



UNIVERSITÀ POLITECNICA DELLE MARCHE
Repository ISTITUZIONALE

An Approach to Compute the Scope of a Social Object in a Multi-IoT Scenario

This is the peer reviewed version of the following article:

Original

An Approach to Compute the Scope of a Social Object in a Multi-IoT Scenario / Causeruccio, F.; Cinelli, L.; Fortino, G.; Savaglio, C.; Terracina, G.; Ursino, D.; Virgili, L.. - In: PERVASIVE AND MOBILE COMPUTING. - ISSN 1574-1192. - 67:(2020). [10.1016/j.pmcj.2020.101223]

Availability:

This version is available at: 11566/283337 since: 2024-05-08T14:07:19Z

Publisher:

Published

DOI:10.1016/j.pmcj.2020.101223

Terms of use:

The terms and conditions for the reuse of this version of the manuscript are specified in the publishing policy. The use of copyrighted works requires the consent of the rights' holder (author or publisher). Works made available under a Creative Commons license or a Publisher's custom-made license can be used according to the terms and conditions contained therein. See editor's website for further information and terms and conditions.

This item was downloaded from IRIS Università Politecnica delle Marche (<https://iris.univpm.it>). When citing, please refer to the published version.

(Article begins on next page)

An Approach to Compute the Scope of a Social Object in a Multi-IoT Scenario

Francesco Cauteruccio¹, Luca Cinelli¹, Giancarlo Fortino², Claudio Savaglio², Giorgio Terracina¹, Domenico Ursino^{3*}, and Luca Virgili³

¹ DEMACS, University of Calabria, {cauteruccio, cinelli, terracina}@mat.unical.it

² DIMES, University of Calabria, g.fortino@unical.it, csavaglio@dimes.unical.it

³ DII, Polytechnic University of Marche, d.ursino@univpm.it, l.virgili@pm.univpm.it

* Contact Author

Abstract

In the last few years, classical social networking is turning into the more complex social internet-working and is extending from human users to objects. Indeed, objects are becoming increasingly complex, smart and social so that several authors have recently started to investigate the Social Internet of Things (SIoT) and the Multiple IoT (MIoT) paradigms. SIoT is more oriented to the technological issues to be faced in presence of multiple IoT interacting with each other. Instead, MIoT addresses data-driven and semantics-based aspects because it considers the contents exchanged by smart objects during their transactions. In such a research context, the concept of *scope* in a Multi-IoT scenario can play an important role. In this paper, we investigate this issue. In particular, first we define the concept of scope in a Multi-IoT scenario. Then, we propose two formalizations of this concept allowing the computation of its values. Afterwards, we present two possible applications of scope. Finally, we describe a set of experiments performed for its evaluation; the last of them compares scope with diffusion degree and influence degree, two parameters already proposed in past literature.

Keywords: Scope; Smart Objects; Internet of Things; Multi-IoT; Social IoT; Social Network Analysis; Impact Degree; Trust Degree

1 Introduction

When we throw a stone in a pond, we can see that the water moves, and small waves are created. These waves are higher in the proximity of the stone and, as we move away from it, they become smaller and smaller until they disappear. Generally, the heavier the stone, the higher the initial waves and the farther they arrive. This image, in our opinion, describes better than anything else what is meant by “scope”. In the Concise Oxford Dictionary ¹, *scope* is defined as “*the extent of the area or subject matter that something deals with or to which it is relevant*”.

¹Concise Oxford Dictionary - <https://en.oxforddictionaries.com>

We can surely find several analogies between scope and some other concepts used in sociology; think, for instance, of centrality, reliability, power, reputation, influence, trust, diffusion, etc. [50, 40]. Actually, scope goes beyond these concepts and simultaneously embraces them and is influenced by all of them.

Scope has been investigated by social network researchers in the past. For example, [29] analyzes the scope of users and hashtags in Twitter, while [26, 33, 34, 37, 46, 52] propose approaches to analyze some aspects of scope (e.g., reliability, trust and influence) for users and/or hashtags. As for the evaluation of user influence, [11] exploits the well known PageRank algorithm to assess the distribution of influence throughout the network. In the meantime, social networks have become more and more complex, and social networking has evolved into social internetworking [43, 8]. In this new context, some social networks interact with each other thanks to some users, called bridges, each joining at least two social networks. Bridges play a key role in social internetworking because they allow users of different social networks to interact with each other.

Along with social internetworking, another key phenomenon we are experiencing in the last few years is the presence of increasingly smart and social objects [19]. This is deeply influencing the Internet of Things (hereafter, IoT) scenario [57]. As a consequence of this fact, an increasingly high number of authors have begun to investigate the behavior of smart objects and to analyze their profiles and social interaction [15]. As a matter of fact, several architectures performing these tasks have been recently proposed in literature; think, for instance, of the most recent ones, i.e., Social Internet of Things (hereafter, SIoT [2]), Multiple IoT Environment (MIE [5]) and Multiple Internets of Things (hereafter, MIoT [6, 30, 50]). MIoT is the most recent of them and, for this reason, considers the most recent results obtained by researchers on IoT. A MIoT can be modeled as a set of IoT, which interact with each other through those objects, called “cross-objects” (analogous to bridges in social internetworking scenarios), which belong to more IoT. From this definition it is clear that the MIoT paradigm is an attempt to extend the social internetworking ideas to IoT.

In spite of the high number of researches on IoT performed in the latest years, to the best of our knowledge no investigation on the scope of an object in a MIoT, or at least in an IoT, has been yet proposed. Actually, some aspects presenting several relationships with scope have been analyzed in IoT or, in some cases, in the SIoT context (think, for instance, of [41, 47, 1, 59, 7]). However, none of them is as general as the investigation of the scope in a MIoT could be.

In this paper, we contribute to fill this gap by introducing and analyzing the concept of scope of a smart object in a MIoT. Specifically, we present two formalizations of this concept. The former is called Naive; it is simple (because it considers only trust), but it does not take into account all the factors that could play a key role in this context. The latter is called Refined; it is quite complex, but it takes all the possible involved factors into account; in fact, it considers trust, proactivity, stimulation capability and security level.

After having introduced both these formalizations, we analyze them through a set of experiments devoted to understand the pros and the cons of each of them. Furthermore, these experiments are conceived to highlight the relationships between centrality measures and scope, as well as the possible connection between this last parameter and network density. Moreover, we experimentally compare our definition of scope with two related concepts (i.e., diffusion degree and influence degree) proposed in past literature on IoT. This analysis reveals that scope provides a balanced assessment of the

“power” of a smart object over its neighbors. Indeed, its assessment is intermediate between the one returned by diffusion degree (which is overly optimistic) and the one provided by influence degree (which is overly pessimistic). We also examine related literature to evidence the analogies and the differences between the previous proposals and the one illustrated in this paper. Finally, we present two case studies (i.e., a smart city and a shopping center) where scope can play an important role.

Summarizing, the main contributions of this paper are the following:

- We extend the definition of scope from Social Networks to Internet of Thing and from multiple Social Networks to multiple IoT, according to a data-driven perspective.
- We present two levels of scope, namely: Naive and Refined. The former is simple and immediate to compute; the latter is more accurate and precise, even if computationally more expensive.

We point out that a very preliminary version of the material presented in this paper can be found in [12]. However, here we introduce many novelties regarding: *(i)* the split of the concept of scope into Naive Scope and Refined Scope; *(ii)* the definition of two use cases; *(iii)* a set of experiments to evaluate our approach from different viewpoints; *(iv)* a large analysis of related literature; *(v)* an experimental comparison of our approach for the computation of scope with two past approaches, the former devoted to compute diffusion degree and the latter conceived to calculate influence degree; both these parameters are related to scope.

The outline of this paper is as follows: In Section 2, we give an overview of related literature. In Section 3, we illustrate the MIoT paradigm. In Section 4, we introduce the concept of scope and present two formalizations of it. In Section 5, we describe two typical use cases benefiting from this information, whereas, in Section 6, we illustrate our set of experiments. Finally, in Section 7, we draw our conclusions and outline some possible future developments of our ideas.

2 Related Work

In this section, we provide a comparison between our approach and related literature. Before starting this discussion, a preliminary consideration about the MIoT model is in order, because it is the substrate which our definition of scope relies on. Indeed, the MIoT model adopts an abstract perspective of IoT, different from a technical one. It does not aim at handling technological heterogeneities and other challenging technological issues. Instead, it aims at providing a high-level representation of interconnected IoT, which, thanks to the adoption of metadata, is independent from the underlying technology. The definition of a semantics-based representation of IoT is currently considered one of the main challenging issues in this research field [2]. Some preliminary attempts in this direction have been recently proposed in literature. One of the most known of these attempts is SIoT [2]. However, this model is still strictly related to technological issues because the forms of relationships between objects proposed by the authors, namely *(i)* parental object relationship; *(ii)* co-location object relationship; *(iii)* co-work object relationship; *(iv)* ownership object relationship; *(v)* social object relationship, are only partially semantic. Actually, the MIoT model captures different aspects w.r.t. SIoT. Indeed, it focuses on data-driven and semantics-based aspects and not on technological ones; as a matter of fact, it considers the contents exchanged by smart objects [21] during their transactions.

After this premise, we can start to overview related literature. In order to perform this activity better and to define some guidelines for comparing other approaches with ours, in Table 1 we provide an overview of the most important features that should characterize approaches conceived to evaluate scope or other related parameters in an IoT scenario. In particular, we consider the following features: *(i)* capability of handling a trade-off between quality of results and running time; *(ii)* capability of handling labeled networks; *(iii)* capability of handling multiple IoT or multiple complex networks; *(iv)* usage of content and relationship data within the approach; *(v)* usage of structural properties; *(vi)* usage of physical information concerning IoT, and *(vii)* application in recommendation services.

	Management of a trade-off between quality of results and execution time	Management of labeled networks	Management of multiple IoT and/or networks	Data-driven approach	Usage of structural properties	Usage of physical information concerning IoT	Applicability in recommendation services
Our approach	✓	✓	✓	✓	✓	-	-
[41]	-*	-	-	✓	-	✓	-
[1]	-*	-	-	✓	✓	✓	-
[59]	-	✓	-	✓	-	✓	-
[39]	-	-	-	✓	-	-	-
[28]	-	-	-	✓	-	-	-
[56]	-	✓	✓	✓	✓	-	✓
[24]	✓	✓	-	-	✓	-	✓
[36]	-	-	-	-	✓	-	-
[51]	✓	-	-	-	✓	-	-
[18]	-*	-	-	✓	-	-	✓

Table 1: A taxonomy of approaches evaluating scope or related parameters in IoT. The symbol * denotes that the corresponding feature is not directly present, but may be re-constructed indirectly

The classical IoT architectures share some similarities with the classical social networks, whereas social IoT paradigms (such as SIoT [2], MIE [5], and MIoT [6]) share some similarities with Social Internetworking Systems [8, 42]. Actually, to the best of our knowledge, no investigation about the scope in a multiple IoT scenario has been proposed in past literature, whereas very few approaches investigate concepts similar to the impact of smart objects in IoT. Furthermore, when this last investigation is performed, it is limited to a single IoT and no extension to multiple IoT is performed. As there is no past approach that simultaneously examines all the issues reported in this paper, in the following, we will focus on single aspects of the overall analysis, such as the kind of interaction, the network complexity, the kind of exchanged information, and so forth.

In the context of social networks, many investigations focusing on the centrality of a node have been performed. The interested reader can see [16] for a survey on this topic. In [35], the authors investigate the evolution of the centrality of nodes in complex dynamic networks, where nodes and links may appear and disappear over time and may move over the network. In [58], the authors propose an analysis of customer engagement in complex social networks. It evidences that many important dimensions used to study customer engagement are similar to the ones that we consider for scope computation. In [48], the authors exploit the posts of users to analyze the information flow in a network. In [60], the authors propose an approach that generates a bipartite graph between users and contents; then, they employ it to measure the influence of users in the corresponding social

network. In particular, this influence is computed by leveraging random walks on this graph, along with a related Markov chain model.

In [45], the authors define a new model where the influence of a user is based on her attractiveness, that is the number of other new users with whom she established relations over time. Another interesting concept introduced in the analysis of content sharing is the one of “information cascade”. This term is used to denote the investigation of how diffusion protocols can affect the way information is diffused within a network. Understanding how information is disseminated among users can support the detection of the most influential ones in a network. This issue has been recently addressed in [14] in the context of complex networks. Information cascade shares some aspects with our concept of scope. However, there is an important difference between these two concepts in that the former aims at modeling the whole information flow in a network, whereas the latter focuses on the evaluation of the impact degree on the subnetwork of the MIoT coinciding with the ego network centered on the node whose scope we want to analyze.

Information diffusion and propagation have been also analyzed in IoT contexts at different levels [41, 47, 1, 59, 7, 53]. For instance, in [41], the authors investigate information diffusion in narrowband IoT with the goal of optimizing information flow at network level. In [1], the authors investigate the adoption of context-aware information diffusion to alert messages in 5G mobile social networks. Both [41] and [1] exploit IoT physical information, which is a feature not considered by our approach. However, several aspects covered by our proposal are not considered in these two approaches. For example, they do not consider the context of multiple IoT and handle a trade-off between quality of results and running time only partially. Finally, [41] does not exploit structural properties of networks.

An interesting approach to content dissemination in the Internet of Vehicles (IoV) is described in [59]. Here, the authors investigate how to combine the information coming from the physical layer with the one regarding the social layer to perform a rapid content dissemination in IoV networks. The approach of [59] exploits physical information, which is not considered by our approach. On the other side, differently from our approach, it does not address the multiple IoT context. Furthermore, it does not provide the possibility to tune a trade-off between quality of results and running time, which is a feature provided by our approach.

Significant research efforts have been devoted to study the interaction between objects in complex IoT [39]. As an example, in [28], the authors present an IoT application in the context of smart cities, a scenario in which an IoT system can reach large scale dimensions. [28] also introduces the concept of IoT hub. The features of these two approaches are only marginally overlapping with our own. In fact, analogously to our approach, they are data driven. However, they do not consider the structural properties of networks, do not handle a multiple IoT scenario, and do not manage a trade-off between quality of results and running time.

Another line of research on IoT regards the design of approaches to recommender systems and services in IoT contexts; an overview of these approaches is presented in [17]. As for this research line, in [18], the authors propose a multi-agent recommender system for IoT aiming at producing a set of significant suggestions for a user with specific characteristics. Here, smart objects are represented through bit vectors, called thing descriptors, managed by cyber-agents. Smart objects can be linked together and, then, can be managed by neighbor cyber-agents. The approach of [18] is more oriented to analyze recommendation processes than to investigate information diffusion, which our approach

is centered on. Differently from our approach, the approach of [18] does not exploit structural properties, and does not handle multiple IoT. Finally, it manages a sort of trade-off, but this last regards the traffic load generated and the number of hops performed and, therefore, is completely different from the trade-off considered by our approach.

In [56], the authors propose an approach that integrates the concept of social network of users and IoT. It merges information coming from social networks of users and correlation networks of things by learning shared latent factors. To perform this task, it exploits a technique for probabilistic matrix factorization. The approach [56] addresses smart object recommendation in IoT, a feature not directly provided by our approach. On the other side, the concept of scope could be adopted in [56] as a further factor to determine relationships across heterogeneous smart objects in IoT. As a consequence, the two approaches can be considered orthogonal, even if they share several common features. In fact, both of them are able to deal with several IoT and labeled networks, and both of them exploit contents and relationships to address their tasks. Differently from our approach, the approach of [56] does not allow the management of the trade-off between quality of results and running time.

Beside the approaches regarding social networks or IoT, several related studies can be found when other forms of complex heterogeneous networks are considered. For instance, Heterogeneous Information Network (hereafter, HIN) is a graph model whose nodes and edges are annotated with types. A challenging issue in HINs is the computation of the closeness between two nodes, interpreted as the relevance of one of them for the other. In [24], the authors address this issue by introducing the concept of meta-structure. This is a directed acyclic graph of object types with edge types connecting in between. The approach of [24] shares several similarities with our own. Indeed, both of them use labeled networks and structural properties, and both of them are able to tune the quality of results and running time based on some parameters. Differently from the approach of [24], our own considers a multiple IoT scenario and exploits data exchanged among objects. On the other side, the approach of [24] differs from ours because it studies the properties of meta-structures in the recommendation context, which is a feature we plan to address in the future.

In [36], the authors propose an analysis for detecting influential nodes in complex networks. To address this issue, they identify relevant graph substructures, called maximal k-trusses, conceived to characterize the ability of influential nodes better than the previously adopted measures, such as node degree, k-core index, etc. In [51], the authors present a new measure, called efficiency centrality, for identifying influential nodes. Like scope, this measure considers nodes and their neighbors. However, it ranks spreaders in the whole network by removing nodes and considering the changes in the degrees of the other nodes of the network after removal. Both [36] and [51] share with our approach the idea to study the influence of smart objects in a network using its structural properties. However, differently from [36] and [51], our approach also considers the data exchanged between smart objects and handles labeled networks. Moreover, it is specifically designed for a multiple IoT scenario. Finally, analogously to our approach, the one described in [51] can handle a trade-off between quality of results and running time.

In [32], the authors propose an extensive review of the identification of vital nodes in complex networks. The concept of vital node reflects a general property of a node that plays a critical role in some specific dynamical processes.

3 The MIoT paradigm

In this section, we provide an overview of the MIoT paradigm, described in detail in [6], because it is the reference one for this paper. A MIoT \mathcal{M} is an ecosystem consisting of a set of m IoT. As shown in Figure 1, it consists of five layers. Three of them regard metadata, specifically object, instance and transaction metadata. The other two layers regard objects and their instances.

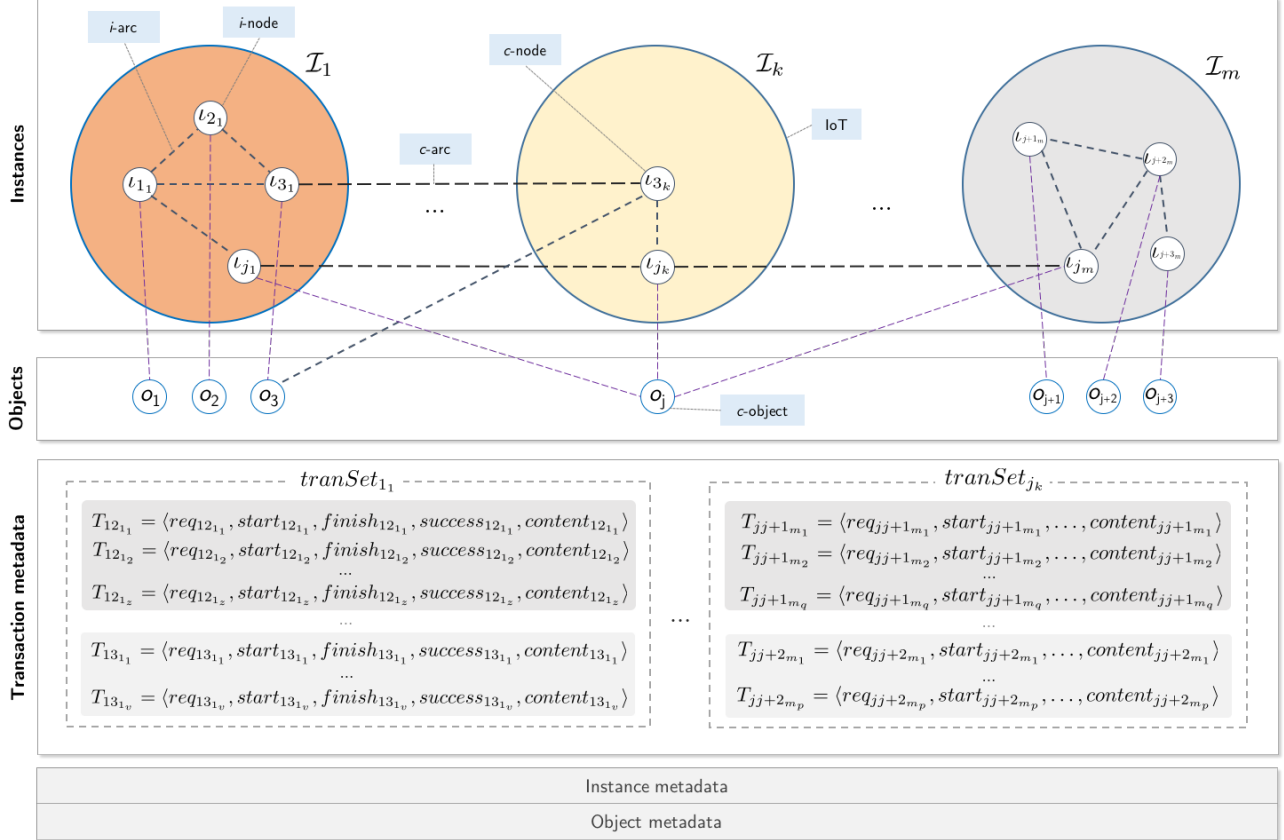


Figure 1: A graphical representation of the MIoT model

Formally speaking:

$$\mathcal{M} = \{\mathcal{I}_1, \mathcal{I}_2, \dots, \mathcal{I}_m\}$$

where \mathcal{I}_k is an IoT.

Let o_j be an object of \mathcal{M} . We assume that, if o_j belongs to \mathcal{I}_k , it has an instance ι_{j_k} , representing it in \mathcal{I}_k . The instance ι_{j_k} consists of a virtual view (or, better, a virtual instance) representing o_j in \mathcal{I}_k . For example, it provides all the other instances of \mathcal{I}_k , and the users interacting with this IoT, with all the necessary information about o_j . The information stored in ι_{j_k} is represented according to the format and the convention adopted in \mathcal{I}_k .

ι_{j_k} has associated a Security Level λ_{j_k} whose possible values are: 1 = low, 2 = medium-low, 3 = medium, 4 = medium-high, 5 = high. It indicates how much the security requirements are tight for

o_j in \mathcal{I}_k . Clearly, it depends on the nature of both o_j and \mathcal{I}_k , as well as on the role that o_j plays in \mathcal{I}_k .

A MIoT \mathcal{M} can be also represented by means of a graph-based notation. In particular, a graph $G_k = \langle N_k, A_k \rangle$ can be associated with an IoT \mathcal{I}_k of \mathcal{M} . In this case:

- N_k is the set of the nodes of G_k ; there is a node n_{j_k} for each instance $\iota_{j_k} \in \mathcal{I}_k$, and vice versa. Since there is a biunivocal correspondence between a node and an instance, in the following we shall use these two terms interchangeably.
- A_k is the set of the arcs of G_k ; there is an arc $a_{jq_k} = (n_{j_k}, n_{q_k})$ if there exists any form of relationship from ι_{j_k} to ι_{q_k} .

Finally:

$$\mathcal{M} = \langle N, A \rangle$$

Here:

$$N = \bigcup_{k=1}^m N_k \quad A = A_I \cup A_C$$

where:

$$A_I = \bigcup_{k=1}^m A_k \quad A_C = \{(n_{j_k}, n_{j_q}) | n_{j_k} \in N_k, n_{j_q} \in N_q, k \neq q\}$$

A_I is the set of the inner arcs (hereafter, *i-arcs*) of \mathcal{M} ; they link instances of different objects belonging to the same IoT. A_C is the set of cross arcs (hereafter, *c-arcs*) of \mathcal{M} ; they link instances of the same object belonging to different IoT. A node connected to at least one c-arc is called *c-node*; otherwise, it is called *i-node*.

Finally, we can introduce the concept of neighborhood of an instance ι_{j_k} in \mathcal{I}_k . Specifically, the neighborhood nbh_{j_k} of ι_{j_k} is defined as:

$$nbh_{j_k} = out_nbh_{j_k} \cup in_nbh_{j_k}$$

where:

$$out_nbh_{j_k} = \{n_{q_k} | (n_{j_k}, n_{q_k}) \in A_I, |tranSet_{jq_k}| > 0\}$$

and

$$in_nbh_{j_k} = \{n_{q_k} | (n_{q_k}, n_{j_k}) \in A_I, |tranSet_{qj_k}| > 0\}$$

In other words, nbh_{j_k} comprises those instances directly connected to ι_{j_k} through an incoming or an outgoing arc, which shared at least one transaction with it performed in the past.

In \mathcal{M} , an object o_j has associated a set MD_j of metadata. Our metadata model refers to the one of the IPSO (Internet Protocol for Smart Object) Alliance². Specifically, MD_j consists of three subsets, namely: (i) MD_j^D , i.e., the set of *descriptive metadata*; (ii) MD_j^T , i.e., the set of *technical*

²IPSO Alliance - <https://www.ipso-alliance.org>

metadata; and, (iii) MD_j^B , i.e., the set of *behavioral metadata*. All details about these metadata can be found in [6].

Given a pair of instances ι_{j_k} of o_j and ι_{q_k} of o_q in \mathcal{I}_k , our model stores the set $tranSet_{jq_k}$ of the transactions from ι_{j_k} to ι_{q_k} . It is defined as:

$$tranSet_{jq_k} = \{T_{jq_{k_1}}, T_{jq_{k_2}}, \dots, T_{jq_{k_v}}\}$$

A transaction $T_{jq_{k_t}} \in tranSet_{jq_k}$ is represented as follows:

$$T_{jq_{k_t}} = \langle req_{jq_{k_t}}, start_{jq_{k_t}}, finish_{jq_{k_t}}, success_{jq_{k_t}}, content_{jq_{k_t}} \rangle$$

Here:

- $req_{jq_{k_t}}$ denotes if ι_{j_k} started $T_{jq_{k_t}}$ as an answer to a specific request of ι_{q_k} or if it started $T_{jq_{k_t}}$ proactively.
- $start_{jq_{k_t}}$ denotes the starting timestamp of $T_{jq_{k_t}}$.
- $finish_{jq_{k_t}}$ indicates the ending timestamp of $T_{jq_{k_t}}$.
- $success_{jq_{k_t}}$ denotes whether $T_{jq_{k_t}}$ was successful or not; it is set to *true* in the affirmative case, to *false* in the negative one, and to NULL if it is still in progress.
- $content_{jq_{k_t}}$ indicates the set of the content topics considered by $T_{jq_{k_t}}$. Specifically, it consists of a set of w keywords:

$$content_{jq_{k_t}} = \{kw_{jq_{k_t}}^1, kw_{jq_{k_t}}^2, \dots, kw_{jq_{k_t}}^w\}$$

Now, we can define the set $tranSet_{j_k}$ of the transactions activated by ι_{j_k} in \mathcal{I}_k . Specifically, let $\iota_{1_k}, \iota_{2_k}, \dots, \iota_{w_k}$ be all the instances belonging to \mathcal{I}_k . Then:

$$tranSet_{j_k} = \bigcup_{q=1..w, q \neq j} tranSet_{jq_k}$$

In other words, the set $tranSet_{j_k}$ of the transactions of an instance ι_{j_k} is given by the union of the sets of the transactions from ι_{j_k} to all the other instances of \mathcal{I}_k .

From the above characterization, it clearly emerges that the MIoT paradigm deeply differs from the so called cross-domain IoT. They both deal with an interconnection of, often heterogeneous, IoT; however, the MIoT adopts an abstract perspective, while the cross-domain IoT a technical one. Indeed, the cross-domain IoT mainly addresses low-level concerns deriving from the technological heterogeneity – typical of IoT belonging to different domains – and places the interoperability issue on the spotlight [20]. The MIoT, instead, is more abstract, yet more flexible, by providing a high-level, technology agnostic (i.e., metadata- and metamodel-based) representation of interconnected and heterogeneous IoT which, in addition, can also be implemented.

As for the socialization level modeled by MIoT, some considerations are in order. To the best of our knowledge, MIoT represents the most advanced attempt of introducing concepts and behaviors

\mathcal{M}	a MIoT
\mathcal{I}_k	an IoT
o_j	an object of a MIoT
ι_{jk}	an instance of an object o_j in \mathcal{I}_k
G_k	a graph associated with an IoT \mathcal{I}_k
N_k	the set of the nodes of G_k
A_k	the set of the arcs of G_k
nbh_{jk}	the neighborhood of an instance ι_{jk} in \mathcal{I}_k
out_nbh_{jk}	the instances connected to ι_{jk} through an outgoing arc
in_nbh_{jk}	the instances connected to ι_{jk} through an incoming arc
$tranSet_{jq_k}$	the set of the transactions from ι_{jk} to ι_{q_k}
$T_{jq_k t}$	a transaction of the set $tranSet_{jq_k}$
$reposted_{jk}$	the set of the transactions received by ι_{jk} and reposted by it
$elaborated_{jk}$	the set of the transactions received by ι_{jk} and whose contents it elaborated for its purposes
$requested_{jk}$	the set of the transactions explicitly requested by ι_{q_k}
PD_{jk}	the proactivity degree of an instance ι_{jk}
π_{jq_k}	the minimum path from an instance ι_{jk} to an instance ι_{q_k}
InD_{jk}	the Inactivity Degree of an instance ι_{jk}
TD_{jq_k}	the Trust Degree of ι_{q_k} in ι_{q_k}
NID_{jk}	the Naive Impact Degree of an instance ι_{jk}
RID_{jk}	the Refined Impact Degree of an instance ι_{jk}
NS	Naive Scope
RS	Refined Scope

Table 2: Main abbreviations used throughout this paper

typical of social networks in the IoT scenario. Clearly, in doing this, we must consider that not all the human behaviors can be “transferred” to smart objects. For instance, while it is possible to model transactions through which smart objects can exchange contents with each other, it is still premature the idea that objects have so much autonomy and reasoning capabilities that they can make decisions about sharing and commenting a content or, even, answering a comment. Probably, the advances in Artificial Intelligence we are assisting to, coupled with the increasingly enhanced processing capabilities of smart objects, will make these characteristics feasible in the future. MIoT can be seen as a first step towards this direction. As far as this fact, we observe that, in past literature, the most advanced attempt to provide smart objects with social features is represented by the SIoT model [2]. However, as pointed out in Section 2, only five simple social relationships among smart objects are possible in this paradigm. Furthermore, these relationships are static, i.e., they have been defined by the authors once and for all. If compared with the SIoT model, the MIoT paradigm captures different aspects. Indeed, it considers the contents exchanged by smart objects during their transactions. As a consequence, it is focused on data-driven and semantic-based aspects and not on technological ones, which are those of reference for SIoT.

In this section, we reported only those aspects of MIoT necessary for this paper. The interested reader can find all details about this paradigm in [6].

4 Scope definition

In this section, we present the definition of the scope of an instance ι_{jk} in an IoT \mathcal{I}_k and the scope of an object o_j in a MIoT \mathcal{M} . For this purpose, we must introduce some preliminary concepts. They are also reported in Table 2.

The first of them regards the *Proactivity Degree* PD_{jk} of an instance ι_{jk} in an IoT \mathcal{I}_k . PD_{jk} ranges in the real interval $[0, 1]$ and is set equal to the fraction of the transactions received by ι_{jk} that it reposts to another instance of \mathcal{I}_k or whose contents it elaborates for its purposes.

To formalize this concept, we must introduce:

- the set $reposted_{j_k}$ of the transactions received by ι_{j_k} and reposted by it;
- the set $elaborated_{j_k}$ of the transactions received by ι_{j_k} and whose contents it elaborated for its purposes.

PD_{j_k} can be formalized as follows:

$$PD_{j_k} = \frac{|tranSet_{j_k} \cap (reposted_{j_k} \cup elaborated_{j_k})|}{|tranSet_{j_k}|}$$

Now, we need to introduce the neighborhood of level t of an instance ι_{j_k} in its IoT \mathcal{I}_k . It is an extension of the concept of $out_nbh_{j_k}$ presented in Section 3. It is defined as follows:

$$out_nbh_{j_k}^t = \begin{cases} out_nbh_{j_k} & \text{if } t = 0 \\ \{\iota_{r_k} | \iota_{r_k} \in out_nbh_{q_k}, \iota_{q_k} \in out_nbh_{j_k}^{t-1}, \iota_{r_k} \notin out_nbh_{j_k}^w, 0 \leq w < t\} & \text{if } t > 0 \end{cases}$$

The concept of $out_nbh_{j_k}^t$ will be extremely important later. In the meantime, we introduce a new concept, namely the minimum path π_{jq_k} from an instance ι_{j_k} to an instance $\iota_{q_k} \in out_nbh_{j_k}^t$. π_{jq_k} is defined as the sequence of instances $\{\iota_{0_k}, \iota_{1_k}, \dots, \iota_{t_k}\}$ such that $\iota_{0_k} = \iota_{j_k}$, $\iota_{t_k} = \iota_{q_k}$, $\iota_{w_k} \in out_nbh_{(w-1)_k}$ for $1 \leq w \leq t$.

Afterwards, we introduce the definition of the *Trust Degree* TD_{jq_k} of an instance ι_{q_k} in the instance ι_{j_k} in \mathcal{I}_k . It can be defined as the fraction of the transactions sent by ι_{j_k} to ι_{q_k} that have been requested by ι_{q_k} or that ι_{q_k} has considered so interesting to repost or elaborate them³. In order to formalize TD_{jq_k} , we must preliminarily introduce the set $requested_{q_k}$ of the transactions explicitly requested by ι_{q_k} . Now, TD_{jq_k} can be expressed as:

$$TD_{jq_k} = \frac{|tranSet_{jq_k} \cap (requested_{q_k} \cup reposted_{q_k} \cup elaborated_{q_k})|}{|tranSet_{jq_k}|}$$

Starting from this definition and the concepts of $out_nbh_{j_k}^t$ and π_{jq_k} , we can proceed with the transitive closure of TD_{jq_k} . In particular, the general definition of TD_{jq_k} is as follows:

$$TD_{jq_k} = \begin{cases} \frac{|tranSet_{jq_k} \cap (requested_{q_k} \cup reposted_{q_k} \cup elaborated_{q_k})|}{|tranSet_{jq_k}|} & \text{if } \iota_{q_k} \in out_nbh_{j_k} \\ \prod_{w=1}^t TD_{((w-1)w)_k} & \text{if } \iota_{q_k} \in out_nbh_{j_k}^t, t > 0, \pi_{jq_k} = \{\iota_{0_k}, \iota_{1_k}, \dots, \iota_{t_k}\} \end{cases}$$

Intuitively, the Trust Degree TD_{jq_k} of ι_{q_k} is given by the base formula if ι_{q_k} is directly connected to ι_{j_k} ; otherwise, it is obtained by the product of the trust degrees associated with the pairs of instances belonging to the minimum path from ι_{j_k} to ι_{q_k} .

The next step regards the definition of the concept of Impact Degree of an instance ι_{j_k} in \mathcal{I}_k . Actually, we can define two forms of Impact Degree. The first one is simple and immediate to compute; we call it *Naive Impact Degree* (hereafter, NID). The second one is more accurate and precise, even if computationally more expensive; we call it *Refined Impact Degree* (hereafter, RID).

³Clearly, it might happen that an unrequested transaction of $tranSet_{jq_k}$ is not considered interesting by ι_{q_k} . In this case, ι_{q_k} neither posts nor elaborates it.

We start by introducing the Naive Impact Degree NID_{j_k} of ι_{j_k} in \mathcal{I}_k . It is defined as the average of the Trust Degrees that all the instances belonging to $out_nbh_{j_k}$ have in ι_{j_k} . It can be formalized as follows:

$$NID_{j_k} = \frac{\sum_{\iota_{q_k} \in out_nbh_{j_k}} TD_{qj_k}}{|out_nbh_{j_k}|}$$

After having defined the Naive Impact Degree, we can introduce the Refined Impact Degree. Its definition is based on the following considerations:

- (C₁) Given an instance ι_{j_k} , the higher the number of transaction requests received by the other instances of \mathcal{I}_k , the higher its RID.
- (C₂) Given an instance ι_{j_k} , the higher its capability of leading an instance ι_{q_k} with a low proactivity degree to send one of its transactions to a further instance of \mathcal{I}_k , the higher its RID.
- (C₃) Given an instance ι_{j_k} , the higher its capability of receiving a transaction sent by an instance ι_{r_k} with a low proactivity degree, the higher its RID.
- (C₄) Given an instance ι_{j_k} , the higher its capability of leading an instance ι_{q_k} with a high RID to repost its transactions, the higher its RID.

Observe that Consideration C_4 is very complex to handle because it implies that the RID of an instance ι_{j_k} depends on the RID of an instance ι_{q_k} . This means that, for the computation of the instance RIDs, it would be necessary to solve (at least in the most complex case) huge systems, characterized by hundreds, or even thousands, of equations and variables. As a consequence, the computation of RID appears difficult to handle without a heuristic. Taking this consideration into account, we have defined a heuristic for the computation of RID. In particular, we consider the NID of ι_{q_k} , instead of the RID of this instance, in the computation of the RID of ι_{j_k} .

Taking Considerations (C₁) - (C₄) into account, RID_{j_k} can be defined as:

$$RID_{j_k} = \frac{\alpha \cdot RID1_{j_k} + \beta \cdot RID2_{j_k} + \gamma \cdot RID3_{j_k} + \delta \cdot RID4_{j_k}}{\alpha + \beta + \gamma + \delta}$$

In other words, RID_{j_k} is obtained as a weighted mean of four components, each formalizing one of the considerations presented above.

$RID1_{j_k}$ is associated with Consideration C_1 . It is defined as follows:

$$RID1_{j_k} = \frac{|reqTranSet_{j_k}|}{maxCardReqTranSet_k}$$

Here:

- $reqTranSet_{j_k}$ is the set of the transactions from ι_{j_k} to any instance of \mathcal{I}_k originated after a specific request:

$$reqTranSet_{j_k} = \bigcup_{\iota_{j_k} \in out_nbh_{q_k}} reqTranSet_{jq_k}$$

In the previous formula, $reqTranSet_{jq_k}$ is the set of the transactions from ι_{j_k} to ι_{q_k} originated after a specific request of ι_{q_k} :

$$reqTranSet_{jq_k} = \{T_{jq_{k_t}} | T_{jq_{k_t}} \in tranSet_{jq_k}, req_{jq_{k_t}} = true\}$$

- $maxCardReqTranSet_k = max_{\iota_{j_k} \in \mathcal{I}_k} |reqTranSet_{j_k}|$.

$RID2_{j_k}$ is related to C_2 . It is defined as follows:

$$RID2_{j_k} = \frac{\sum_{\iota_{q_k} \in out_nbh_{j_k}} \frac{InD_{q_k}}{InD_k^{max}} \cdot \frac{|tranSet_{jq_k} \cup reposted_{q_k}|}{|tranSet_{jq_k}|}}{|out_nbh_{j_k}|}$$

Here:

- InD_{q_k} is the *Inactivity Degree* of ι_{q_k} and is defined as $InD_{q_k} = 1 - PD_{q_k}$;
- InD_k^{max} is the maximum Inactivity Degree of an instance of \mathcal{I}_k .

$RID3_{j_k}$ is associated with C_3 . It can be defined as follows:

$$RID3_{j_k} = \frac{\sum_{\iota_{r_k} \in in_nbh_{j_k}} \frac{InD_{r_k}}{InD_k^{max}} \cdot \frac{|tranSet_{rj_k}|}{|tranSet_{r_k}|}}{|in_nbh_{j_k}|}$$

Finally, $RID4_{j_k}$ is related to C_4 . Taking into account the aforementioned reasoning about the need to simplify its computation by substituting RID_{j_k} with NID_{j_k} , it can be defined as follows:

$$RID4_{j_k} = \frac{\sum_{\iota_{q_k} \in out_nbh_{j_k}} \frac{NID_{q_k}}{NID_k^{max}} \cdot \frac{|tranSet_{jq_k} \cup reposted_{q_k}|}{|tranSet_{jq_k}|}}{|out_nbh_{j_k}|}$$

Here, $NID_{j_k}^{max}$ is the maximum Naive Impact Degree of an instance of \mathcal{I}_k .

Having defined the Naive and the Refined Impact Degree, we have almost all parameters necessary to define the Naive and the Refined Scope. Indeed, we need to define only a last one. It is the *Security Requirement Degree* SRD_{qj_k} and takes the level of the security tightness of ι_{j_k} and ι_{q_k} into account. In particular, it is defined as:

$$SRD_{qj_k} = \min\left(1, \frac{\lambda_{j_k}}{\lambda_{q_k}}\right)$$

The rationale underlying this formula is as follows: as we will see later, SRD_{qj_k} contributes, along with TD_{qj_k} , to weight the Impact Degree that ι_{j_k} has on ι_{q_k} . If $\lambda_{j_k} < \lambda_{q_k}$ then the Security Level of ι_{q_k} is tighter than the one of ι_{j_k} ; this condition represents an obstacle to the propagation of the contents of ι_{j_k} towards ι_{q_k} . Vice versa, if $\lambda_{j_k} \geq \lambda_{q_k}$ then the Security Level of ι_{j_k} is higher than or equal to the one of ι_{q_k} . This implies that, from the security viewpoint, there is no obstacle for the propagation of the contents of ι_{j_k} towards ι_{q_k} .

Observe that, if an instance ι_{j_k} has a high Security Level λ_{j_k} (for instance, $\lambda_{j_k} = 5$), then SRD_{qj_k} is high; as a consequence, ι_{j_k} can propagate all its contents towards the other instances. This because

having a high Security Level means being highly secure or, in other words, having highly verified contents. This represents a pass for the other instances that trust to receive content sent by ι_{jk} . Therefore, in this sense, having a high Security Level makes it easy having a high scope.

We are now able to define the *Naive Scope* NS_{jk}^t (resp., the *Refined Scope* RS_{jk}^t) of level t of an instance ι_{jk} in \mathcal{I}_k . It is obtained as the weighted sum of the Naive Impact Degrees (resp., Refined Impact Degrees) of the instances belonging to $out_nbh_{jk}^t$, where the weights are the trust and the security values that these instances have in ι_{jk} . This sum is, then, averaged by the number of instances belonging to $out_nbh_{jk}^t$. Formally speaking:

$$NS_{jk}^t = \frac{\sum_{\iota_{qk} \in out_nbh_{jk}^t} TD_{qjk} \cdot NID_{qk} \cdot SRD_{qjk}}{|out_nbh_{jk}^t|} \quad RS_{jk}^t = \frac{\sum_{\iota_{qk} \in out_nbh_{jk}^t} TD_{qjk} \cdot RID_{qk} \cdot SRD_{qjk}}{|out_nbh_{jk}^t|}$$

Now, we can define the *Naive Scope* NS_j^t (resp., the *Refined Scope* RS_j^t) of level t of an object o_j in the MIoT. It is obtained by averaging the Naive Scopes (resp., the Refined Scopes) of level t of its instances in the corresponding IoT. Specifically, let $Inst_j = \{\iota_{j1}, \iota_{j2}, \dots, \iota_{ji}\}$ be the instances of o_j in the IoT of the MIoT. Then:

$$NS_j^t = \frac{\sum_{\iota_{jk} \in Inst_j} NS_{jk}^t}{|Inst_j|} \quad RS_j^t = \frac{\sum_{\iota_{jk} \in Inst_j} RS_{jk}^t}{|Inst_j|}$$

4.1 Discussion

After having provided a formalization of Naive and Refined Scope, we now present some considerations that highlight the connection between the formalized concepts and the general definition of scope. In this discussion, we mainly focus on Refined Scope, because this is the most advanced definition. We observe that our formalization of Refined Scope makes it holistic, allowing it to take a large variety of aspects into consideration. As a matter of fact, the Refined Scope of an instance ι_{jk} considers the trust that the other instances of \mathcal{I}_k have on it, the impact exerted by it on the other nodes and the tightness and the severity of its security requirements. In turn, the impact of ι_{jk} considers its capability of receiving transaction requests from the other instances of \mathcal{I}_k and its ability to stimulate them to deliver its contents. The overall set of these features is well suited to model, in the multiple IoT scenario, the concept of scope intended as “the extent of the area or subject matter that something deals with or to which it is relevant”, as reported in the Concise Oxford Dictionary.

Even if scope may seem similar to context-awareness at a first sight, it actually presents important differences. Indeed, context-awareness in IoT is defined as any implicit or explicit information – current location, identity, activity, and physical condition – about the involved service stakeholders [44, 9]. By contrast, Refined Scope is a data-driven and transaction-oriented concept, dealing with the contents exchanged among nodes and not with physical aspects.

Finally, observe that Refined Scope also handles privacy aspects, even if indirectly, thanks to the usage of the concepts of trust and security. As a matter of fact, in several scenarios, it is possible to find a certain correlation between trust and privacy in that the higher the trust, the higher the availability to exchange information. Analogously, the higher the Security Level of an instance, the higher its reliability and the higher the interactions and information exchange stimulated by it.

At a first glance, some of the concepts, and especially some of the activities, described above could appear far away from the IoT context. Think, for instance, of the concept of proactivity of a smart object and of the posting and elaborating activities. Actually, especially in the SIoT context, several models proposing concepts and activities similar to ours have been presented in recent literature. Indeed, one of these models is described in [23], where the authors discuss the Adaptive Interest Forward strategy. Some of the ideas underlying this strategy are close to the Considerations $C_1 - C_4$ representing the bases for the definition of the RID parameter in Section 4. In fact, in [23], the authors take two kinds of device into account, namely high- and low-capability devices⁴. The Adaptive Interest Forwarding strategy proceeds by prioritizing forwarding tasks from the node with the highest capabilities, while constrained nodes can transmit only if they do not overhear packet transmission from their neighbors.

Even if the two policies leading smart objects to transmit are different, it is possible to observe a parallelism between them. In fact, being proactive and able to stimulate the interest in the information sent through a transaction plays, in our approach, the same role as having capabilities in the approach of [23].

Actually, the parallelism is even closer. Indeed, we recognize a high similarity between:

- the situation in our approach where a smart object must decide whether or not reposting (intended as forwarding to other linked smart objects) a transaction received from another smart object, and
- the situation in the approach of [23] where an Information Centric Networking (hereafter, ICN) node receiving an Interest must decide whether or not forwarding it towards the producer.

In the same way, we can recognize a high similarity between:

- the situation in our approach where a smart object decides to elaborate the content of a transaction (which could mean, for instance, selecting a part of a text or reducing the quality or the length of a video before reposting it), and
- the situation in the approach of [23] where an ICN receiving an Interest can decide to cache the content and send it according to an Adaptive Interest Forwarding strategy considering the status of node resources.

5 Application scenarios

In a scenario characterized by the pervasive diffusion of increasingly intelligent and social objects, our approach for the computation of scope can have a large variety of applications. To give an idea of real cases that can benefit from our approach, in the next subsections, we examine two of them.

⁴For the sake of clarity, we outline that the capability considered in [23] regards mainly energy and storage.

5.1 Scope for smart cities

As a first example case, consider some public areas (such as parks, squares, shopping centers, etc.) in a (smart) city, and assume that a group of people actively visits these areas. Each area is equipped with several smart objects for monitoring weather, air quality, traffic conditions, level of noise, etc., along with several actuators, such as smart lamps or information hubs provided as online services. Each person may have several smart devices, such as smartwatches, smartphones, other wearable devices, and so forth. People and places can interact with each other through their smart objects [10].

Such a scenario can be modeled through a MIoT \mathcal{M} consisting of a set $\{\mathcal{I}_1, \mathcal{I}_2, \dots, \mathcal{I}_m\}$ of IoT, each representing a public area. The set of the objects of \mathcal{M} comprises the smart objects in the public areas and the set of personal devices of people visiting them. If an object o_j of the MIoT is active in the k^{th} public area, it has an instance ι_{jk} in the IoT \mathcal{I}_k . Clearly, when a person with a smart object o_j moves around different public areas corresponding to different IoT, o_j will have different instances, one for each IoT.

Each visitor of an area is generally interested in a certain kind of activity; for instance, she could be a fitness runner. The final goal of the MIoT is supporting people to get the best experience from their activities. In this setting, scope can play a key role in reaching this objective. In the following, we report some possible usage scenarios.

Assume that a person wants to go out for a run. First, she needs to choose the best area for the run, based on weather conditions, traffic and other parameters that she considers relevant. To carry out her choices, she can contact, through her device, the sensors of each public area of her interest, the information hubs and the devices of other trusted runners in order to ask for weather, traffic and other conditions. The choice of the information sources to consult is usually related to the corresponding trustworthiness and the easiness of getting the desired information from it. These two properties are clearly strictly correlated to the scope of the source; indeed, this scope can be seen as a “summary” of these two parameters and some other related ones, such as accuracy, reputation, impact, etc. Once a person has performed her choice, she can decide to send this information to the MIoT in such a way as to serve, in her turn, as information provider for the community.

A similar activity flow may happen in several other circumstances in which there is a decision to make, e.g., when a user must choose the best shopping center where she can buy a given object, the best cinema where she can see a movie, etc.

In all these cases, data regarding the choices of a user can be coupled with those registered during the activities she performed as a consequence of these choices (e.g., data coming from personal smartwears) in such a way as to confirm the correctness of the choice or, on the contrary, to alert the other users of the evaluation errors. For instance, imagine a scenario in which a person verifies that the weather was actually too cold for the clothes she had selected (interestingly, this information could be automatically detected and sent by the sensors present in her smartwears). In this case, the scope of the smartwears is useful to understand how extended and how strong is their capability of influencing the decision of the other users. In other words, the scope of an object o_j in this scenario determines how many users are impacted by the data sent by it and how much strong this impact is.

It is worth pointing out the relevance of the scope in this context. As a matter of fact, the knowledge of the objects with the highest impacts in the MIoT allows the improvement of the efficiency and the

effectiveness of the information disseminated through the network. At a higher abstraction level, some smart objects of the MIIoT could assume the role of reliable information hubs for the whole MIIoT if their scope is particularly high and extended.

Recall that scope depends not only on the Impact Degree but also on Trust Degree and Security Level. According to the definitions of Naive and Refined Scope in Section 4, a high value of scope (which is a condition for being an information hub) can be obtained only if all the three parameters defining the scope (i.e., impact, trust and security) are high.

Scope may also have an important role in the detection and the management of possible anomalies characterizing one or more devices in the network. As an example, assume that a weather sensor in a public area is malfunctioning; in this case, all the objects relying on its data will be affected by this anomaly. Knowing the scope of an object may help in the detection and management of its possible anomalies. For instance, in the previous case, if one or more other trustworthy weather devices are present in the same area, they could help the whole MIIoT to determine the sensor malfunction, to avoid the propagation of its effects and, finally, to repair the anomalous device.

5.2 Scope for shopping centers

Another possible scenario where scope plays an important role is a big shopping center consisting of several buildings, each dedicated to specific product typologies, such as food, clothing, do-it-yourself, electronic devices, and so on. In this context, smart devices can be modeled by a MIIoT \mathcal{M} consisting of m IoT, one for each building. The set of the objects of \mathcal{M} consists of the set of the intelligent sensors present in each building (including video surveillance, temperature sensors, fire sensors, presence sensors, etc.) and the set of personal devices of visitors (including smartphones, tablets, smartwatches, etc.).

Each object o_j that interacts with the ones of the k^{th} building has an instance ι_{j_k} representing it in \mathcal{I}_k . Clearly, when the owner of an object o_j , such as a smartphone, moves throughout the buildings of the shopping centers, o_j will have different instances associated with the different buildings of the center.

Here, an intelligent system of the shopping center could push offers to the enabled customer devices based on proximity, past preferences, habits, and so on. Analogously, a personal device can suggest its owner the most comfortable and promising places to visit during her stay in the shopping center based on the knowledge provided by the smart objects and the sensors dispersed in the shopping center.

In this scenario, each person connected to the MIIoT is interested in a certain kind of activity, somehow related to shopping. Indeed, users can play several roles ranging from vendors, suppliers or customers. In this context, an innovative role is the one of the personal shopper, i.e., a person, who helps customers by giving them alerts or making them suggestions. Personal shoppers are often employed directly by stores and boutiques, but the number of freelancers or online personal shoppers is constantly growing.

While a customer visits the building of a shopping center, her device may constantly locate the nearest devices and query for interesting products or offers. In the meantime, it could query other objects of the customer (for instance, wearable devices) to measure her vital parameters in order to evaluate her pleasure in checking the products of a shopper. This can represent feedback information

that the device supplies to the MIoT. Furthermore, it can act as a personal shopper. Indeed, it interacts with the other objects of the MIoT, considers the offers of the shops, elaborates this information through machine learning algorithms, makes some proposals to its customer, registers her feedbacks and transmits them to the other devices in such a way as to improve the quality of its recommendations.

Assume, now, that a customer wants to go out for shopping. First, she needs to locate the best building to start with. This activity can be carried out by contacting the preferred personal shopper or by checking the preferred destinations of “special” customers (for instance, the most influential ones) or, again, by detecting the most comfortable shops. All these activities can be done by her personal device that can contact the other ones of the MIoT for acquiring all necessary data. Once the desired knowledge has been obtained, the device can process it to make its suggestions. Clearly, once the customer has made her choices and has performed her shopping activities, she can share information about her experience. In this way, she and/or her devices can become information providers for other customers. Scope plays an important role in this scenario. Indeed, the scope of each smart object determines how many devices (and, ultimately, people) it can influence and how strong its influence is.

Again, this depends on its Impact Degree, its Trust Degree and its Security Level. The higher each of these parameters, the higher the corresponding scope and, consequently, the stronger its influence.

As in the previous scenario, an important issue to investigate and address is the presence of possible anomalies. The impact of an anomaly depends on several factors; the scope of the affected objects is certainly one of the most important. As an example, given an anomaly of the device acting as a personal shopper, for instance the loss of historical data on product prices, the corresponding suggestions might not be the most convenient ones for its owner. In this case, the anomaly will certainly have a high impact on the device’s owner. Furthermore, it can have an impact, even if smaller, on all the other objects (and, ultimately, on the corresponding customers) that it can reach and influence. The extension and the strength of the impact of an object o_j on a object o_q depends on the value of the scope of o_j on o_q .

Assume, now, that an anomaly affects the system for the temperature detection of a building or, even, of the whole shopping center. Clearly, the scope of this system is much larger and stronger than the one of a personal device. Indeed, this anomaly impacts on all the customers present in the building or, even, in the shopping center because, due to it, the air conditioning system will determine an uncomfortable situation for all the people present therein. This last example allows us to draw a further conclusion, i.e., knowing the scope of the devices of a MIoT is also relevant to properly prioritize anomaly management.

6 Experiments

In this section, we present the experiments we carried out to evaluate the performance of our approach from several viewpoints. Specifically, we describe our testbed in Subsection 6.1. In Subsection 6.2, we investigate the variation of Naive and Refined Scope against the increase of the neighborhood level for instances and objects. In Subsection 6.3, we analyze the possible relationships between the scope and the most known forms of centrality. In Subsection 6.4, we compare the Naive and Refined Scope to determine their strengths and their weaknesses. In Subsection 6.5, we investigate the possible

relationships between the scope and the MIoT density. Finally, in Subsection 6.6, we compare scope with two related concepts (i.e., diffusion degree and influence degree) and approaches described in Section 2.

6.1 Adopted Testbed

In order to perform our experiments, as real MIoT with the dimension and the variety handled by our model do not exist yet, we constructed a MIoT simulator. This tool starts from real data and returns simulated MIoT with certain characteristics specified by the user.

The MIoT created by our simulator follow the paradigm described in Section 3. Our simulator is also provided with a suitable interface allowing a user to “personalize” the MIoT to build by specifying the desired values for several parameters, such as the number of nodes, the maximum number of instances of an object, and so forth.

To make “concrete” and “plausible” the simulated MIoT, we had the necessity that our simulator was capable of returning MIoT having the characteristics specified by the user and being as close as possible to real-world scenarios. In the simulator design, and in the next construction of the MIoT to use for the experiments, we followed the ideas expressed in [3, 4], in which the authors highlight that one of the main factors used to build links in an IoT is node proximity. In order to reproduce the creation of links among objects, we decided to leverage information about real-life paths in a city. In fact, having this information at disposal, we may associate each path with an object and link two objects if their paths have been near enough for a sufficient time period. As for a dataset containing real-life paths in a city, we selected the one reported in <http://www.geolink.pt/ecmplpkdd2015-challenge/dataset.html>. It regards taxi routes in the city of Porto from July 1st 2013 to June 30th 2014. Each route contains several Points of Interests corresponding to the GPS coordinates of the vehicles. As said above, our simulator associates an object with a given route recorded in the dataset. Furthermore, it creates an arc between two nodes if the distance between the corresponding routes is less than a certain threshold th_d for a predefined time interval th_t . The value of th_d and th_t can be specified through the constructor interface. Clearly, the higher the value of th_d and the lower the value of th_t , the more connected the constructed MIoT. The interested reader can find the MIoT created in this phase at the address <http://daisy.dii.univpm.it/miot/datasets/scope>. This MIoT consists of 1256 nodes. The six IoT of the MIoT had 128, 362, 224, 280, 98, and 164 nodes, respectively. The constructed MIoT is returned in a format that can be directly processed by the cypher-shell of Neo4J.

We carried out all the tests presented in this section on a server equipped with an Intel I7 Quad Core 7700 HQ processor and 16 GB of RAM with the Ubuntu 16.04 operating system. To implement our approach, we adopted (i) Python, as programming language, and (ii) Neo4J (Version 3.4.5), as underlying DBMS. In Figure 2, we report the activity diagram describing the various tasks performed by our MIoT simulator, along with the underlying logic. Furthermore, the code of our simulator is open source; the interested reader can access it at the address: <https://github.com/lucav48/miot-simulator>.

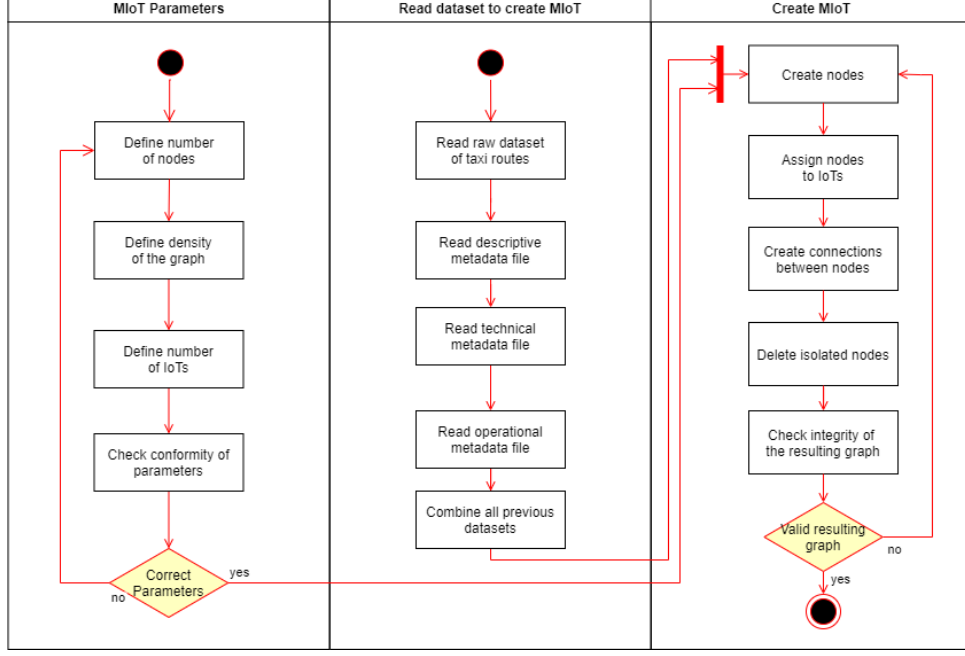


Figure 2: Activity diagram of our MIoT simulator

6.2 Variation of the scope against the neighborhood level

In this experiment, we aimed at investigating the trend of the Naive Scope (hereafter, NS) and the Refined Scope (hereafter, RS) against the neighborhood level t (see Section 3). In particular, for each instance ι_{j_k} of the MIoT, we computed $NS_{j_k}^t$ and $RS_{j_k}^t$ when t increases from 1 to the diameter of \mathcal{I}_k . After this, we grouped the instances of our MIoT into clusters, based on some specific rationales, and we computed the variation of the average values of NS and RS for each group.

As a first task of this activity, we computed the variation of the average values of NS and RS for each IoT of the MIoT. This is equivalent to say that clusters coincided with IoT. The results obtained are reported in Figure 3. From the analysis of this figure, we can observe that, in each IoT, the values of NS and RS decrease quite quickly. As for NS, its value is extremely high when $t = 1$ in all the IoT. When $t = 2$, the value of NS is high for the largest IoT, whereas it is intermediate for the other ones. In any case, the values of NS become very low when t is greater than 3 for small IoT and when t is greater than 4 for large ones. As for RS, its trend against t is analogous to the one of NS. However, RS appears more capable than NS in distinguishing the neighborhoods with a high scope from those with a low one. In fact, in Figure 3, we can observe that the decrease from the high values of scope to the low ones is much steeper in RS than in NS. In our opinion, the capability of clearly discriminating the neighborhoods with high values of scope from the ones with low values of this parameter is an important feature for an approach aiming at formalizing the concept of scope.

As a second task, we computed the variation of the average values of NS and RS for the whole MIoT. This is equivalent to say that we had a unique cluster coinciding with the MIoT. The results obtained are reported in Figure 4. From the analysis of this figure, we can conclude that NS (resp., RS) presents a trend similar to the one shown by it in the largest IoT of Figure 3. In particular,

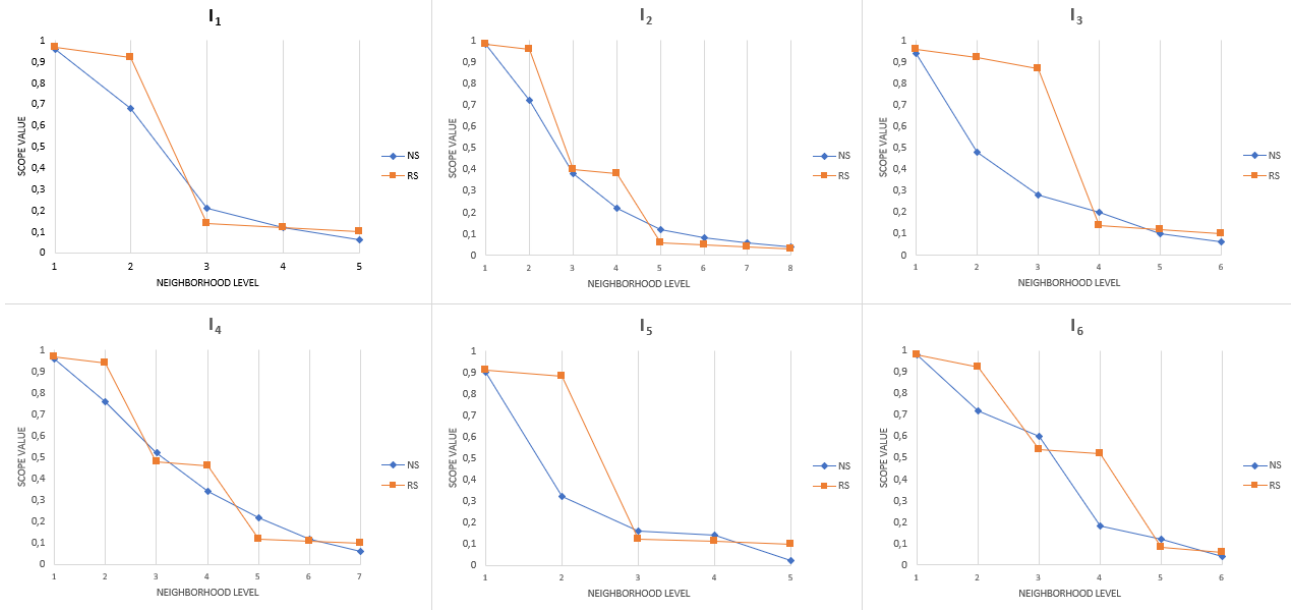


Figure 3: Variation of the average values of NS and RS for each IoT of the MIoT against the neighborhood level

NS is very high for $t = 1$; it is high for $t = 2$; it has an intermediate value for $t = 3$, whereas it is low for $t > 5$. Instead, RS presents high values for $t = 1$ or $t = 2$; it shows intermediate values for $t = 3$ and $t = 4$ and low values for $t \geq 5$. Again, RS is more capable than NS in discriminating the neighborhoods with a high value of scope from the ones characterized by an intermediate value of this parameter, and these last ones from the neighborhoods where RS has low values.

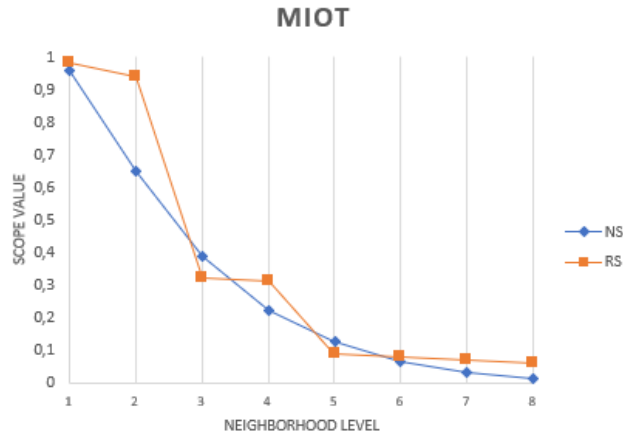


Figure 4: Variation of the average values of NS and RS for the whole MIoT against the neighborhood level

As a final task, we grouped the available instances in two clusters containing c-nodes and i-nodes, respectively. Then, we computed the variation of the average values of NS and RS for the two clusters.

The final goal of this task was to verify if i-nodes and c-nodes had different behaviors as far as their value of scope was concerned. The results obtained are reported in Figure 5. From the analysis of this figure we can observe that the values of NS decrease for both i-nodes and c-nodes. However, the corresponding trends are different. Indeed, the decrease is much smoother for i-nodes than for c-nodes. In particular, as for c-nodes, the decrease is very steep because the scope is less than 0.2 already for $t = 3$. As for RS, its trend for c-nodes is steeper than the one of NS; again, RS is more capable than NS in discriminating the neighborhoods with high, intermediate and low values of scope. Instead, the trend of RS for c-nodes is very similar to the corresponding trend of NS. Actually, this could have been expected because the trend of scope for NS was already very steep. The different trends of the values of scope for i-nodes and c-nodes can be explained by considering that, analogously to what was made in all the past approaches, our definition of neighborhood (which plays a key role in our definition of scope) considers as neighbors of a node only other nodes of the same IoT. In other words, it takes only i-arcs into account. Actually, we believe (and the results of Figure 5 confirm our belief) that it is worthwhile to investigate the role of c-arcs in the computation of the neighborhood of a node, and we plan to make this investigation in the future.

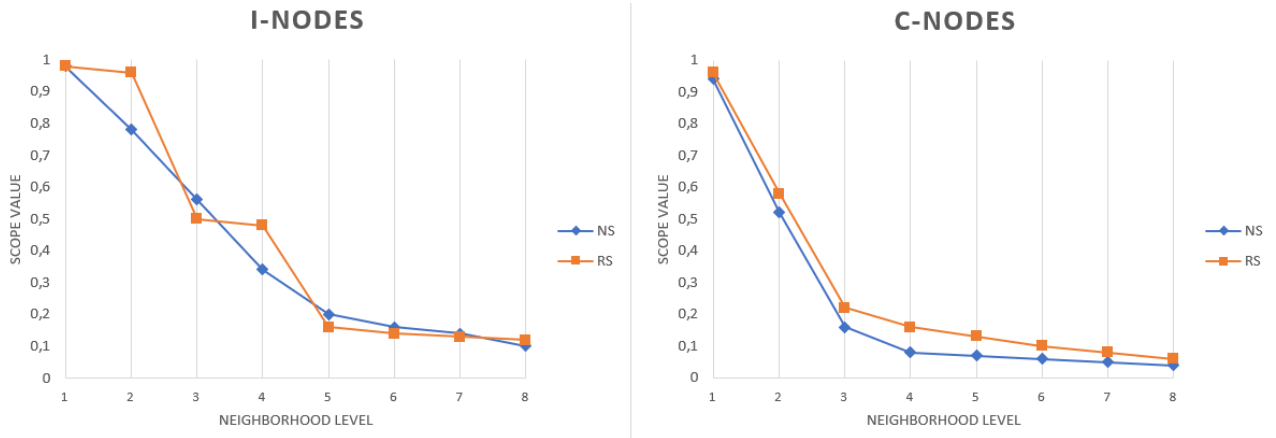


Figure 5: Variation of the average values of NS and RS for the i-nodes and the c-nodes of the MIoT against the neighborhood level

As for the analysis of the values of NS and RS for objects, we observe that they are obtained by averaging the values of NS and RS of the corresponding instances. As a consequence, it does not make sense to perform the first and the final tasks of the previous activity. The only task that makes sense is the second one; in this case, the variation of the average values of NS and RS for the whole MIoT is reported in Figure 6.

As we could have expected, this trend is very similar (or, better, almost identical) to the one of Figure 4. This was not surprising for us; indeed, the value of NS and RS of an object is obtained by averaging the values of NS and RS of the corresponding instances. Therefore, it was to be expected that the trends of NS and RS for objects could not have been very different from the ones of NS and RS for instances.

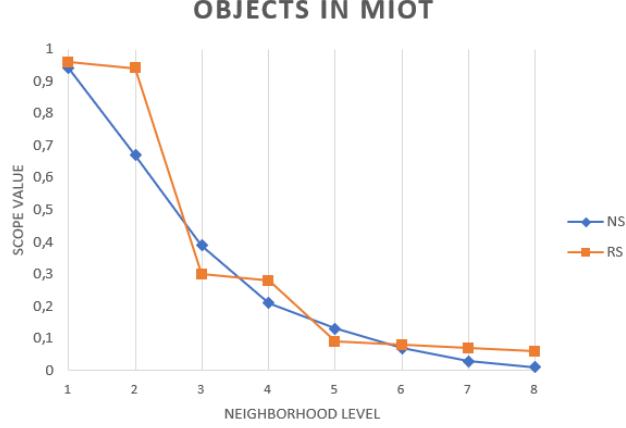


Figure 6: Variation of the average values of NS and RS for the objects of the MIoT against the neighborhood level

6.3 Relationship between scope and centrality

In this second experiment, we aimed at investigating the relationships possibly existing between the scope and the main forms of centrality already considered in the literature. For this purpose, first we computed the degree, the closeness, the betweenness and the eigenvector centralities of all the instances of the MIoT. Then, we constructed the cluster \mathcal{D} (resp., \mathcal{C} , \mathcal{B} and \mathcal{E}) containing the 100 instances having the highest values of the degree (resp., closeness, betweenness and eigenvector) centrality. Finally, we computed the variation of the average values of NS and RS against the neighborhood level for the four groups. The results obtained are reported in Figure 7.

From the analysis of this figure, we can draw very interesting considerations. Preliminarily, we observe that this experiment confirms the results of the previous one on the fact that RS is more capable than NS in distinguishing neighborhoods with high, intermediate and low values of scope. We can also observe that:

- The nodes with a high degree centrality present a very high value of scope in their closest neighborhoods, i.e., when $t = 1$. Already for $t = 2$ we observe a steep decay of scope. This parameter becomes very low for $t = 3$ and further decreases for $t \geq 4$. This trend can be explained by considering that degree centrality privileges nodes with a high number of outgoing arcs, which, thanks to this property, can easily have a high impact on their immediate neighbors. However, it is not guaranteed that the neighbors of the nodes with a high degree centrality have, in their turn, a high degree centrality. Rather, this does not generally happen because degree centrality follows a power law distribution, which implies that most of the nodes in the network have a low value of this parameter. As a consequence, already for $t = 2$, the value of scope rapidly decreases.
- The nodes with high values of closeness and/or betweenness centrality present high values of scope for $t = 1$. When t increases, the scope decays; however, this happens smoothly. This trend can be explained by considering that closeness and betweenness centralities privilege nodes that

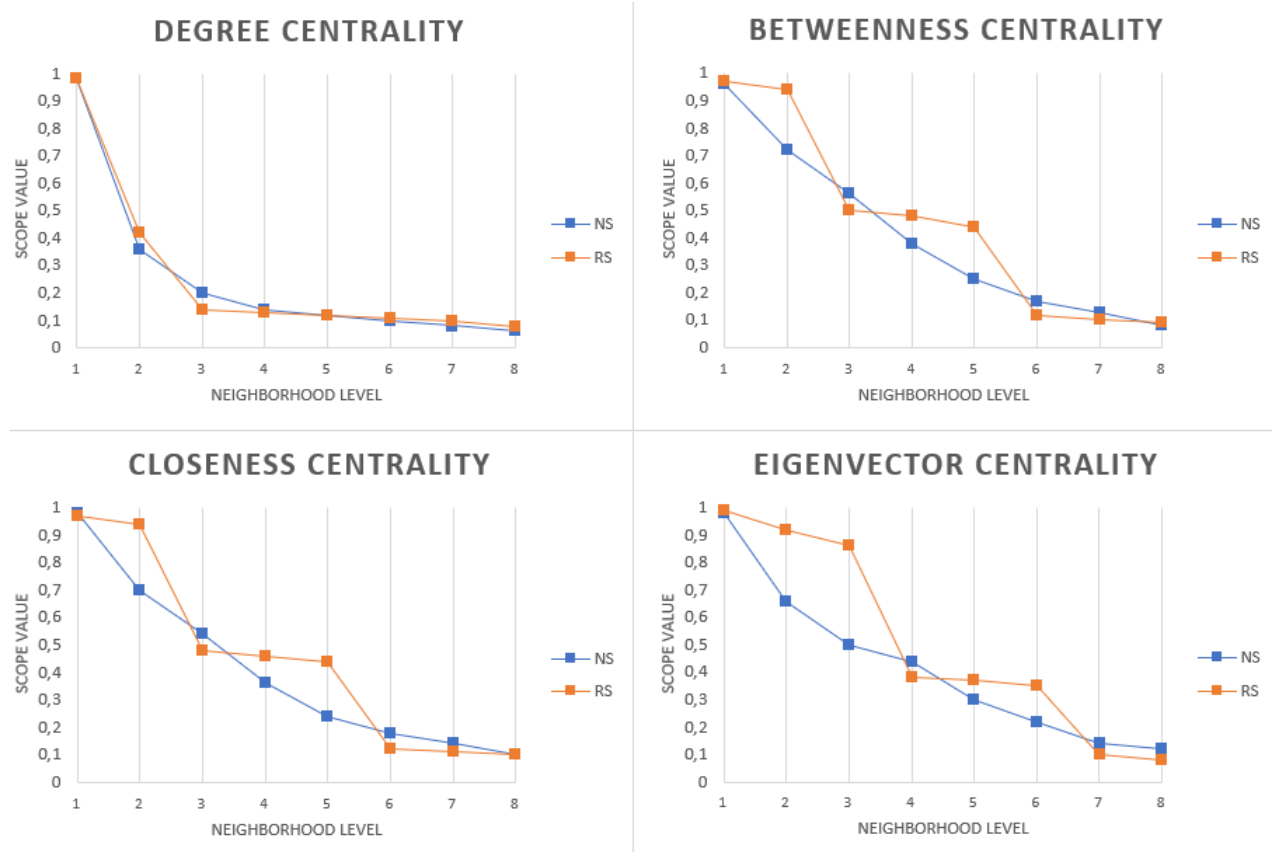


Figure 7: Relationship between NS and RS, on the one side, and centrality measures, on the other side

are, on average, close to the other ones or that are crucial to reach some other ones. In the past, it was shown [49] that these nodes rarely present a high outdegree; instead, most of them have an intermediate outdegree but, on the other side, they can reach a lot of nodes in few steps. As a further confirmation of the correctness of this result, we observe that, in the literature, it was found that, with these two centrality measures, the distribution of nodes tends to be gaussian, differently from what happens for degree centrality, whose distribution follows a power law.

- The nodes with a high eigenvector centrality present high values of scope for $t = 1$ and $t = 2$. These values become quite high for $t = 3$ and intermediate for $t = 4$. Afterwards, they rapidly decrease for $t \geq 5$. This trend can be explained by considering that nodes with a high value of eigenvector centrality are generally characterized by a high value of outdegree and are linked to other nodes that, in their turn, generally have the same characteristics. This feature allows them to have a high scope on the immediate neighborhoods (and this property is similar to the one characterizing the nodes with a high degree centrality). Furthermore, since also the nodes present therein have a high eigenvector centrality (and, therefore, a high outdegree), the impact of the original nodes can easily be preserved also in the neighbors of the neighbors, and so forth, for some steps. Clearly, when $t \geq 4$, this impact inevitably decreases, and this fact is intrinsic

to the very concept of network.

6.4 Analysis of the approximation and the computation time of the Naive Scope w.r.t. the Refined Scope

This experiment aimed at evaluating the strengths and the weaknesses of NS and RS and at determining in which situations one should be preferred to the other. Actually, NS and RS are complementary because the strengths of the former represent the weaknesses of the latter, and vice versa. In particular, quickness is the main strength of NS, whereas accuracy is the main strength of RS.

The trends of NS and RS against the variation of the neighborhood level t in several circumstances have been reported in Figures 3 - 5. Starting from them, if we consider correct the values of RS, we can compute the approximation degree of NS w.r.t. RS by means of the formula:

$$\alpha_{jk}^t = RS_{jk}^t - NS_{jk}^t$$

We computed the values of α_{jk}^t for all the circumstances considered in Figure 3 - 5. The corresponding results are reported in Figures 8 - 10.

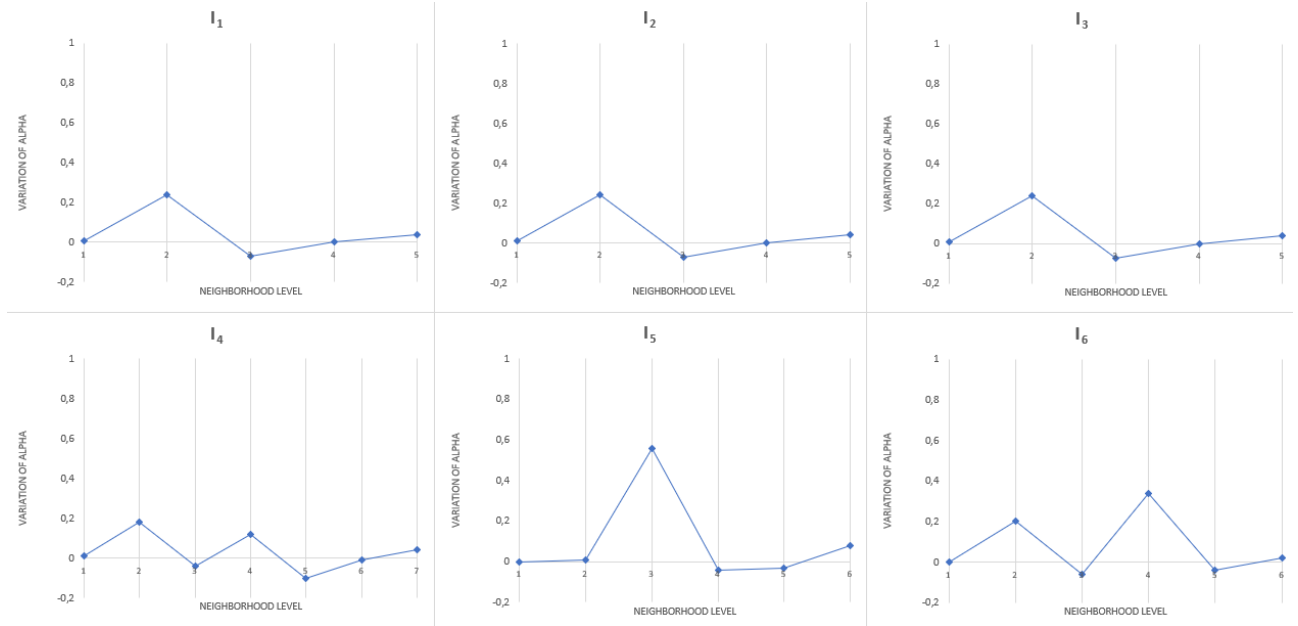


Figure 8: Variation of α_{jk}^t for each IoT of the MIoT against the value of the neighborhood level

From the analysis of these figures, we can observe that, for the neighborhoods in which scope is stably low, the value of α_{jk}^t is minimal. By contrast, when the values of scope are not stable (this, generally, happens for intermediate values and, in some cases, for high values of both the scope and the neighborhood level), the value of α_{jk}^t could become significant. These figures represent a further confirmation of the main feature characterizing RS and not present in NS, i.e., the capability of clearly distinguishing the neighborhoods with a high level of scope from the ones where the value of this parameter is low.

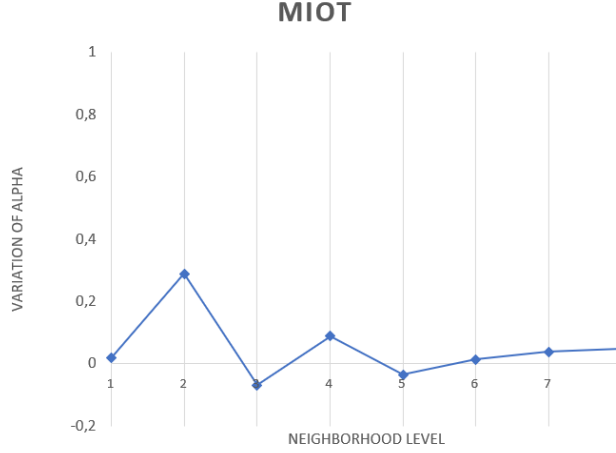


Figure 9: Variation of α_{jk}^t for the whole MIoT against the value of the neighborhood level

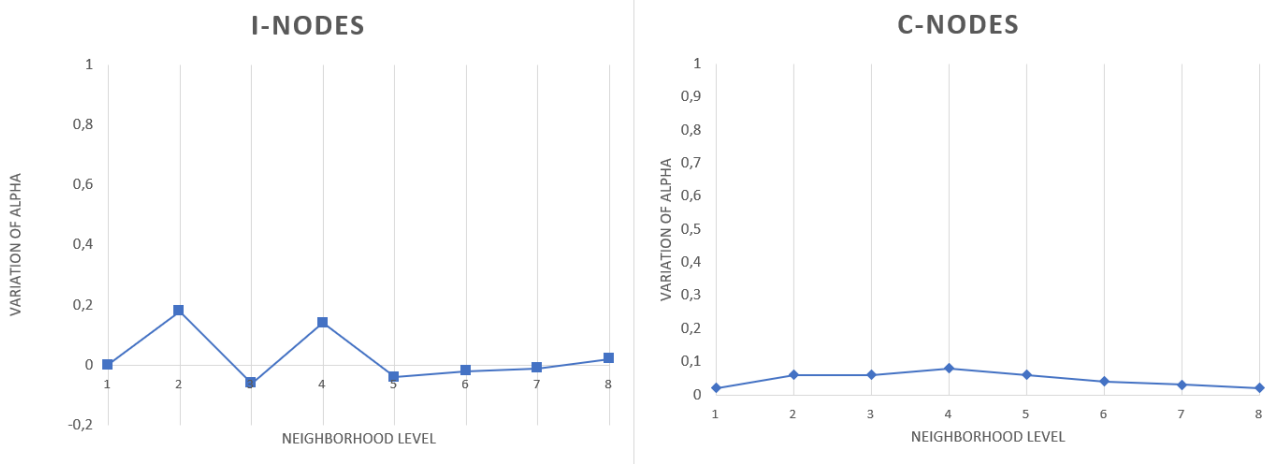


Figure 10: Variation of α_{jk}^t for the i-nodes and the c-nodes of the MIoT against the value of the neighborhood level

Afterwards, we determined the computation time necessary to evaluate the average values of NS and RS on the whole MIoT (which, we recall, consists of 1256 nodes). The results obtained are reported in Table 3.

This table evidences that the time necessary for computing RS is higher than the one required to compute NS. Furthermore, the difference between the two times increases when t increases and becomes more evident for $t \geq 6$. If we combine this result with the previous ones concerning the approximation of NS w.r.t. RS (Figures 8 - 10) and the values of NS and RS against t (Figures 3 - 6) we can define important guidelines on how to proceed for scope computation. In particular, when t has low or intermediate values (i.e., $t < 6$), it is better to adopt RS because it is more accurate and the time necessary for its computation is acceptable. Vice versa, when t has high values (i.e., $t \geq 6$) it is better to adopt NS because its computation is much less expensive and both the involved values

Parameter	Average computation time (s)							
	t=1	t=2	t=3	t=4	t=5	t=6	t=7	t=8
NS	22	89	213	364	512	657	788	927
RS	45	124	246	420	670	884	993	1221

Table 3: Computation time (in seconds) necessary to evaluate the average values of NS and RS on the reference MIoT

and the corresponding approximations are negligible.

Actually, a complete and satisfactory analysis of the computation time can be performed only if we consider MIoT with different numbers of nodes. For this reason, we repeated the task described above for six different MIoT having 176, 301, 485, 778, 1256 and 2028 nodes, respectively. The results obtained are reported in Figure 11.

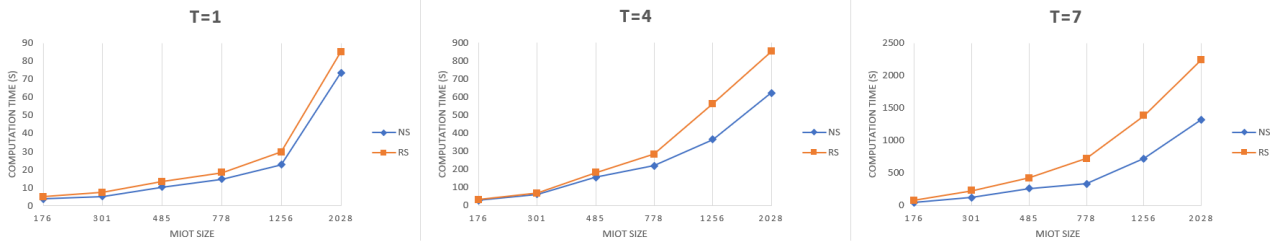


Figure 11: Variation of the average computation time against the size of the MIoT

This figure fully confirms our previous conclusions. As a matter of fact, when $t = 1$, the differences between the computation time of NS and RS are negligible for MIoT with less than 1000 nodes, and very small in the other cases. When $t = 4$, these differences are very small for MIoT with less than 400 nodes; they are intermediate for MIoT with a number of nodes between 400 and 1000; finally, they become high for MIoT with more than 1000 nodes. When $t = 7$ the differences between the computation time of NS and RS are always significant, as we could have expected.

6.5 Relationship between scope and density

In this experiment, we aimed at investigating the relationship possibly existing between the scope and the average density of a MIoT. Here, we consider the average density of a MIoT as the weighted mean of the average densities of the IoT composing it. The weight of each IoT corresponds to the number of its nodes. We recall that, given an IoT \mathcal{I}_k , represented by means of a graph $G_k = \langle N_k, A_k \rangle$, the corresponding density δ_k is defined as:

$$\delta_k = \frac{|A_k|}{|N_k| \cdot (|N_k| - 1)}$$

In order to perform our investigations, we considered our reference MIoT and computed the corresponding density. Then, we decreased its value of 5%, 10%, 15%, 20%, 25% and 30%. We performed this task by randomly removing some previously existing arcs. For each of the six configurations thus obtained, we computed the corresponding values of NS and RS, averaged on the whole MIoT, for $t = 1$, $t = 3$ and $t = 6$. After this, we increased the original density of the MIoT of 5%, 10%,

15%, 20%, 25% and 30%. To obtain these new configurations, we randomly added new arcs to the original MIoT, along with a suitable set of transactions performed on them. Again, for each of these configurations, we computed the values of NS and RS, averaged on the whole MIoT, for $t = 1$, $t = 3$ and $t = 6$. In Figure 12, we report the results obtained.

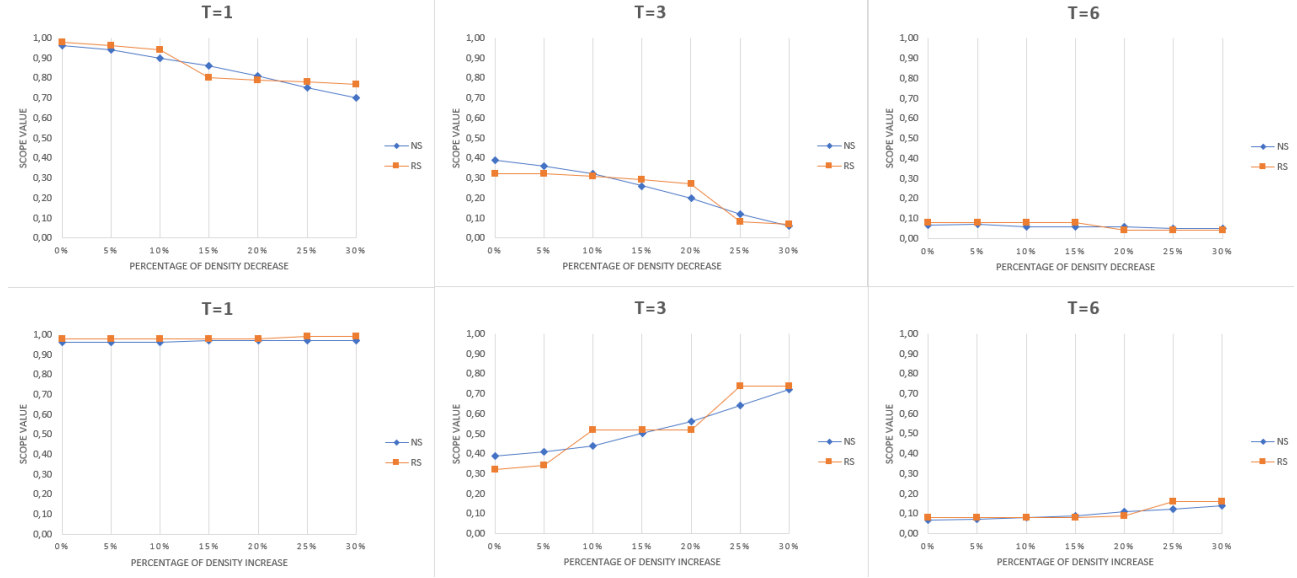


Figure 12: Variation of the values of NS and RS of a MIoT against the variation of the corresponding density

From the analysis of this figure, we can observe that the correlation between density and scope is evident, at least in several cases. In particular, when density increases, scope increases too; instead, a decrease of density implies a decrease of scope. The correlation degree between density and scope depends on the value of t . Indeed, when t is low or t is high, the impact of density on scope is low. By contrast, when t has an intermediate value, this impact is high. These trends can be explained by considering the information diffusion theory in Social Network Analysis. In fact, the intermediate values of t correspond to those scenarios in which the critical mass has been reached and structural holes started to transform into closed triads [49].

6.6 Comparing scope with related concepts and approaches described in Section 2

In this section, we compare our scope parameter and our approach to its computation with related concepts and approaches described in Section 2. As said in that section, to the best of our knowledge, the concept of scope has never been investigated in IoT. Therefore, an experimental comparison is only possible with other approaches working on IoT and proposing parameters related to scope, although different from it.

Proceeding in this way, we decided to compare the scope in a MIoT with: (i) the diffusion degree returned by the SIR model and used to test the approach of [36]; (ii) the influence degree introduced in Social Network Analysis [11] and, then, extended to the SIoT scenario [22]. Both these parameters

are well known in past literature and have been adopted to investigate a large variety of phenomena belonging to very heterogeneous fields.

6.6.1 Comparing scope with diffusion degree

In this section, we compare the scope in a MIoT with the diffusion degree returned by the SIR model used to test the approach of [36].

Susceptible-Infected-Removed (SIR) is a well known model used to test spreading behaviors in several contexts. It describes the spreading of an infectious disease in a population of individuals. Originally proposed by Kermack & McKendrick [27], this model assumes that the population consists of three classes of individuals, namely Susceptible (S), Infective (I) and Recovered (R). The three variables S , I and R represent the number of individuals in each class. S is the number of individuals recovered, who are not infected but could become infected in the future; I is the number of individuals affected by the disease and capable of transmitting it to susceptible individuals; R is the number of individuals recovered, who cannot become infected again. The SIR model is defined by a set of differential equations and is governed by two parameters, namely β and γ , representing the infection rate and the recovery rate, respectively. At each time step, the infection rate β denotes the probability that infected nodes infect their susceptible neighbors; the recovery rate γ indicates the probability that infected nodes recover from the infection.

In our comparison, we are interested in the infection degree that can be derived from the model as the fraction of individuals who are currently infected.

We point out that the SIR model is used to investigate not only infections, but also several phenomena, such as information diffusion and spreading [38, 54, 36, 51], news and rumor modelling in social networks [25], attacks towards wireless networks [31], and so forth. It is exactly these types of phenomena (in particular, information diffusion and spreading) that is relevant in our experiments. Therefore, in the following, we will speak about *diffusion degree* to indicate the infection degree modeled by SIR when this model is applied to information diffusion in an IoT context. In particular, it indicates the fraction of smart objects reached by a given information sent by a node through a chain of transactions (see below).

Clearly, in order to be able to compare diffusion degree with scope, it is necessary to plan the experiment so that the two parameters are comparable.

For this purpose, we have considered the six IoT $\{\mathcal{I}_1, \mathcal{I}_2, \dots, \mathcal{I}_6\}$ used in the experiment described in Section 6.2, because we want to take the variation of RS against the neighborhood level as the reference measure for scope evaluation.

Given an IoT \mathcal{I}_k and a node n_{i_k} , we focused on computing the variation of the diffusion degree against the level t of the neighborhood $out_nbh_{j_k}^t$ of n_{j_k} . Specifically, the diffusion degree of $out_nbh_{j_k}^t$ at a certain time instant is equal to the fraction of its nodes reached by a certain information sent by n_{j_k} through a chain of transactions starting from it and reaching the nodes of that neighborhood. Recall that, in the SIR model, an infected node can heal, in which case it can no longer transmit the infection. From the information diffusion viewpoint, this scenario is equivalent to the one of a node reached by a certain information that it no longer wants to transmit to its neighbors.

For the computation of the diffusion degree against t , we decided to operate as follows. First, we

had to set the parameters of the SIR model. For this purpose, according to [36, 13], we set β to the so called epidemic threshold $1/\lambda_k$, where λ_k is the largest eigenvalue of the adjacency matrix of the IoT \mathcal{I}_k . Thus, we have a different value of β for each IoT. As for γ , following the guidelines in [36], we set it to 0.8.

Analogously to SIR, our model for the computation of the diffusion degree assumes that, at each time instant, a node can infect only its direct neighbors. As a consequence, at the first time instant ($\tau = 1$), a node n_{j_k} can infect only the nodes belonging to $out_nbh_{j_k}^1$. At the second time instant ($\tau = 2$), n_{j_k} continues to infect other nodes of $out_nbh_{j_k}^1$. In addition, the nodes of $out_nbh_{j_k}^1$ can, in turn, infect their direct neighbors. As a result, at the time instant $\tau = 2$, the infection can reach the nodes belonging to $out_nbh_{j_k}^2$.

At the third time instant, n_{j_k} continues to infect other nodes of $out_nbh_{j_k}^1$ that have not been infected previously. The nodes of $out_nbh_{j_k}^1$ infected at time $\tau = 1$ and not yet healed, may continue to infect other nodes of $out_nbh_{j_k}^2$. At the same time, the nodes of $out_nbh_{j_k}^2$ already infected at the time instant $\tau = 2$ may, in turn, begin to infect their direct neighbors, i.e., the nodes of $out_nbh_{j_k}^3$. Usually, at the time instant $\tau = h$, an infected node n_{j_k} can spread its infection until to the nodes of $out_nbh_{j_k}^h$. The infection process continues with the above rules but, as time goes by, many infected people heal and can no longer be infected.

In order to compare scope with diffusion degree, since the latter is dependent on the time instant τ considered, we decided to make our comparison with reference to a time instant τ_m equal to the maximum level of neighborhood associated with \mathcal{I}_k in Figure 3 (and, therefore, $\tau_m = 5$ for \mathcal{I}_1 and \mathcal{I}_5 , $\tau_m = 6$ for \mathcal{I}_3 and \mathcal{I}_6 , $\tau_m = 7$ for \mathcal{I}_4 and $\tau_m = 8$ for \mathcal{I}_2). Moreover, given the neighborhood $out_nbh_{j_k}^h$, $1 \leq h \leq \tau_m$, the diffusion degree of n_{j_k} for that neighborhood at the time instant τ_m will be equal to the fraction of its nodes reached by the information initially sent by n_{j_k} .

What we have described so far applies to the computation of the diffusion degree of a single node. We performed this task for all the nodes of the network and, then, averaged the corresponding values. After this, we compared the average value thus obtained with the one of RS shown in Figure 3.

The results obtained for the six IoT are shown in Figure 13 and the one regarding the whole MIoT are represented in Figure 14.

From the analysis of these figures we can observe that the trends of RS and DD are similar because both decrease as the neighborhood level grows. However, there are some differences in the way the decrease of the two parameters happens. In fact, DD decreases much more slowly than RS and its decrease is quite regular. Instead, RS decreases more quickly and its decrease has a rather irregular characteristic shape, with some steps when passing from one level to another (look, for instance, at the step present when passing from level 2 to level 3 in \mathcal{I}_1 , or the steps present when passing from level 2 to level 3 and from level 4 to level 5 in the MIoT). In Section 6.2, we have seen that this trend is characteristic both of RS and NS and that it is to be considered a positive property of scope because it is able to clearly distinguish the neighborhoods in which a node exerts a “power” from those in which such a “power” is lacking.

In this section, we want to go one step further and try to understand the reasons for this trend and, ultimately, for this important property of RS. In Section 3, we have seen that each node of an IoT corresponds to a smart object. In Section 4, we have seen that the scope of a node depends on the number of transaction requests received by the smart object corresponding to that node, its ability to

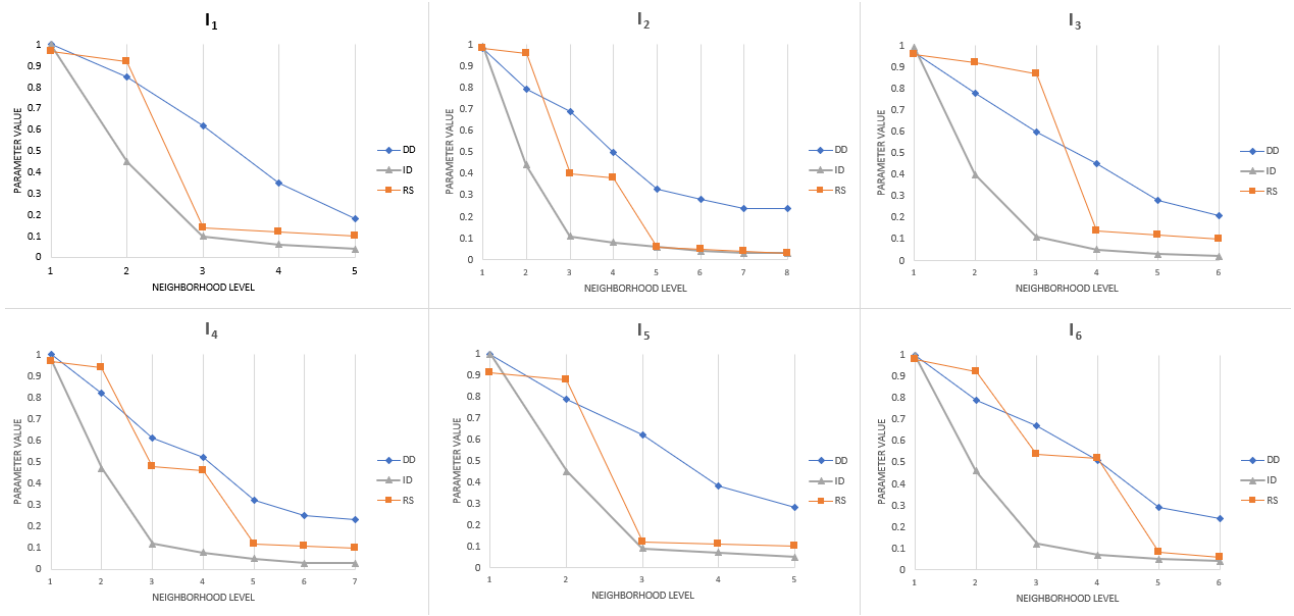


Figure 13: Variation of the average values of the Diffusion Degree DD, Refined Scope RS and Influence Degree ID for each IoT of the MIoT against the neighborhood level

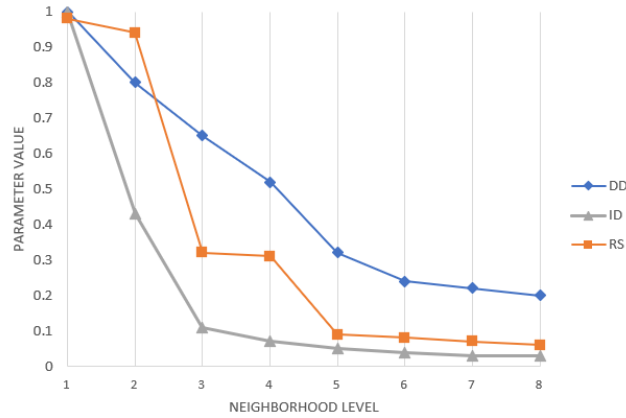


Figure 14: Variation of the average values of the Diffusion Degree DD, Refined Scope RS and Influence Degree ID for the whole MIoT against the neighborhood level

stimulate not very proactive objects to repost its transactions or to activate transactions with it and, finally, its ability to stimulate smart objects with a high scope to repost its transactions. Ultimately, the scope of a node models its “power” on the other nodes of the network.

Both the experience with Online Social Networks and the theory related to Social Network Analysis reveal us that the “power” exerted by a node remains strong as long as we move towards its neighbors or the neighbors of its neighbors. As we move further away from the node, the possibility of finding a node on which the original node keeps its “power” intact decreases.

Now, the values of RS of a node for the different neighborhood levels in Figures 13 and 14 are

average values obtained by considering all the nodes of the neighborhood. When we move from a neighborhood level to the next, the number of nodes at the new level increases, and this increase can also be significant if the network is very connected. If the “power” of the original node remains intact on all the elements of the new neighborhood, the average value of RS does not change significantly.

But if (as it happens from level 3 onwards) there is a significant decrease of the number of nodes on which the “power” of the original node remains intact, together with a significant increase of the number of nodes on which the “power” is considerably reduced, we have that the huge increase in the denominator of the average is no longer counterbalanced by an equal increase in the numerator. As a consequence of this fact, there is a collapse of the overall value, and therefore of the value of RS, in correspondence with the level of the new neighborhood.

This collapse leads to the characteristic stepped shape that can be observed on the trend of the scope against the neighborhood level almost always and, as far as it is concerned here, in Figures 13 and 14.

6.6.2 Comparing scope with influence degree

In this section, we compare our scope parameter with influence degree, which was initially proposed in Social Network Analysis [11] and later extended to Social IoT [22].

The influence degree of a node in a social network is an indicator of how much the information it sends to its neighbors appears so interesting that they in turn forward it to their neighbors. This definition of influence degree is based on the information delivered; however, it is possible to think of similar definitions taking into account services provided or other phenomena originating from the node whose influence degree is to be measured [49]. The most immediate way to extend the concept of influence degree of a node n_{j_k} to our MIoT scenario is to consider the fraction of the transactions activated by n_{j_k} that are, in turn, reposted by the nodes belonging to its neighborhoods.

To carry out this experiment, we started from the six IoT $\{\mathcal{I}_1, \mathcal{I}_2, \dots, \mathcal{I}_6\}$ considered in all the experiments described in this paper and, once again, we decided to take the variation of RS against the neighborhood level as the reference parameter for scope.

Given an IoT \mathcal{I}_k and a node n_{j_k} , we focused on the variation of the influence degree against the neighborhood level. According to what stated above, influence degree was measured considering the fraction of the transactions activated by n_{j_k} and reposted by at least one node of the neighborhood level into consideration. We observe that the trend of the influence degree is anti-monotonous because the number of transactions originally sent by n_{j_k} reposted by the nodes of $out_nbh_{j_k}^t$ can only be less than or equal to the corresponding number of transactions reposted by $out_nbh_{j_k}^{t-1}$.

As in the experiment described in Section 6.6.1, also in this case we first computed the influence degree of each node n_{j_k} of an IoT \mathcal{I}_k and, then, we averaged the values thus obtained. Finally, we compared the average influence degree with the average value of RS shown in Figure 3.

The results obtained for the six IoT are reported in Figure 13, while the results for the whole MIoT are presented in Figure 14. From the analysis of these figures, we can see that the trend of the scope and the one of the influence degree are similar because both these parameters decrease with the increase of the neighborhood level. However, we can observe differences in the way they decrease. In fact, the decrease of influence degree is steeper and more regular than the one of scope.

6.6.3 Final considerations

To better understand the results of the comparison between Refined Scope RS, Influence Degree ID and Diffusion Degree DD, we must first keep in mind what is the goal of scope. Actually, this parameter was introduced to measure the “power” of a node versus the other nodes of its IoT or versus the nodes of the MIoT. Therefore, the ability of the scope to be a valid parameter for measuring the “power” of a node is closely related to its ability to correctly model what happens in real social networks about this phenomenon, also taking into account the results of past research on Social Network Analysis.

As we have seen in Section 6.6.1, Online Social Networks assume that generally the “power” of a person joining them extends to the neighbors of the neighbors and, thus, to the neighborhood of level 2. Moving from the neighborhood of level 2 to the neighborhood of level 3 there is a first significant decrease of this “power”. This decrease becomes very quick in subsequent neighborhood levels, until the “power” becomes almost null from the neighborhoods of level 4 or 5 onwards.

These assumptions made in Online Social Networks are confirmed by research on Social Network Analysis, in particular by the theory of six degrees of separation and the one of the Dumbbar Pyramid [49]. The former tells us that, given two people totally unknown to each other and that, perhaps, are at the antipodes of our planet, there are at most six relationships of friendship to separate them. All this is confirmed by the theory of the Dumbbar Pyramid, which sets the number of intimate contacts (i.e., friends or relative) of a person at about 20, and the maximum number of (even loose) contacts that a person can handle at about 150.

The above reasoning shows that the ideal parameter for measuring the “power” of a node in an IoT or a MIoT should have a high value for the neighbors of level 1 and 2, an intermediate value for the neighbors of level 3 and, possibly, for those of level 4; finally, it should have low values for the neighbors of level 5 onwards. Instead, a too optimistic parameter, which assumes significant values even for neighbors of level 4 or higher, is not a good indicator of the “power” of a node in a network. On the other hand, a too pessimistic parameter, which assumes low values even for the neighbors of levels 2 and 3, is not adequate for the opposite reasons.

Now, if we consider Figures 13 and 14, we can observe that Diffusion Degree DD is too optimistic while Influence Degree ID is too pessimistic. Although for opposite reasons, both of them are not accurate in modeling the trend of the “power” of a node in an IoT or a MIoT.

Conversely, the same figures show that RS has an intermediate behavior between DD and ID assuming high values for the neighbors of level 1 and 2, intermediate values for the neighbors of level 3 and very low values for the neighbors of level 5 onwards. This trend is totally in line with the behavior that both the Online Social Networks and the research on Social Network Analysis assume should characterize the “power” of a node in a network. This allows us to conclude that RS is actually the best parameter to model this phenomenon.

7 Conclusion

Social internetworking and the IoT are becoming more and more contiguous giving rise to several social and/or multiple IoT paradigms. In this new scenario, we introduced the concept of scope of a smart object in a MIoT, we presented two formalizations (one naive and one refined) of this concept

and we illustrated two possible applications (one regarding a smart city and the other concerning a shopping center). Afterwards, we presented a set of experiments to analyze the main features of our approach and we saw that scope is really capable of estimating the “power” of a smart object in a MIoT. Moreover, we examined several related approaches and we evidenced the analogies and the differences between them and ours. Finally, for two of these approaches, we performed an experimental comparison with scope.

This paper provides several contributions to the research on IoT. Indeed: *(i)* it extends the concept of scope from Social Network Analysis to IoT; *(ii)* it introduces two kinds of scope, namely Naive and Refines Scope, and evaluates the pros and the cons of each of them; *(iii)* it proposes two use cases benefiting from scope; *(iv)* it evaluates scope against neighborhood level, centrality, density, accuracy, computation time, diffusion degree, influence degree and other related concepts and approaches proposed in past research on IoT.

This paper should not be considered as an ending point. Instead, it could be the starting point of many researches in this field. Indeed, there are several future related investigations that could be made in this context. First, we would like to analyze the role of possible constraints involving network nodes or arcs in the definition of scope. Then, we plan to study the role of scope in the detection of anomalies and, even more, in understanding the extension and the importance of the damage caused by them. We would also like to analyze the adoption of scope in predictive maintenance, which is currently one of the most important research issues in manufacturing industry [55].

Finally, we observe that the current version of the MIoT model is based on a static network of smart objects. This is suited in all those cases in which the network of smart objects changes rarely over time, meaning that objects join the network or leave it infrequently. Actually, many application scenarios involving IoT are dynamic and mobile because, often, new devices join the network and other ones leave it frequently. As a consequence, it appears challenging to evolve our system from static to dynamic. This could be carried out in several ways. For instance, it would be possible to define an incremental approach for the dynamic management of a MIoT, capable of registering each join or each leave of a smart object from the network. The strength of this approach would be its accuracy, whereas its weakness would be its computational complexity. In those cases where this last parameter is high, it would be possible to define an alternative approach that registers the join or the leave of nodes from the network only periodically, with the period length depending on the computational complexity and the available resources.

Acknowledgments

This work was partially supported by: *(i)* the Italian Ministry for Economic Development (MISE) under the project “Smarter Solutions in the Big Data World”, funded within the call “HORIZON2020” PON I&C 2014-2020 (CUP B28I17000250008), *(ii)* the Department of Information Engineering at the Polytechnic University of Marche under the project “A network-based approach to uniformly extract knowledge and support decision making in heterogeneous application contexts” (RSAB 2018), and *(iii)* the PRIN Project FluidWare funded by Italian Government (MIUR) N. 2017KRC7KT.

References

- [1] G. Araniti, A. Orsino, L. Militano, L. Wang, and A. Iera. Context-Aware Information Diffusion for Alerting Messages in 5G Mobile Social Networks. *IEEE Internet of Things Journal*, 4(2):427–436, 2017.
- [2] L. Atzori, A. Iera, and G. Morabito. SIoT: Giving a social structure to the Internet of Things. *IEEE Communications Letters*, 15(11):1193–1195, 2011. IEEE.
- [3] L. Atzori, A. Iera, and G. Morabito. Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks*, 56:122–140, 2017. Elsevier.
- [4] L. Atzori, A. Iera, G. Morabito, and M. Nitti. The Social Internet of Things (SIoT)– when social networks meet the Internet of Things: Concept, architecture and network characterization. *Computer networks*, 56(16):3594–3608, 2012. Elsevier.
- [5] G. Baldassarre, P. Lo Giudice, L. Musarella, and D. Ursino. A paradigm for the cooperation of objects belonging to different IoTs. In *Proc. of the International Database Engineering & Applications Symposium (IDEAS 2018)*, pages 157–164, Villa San Giovanni, Italy, 2018. ACM.
- [6] G. Baldassarre, P. Lo Giudice, L. Musarella, and D. Ursino. The MIoT paradigm: main features and an “ad-hoc” crawler. *Future Generation Computer Systems*, 92:29–42, 2019. Elsevier.
- [7] P. Bourelos, G. Kousiouris, O. Voutyras, and T.A. Varvarigou. Heating schedule management approach through decentralized knowledge diffusion in the context of social internet of things. In *Proc. of the Panhellenic Conference on Informatics (PCI 2015)*, pages 103–108, Athens, Greece, 2015. ACM.
- [8] F. Buccafurri, V.D. Foti, G. Lax, A. Nocera, and D. Ursino. Bridge Analysis in a Social Internetworking Scenario. *Information Sciences*, 224:1–18, 2013. Elsevier.
- [9] R. Casadei, G. Fortino, D. Pianini, W. Russo, C. Savaglio, and M. Viroli. A development approach for collective opportunistic edge-of-things services. *Information Sciences*, 498:154–169, 2019.
- [10] R. Casadei, G. Fortino, D. Pianini, W. Russo, C. Savaglio, and M. Viroli. Modelling and simulation of Opportunistic IoT Services with Aggregate Computing. *Future Generation Computer Systems*, 91:252–262, 2019.
- [11] M. Cataldi, L. Di Caro, and C. Schifanella. Emerging Topic Detection on Twitter Based on Temporal and Social Terms Evaluation. In *Proc. of the International Workshop on Multimedia Data Mining (MDMKDD 2010)*, pages 4–13, Washington, DC, USA, 2010. ACM.
- [12] F. Cauteruccio, L. Cinelli, G. Terracina, D. Ursino, and L. Virgili. Investigating the scope of a thing in a multiple Internet of Things scenario. In *Atti del Ventisettesimo Convegno Nazionale su Sistemi Evoluti per Basi di Dati (SEBD’19)*, Castiglione della Pescaia (GR), Italy, 2019.
- [13] D. Chakrabarti, Y. Wang, C. Wang, J. Leskovec, and C. Faloutsos. Epidemic thresholds in real networks. *ACM Transactions on Information and System Security*, 10(4), 2008. ACM.
- [14] J. Cheng, J. M. Kleinberg, J. Leskovec, D. Liben-Nowell, B. State, K. Subbian, and L. A. Adamic. Do Diffusion Protocols Govern Cascade Growth? In *Proc. of the International Conference on Web and Social Media (ICWSM 2018)*, pages 32–41, Stanford, CA, USA, 2018. AAAI Press.
- [15] E. Curry, W. Derguech, S. Hasan, C. Kouroupetroglou, and U. ul Hassan. A Real-time Linked Dataspace for the Internet of Things: Enabling “Pay-As-You-Go” Data Management in Smart Environments. *Future Generation Computer Systems*, 90:405–422, 2019. Elsevier.
- [16] K. Das, S. Samanta, and M. Pal. Study on centrality measures in social networks: a survey. *Social Network Analysis and Mining*, 8(1):13, 2018.
- [17] A. Felfernig, S. Polat-Erdeniz, C. Uran, S. Reiterer, M. Atas, T.N.T. Tran, P. Azzoni, C. Kiraly, and Dolui K. An overview of recommender systems in the Internet of Things. *Journal of Intelligent Information Systems*, pages 1–25, 2018.
- [18] A. Forestiero. Multi-agent recommendation system in Internet of Things. In *Proc. of the IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, (CCGRID 2017)*, pages 772–775, Madrid, Spain, 2017. IEEE Computer Society / ACM.

- [19] G. Fortino, W. Russo, C. Savaglio, W. Shen, and M. Zhou. Agent-Oriented Cooperative Smart Objects: From IoT System Design to Implementation. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 48(11):1939–1956, 2018.
- [20] G. Fortino, C. Savaglio, C.E. Palau, J. Suarez de Puga, M. Ganzha, M. Paprzycki, M. Montesinos, A. Liotta, and M. Llop. Towards multi-layer interoperability of heterogeneous iot platforms: The inter-iot approach. In *Integration, interconnection, and interoperability of IoT systems*, pages 199–232. Springer, 2018.
- [21] G. Fortino and P. Trunfio, editors. *Internet of Things Based on Smart Objects, Technology, Middleware and Applications*. Springer, 2014.
- [22] B. Guo, Z. Yu, X. Zhou, and D. Zhang. Opportunistic IoT: Exploring the social side of the internet of things. In *Proc. of the International Conference on Computer Supported Cooperative Work in Design (CSCWD’12)*, pages 925–929, Wuhan, China, 2012. IEEE Press.
- [23] M.A.M Hail, M. Amadeo, A. Molinaro, and S. Fischer. On the performance of caching and forwarding in information-centric networking for the IoT. In *Proc. of the International Conference on Wired/Wireless Internet Communication (WWIC’15)*, pages 313–326, Malaga, Spain, 2015. Springer.
- [24] Z. Huang, Y. Zheng, R. Cheng, Y. Sun, N. Mamoulis, and X. Li. Meta Structure: Computing Relevance in Large Heterogeneous Information Networks. In *Proc. of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD ’16)*, pages 1595–1604, New York, NY, USA, 2016. ACM.
- [25] F. Jin, E. Dougherty, P. Saraf, Y. Cao, and N. Ramakrishnan. Epidemiological modeling of news and rumors on twitter. In *Proceedings of the 7th Workshop on Social Network Mining and Analysis (SNAKDD ’13)*, Chicago, Illinois, 2013. ACM.
- [26] D. Kempe, J. Kleinberg, and É. Tardos. Maximizing the spread of influence through a social network. In *Proc. of the International ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD 2003)*, pages 137–146, Washington, DC, USA, 2003. ACM.
- [27] W.O. Kermack and A.G. McKendrick. A contribution to the mathematical theory of epidemics. *Proceedings of the Royal Society of London. Series A.*, 115(772):700–721, 1927. The Royal Society London.
- [28] R. Lea and M. Blackstock. Smart Cities: an IoT-centric Approach. In *Proc. of the International Workshop on Web Intelligence and Smart Sensing (IWWISS ’14)*, pages 12:1–12:2, Saint Etienne, France, 2014. ACM.
- [29] D. Leggio, G. Marra, and D. Ursino. Defining and investigating the scope of users and hashtags in Twitter. In *Proc. of the International Conference on Ontologies, DataBases, and Applications of Semantics (ODBASE 2014)*, pages 674–681, Amantea (CS), Italy, 2014. Lecture Notes in Computer Science. Springer.
- [30] P. Lo Giudice, A. Nocera, D. Ursino, and L. Virgili. Building Topic-Driven Virtual IoTs in a Multiple IoTs Scenario. *Sensors*, 19(13):2956, 2019. MDPI.
- [31] M. López, A. Peinado, and A. Ortiz. An extensive validation of a sir epidemic model to study the propagation of jamming attacks against iot wireless networks. *Computer Networks*, 165:106945, 2019.
- [32] L. Lü, D. Chen, X.L. Ren, Q.M. Zhang, Y.C. Zhang, and T. Zhou. Vital nodes identification in complex networks. *Physics Reports*, 650:1–63, 2016. Elsevier.
- [33] Z. Ma, A. Sun, and G. Cong. Will this #Hashtag be Popular Tomorrow? In *Proc. of the ACM SIGIR International Conference on Research and Development in Information Retrieval (SIGIR 2012)*, pages 1173 – 1174, Portland, OR, USA, 2012. ACM.
- [34] Z. Ma, A. Sun, and G. Cong. On Predicting the Popularity of Newly Emerging Hashtags in Twitter. *Journal of the Association for Information Science and Technology*, 64(7):1399–1410, 2013.
- [35] C. Magnien and F. Tarissan. Time evolution of the importance of nodes in dynamic networks. In *2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2015)*, pages 1200–1207, Paris, France, 2015. IEEE.
- [36] F. Malliaros, M. Rossi, and M. Vazirgiannis. Locating influential nodes in complex networks. *Scientific reports*, 6:19307, 2016. Nature.

- [37] Z. Miller, B. Dickinson, W. Deitrick, W. Hu, and A. H. Wang. Twitter Spammer Detection Using Data Stream Clustering. *Information Sciences*, 260:64–73, 2014.
- [38] G. Miritello, E. Moro, and R. Lara. Dynamical strength of social ties in information spreading. *Phys. Rev. E*, 83:045102, 2011. American Physical Society.
- [39] B. Negash, T. Westerlund, and H. Tenhunen. Towards an interoperable Internet of Things through a web of virtual things at the Fog layer. *Future Generation Computer Systems*, 91:96–107, 2019. Elsevier.
- [40] S. Nicolazzo, A. Nocera, D. Ursino, and L. Virgili. A Privacy-Preserving Approach to Prevent Feature Disclosure in an IoT Scenario. *Future Generation Computer Systems*. Forthcoming.
- [41] Z. Ning, X. Wang, X. Kong, and W. Hou. A social-aware group formation framework for information diffusion in narrowband internet of things. *IEEE Internet of Things Journal*, 5(3):1527–1538, 2018.
- [42] A. Nocera and D. Ursino. PHIS: a system for scouting potential hubs and for favoring their “growth” in a Social Internetworking Scenario. *Knowledge-Based Systems*, 36:288–299, 2012. Elsevier.
- [43] Y. Okada, K. Masui, and Y. Kadobayashi. Proposal of Social Internetworking. In *Proc. of the International Human.Society@Internet Conference (HSI 2005)*, pages 114–124, Asakusa, Tokyo, Japan, 2005. Lecture Notes in Computer Science, Springer.
- [44] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos. Context aware computing for the internet of things: A survey. *IEEE communications surveys & tutorials*, 16(1):414–454, 2013. IEEE.
- [45] Z. Qasem, M. Jansen, T. Hecking, and H.U. Hoppe. On the Detection of Influential Actors in Social Media. In *Proc. of the International Conference on Signal-Image Technology & Internet-Based Systems, (SITIS 2015)*, pages 421–427, Bangkok, Thailand, 2015. IEEE Computer Society.
- [46] D.M. Romero, W. Galuba, S. Asur, and B.A. Huberman. Influence and passivity in social media. In *Proc. of the International Conference on World Wide Web (WWW’11)*, pages 113–114, Hyderabad, India, 2011. ACM.
- [47] Y. Saleem, N. Crespi, M. H. Rehmani, R. Copeland, D. Hussein, and E. Bertin. Exploitation of social IoT for recommendation services. In *Proc. of the IEEE World Forum on Internet of Things (WF-IoT 2016)*, pages 359–364, Reston, VA, USA, 2016. IEEE Computer Society.
- [48] B. Sun and V.T.Y. Ng. Identifying influential users by their postings in social networks. In *Proc. of the International Workshop on Modeling Social Media (MSM 2012)*, pages 1–8, Milwaukee, WI, USA, 2012. ACM.
- [49] M. Tsvetovat and A. Kouznetsov. *Social Network Analysis for Startups: Finding connections on the social web*. Sebastopol, CA, USA, 2011. O’Reilly Media, Inc.
- [50] D. Ursino and L. Virgili. Humanizing IoT: defining the profile and the reliability of a thing in a Multi-IoT scenario. *Towards Social Internet of Things: Enabling Technologies, Architectures and Applications*, Forthcoming. Springer Nature.
- [51] S. Wang, Y. Du, and Y. Deng. A new measure of identifying influential nodes: Efficiency centrality. *Communications in Nonlinear Science and Numerical Simulation*, 47:151 – 163, 2017. Elsevier.
- [52] J. Weng, E. Lim, J. Jiang, and Q. He. TwitterRank: Finding Topic-sensitive Influential Twitterers. In *Proc. of the ACM International Conference on Web Search and Data Mining (WSDM 2010)*, pages 261–270, New York, NY, USA, 2010. ACM.
- [53] P. Wu, Z. Lu, Q. Zhou, Z. Lei, X. Li, M. Qiu, and P.C.K. Hung. Bigdata logs analysis based on seq2seq networks for cognitive Internet of Things. *Future Generation Computer Systems*, 90:477–488, 2019. Elsevier.
- [54] O. Yagan, D. Qian, J. Zhang, and D. Cochran. Conjoining speeds up information diffusion in overlaying social-physical networks. *IEEE Journal on Selected Areas in Communications*, 31(6):1038–1048, 2013. IEEE.
- [55] J. Yan, Y. Meng, L. Lu, and L. Li. Industrial big data in an industry 4.0 environment: Challenges, schemes, and applications for predictive maintenance. *IEEE Access*, 5:23484–23491, 2017.
- [56] L. Yao, Q. Z. Sheng, A.H.H. Ngu, and X. Li. Things of interest recommendation by leveraging heterogeneous relations in the internet of things. *ACM Transaction on Internet Technology*, 16(2):9:1–9:25, 2016.

- [57] C. Zhang, L. Zhu, C. Xu, K. Sharif, X. Du, and M. Guizani. LPTD: Achieving lightweight and privacy-preserving truth discovery in CIoT. *Future Generation Computer Systems*, 90:175–184, 2019. Elsevier.
- [58] M. Zhang, L. Guo, M. Hu, and W. Liu. Influence of customer engagement with company social networks on stickiness: Mediating effect of customer value creation. *International Journal of Information Management*, 37(3):229–240, 2017. Elsevier.
- [59] Z. Zhou, C. Gao, C. Xu, Y. Zhang, S. Mumtaz, and J. Rodriguez. Social Big-Data-Based Content Dissemination in Internet of Vehicles. *IEEE Transactions on Industrial Informatics*, 14(2):768–777, 2018.
- [60] Z. Zhu, J. Su, and L. Kong. Measuring influence in online social network based on the user-content bipartite graph. *Computers in Human Behavior*, 52:184–189, 2015.