future internet

MDPI

Article

NB-IoT for D2D-Enhanced Content Uploading with Social Trustworthiness in 5G Systems †

Leonardo Militano [1], Antonino Orsino [2,*], Giuseppe Araniti [1,3] and Antonio Iera [1]

1 DIIES Deparment, University "Mediterranea" of Reggio Calabria, Reggio Calabria 89100, Italy; leonardo.militano@unirc.it (L.M.); araniti@unirc.it (G.A.); antonio.iera@unirc.it (A.I.)
2 ELT Deparment, Tampere University of Technology, Tampere 33720, Finland
3 API Deparment, Peoples' Friendship University of Russia (RUDN University), Moscow 101000, Russia
* Correspondence: antonino.orsino@tut.fi; Tel.: +358-44-299-2908
† Militano, L.; Orsino, A.; Araniti, G.; Nitti, M.; Atzori, L.; Iera, A. Trusted D2D-based data uploading in in-band narrowband-IoT with social awareness. In Proceedings of the IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Valencia, Spain, 2016; pp. 1–6.

Academic Editor: Boon-Chong Seet
Received: 14 June 2017; Accepted: 6 July 2017; Published: 8 July 2017

Abstract: Future fifth-generation (5G) cellular systems are set to give a strong boost to the large-scale deployment of Internet of things (IoT). In the view of a future converged 5G-IoT infrastructure, cellular IoT solutions such as narrowband IoT (NB-IoT) and device-to-device (D2D) communications are key technologies for supporting IoT scenarios and applications. However, some open issues still need careful investigation. An example is the risk of threats to privacy and security when IoT mobile services rely on D2D communications. To guarantee efficient and secure connections to IoT services involving exchange of sensitive data, reputation-based mechanisms to identify and avoid *malicious* devices are fast gaining ground. In order to tackle the presence of malicious nodes in the network, this paper introduces *reliability* and *reputation* notions to model the level of *trust* among devices engaged in an opportunistic hop-by-hop D2D-based content uploading scheme. To this end, *social awareness* of devices is considered as a means to enhance the identification of trustworthy nodes. A performance evaluation study shows that the negative effects due to malicious nodes can be drastically reduced by adopting the proposed solution. The performance metrics that proved to benefit from the proposed solution are data loss, energy consumption, and content uploading time.

Keywords: trustworthiness; D2D communications; 5G systems; Internet of things; NB-IoT

1. Introduction

The expected drastic increase in Internet of things (IoT) connected devices will definitely produce huge demands for data transmission over wireless systems. At the same time, a plethora of new IoT use cases are emerging across the domains of intelligent transportation systems, smart grid automation, remote health care, smart metering, industrial automation and control, remote manufacturing, and public safety surveillance, among others [1]. Most IoT devices operate through their virtual representations within a digital overlay information system, built over the physical world. Therefore, the majority of current IoT solutions rely on cloud services, leveraging on their virtually unlimited capabilities to effectively exploit the potential of massive tiny sensors and actuators towards the so-called cloud of things. Given the complexity and the challenging requirements of future IoT ecosystems, experts in the field share the opinion that the upcoming fifth generation (5G) cellular systems will represent a strong boost for actual IoT deployment [2]. This vision is sustained by the fervent activities, aimed at designing IoT-oriented 5G wireless systems, conducted by academic, industrial, and standardization bodies [3,4], worldwide. Several types of interactions

may coexist within an IoT ecosystem, including machine-to-machine (M2M), machine-to-human, human-to-machine, and machine-to-cloud interactions. All require ubiquitous connectivity. For this purpose, device-to-device (D2D) communications appears as a promising paradigm to support the interconnection of heterogeneous objects [5].

Short-range D2D cooperation among devices may introduce benefits in terms of improved spectrum utilization, higher throughput, and lower energy consumption, which is important for constrained IoT devices. However, there are still several open issues that need to be solved in order to achieve a seamless, effective, and reliable deployment of proximity-based communications for IoT systems [6,7].

For an effective implementation of proximity communications, one of the most important challenges is to understand how the node-originated information shall be processed so as to build a reliable system on the basis of the objects' behavior, namely the need for *trustworthiness* [8]. Indeed, in realistic scenarios, where human interactions and human behavior are also to be considered, the presence of *malicious* nodes in the network is a constant threat for successful cooperation. Accordingly, without effective trust management foundations, attacks and malfunctions are likely to outweigh any possible cooperation benefits [8].

For the reference scenario in this paper, we consider that groups of devices in close proximity are willing to upload contents to the Cloud or to a central server and end users may not be aware of whom they are going to forward the data to. Typical sample scenarios are small-scale crowded environments (e.g., stadiums, university campuses, music theaters, or fairs) where devices can exploit opportunistic data forwarding over other devices in proximity. In these contexts, malicious nodes may decide to drop the data packets they are expected to forward or even modify the data packets before forwarding the corrupted content. To cope with these threats, *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, in this paper we consider the sociality level of the devices to model the *reliability* of the communication. The historical *reputation* of the cooperative users will be considered to offer rational users the possibility to filter out untrusted users and avoid unsuccessful opportunistic hop-by-hop D2D interactions. An initial investigation in this direction was made in our previous paper [9] in long-term evolution-advanced (LTE-A) scenarios where multihop cooperative uploading is implemented over cellular D2D resources [10]. In this paper we take forward our research, investigating among other issues the use of the recent narrowband IoT (NB-IoT) standard [11], which is currently considered the reference cellular technology for IoT communications for the next 5G systems. The *trust* constraints for successful D2D-based content uploading are modeled by including sociality among devices, as a measure of *reliability*, and historical *reputation*. The objective is to define multihop D2D topologies that meet the constraints of reciprocal user equipment (UE) proximity for the direct links activation and, at the same time, of an adequate *trust* level among the cooperating devices. Through simulation-based performance evaluations, we show that it is possible to significantly reduce the impact of malicious behaviors on the performance of involved devices, with gains in terms of data loss, energy consumption, and data uploading time.

The remainder of the paper is organized as follows: Section 2 reviews the related work; Section 3 introduces the research background and motivation; the algorithmic solution for the definition of trusted D2D cooperative topologies is given in Section 4; a detailed description of the proposed trust model and the sociality concepts is given in Section 5; and numerical results and conclusions are provided in Section 6 and Section 7, respectively.

2. Related Work

Security is one of the key issues for an effective and widespread adoption of D2D communications [12] in IoT scenarios [13]. This is particularly relevant in a cooperative context such as the one studied in this paper, where the multihop D2D data forwarding paradigm is based on the assumption that the involved devices behave in a trusted and secure way [14]. Unfortunately, this is not

always the case as *malicious* nodes may be active in the network by either dropping or manipulating the data to be forwarded.

Generally, trust is defined as the quantified belief of a truster with respect to the competence, honesty, security and dependability of a trustee within a specified context [15]. 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 D2D multihop scenario, the node acting as relay/gateway towards another node will be the trustee and the source node of the relayed data is the truster. The cooperative topology formation exploits a game theoretic coalition formation model as proposed in [10]. Game theoretic approaches have found several applications also in the field of D2D communications given the potential to model the user behavior (see e.g., [16,17]). The trustworthiness of the truster with respect to the trustee can be determined by 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 other actors in the community have about the trustee.

In the literature, several trust models have been proposed to represent both reliability and reputation [15]. A way to reach trustworthiness in communication is to exploit sociality among devices [9,18]. 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). Socially-aware D2D communications have attracted high interest in recent research activity, such as for instance in [19–22]. With respect to the works in the literature, we consider the potential of the SIoT model defined in [23], to embrace the social networking concepts and build trustworthy relationships among devices [24,25]. In particular, mobility patterns and relevant context can be considered to configure the appropriate forms of socialization among the UE. 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.

3. NB-IoT and D2D Communications in the 5G Era

The upcoming fifth generation (5G) wireless systems are being considered as the best candidate to allow effective interworking of IoT devices, thanks to the benefits these offer in terms of enhanced coverage, high data rate, low latency, low cost per bit, and high spectrum efficiency. There is a general consensus among academia and industries that 5G will have a huge impact in three main areas of communication: (1) enhanced mobile broadband (eMBB); (2) massive-machine type communication (M-MTC); and (3) critical-MTC (c-MTC). In particular, these three areas have different requirements and applications. Nevertheless, those are not standalone use cases, but may overlap in some cases. In our work, we take into consideration a use case that is somehow in the middle between c-MTC and M-MTC. We may think of process automation within a factory or other similar scenarios. In these cases, available and reliable connections for monitoring and diagnosis of a high number of industrial elements (i.e., M-MTC) are the most important. Nevertheless, even if the measured values from the sensors change relatively slowly, it is still important to have reasonable latency (e.g., from 20 to 50 ms) in order to react in a timely manner to an issue that can occur on the way (e.g., c-MTC).

With reference to typical machine-type communications (MTC), the Third Generation Partnership Project (3GPP) has introduced novel features [26] that better support the intrinsic battery-constrained capabilities of IoT devices and the typical small data packets over licensed bands (e.g., LTE). In September 2015, 3GPP standardized *narrowband IoT (NB-IOT)*, a new narrowband radio technology

to address the requirements of the Internet of things (IoT). This new technology provides improved indoor coverage, support of massive number of low throughput devices, has low delay sensitivity, ultra-low device cost, low device power consumption and an optimized network architecture.

At the time we are writing this paper, a first release of NB-IoT had been completed by 3GPP. However, the standardization process is still ongoing and further enhancements and new features are expected in 3GPP Release 14 (updated according to the last 3GPP meetings) and Release 15. Further, NB-IoT is expected to be released in a form of a software update for the network operators and is fully backward compatible with existing 3GPP devices and infrastructure. In particular, given an available bandwidth of around 200 kHz for both downlink and uplink, the air interface of NB-IoT is optimized to ensure harmonious coexistence with LTE. In particular, the technology can be deployed "in-band" using the resource blocks within a normal LTE carrier (an LTE operator can deploy NB-IoT inside an LTE carrier by allocating one of the physical resource blocks (PRB) of 180 kHz to NB-IoT), or in the unused resource blocks within a LTE carrier guard-band (for instance, for an LTE bandwidth of 10 MHz (i.e., 56 resource blocks—RBs), 6 RBs are reserved for guard subcarriers and can be used for NB-IoT), or in "standalone" manner for deployments in dedicated spectrum [27]. Thanks to this latter feature whereby NB-IoT may be deployed as a stand-alone carrier using any available spectrum exceeding 180 kHz, a Global System for Mobile Communications (GSM) operator can also replace a GSM carrier (200 kHz) with NB-IoT. As reported in the white paper from Nokia [11], the maximum data rates (i.e., by considering the overall bandwidth) in terms of instantaneous peak rates provided by the NB-IoT technology are: *170 kbps (Downlink – DL)* and *250 kbps (Uplink – UL)*. To enable the allocation of small portions of bandwidth, NB-IoT uses tones or subcarriers instead of resource blocks. The subcarrier bandwidth for NB-IoT is 15 kHz (or 3.75 kHz in some cases), compared with a resource block, which has an effective bandwidth of 180 kHz. Furthermore, the data rates available for the single tone in downlink and uplink are 680 bits and 1000 bits, respectively. These values will satisfy most of the communication requirements for IoT-based services where very small data packets are usually transferred.

Another form of technology which has gained high momentum in the evolution towards 5G systems is D2D communication where devices communicate directly over cellular resources or Wi-Fi/Bluetooth technologies without routing the data over a base station (BS) or an access point (AP). Recent studies showed how D2D communications may find important applications in IoT/5G integration [6,7]. Indeed, D2D communications not only allow for extending the coverage and overcoming the limitations of conventional cellular systems, but they represent a fertile ground for use cases and services (e.g., social interactions and gaming, local information exchange, etc.). For instance two users can find each other whenever in proximity and share data or play interactive games. Moreover, social applications, public safety and emergency handling may benefit from D2D communications as devices can provide local connectivity in case of damage to the network infrastructure. Other fields of applications may be vehicle-to-vehicle (V2V) communication in intelligent traffic systems (ITS) where D2D communications can be exploited for traffic control/safety applications among others.

Several works in the recent literature have investigated the benefits D2D communications can introduce, making it a very appealing solution for the exacting requirements of IoT emerging 5G network scenarios [28,29]. The most important of these benefits are [30]: (1) higher data rate in the communications; (2) reliability in the communications including in the case of network failure; (3) energy savings due to lower transmission power levels for devices in proximity; (4) reduced number of cellular connections (known as traffic offloading); and (5) possibility for instantaneous communications between devices.

In this paper, the potential benefits of NB-IoT and D2D communications are jointly exploited for cooperative content uploading from a set of devices to the cellular base station, through short-range multihop relaying. In particular, NB-IoT is exploited for radio links between users and the eNodeB, whereas proximity-based transmissions (i.e., D2D) are established among devices in mutual proximity.

However, 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 channels is higher than the one of the separate links to the Internet. 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, as is the case of the Internet of vehicles, an instance of the IoT where objects are represented by cars [31]. The content we have in mind for the devices in the scenario is small data coming for instance from sensing activities, security or monitoring applications with limited amount of data to transmit, typical of IoT applications. NB-IoT is, in fact, not thought of for bandwidth-hungry applications, e.g., videos, or big file transmissions. Currently IoT devices are equipped with a wide range of radio technologies. For instance, Pycom (https://www.pycom.io/) provides some shields for IoT applications that include both long- and short-range connectivity such as LoRa, LTE, NB-IoT, Bluetooth, and LTE Cat-M1. The idea we want to investigate is to offload the part of the traffic that cannot be handled entirely by NB-IoT via short-range links over the D2D technology.

4. Cooperative Multihop D2D-Based Data Uploading

We consider a single LTE-A cell with multiple devices interested in uploading their content to the Internet by adopting an *in-band NB-IOT* solution. Data uploading according to the traditional *cellular-mode* is performed through the activation of separate links from each device to the eNodeB. The alternative solution proposed in this paper is the cooperative content uploading controlled by the eNodeB (i.e., network-assisted D2D), where the UE organizes itself to form a "logical multihop D2D topology" and cooperates in uploading the content generated by *all* the involved devices. The cooperative topology formation is implemented according to a game theoretic coalition formation model as proposed in [10].

In the formed cooperative topology, the user equipment (UE) located farther from the base station relays its content to nearby UE and only the UE playing the head-end role in the topology, the so-called *gateway*, is in charge of uploading all the contents received from the rest of the UE to the eNodeB. The UE with the best link quality in the coalition is chosen as the gateway and may receive (if needed) all the radio resources that would have been separately allocated by the eNodeB to the UE in the coalition. Of course, since NB-IoT technology is used, in this case the radio resources are "tones" rather than the classic definition of resource blocks (RBs). For example, a channel bandwidth of 20 Mhz corresponds to 100 RB of LTE-A. The RB corresponds to the smallest time frequency resource that can be allocated to a user (12 sub-carriers) in LTE. The intermediate UE in the topology also acts as *relays* for the contents received from the upstream UE. In doing this, they benefit from the higher quality of the short D2D links with respect to the direct cellular link. In the most general configuration, each relay has one or more links active to receive data from the preceding sources in the 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 UE in the topology. In particular, the transmission starts only after the generic UE has received the whole content (in other words, UE uses the decode-and-forward relaying protocol).

We remark that all the transmission between one single device towards the eNodeB exploits the NB-IoT tones, whereas D2D links are activated over the legacy LTE spectrum (thus using RBs instead of tones). The motivation of this choice is driven by the fact that NB-IoT does not yet support proximity-based transmission even if this feature is actually been discussing during the 3GPP Release 15 standardization.

In realistic scenarios, end-users may not be aware of whom they are going to be connected to and *malicious* devices may decide to either modify the received content before forwarding a corrupted packet or drop data packets they are expected to forward without informing the interested users.

In the remainder of the paper we will refer to these two different types of malicious nodes as *type A* and *type B*, respectively. Whenever a malicious node in the coalition either modifies or drops the data packets, we assume that the source node will be informed by the eNodeB and will perform standard data uploading. This will introduce both a delay in the data delivery and an increase in the energy consumption for the involved nodes. However, there is a difference, since the effect of a *type B* malicious node is identified earlier than the effect of a *type A* (note that type A malicious nodes are present only when unencrypted payloads are delivered) node. In fact, if a timeout is enough to identify a packet dropping, a corrupted packet will first have to reach the eNodeB passing through all the intermediate nodes before the system is aware of data corruption (we assume the eNodeB will be able to identify data corruption).

We imagine a possible way for the eNodeB (eNB) to detect a packet to be dropped (when a *type B* malicious node is present). A straightforward solution is to rely on the acknowledgment message (ACK) that has to be sent to the UE once the packet has been received by the network. In this case, once the UE reaches the maximum number of re-transmitted Protocal Data Units (PDUs), a radio link failure (RLF) is triggered and sent over the signal radio bearers (SRBs). Since in our work we assume that malicious nodes of type B drop the packets, we think that the best way to proceed is for the eNB to send the ACKs directly to each UE of the chain. Then, if a RLF is experienced (due to no ACK being received, i.e., the gateway does not forward anything), this is triggered separately by each UE towards the eNB. The identification of a corrupted packet is a bit more complex. This may be done through the checksum of the packets (i.e., at the higher layer of the protocol stack) or, alternatively, through the integrity protection that at the moment is done for the SRBs. We are aware that integrity protection is not present for the data radio bearer (DRBs), but with the ongoing standardization of 5G New Radio (NR) and LTE Evolution (LTE-Evo) we may expect this kind of enhancements or new features. Other solutions may be applied for detecting a not correct node behavior, but this is out of the scope of this work.

To cope with the threats coming from the malicious nodes, when defining the cooperative topologies, countermeasures must be considered to offer rational users the possibility to filter out untrusted users, block the unsecure links and avoid unsuccessful opportunistic hop-by-hop D2D interactions, as sketched in Figure 1. The solution we propose for effective and trusted D2D-based data uploading can be summarized as follows:

Channel quality indicator (CQI) collection: the eNodeB collects the CQI values from each unit of UE, relevant to the direct links with all its neighbors and to the uplink toward the eNodeB.

Virtual resource allocation: the eNodeB considers the situation where the single UE devices are transmitting in unicast over their uplink and computes the radio resources according to the scheduling policy. The so-computed radio resources are considered as "virtual" since they are not yet allocated to the UE because the UE may actually form a cooperative multihop topology (i.e., a coalition). Whenever a coalition is formed, the pool of "virtual" resources of all the UE in the coalition will be assigned to the respective gateway.

Cooperative coalition formation: in this step a set of stable coalitions are determined where for each coalition the roles for the nodes in the cooperative D2D-based data uploading are defined, as well as the routing path for the data from each node. To produce stable coalitions, the eNodeB will rely on a game theoretic model such as the one defined in [10]. A classic merge and split algorithm is implemented where the device preference to join or leave a coalition is based on the estimated data uploading time. In the coalition formation algorithm two main constraints are considered: (1) two consecutive nodes in the data routing path built on a cooperative coalition must be in coverage for a D2D link (otherwise the data routing would fail); and (2) the devices in the cooperative coalitions should guarantee a minimum value of trust which we define as *feasibility threshold* FT. Indeed, we consider a coalition as *not feasible* if at least one link $i \rightarrow j$ in the topology does not meet the constraint:

$$pt_{i,j} \cdot d_{i,j} \geq FT \tag{1}$$

where $pt_{i,j} \rightarrow [0,1]$ is the *player trust* that player i (a device in a coalition) associates to player j (see Section 5). The second term $d_{i,j}$ is a binary function taking value 0 if users i and j are not in proximity, and value 1 otherwise. A link not meeting the mentioned constraint is represented in Figure 1 as a blocked link.

Data transmission configuration: For each coalition that is formed, the eNodeB assigns the respective pool of virtual radio resources to the gateway, and transmits all the required information to the UE so that the transmissions can start. The devices in different coalitions are always allocated to orthogonal frequency resources by the scheduler (we consider a *maximum throughput* scheduler) so that mutual interference is avoided. The configuration of the D2D communications assumes that UE simultaneously transmitting in the same coalition adopts different RBs to avoid any mutual interference (this leads to a worst case analysis and better results can be obtained with enhanced interference management).

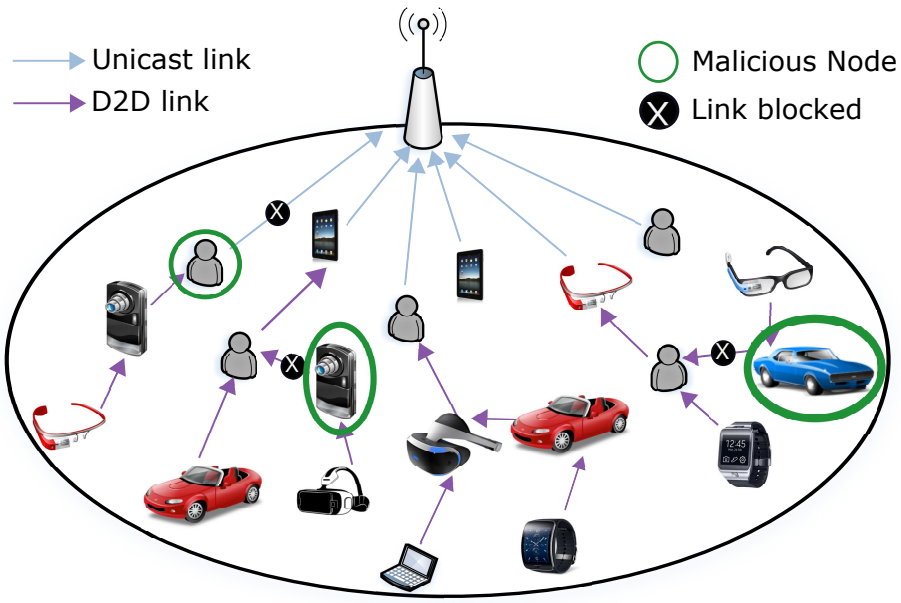


Figure 1. Cooperative multihop content uploading based on trustworthy device to device (D2D) links.

5. The Social-Aware Trust Model

In our scenario the eNodeB acts as a trusted third party that implements the coalition formation model based on social-aware trustworthiness. To this aim, we evaluate the potential of the SIoT model to embrace the social networking concepts and build trustworthy relationships among the devices [25]. The eNodeB will store information about the reliability, reputation and trust of the users in the network. We define a *player trust matrix (PTM)* as the data structure stored in the eNodeB containing information for every pair of devices. This information will be used whenever a new coalition formation is triggered. Every element (i-th row and j-th column) of the PTM refers to a D2D link connecting the corresponding $i \rightarrow j$ nodes in the coalition being considered at time t, where node j is the 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 eNodeB will also act as a controller of the data uploading success as it will send an acknowledgment to the respective source nodes after each cooperative data transmission. Whenever data loss or data corruption is detected by the eNodeB, malicious behavior

will be detected and the information about the reliability of the interested devices will be respectively updated. We assume that control messages (sent over control channels) are very small compared to the main content to be sent and therefore, the relative transmission time and energy consumption are assumed to be negligible. The parameters used to define the level of trust are the following:

Social player reliability ($spr_{i,j}$): this parameter has a value in $[0,1]$ and measures the reliability that node i assigns to player j based on the social relationship between the two devices;

Player reliability ($pr^t_{i,j}$): this parameter has a value in $[0,1]$ and is representative of the reliability at time instant t that player i assigns to player j. To determine this value, each player will consider both the *social player reliability* and the outcome of past interactions (only those cases are considered where player j was expected to act as relay/gateway for player i).

Recommendation reliability ($rr_{i,j}$): this parameter has a value in $[0,1]$ and is a measure of the reliability assigned by node i to the recommendations it receives from another device j about third devices in the network. In our model we consider this parameter to be influenced by the social relationship between the interested UE.

Player reputation ($pp^t_{i,j}$): this parameter has a value in $[0,1]$ and measures the reputation of player j for player i according to the information he received through the recommendation values from third players in the network at a given time instant t.

Player trust ($pt^t_{i,j}$): this parameter has a value in $[0,1]$ and measures the level of trust for player j at time t as evaluated by player i. This is the most important parameter as it will determine whether player i is willing to consider player j as relay/gateway node in a D2D-based cooperative coalition. For the computation of its value player i will use a weighted combination of the reliability $pr^t_{i,j}$ and the reputation $pp^t_{i,j}$ parameters.

As commented above, the *player reliability* parameter is a function of the time instant t. In particular, its value is updated at every time instant based on the experienced behavior of the devices in the cooperative data uploading. To make this work, for each cooperative interaction the eNodeB sends an acknowledgment to the source nodes with information about the data being successfully received. Of note, this does not allow to determine which node in the cooperative topology has actually dropped or corrupted the data. Therefore, 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 $i \rightarrow j$. At time instant $t = 0$ the only information the interested devices can exploit for judging the *player reliability* is *social player reliability* ($spr_{i,j}$) which is set according to predefined values (see Table 1). If two communicating entities are tied by two or more types of relationships, the strongest tie with the highest factor has to be considered [25]. At subsequent time instants $t > 0$, the results of cooperative interactions can be used to determine the player reliability $pr^t_{i,j}$ with j acting as relay/gateway for data sent by i. In particular, 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 equal to the total percentage of data that has been successfully forwarded by node j and reached the eNodeB. Summarizing, we define the player reliability $pr^t_{i,j}$ as follows:

$$pr^t_{i,j} = \begin{cases} spr_{i,j} & t = 0 \\ \alpha \cdot spr_{i,j} + (1-\alpha) \cdot \frac{\sum_{d \in \Delta^t_{i,j}} \delta_d}{|\Delta^t_{i,j}|} & t > 0 \end{cases} \quad (2)$$

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

The other parameter that is being updated after each cooperative interaction is the player *reputation* which is based on the opinions of the community in the network. If, for instance, a player i asks the opinion about player j to the community, it will receive an opinion from a set of players in the network. Let us say this set of players is $\mathcal{K} \subseteq \mathcal{N} \backslash \{i\}$, where $\mathcal{N}$ is the total set of devices in the network. The opinion player k will provide is its own measure of trust about player j at time instant t, namely $pt^t_{k,j}$.

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

Relationship	Description	Social player Reliability ($spr_{i,j}$)	Recommendation 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

To best weigh the opinions received from the other players, a confidence factor called *recommendation reliability* ($rr_{i,k}$) is used. In our proposed model this is set according to the social relationship between the involved devices as reported in Table 1. Note that we assumed the *recommendation reliability* to have a lower value with respect to *social player reliability* in general. The motivation for this is that the recommendation received by a socially related device may be influenced by the outcome of past cooperative iterations which affected the ability to provide an objective recommendation. Given the collected information, the *player reputation* at time t is computed as follows:

$$pp_{i,j}^{t} = \frac{\sum\limits_{k \in \mathcal{K}} rr_{i,k} \cdot pt_{k,j}^{t}}{\sum\limits_{k \in \mathcal{K}} rr_{i,k}} \tag{3}$$

Player i can then determine the player trust value $pt_{i,j}^{t}$ it associates to player j at time instant t, as a combination of the player reliability ($pr_{i,j}^{t}$) and the player reputation ($pp_{i,j}^{t}$) weighted by a real coefficient β ranging in $[0,1] \in \mathbb{R}$:

$$pt_{i,j}^{t} = \begin{cases} 0.5 & t = 0 \\ \beta \cdot pr_{i,j}^{t} + (1-\beta) \cdot pp_{i,j}^{t} & t > 0 \end{cases} \tag{4}$$

The choice to set the initial trust value to 0.5 is caused by *whitewashing strategies* where a malicious adviser can whitewash its low trustworthiness starting a new account with the initial trustworthiness value.

6. Performance Evaluation

In this section we provide the output of an extensive simulation campaign finalized to demonstrate the robustness of the proposed solution to the presence of malicious nodes. The presented results are obtained using a built-in simulator in Matlab already used in previous works [9,10]. The proposed solution, hereafter named *trust-based*, is compared to an alternative *basic* approach that does not take into account any trustworthiness for the involved users and is unable to detect the malicious behavior. As discussed earlier (see Section 4), we consider two different types of malicious nodes, i.e., (1) *type A*, where users forward corrupted packets (for instance) to perform an attack to security, and (2) *type B*, where users drop the packets to exploit the benefits given by multi-hop D2D connections without forwarding any content further in the chain.

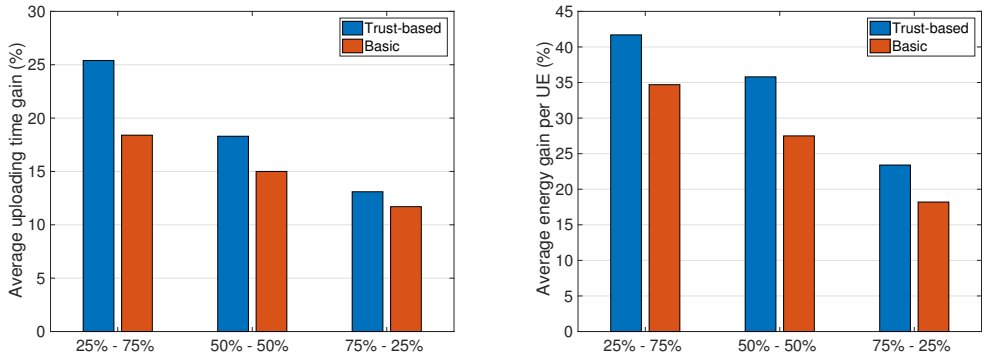
The reference scenario is composed by a single LTE-A cell with a 500-m radius and 10-MHz bandwidth (i.e., 50 RBs available) where 20 UE devices are uniformly distributed. As for the NB-IoT, we use the "in band" where 6 RBs (for a total number of 288 tones) are allocated for the transmissions among the selected gateways and eNodeB. The main simulation parameters are listed in Table 2. The content size for all the nodes is set to 50 MB and radio resources used on a D2D transmission are limited to the so-called "virtual resources" allocated by the eNodeB to the involved pairs of UE (see Section 4 for more details). The performance parameters we focus on for the system-level performance are: (1) *data loss*; (2) *average data uploading time gain*; and (3) *average energy consumption gain*.

In particular, the latter two parameters represent the gain achieved by the cooperative upload a pure cellular upload solution where each user uploads directly the content to the network infrastructure by using standard LTE unicast transmissions.

Table 2. Main simulation parameters. NB-IoT: narrowband Internet of things; CQI: channel quality indicator; MCS: modulation and coding scheme; TTI: Transmission time interval; TDD: Time division duplex.

Parameter	Value
Cell radius	500 m
Maximum D2D link coverage	100 m
TTI	1 ms
TDD configuration (D2D)	0
Carrier frequency	2.1 GHz
Tx Cellular power (NB-IoT)	23 dBm
Tx D2D power	−19 dBm
CQI-MCS mapping for D2D links	"refer to [32]"
Noise power	−174 dBm/Hz
Cellular link model	Rayleigh fading channel
D2D link model	Rician fading channel
NB-IoT tones	288 (i.e., 6 RBs)
Content size	50 MB
Weighting factors $\alpha = \beta$	0.5
Simulation time	100 s
# of Runs	500

The first analysis we discuss is the impact that the two classes of malicious nodes have on the uploading time and the energy consumption. In particular, we consider three different distributions of malicious nodes in the system, namely: (1) prevalence of type A (i.e., 75–25%) malicious node; (2) equal number of type A and type B malicious nodes (i.e., 50–50%); and (3) prevalence of type B malicious nodes (i.e., 25–75%). As we can observe from Figure 2, the proposed trust-based solution always performs better compared to the basic strategy (we consider here the sample case with FT = 0.5). In particular, when there is a prevalence of type A malicious nodes in the system we obtain lower benefits in terms of uploading time and energy consumption. The motivation behind this is that the energy consumed for a UE when receiving corrupted packets is added to the energy required to upload the content with a unicast link to the eNodeB. In the presence of type B malicious nodes (i.e., dropping packets), instead, the only energy consumption for the UE is due to the unicast uplink transmission from the UE to the eNodeB. Same motivations yield for the differences observed in the uploading time gain, which, as shown in Figure 2a, results to be higher when we have a prevalence of type B malicious nodes.



(**a**) (**b**)

Figure 2. Impact of type A and type B malicious nodes (feasility threshold, FT = 0.5). (**a**) Uploading time gain; (**b**) Average energy gain.

The next analysis shows the results when the percentage of malicious nodes in the system varies in the range [15–90%]. Here it is assumed that there is an equal number of malicious nodes of type A and type B and FT = 0.5. As we can observe from the plots in Figure 3a,b, the proposed trust-based solution obtains better performance. In particular, the average uploading time gain and the energy consumption gain are higher with the proposed solution. In fact, with our approach users forward data to trusted devices in proximity by avoiding transmissions with malicious nodes. In details, the achieved gain compared to the basic solution reaches the value of +5% and +7% (on average) for uploading time and energy consumption, respectively. This behaviour is also confirmed by curves in Figure 3c showing the amount of data loss due to malicious nodes. Here, the trust-based solution has a percentage of data loss that is 19% (on average) less than the data loss with the basic approach.

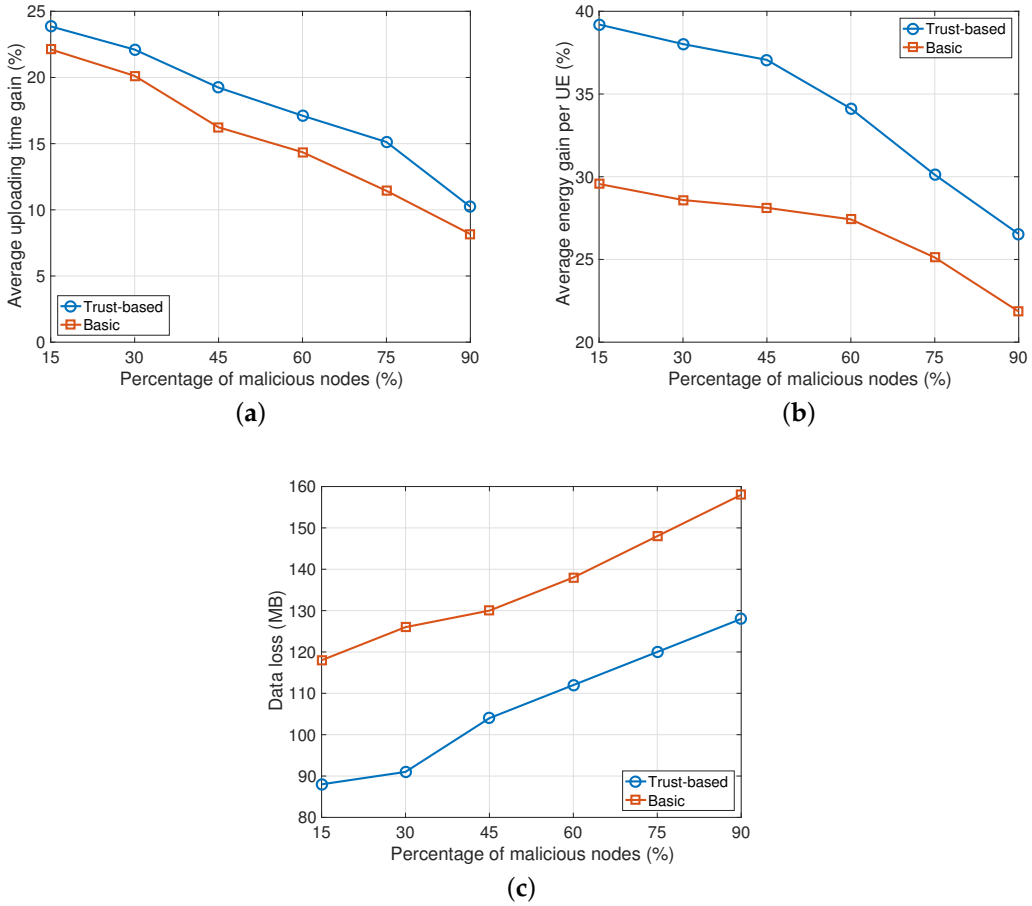


Figure 3. Impact of malicious nodes percentage (half of type A and half of type B malicious nodes are considered, FT = 0.5). (**a**) Uploading time gain; (**b**) Average energy gain; (**c**) Data loss.

The last analysis has the objective to show the effects of the *feasibility threshold* on the system-level performance. In Figure 4 results are presented when varying the *FT* value from 0.2 to 1.0, under the condition of 50% malicious nodes in the system. Interestingly, the gain achieved in terms of uploading time increases linearly with the value of FT until reaching a value of 31% (see Figure 4a). However, this result is obtained at the cost of a higher energy consumption for the nodes. As shown in Figure 4b, the energy consumption gain decreases with the FT and the proposed solution performs even worse than the basic one for FT values beyond 0.5. The reason is that the devices select only nodes with high trustworthiness to forward data. For this reason, the selection of the links to forward the data is strongly constrained and it may be that transmissions occur over low capacity links which require more energy. However, users are able to upload their data without requiring additional transmissions

toward the eNodeB. In the extreme case, when the feasibility threshold is set to 1 the amount of data loss is about 19 MB compared to 120 MB for the basic solution.

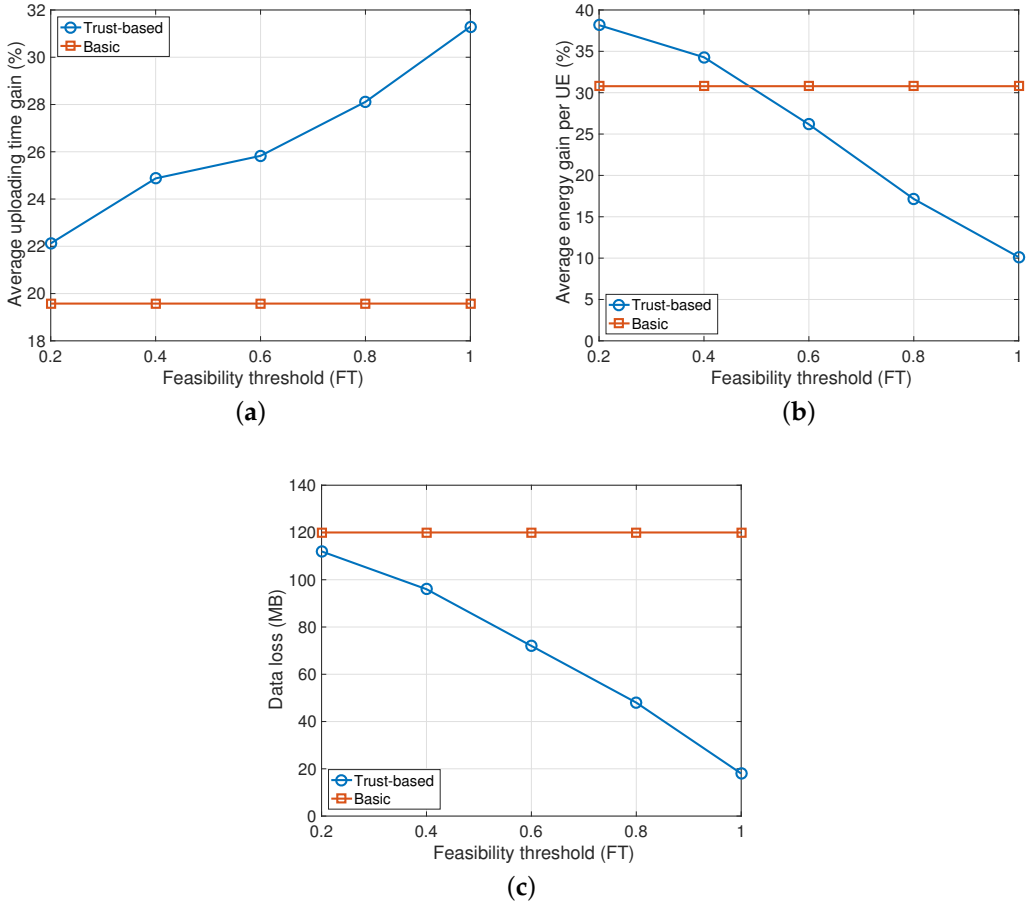


Figure 4. Impact of feasibility threshold (50% of malicious nodes, half of type A and half of type B). (**a**) Uploading time gain; (**b**) Average energy gain; (**c**) Data loss. UE: user equipment.

In conclusion, the proposed trust-based approach outperforms the basic solutions. Moreover, the highest benefits are obtained by tuning the feasibility threshold to the estimated number of malicious nodes in the system and to the desired performance parameter. In fact, even if a high feasibility threshold increases the chances of correctly forwarding the data towards to eNodeB with lower uploading times and data losses, this can result in a higher energy consumption.

7. Conclusions

In this paper we proposed a trust-based solutions for effective D2D-enhanced cooperative content uploading in narrowband-IoT cellular environments. To limit the impact of the malicious nodes either dropping or corrupting the data packets in a cooperative multihop coalition, social awareness has been modeled to evaluate the reliability for the nodes and to suitably weigh the recommendations exchange for the reputation definition. A simulative analysis validated the proposed solution in a wide range of settings for small-scale IoT scenarios. The results showed how the social-based trusted solution guarantees higher gains in the content uploading time, in the energy consumption, and has the ability to increase the amount of successful cooperative interactions by filtering out the malicious nodes.

Acknowledgments: The publication was financially supported by the Ministry of Education and Science of the Russian Federation (the Agreement number 02.a03.21.0008).

Author Contributions: In this paper, the first three authors Antonino Orsino, Giuseppe Araniti and Leonardo Militano conceived the idea, organized the work and designed the analytical model and the proposed algorithms; Antonino Orsino and Leonardo Militano conceived and designed the experiments, analyzed the results and wrote the paper; Antonino Orsino performed the experiments; Antonio Iera supervised the work; all the authors reviewed the writing of the paper, its structure and its intellectual content.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Fantacci, R.; Pecorella, T.; Viti, R.; Carlini, C. A network architecture solution for efficient IOT WSN backhauling: Challenges and opportunities. *IEEE Wirel. Commun.* **2014**, *21*, 113–119.
2. Soldani, D.; Manzalini, A. Horizon 2020 and Beyond: On the 5G Operating System for a True Digital Society. *IEEE Veh. Technol. Mag.* **2015**, *10*, 32–42.
3. Sachs, J.; Beijar, N.; Elmdahl, P.; Melen, J.; Militano, F.; Salmela, P. Capillary networks: A smart way to get things connected. *Ericsson Rev.* **2014**, *8*, 1–8.
4. Andreev, S.; Galinina, O.; Pyattaev, A.; Gerasimenko, M.; Tirronen, T.; Torsner, J.; Sachs, J.; Dohler, M.; Koucheryavy, Y. Understanding the IoT connectivity landscape: A contemporary M2M radio technology roadmap. *IEEE Commun. Mag.* **2015**, *53*, 32–40.
5. Boccardi, F.; Heath, R.W.; Lozano, A.; Marzetta, T.L.; Popovski, P. Five disruptive technology directions for 5G. *IEEE Commun. Mag.* **2014**, *52*, 74–80.
6. Bello, O.; Zeadally, S. Intelligent Device-to-Device Communication in the Internet of Things. *IEEE Syst. J.* **2014**, *10*, 1–11.
7. Militano, L.; Araniti, G.; Condoluci, M.; Farris, I.; Iera, A. Device-to-Device Communications for 5G Internet of Things. *EAI Endorsed Trans. Internet Things* **2015**, *15*. doi:10.4108/eai.26-10-2015.150598.
8. Roman, R.; Najera, P.; Lopez, J. Securing the internet of things. *Computer* **2011**, *44*, 51–58.
9. Militano, L.; Orsino, A.; Araniti, G.; Nitti, M.; Atzori, L.; Iera, A. Trusted D2D-based data uploading in in-band narrowband-IoT with social awareness. In Proceedings of the IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Valencia, Spain, 4–8 September 2016; pp. 1–6.
10. Militano, L.; Orsino, A.; Araniti, G.; Molinaro, A.; Iera, A. A Constrained Coalition Formation Game for Multihop D2D Content Uploading. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 2012–2024.
11. Nokia. LTE Evolution for IoT Connectivity White Paper. In Nokia White Paper. Available online: https://resources.ext.nokia.com/asset/200178 (accessed on 6 December 2016).
12. Gandotra, P.; Jha, R.K.; Jain, S. A survey on device-to-device (D2D) communication: Architecture and security issues. *J. Netw. Comput. Appl.* **2016**, *78*, 9–29.
13. Sicari, S.; Rizzardi, A.; Grieco, L.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164.
14. Ometov, A.; Orsino, A.; Militano, L.; Moltchanov, D.; Araniti, G.; Olshannikova, E.; Fodor, G.; Andreev, S.; Olsson, T.; Iera, A.; et al. Toward trusted, social-aware D2D connectivity: Bridging across the technology and sociality realms. *IEEE Wirel. Commun.* **2016**, *23*, 103–111.
15. Grandison, T.; Sloman, M. Trust management tools for internet applications. In *Trust Management*; Springer: Berlin, Germany, 2003; pp. 91–107.
16. Antonopoulos, A.; Kartsakli, E.; Verikoukis, C. Game theoretic D2D content dissemination in 4G cellular networks. *IEEE Commun. Mag.* **2014**, *52*, 125–132.
17. Antonopoulos, A.; Verikoukis, C. Multi-player game theoretic MAC strategies for energy efficient data dissemination. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 592–603.
18. Ometov, A.; Olshannikova, E.; Masek, P.; Olsson, T.; Hosek, J.; Andreev, S.; Koucheryavy, Y. Dynamic Trust Associations Over Socially-Aware D2D Technology: A Practical Implementation Perspective. *IEEE Access* **2016**, *4*, 7692–7702.
19. Wu, D.; Zhou, L.; Cai, Y. Social-Aware Rate Based Content Sharing Mode Selection for D2D Content Sharing Scenarios. *IEEE Trans. Multimed.* **2017**, *99*, doi:10.1109/TMM.2017.2700621.
20. Datsika, E.; Antonopoulos, A.; Zorba, N.; Verikoukis, C. Green cooperative device-to-device communication: A social-aware perspective. *IEEE Access* **2016**, *4*, 3697–3707.

21. Huang, Z.; Tian, H.; Fan, S.; Xing, Z.; Zhang, X. Social-Aware Resource Allocation for Content Dissemination Networks: An Evolutionary Game Approach. *IEEE Access* **2016**, *5*, 9568–9579.
22. Wang, Z.; Sun, L.; Zhang, M.; Pang, H.; Tian, E.; Zhu, W. Propagation-and mobility-aware d2d social content replication. *IEEE Trans. Mob. Comput.* **2017**, *16*, 1107–1120.
23. Atzori, L.; Iera, A.; Morabito, G.; Nitti, M. The Social Internet of Things (SIoT)—When social networks meet the Internet of Things: Concept, architecture and network characterization. *Comput. Netw.* **2012**, *56*, 3594–3608.
24. Nitti, M.; Murroni, M.; Fadda, M.; Atzori, L. Exploiting Social Internet of Things Features in Cognitive Radio. *IEEE Access* **2016**, *4*, 9204–9212.
25. Nitti, M.; Girau, R.; Atzori, L. Trustworthiness Management in the Social Internet of Things. *IEEE Trans. Knowl. Data Eng.* **2014**, *26*, 1253–1266.
26. 3GPP. *TS 22.368, Service Requirements for Machine-Type Communications (MTC), V13.1.0*; Technical Report; European Telecommunications Standards Institute: Sophia Antipolis Cedex, France, 2014.
27. 3GPP. *TSG RAN Meeting #69, Narrowband IoT*; Technical Report; European Telecommunications Standards Institute: Sophia Antipolis Cedex, France, 2015.
28. Pan, Y.; Pan, C.; Zhu, H.; Ahmed, Q.Z.; Chen, M.; Wang, J. On consideration of content preference and sharing willingness in D2D assisted offloading. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 978–993.
29. Datsika, E.; Antonopoulos, A.; Zorba, N.; Verikoukis, C. Cross-Network Performance Analysis of Network Coding Aided Cooperative Outband D2D Communications. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 3176–3188.
30. Zhou, B.; Hu, H.; Huang, S.Q.; Chen, H.H. Intracluster device-to-device relay algorithm with optimal resource utilization. *IEEE Trans. Veh. Technol.* **2013**, *62*, 2315–2326.
31. Yang, F.; Wang, S.; Li, J.; Liu, Z.; Sun, Q. An overview of Internet of Vehicles. *China Commun.* **2014**, *11*, 1–15.
32. Iturralde, M.; Yahiya, T.; Wei, A.; Beylot, A. Interference mitigation by dynamic self-power control in femtocell scenarios in LTE networks. *IEEE Glob. Commun. Conf.* **2012**, 4810–4815, doi:10.1109/GLOCOM.2012.6503880.