $pt_{i,j} \rightarrow [0, 1]$ is the *player trust* that player i associates to player j as defined in equation (3), whereas the second term $d_{i,j}$ is a binary function taking the value of 0 if the users i and j are not in proximity, and taking the value of 1 otherwise.

Since $\mathcal{Q} \neq \emptyset$, it is implicitly said that the grand coalition is not formed as it is certainly not a *feasible* coalition. To characterize the *feasible coalitional structure* to form for the CCF game, we propose simple merge-and-split rules. The key mechanism is to enable players to join or leave a coalition based on well-defined preferences so that each player is able to compare and order its potential coalitions based on which coalition it prefers to belong to. To do this, let us introduce a preference relation over coalitions. The preference order $\succ_i$ for any player $p_i \in \mathcal{N}$, is defined as a complete, reflexive, and transitive binary relation over the set of all feasible coalitions that player p_i can possibly form, i.e., the set Π_i of coalitions containing p_i. A UE can decide to join or leave a coalition according to its preference order. In particular, for each player p_i, if $C \succ_i C'$, p_i prefers being a member of coalition C more than coalition C'. Noteworthy, under this preference order definition a tree topology for the overlapping coalitions can be formed, as the uploading time for the UEs that are part of multiple coalitions is not negatively affected. This is due to the forwarding priority given to its own data compared to the data from the incoming D2D links.

To correctly define the coalition formation game, the coalition preference relation has to be defined over all pairs of coalitions in Π_i. In this paper, the

preference order is defined according to its *individual cost*. Thus, for each UE $p_i \in \mathcal{N}$ and for all $C, C' \in \Pi_i$, we say that:

$$C \succ_i C' \Leftrightarrow c_i(C) < c_i(C') \wedge c_j(C') \leq c_j(C' \backslash \{i\}), \\ \forall j \in \{C' \backslash \{i\}\} \wedge c_j(C) \leq c_j(C \backslash \{i\}), \forall j \in \{C \backslash \{i\}\} \quad (5)$$

In words, with this definition, any UE i prefers being a member of coalition C over C' if it obtains a lower individual cost $c_i(C)$, without causing an increase in the cost for any other player in C and C' (also known as *Pareto order* preference). The so-defined individual preference order is adopted for two simple rules for the feasible coalition formation game.

Definition 1 (Merge rule). *Merge any pair of coalitions C and C' in a unique feasible coalition $\{C \bigcup C'\} \Leftrightarrow [(\exists k \in C \ s.t. \ \{C \bigcup C'\} \succ_k C) \vee (\exists k \in C' \ s.t. \ \{C \bigcup C'\} \succ_k C')] \wedge \{C \bigcup C'\}$ is feasible.*

Definition 2 (Split Rule). *Split any coalition $\{C \bigcup C'\}$ in feasible coalitions $\{C, C'\} \Leftrightarrow [(\exists i \in C \ s.t. \ C \succ_i \{C \bigcup C'\}) \vee (\exists j \in C' \ s.t. \ C' \succ_j \{C \bigcup C'\})] \wedge \{C, C'\}$ are feasible.*

The merge rule implies that two coalitions join to form a larger *feasible coalition* if operating all together strictly improves the cost for at least one player while all the other involved players are not having a higher cost. The split rule implies that a coalition splits only if there exists at least one player that obtains a lower cost, under the constraint that this has no negative effect on the cost of other players and the resulting coalitions are both *feasible*.

Once the merge-and-split operations are defined, then the CCF game for the cooperative multihop D2D data uploading can be modeled. The objective of a UE is to find a coalition with the lowest uploading time through an iterative application of the merge and the split rules. By starting from an initial partition $\Pi^{ini}(N) = \mathcal{N} = \{p_1, p_2, \ldots, p_N\}$, the eNodeB iteratively applies the merge-and-split rules to any pair of coalitions in the partition. In particular, by first considering the merge rule, for every pair of coalitions if the merged coalition is preferred w.r.t. the separated coalitions, then a new merged coalition is considered for the partition. The merging stops when no couple of coalitions exists in the current partition $\Pi^{cur}(N)$ that can be merged. Thus, the split rule is applied to every coalition in the partition.When no split occurs, the algorithm considers again the merging function. The algorithm terminates when no merging or splitting occurred in the last iteration. In this case, the final resulting partition $\Pi^{fin}(N)$ will be adopted by the eNodeB. It can be demonstrated (proof not shown due to length constraints) that the proposed coalition formation algorithm converges to a partition of disjoint coalitions of UEs that is Nash-stable. A partition $\Pi(N)$ is said Nash-stable if no player i has an incentive to move from its current coalition in the partition to join a different coalition of $\Pi(N)$ or to act in a non-cooperative way.

4.1. Content uploading time model

Let $\mathcal{N}$ be the set of UEs in the coalition and let each UE $i \in \mathcal{N}$ have some content of size $b_i \neq 0$ to upload and r_i^c be the data rate for user i when transmitting in traditional cellular-mode (i.e., directly to the eNodeB). The "virtual" radio resources for the UEs in the coalition are all allocated to the gateway. This implies having more resources available and achieving a consequent improved uplink data rate $r_i^{c'}$ for the gateway-eNodeB link. For the sake of notation simplicity, let us consider an N-hops D2D coalition with $i = 1$ being the gateway and $i = N$ be the last UE in the multi-hop coalition. Then, let r_i^d be the data rate for UE i on the D2D link that it uses to forward its data to the next UE.

The detailed modeling of the uploading time for all UEs in a multihop D2D coalition is derived from the analysis conducted in a previous paper of ours [9]. For completeness in the presentation we report here the main findings. To model the uploading time the channel occupation time for a generic UE i in the D2D coalition is computed as the time spent by the UE to transmit to the next hop its own data and the data received from the previous UE (or multiple UEs) in the coalition. Let us consider UE N as the last UE in the coalition. This UE will occupy the channel for a time $T_N = b_N/r_N^d$ to forward its data b_N to UE $N-1$ over the D2D link having data rate r_N^d. Considering UE $N-1$, it will send its own data b_{N-1} and the data received from the previous UE b_N and occupy the channel for the time $T_{N-1} = b_{N-1}/r_{N-1}^d + \left(b_N/r_N^d + b_N/r_{N-1}^d\right)$. By repeating this reasoning for all UEs in a coalition, and considering that the gateway, UE 1, transmits to the eNodeB with a data rate $r_1^{c'}$, the channel occupation time for UE 1 to upload all data from the coalition to the eNodeB is computed as a function of the number of UEs in the topology:

$$T_1(N) = \frac{b_1}{r_1^{c'}} + \ldots + \left(\frac{b_N}{r_N^d} + \frac{b_N}{r_{N-1}^d} + \ldots + \frac{b_N}{r_1^{c'}}\right) = \sum_{i=1}^{N}\left(\frac{b_i}{r_1^{c'}} + \sum_{j=2}^{i}\frac{b_i}{r_j^d}\right) \tag{6}$$

The formulation can be generalized to represent the channel occupation time for any UE $n = \{1, \ldots, N\}$ in the multi-hop coalition. This time includes the time to forward to the next hop in the chain all data generated by UEs n and the data from its previous UEs in the chain (until the last UE N) and can be written as follows:

$$T_n(N) = \begin{cases} \sum\limits_{i=n}^{N}\left(\frac{b_i}{r_1^{c'}} + \sum\limits_{j=2}^{i}\frac{b_i}{r_j^d}\right) & n = 1 \\ \sum\limits_{i=n}^{N}\sum\limits_{j=n}^{i}\frac{b_i}{r_j^d} & n > 1 \end{cases} \tag{7}$$

The content uploading time to the eNodeB for a coalition is given by the number of data frames needed, under the constraints posed by the data rate over the involved communication links and the communication assumptions in the topology. This corresponds to the cost $c(N)$ associated to the corresponding coalition in the game theoretic model. Moreover, this time is determined by the

data frame organization where, given the UE half-duplex operation, the uplink sub-frames will be used either for D2D communications or for transmissions towards the eNodeB (the interested reader can find more details on the model in [9]). Moreover, the transmitting UEs will use either the same or separate RBs, according to the interference level experienced on each link.

The content uploading time has also a direct impact on the UEs' energy consumption, which is defined, as in the non-cooperative case, as: $E_i^c(b_i) = (P_{tx}^c + P_0) \cdot \frac{b_i}{r_i^c}$, where P_{tx}^c is the transmission power and P_0 the circuit power. When considering the cooperative data uploading, we have three cases: (1) the UE is the gateway; it consumes energy in receiving data from the second UE and in transmitting data to the eNodeB; (2) the UE is the last UE in the chain; it only consumes energy in transmitting its own data to the next UE in the D2D chain; (3) the UE is an intermediate UE in the chain; it consumes energy to receive data from the previous UE and to transmit data to the next UE in the chain. In all three cases, energy is also spent during the idle times on the channel. However, according to [22] the power consumption in idle times is as low as $-50dbm$; therefore, this contribution can be neglected and only the transmitting and receiving power on the D2D links, P_{tx}^d and P_{rx}^d, are considered. The energy consumption for a generic UE i in the D2D chain will be the sum of the energy spent for transmission and for reception: $E_i(N) = Etx_i^d(N) + Erx_i^d(N)$.

$$
\begin{aligned}
Etx_i^d(N) &= \begin{cases} (P_{tx}^c + P_0) \sum_{j=1}^{N} \frac{b_j}{r_1^{c'}} & i = 1 \\ (P_{tx}^d + P_0) \sum_{j=i}^{N} \frac{b_j}{r_i^d} & 1 < i \leq N \end{cases} \\
Erx_i^d(N) &= \begin{cases} (P_{rx}^d + P_0) \sum_{j=i+1}^{N} \frac{b_j}{r_{i+1}^d} & 1 \leq i < N \\ 0 & i = N \end{cases}
\end{aligned} \tag{8}
$$

5. Performance evaluation

In this section we evaluate the performance of the proposed solution for Social Cyber Physical Systems and its ability to cope with malicious nodes. The assessment campaign is conducted by following the system model guidelines in [16]. The main simulation parameters are listed in Table 2. A single cell with available radio resources $RB = 50$ is considered, wherein up to 20 UEs are uniformly distributed. The radio resources that can be used on a single D2D link of the multihop topology depend on the frequency reuse efficiency and we assume, without losing generality, that all radio resources can be reused on the D2D links. We consider that 30% of the UEs are malicious, which means they drop all the incoming data from the upstreams in the cooperating topology. We compare our *trust-based* proposal with a so-called *basic* solution where the coalition formation game completely disregards the trustworthiness analysis.

Table 2: Main Simulation Parameters

Parameter	Value
Cell radius	500 m
Maximum D2D link coverage	100 m
Frame Structure	Type 2 (TDD)
TTI	1 ms
TDD configuration	0
Carrier Frequency	2.1 GHz
Cellular transmission power consumption	23 dBm
D2D power consumption	-19 dBm
CQI-MCS mapping for D2D links	[23]
Noise power	-174 dBm/Hz
Cellular link model	Rayleigh fading channel
D2D link model	Rician fading channel [24]
Path loss (cell link)	128.1 + 37.6 log(d), d[km]
Path loss (D2D link, NLOS)	40 log(d) + 30 log(f) + 49, d[km], f[Hz]
Path loss (D2D link, LOS)	16.9 log(d) + 20 log (f/5) + 46.8, d[m], f[GHz]
Shadowing standard deviation	10 dB (cell mode); 12 dB (D2D mode)
Content size	50 MB
Weighting factors $\alpha = \beta$	0.5
# Malicious nodes	30% of UEs
Simulation time	100 s
# of Runs	500

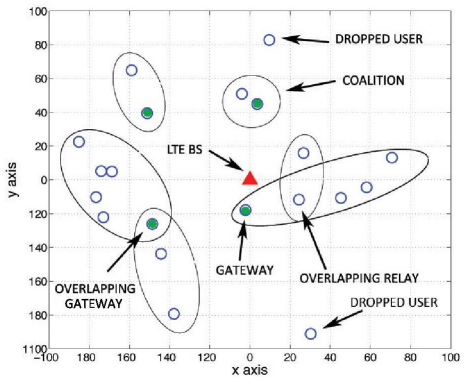


Figure 2: Example of coalitions being formed: 20 UEs, 50MB of data size, MT resource allocation policy.

The performance parameters we focus on are: (i) *data losses*, (ii) *average data uploading time gain*, and (iii) *average energy consumption gain*. In particular, the latter two parameters represent the gain achieved by the cooperative upload w.r.t. a pure cellular upload modality. The analysis also evaluates the effects of the radio resource allocation policy implemented by the eNodeB, considering either a *maximum throughput (MT)* or a *proportional fair (PF)* scheduler.

Before illustrating the performance results, in Fig. 2 we show an example of coalitions formed by applying the proposed scheme with 20 UEs uniformly deployed within the LTE cell (MT scheduler is adopted and the packet size is set to 50MB). As we can observe, two users are dropped by the packet scheduler, whereas the remaining UEs are grouped in coalitions. The UEs highlighted in green represent the gateway nodes appointed to upload the data from the UEs belonging to the respective coalitions. In addition, we observe that there are two overlapping coalitions sharing an overlapping relay and an overlapping gateway.

The first analysis shows the impact of the feasibility threshold in the coalition formation process in a study case with 20 UEs. In particular, we consider three different values for the FT parameter, which, we recall, gives the minimum level of trust required for each D2D link within a coalition. As we can observe from Fig. 3, the data loss strongly depends on this value since for higher FT values the proposed solution is able to better filter out the malicious nodes in the network coalition. Noteworthy, in all cases our solution outperforms the basic solution. In particular, with a threshold equal to 0.6 we achieve a reduction of 45% and 34% w.r.t. the basic approach for the PF and MT schedulers respectively. This improvement reaches up to 86% and 68% if the FT value is set to 0.8.

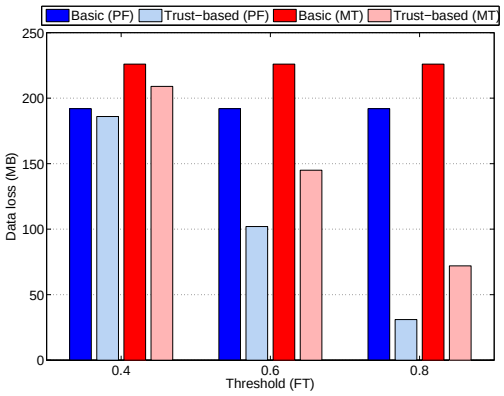
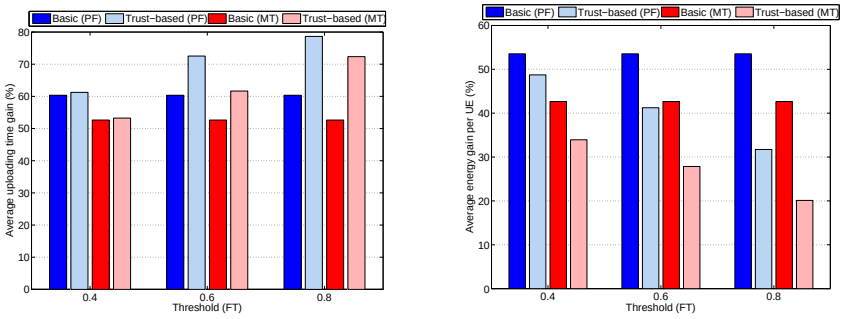


Figure 3: Data loss in scenarios with 20 UEs.

In 4(a), instead, results in terms of content uploading time are reported. For this parameter as well, the gain for the device in using the mobile networking in proximity paradigm w.r.t. to the cellular mode data uploading is higher for the proposed social-based trusted solution. In particular, compared to the basic

solution this gain is up to 18% higher in the best case (FT=0.8). The motivation of this result is that when malicious nodes are involved in a coalition, all the users within the coalition achieve an uploading time gain that is equal to zero since no data are uploaded to the eNodeB. Considering our trust-based approach, instead, users tend to form coalition only among trusted users increasing the probability for the content to successfully reach the eNodeB.

When considering the average energy consumption gain for the nodes in the scenario, we observe in Fig. 4(b) that the trust-based solution actually has lower energy savings w.r.t. to the basic solution. This result should not surprise since, with the trust-based solution, the malicious nodes are isolated and need to upload their content using more energy demanding unicast transmissions towards the eNodeB. As a consequence, the positive effects of adopting low power D2D communications among the nodes is limited to the set of nodes.



(a) Content uploading time.

(b) Energy consumption.

Figure 4: Average gains in multihop content uploading (20 UEs).

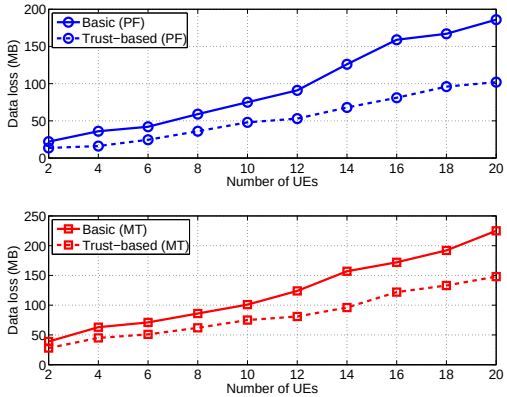
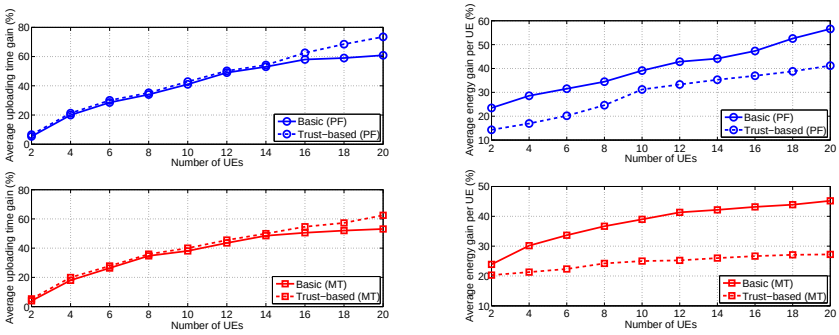


Figure 5: Data loss by varying the number of UEs.

5.1. Analysis by varying the number of UEs

The next analysis shows the results by varying the number of UEs in the range of $[2 - 20]$, when setting the FT parameter to a sample value of 0.6. When considering the data loss parameter, in Fig. 5 we can observe that the gap between the basic and the trust-based solution increases linearly with the number of UEs for both the considered schedulers.

When considering the average uploading gain achieved by the users, the trust-bases solution overcomes the basic solution in all cases. As plotted in Fig. 6(a), the gain increment with the proposed solution considering the PF and MT scheduler is equal to 15% and 8% respectively for 20 UEs. Finally, the energy consumption gain results plotted in Fig. 6(b) confirm the trend already observed in Fig. 4(b). In fact, the trust-based solution experiences lower energy consumption gains when the number of UEs is high. The motivation again is that the malicious nodes are isolated and work with the energy demanding cellular mode uploading lowering the benefits of low power D2D communications in the coalitions.



(a) Content uploading time. (b) Energy consumption.

Figure 6: Average gains in multihop content uploading with varying number of UEs.

6. Conclusions

In this paper a novel trust-based solution has been proposed to model effective cooperative content uploading in cellular environments based on D2D proximity communications. Social-awareness for the devices has been considered to evaluate the reliability for the nodes and to suitably weight the recommendations exchange for the reputation definition. A constrained coalition formation game has been studied where both coverage constraints and trust constraints are considered. This allowed to implement a cooperative and opportunistic hop-by-hop forwarding exploiting low energy consuming and high data rate D2D links and at the same time to filter out malicious nodes in the network. The cooperating devices are assumed to be rational self-interested players aiming at maximizing their uploading time gain w.r.t. cellular mode transmissions.

A simulative analysis validated the proposed solution in a variety of scenarios showing how the social based trusted solution guarantees higher gains in the content uploading time and has the ability to increase the amount of successful cooperative interactions reducing the amount of data losses in the network.

References

[1] D. Soldani, A. Manzalini, Horizon 2020 and beyond: On the 5g operating system for a true digital society, Vehicular Technology Magazine, IEEE 10 (1) (2015) 32–42.

[2] F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta, P. Popovski, Five disruptive technology directions for 5g, Communications Magazine, IEEE 52 (2) (2014) 74–80.

[3] L. Lei, Z. Zhong, C. Lin, X. Shen, Operator controlled device-to-device communications in LTE-advanced networks, IEEE Wireless Communications 19 (3) (2012) 96–104.

[4] S. Mumtaz, L.-L. Yang, C. Wang, F. Adachi, N. Ali, Smart-device-to-smart-device communications, Communications Magazine, IEEE 52 (4) (2014) 18–19.

[5] F. Rango, A. Socievole, S. Marano, Exploiting online and offline activity-based metrics for opportunistic forwarding, Wireless Networks 21 (4) (2015) 1163–1179. doi:10.1007/s11276-014-0842-7.

[6] H. Nishiyama, M. Ito, N. Kato, Relay-by-smartphone: realizing multihop device-to-device communications, Communications Magazine, IEEE 52 (4) (2014) 56–65.

[7] Y. Wang, A. V. Vasilakos, Q. Jin, J. Ma, Survey on mobile social networking in proximity (msnp): approaches, challenges and architecture, Wireless networks 20 (6) (2014) 1295–1311.

[8] V. Nurmela, P. Kyosti, A spatially consistent radio channel model enabling dual mobility, in: Vehicular Technology Conference (VTC Fall), 2014 IEEE 80th, IEEE, 2014, pp. 1–5.

[9] L. Militano, A. Orsino, G. Araniti, A. Molinaro, A. Iera, A constrained coalition formation game for multihop d2d content uploading, Wireless Communications, IEEE Transactions on PP (99) (2015) 1–1.

[10] Z. Yan, P. Zhang, A. V. Vasilakos, A survey on trust management for internet of things, Journal of network and computer applications 42 (2014) 120–134.

[11] S. Sicari, A. Rizzardi, L. Grieco, A. Coen-Porisini, Security, privacy and trust in internet of things: The road ahead, Computer Networks 76 (2015) 146–164.

[12] L. Atzori, A. Iera, G. Morabito, M. Nitti, The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization, Computer Networks 56 (16) (2012) 3594–3608.

[13] M. Nitti, R. Girau, L. Atzori, Trustworthiness Management in the Social Internet of Things, IEEE Transactions on Knowledge and Data Engineering 26 (5) (2014) 1253–1266.

[14] Y. Li, D. Jin, J. Yuan, Z. Han, Coalitional games for resource allocation in the device-to-device uplink underlaying cellular networks, Wireless Communications, IEEE Transactions on 13 (7) (2014) 3965–3977.

[15] 3GPP, TS 36.300, Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN), Rel. 11, Tech. rep. (Sep. 2012).

[16] 3GPP, TS 36.213 Evolved Universal Terrestrial Radio Access (E-UTRA): Physical layer procedures, Rel. 11, Tech. rep. (Dec. 2012).

[17] M. Feldman, J. Chuang, Overcoming free-riding behavior in peer-to-peer systems, ACM SIGecom Exchanges 5 (4) (2005) 41–50.

[18] H. Li, M. Singhal, Trust management in distributed systems, Computer (2) (2007) 45–53.

[19] T. Grandison, M. Sloman, Trust management tools for internet applications, in: Trust Management, Springer, 2003, pp. 91–107.

[20] G. Zacharia, P. Maes, Trust management through reputation mechanisms, Applied Artificial Intelligence 14 (9) (2000) 881–907.

[21] X. Lu, P. Wang, D. Niyato, A layered coalitional game framework of wireless relay network, Vehicular Technology, IEEE Transactions on 63 (1) (2014) 472–478. doi:10.1109/TVT.2013.2274533.

[22] 3GPP, TS 36.101, LTE Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception, Rel. 10, Tech. rep. (Jun. 2011).

[23] M. Iturralde, T. Yahiya, A. Wei, A.Beylot, Interference mitigation by dynamic self-power control in femtocell scenarios in LTE networks, IEEE GLOBECOM (2012) 4810–4815.

[24] M. Lin, J. Ouyang, W. Zhu, Joint beamforming and power control for device-to-device communications underlaying cellular networks, Selected Areas in Communications, IEEE Journal on.

Authors' Biographies

Leonardo Militano is currently an Assistant Professor at the Mediterranea University of Reggio Calabria, Italy. He received his M.Sc. degree in Telecommunications Engineering in 2006 and his Ph.D in Telecommunications Engineering in 2010 from the University of Reggio Calabria. He has been a visiting Ph.D student at the Mobile Device group at University of Aalborg, Denmark. His major areas of research are wireless networks optimization, user and network cooperation, device-to-device communications and game theory.

Antonino Orsino received his B.Sc. degrees in Telecommunication Engineering from University Mediterranea of Reggio Calabria, Italy, in 2009 and his M.Sc. from University of Padova, Italy, in 2012. Currently, he is a Ph.D. student at the DIIES Department, University Mediterranea of Reggio Calabria. His current research interests include Device-to-Device and Machine-to-Machine communications in 4G/5G cellular systems. He has served as a reviewer for several major IEEE conferences and journals.

Giuseppe Araniti is an Assistant Professor of Telecommunications at the University Mediterranea of Reggio Calabria, Italy. From the same University he received the Laurea (2000) and the Ph.D. degree (2004) in Electronic Engineering. His major area of research includes personal communications systems, enhanced wireless and satellite systems, traffic and radio resource management, multicast and broadcast services, device-to-device (D2D) and machine-type communications (M2M/MTC) over 5G cellular networks. He is a senior member of IEEE.

Michele Nitti is an assistant professor in the Department of Electrical and Electronic Engineering at the University of Cagliari, Italy. His research interests include the Internet of Things, particularly the creation of a network infrastructure to allow the objects to organize themselves according to a social structure. Nitti has a PhD in electronic and computer engineering from University of Cagliari, Italy.

Luigi Atzori LUIGI ATZORI is an associate professor in the Department of Electrical and Electronic Engineering at the University of Cagliari, Italy. His research interests include multimedia communications and computer networking (wireless and wireline), with emphasis on multimedia quality of experience (QoE), multimedia streaming, Next Generation Network service management, service management in wireless sensor networks, and architecture and services in the Internet of Things. Atzori has a PhD in electronic and computer engineering from University of Cagliari, Italy. He's a senior member of IEEE.

Antonio Iera graduated in Computer Engineering at the University of Calabria, Italy, in 1991 and received a Master Diploma in Information Technology from CEFRIEL/Politecnico di Milano, Italy, in 1992 and a Ph.D. degree from the University of Calabria in 1996. Since 1997 he has been with the University of Reggio Calabria and currently holds the position of full professor of Telecommunications and Director of the Laboratory for Advanced Research into Telecommunication Systems (www.arts.unirc.it). IEEE Senior Member since 2007. His research interests include, next generation mobile and wireless systems, RFID systems, and Internet of Things.

***Author Photo**

Authors' Photos