# Investigating the scope of a thing in a multiple Internet of Things scenario

Francesco Cauteruccio[1], Luca Cinelli[1], Giorgio Terracina[1], Domenico Ursino[2], and Luca Virgili[2]

[1] DEMACS, University of Calabria
[2] DII, Polytechnic University of Marche

**Abstract.** In this paper, we investigate the scope of a thing in a multiple IoT scenario. First we introduce the concept of scope in general, and we illustrate how it has been investigated and applied in social networking. Then, we define the scope of a thing in a Multi-IoT scenario, modeled as an extension of a Social Internetworking System, and we propose a formalization of scope allowing the computation of its values. Finally, we present a possible application of scope and describe some tests that we performed for evaluation purposes.

**Keywords**: Scope; Social Object; Internet of Things; Multiple IoTs; Trust Degree; Neighborhood of a Thing



## 1 Introduction

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*". Scope has certainly some similitudes with several other concepts investigated in sociology, such as influence, power, centrality, impact, reliability, and so forth. However, it goes beyond each of these terms and, at the same time, summarizes all of them and is influenced by each of them.

In the past, scope has been studied in the context of social networks. For instance, in [12], the authors investigate the scope of users and hashtags in Twitter, whereas in [10, 13–15, 18, 19], the authors propose approaches to computing some aspects of scope (e.g., influence, trust, reliability) for users and/or hashtags. In the meantime, the social network scenario has become increasingly complex and we have passed from social networking to social internetworking [17, 7]. In this last case, several social networks simultaneously coexist and cooperate through specific users, called bridges, who join more social networks.

Parallel to the transition from social networking to social internetworking, in the last few years, we are experiencing the presence of objects that are becoming

increasingly smart and social. This phenomenon is revolutionizing the Internet of Things. As a proof of this, more and more authors are starting to study the behavior of things, to talk about their profiles and their social interactions. In fact, different architectures implementing these ideas are frequently proposed in the current literature. Social Internet of Things (hereafter, SIoT [4]), Multiple IoT Environment (hereafter, MIE [5]) and Multiple Internets of Things (hereafter, MIoT [6]) are only three of the latest architectures with these characteristics. In particular, MIoT is the latest of them and, therefore, takes into account the most recent results obtained in the IoT research. A MIoT can be seen as a set of Internets of Things interacting with each other through specific objects, called "cross objects", that belong to more IoTs. The MIoT paradigm represents the extension of the ideas underlying social internetworking to the IoT.

In spite of this enormous interest that increasingly numerous researchers are posing on the IoT, to the best of our knowledge, no analysis about the scope of a thing in a Multi-IoT, or at least in an IoT, scenario has been presented yet. Certainly, several aspects someway related to the scope have been considered in the IoT or, in limited cases, in the SIoT scenario. As an example, in [16], the authors investigate information diffusion in a narrowband IoT with the goal of optimizing information flow at network level. In [3], the authors investigate the adoption of context-aware information diffusion to alert messages in 5G mobile social networks. Context-aware information is collected from different devices deployed in the environment. An interesting approach to content dissemination in the Internet of Vehicles (IoV) is described in [21]. Here, the authors analyze 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. In [11], the authors present an IoT application in the context of smart cities, a scenario in which an IoT system can reach large scale dimensions. [11] also introduces the concept of IoT hub. This aggregates the information coming from related devices and, therefore, contributes to improve the interoperability between things in a urban-scale IoT system. Furthermore, different approaches on recommender systems and services in IoT have been proposed in the literature; an overview of them is presented in [8]. In particular, in [9], the authors propose a multi-agent recommender system for the IoT aiming at producing a set of significant suggestions for a user with specific characteristics. Here, things are represented through bit vectors, called thing descriptors, managed by cyber-agents. Things can be linked together and, then, can be managed by neighbor cyber-agents. In [20], the authors propose an approach that integrates the concept of social networks of users and Internet of Things. 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.

All the approaches mentioned above are extremely interesting; furthermore, several other related approaches proposed in the past to evaluate the relevance or the impact of a node in the Internet of Things could be mentioned. However, none of them has been conceived to operate in a complex scenario consisting of

multiple IoTs, which interact with each other through smart and social objects that simultaneously belong to more of them and act as "bridges".

In this paper, we aim at providing a contribution in this setting by proposing an approach to computing the scope of a thing in a MIoT. Specifically, after having provided an overview on the MIoT paradigm (Section 2), we present a definition of scope along with a formalization allowing the computation of the corresponding values (Section 3). Then, we illustrate an application of scope in the context of smart cities, where it can play a key role (Section 4). Thereafter, we present some tests conceived to understand its main features (Section 5). Finally, we draw our conclusions and have a look at some possible future developments of our ideas (Section 6).

## 2 The MIoT paradigm

In this section, we provide an overview of the MIoT paradigm, described in detail in [6]. A MIoT $\mathcal{M}$ consists of a set of $m$ Internets of Things. Formally speaking:

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

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 $\iota_{j_k}$, representing it in $\mathcal{I}_k$. The instance $\iota_{j_k}$ consists of a virtual view (or, better, a virtual agent) representing $o_j$ in $\mathcal{I}_k$. For example, it provides all the other instances of $\mathcal{I}_k$, and the users who interact with this IoT, with all the necessary information about $o_j$. Information stored in $\iota_{j_k}$ is represented according to the format and the conventions adopted 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 a link from $n_{j_k}$ to $n_{q_k}$. A label can be associated with $a_{jq_k}$; it stores the set $tranSet_{jq_k}$ of the transactions performed from $\iota_{j_k}$ to $\iota_{q_k}$ in the past.

Finally:

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

Here:

- $N = \bigcup_{k=1}^{m} N_k$;
- $A = A_I \cup A_C$, where $A_I = \bigcup_{k=1}^{m} A_k$ and $A_C = \{(n_{j_k}, n_{j_q}) | n_{j_k} \in N_k, n_{j_q} \in N_q, k \neq q\}$.

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

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 Objects) Alliance [2]. 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 metadata*; *(iii)* $MD_j^B$, i.e., the set of *behavioral metadata*. All details about these metadata can be found in [6].

Now, we can define the set $tranSet_{j_k}$ of the transactions activated by $\iota_{j_k}$ in $\mathcal{I}_k$. Specifically, let $\iota_{1_k}, \iota_{2_k}, \cdots, \iota_{w_k}$ 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, $tranSet_{j_k}$ is given by the union of the sets of the transactions from $\iota_{j_k}$ to all the other instances of $\mathcal{I}_k$.

## 3 Scope definition

In this section, we present the definition of the scope of an instance $\iota_{j_k}$ in an IoT $\mathcal{I}_k$ and of the scope of an object $o_j$ in a MIoT. For this purpose, we must introduce some preliminary concepts.

The first of them is the one of neighborhood of an instance $\iota_{j_k}$ in $\mathcal{I}_k$. Specifically, the neighborhood $nbh(\iota_{j_k})$ of $\iota_{j_k}$ 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 $\iota_{j_k}$ through an incoming or an outgoing arc, which shared at least one transaction with $\iota_{j_k}$. In the following of this paper, we are interested only to $out\_nbh_{j_k}$; as a consequence, when we will use the term "neighborhood", we will implicitly mean "out_neighborhood".

Now, we need to introduce *the neighborhood of level t* of an instance $\iota_{j_k}$ in its IoT $\mathcal{I}_k$. It is an extension of the concept of $out\_nbh_{j_k}$ and is defined as follows:

$$out\_nbh_{j_k}^t =$$

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

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

After this, we must introduce the definition of the Trust Degree $TD_{qj_k}$ of an instance $\iota_{q_k}$ in the instance $\iota_{j_k}$ in $\mathcal{I}_k$. It can be defined as the fraction of the transactions sent by $\iota_{j_k}$ to $\iota_{q_k}$ that have been requested by $\iota_{q_k}$ or that $\iota_{q_k}$ did not request but it has considered so interesting to repost or to elaborate them[3]. In order to formalize $TD_{qj_k}$, we must introduce:

- the set $reposted_{q_k}$ of the transactions received by $\iota_{q_k}$ of $\mathcal{I}_k$ and reposted by it;
- the set $elaborated_{q_k}$ of the transactions received by $\iota_{q_k}$ whose contents it elaborated for its purposes;
- the set $requested_{q_k}$ of the transactions explicitly requested by $\iota_{q_k}$.

If $\iota_{q_k}$ belongs to $out\_nbh_{j_k}$, $TD_{qj_k}$ can be expressed as:

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

Starting from this definition and from the concept of $out\_nbh_{j_k}^t$, we can proceed with the transitive closure of $TD_{qj_k}$ in such a way as to extend it to the case in which $\iota_{q_k}$ is indirectly connected to $\iota_{j_k}$. In particular, the general definition of $TD_{qj_k}$ is as follows:

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

The next step regards the definition of the concept of Impact Degree $ID_{j_k}$ of an instance $\iota_{j_k}$ 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 $\iota_{j_k}$. It can be formalized as follows:

$$ID_{j_k} = \frac{\sum_{\iota_{q_k} \in out\_nbh_{j_k}} TD_{qj_k}}{|out\_nbh_{j_k}|}$$

We are now able to define the Scope $Sc_{j_k}^t$ of level $t$ of an instance $\iota_{j_k}$ of $\mathcal{I}_k$. Specifically, $Sc_{j_k}^t$ is defined as the weighted sum of the Impact Degrees of the

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

instances belonging to $out\_nbh^t_{j_k}$, where the weights are the trust values that these instances have in $\iota_{j_k}$. This sum is then averaged by the number of the instances belonging to $nbh^t_{j_k}$. Formally speaking:

$$Sc^t_{j_k} = \frac{\sum_{\iota_{q_k} \in out\_nbh^t_{j_k}} TD_{qj_k} \cdot ID_{q_k}}{|out\_nbh^t_{j_k}|}$$

Now, we can define the Scope $Sc^t_j$ of level $t$ of an object $o_j$ in the MIoT. It is obtained by averaging the Scope of level $t$ of its instances in the corresponding IoTs. Specifically, let $Inst_j = \{\iota_{j_1}, \iota_{j_2}, \cdots, \iota_{j_l}\}$ be the instances of $o_j$ in the IoTs of the MIoT. Then:

$$Sc^t_j = \frac{\sum_{\iota_{j_k} \in Inst_j} Sc^t_{j_k}}{|Inst_j|}$$

From the definitions of $TD_{qj_k}$, $ID_{qj_k}$, $Sc^t_{jk}$ and $Sc^t_j$ it emerges that each of these parameters belongs to the real interval $[0, 1]$.

## 4 Applications

In a scenario characterized by the pervasive diffusion of increasingly intelligent and social objects, our approach can have a large variety of applications. Two very interesting ones regard smart cities and shopping centers. Due to space limitations, we describe in detail only the first one.

Consider some public areas (such as parks, squares, shopping centers, etc.) in a (smart) city, and assume that a set 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 be provided with several smart devices, such as smartwatches, smartphones, other wearable devices, and so forth. Persons and places can interact with each other through the corresponding smart objects.

Such a scenario can be modeled through a MIoT $\mathcal{M}$ consisting of a set $\{\mathcal{I}_1, \mathcal{I}_2, \cdots, \mathcal{I}_m\}$ of IoTs, each representing a public area. The set of the objects of $\mathcal{M}$ comprises the smart objects installed 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 $\iota_{j_k}$ in the IoT $\mathcal{I}_k$. Clearly, when a person with a smart object $o_j$ moves around different public areas corresponding to different IoTs, $o_j$ will have different instances, one for each IoT.

Each visitor of an area is generally interested to 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 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 check data provided by the sensors of each public area of her interest, the information hubs or other trusted runners. The choice of the data sources to consult is usually related to the corresponding trustworthiness and the easiness of getting desired information from them. 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 the person has performed her choice, she can send 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 made, 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 user choices can be coupled with those registered during the activities she performed therein (e.g., data coming from personal smart wears) 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 in her smart wears. In this case, the scope of the smart wears is useful to understand how extended and how strong is its 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 scope in this context. As a matter of fact, knowing the objects with the highest impact 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 MIoT could assume the role of reliable information hubs for the whole MIoT if their scope is particularly strong and large over time.

## 5 Experiments

In order to perform our experiments, since real MIoTs 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 MIoTs with certain characteristics specified by the user.

The MIoTs created by our simulator follow the paradigm described in Section 2. 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 created MIoTs, our simulator leverages a real dataset. It regards the taxi routes in the city of Porto from July $1^{st}$ 2013 to June $30^{th}$ 2014. It can be found at the address `http://www.geolink.pt/`

ecmlpkdd2015-challenge/dataset.html. Each route contains several Points of Interests corresponding to the GPS coordinates of the vehicle.

We partitioned the city of Porto in six areas and associated a real IoT with each area. Our simulator associates an object with a given route recorded in the dataset and an object instance with each partition of a route belonging to an area. It creates a MIoT node for each instance and a c-arc for each pair of instances belonging to the same route. Furthermore, it creates an i-arc between two nodes of the same IoT if the length of the time interval between the corresponding routes is less than a certain threshold $th_t$. The value of $th_t$ can be specified through the constructor interface. Clearly, the higher $th_t$ the more connected the constructed MIoT.

The MIoT for this experiment, which we constructed through our simulator, consisted of 1256 nodes. This number of nodes is much higher than the ones presently characterizing real MIoTs. However, we preferred to construct such a large MIoT because we think that, with the enormous development of the IoT, in the future there could exist MIoTs consisting of thousands of nodes. On the other side, we did not adopt larger MIoTs because they required excessive computation times without providing more knowledge on scope than the one we could have acquired with a MIoT of about 1000 nodes. The six IoTs 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. The interested reader can find the MIoT adopted in the experiments described here at the address http://daisy.dii.univpm.it/miot/datasets/scope.

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:

- Python, as programming language;
- Neo4J (Version 3.4.5), as underlying DBMS.

In these experiments, we aimed at investigating the trend of the scope against the neighborhood level $t$. In particular, for each instance $\iota_{j_k}$ of the MIoT, we computed $Sc^t_{j_k}$ when $t$ increases from 1 to the diameter of $\mathcal{I}_k$. After this, we grouped the instances of our MIoT in several ways (one for each test), based on some specific rationales, and we computed the variation of the average values of the scope for each group.

As a first task of this activity, we computed the variation of the average values of the scope for each IoT of the MIoT. This is equivalent to say that the instances of the MIoT were grouped in the corresponding IoTs (one group for each IoT). The obtained results are reported in Figure 1. From the analysis of this figure, we can observe that, in each IoT, the scope decreases quite quickly. Indeed, it is extremely high when $t = 1$ in all the IoTs. When $t = 2$, the scope is high for the largest IoTs, whereas it has an intermediate value for the other ones. In any case, the scope becomes very low when $t$ is greater than or equal to 4 for small networks and when $t$ is greater than or equal to 5 for the large ones.

As a second task, we computed the variation of the average values of the scope for the whole MIoT. This is equivalent to say that we had a unique group

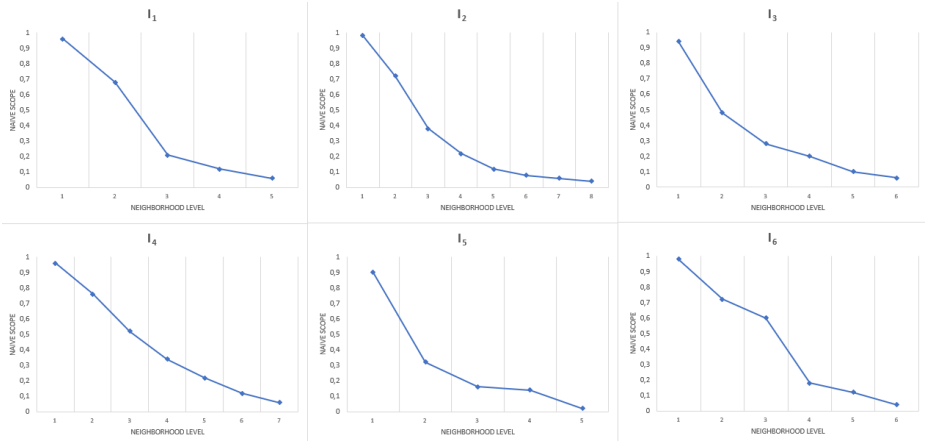


**Fig. 1.** Variation of the average scope for each IoT of the MIoT against the neighborhood level

comprising all the instances of the MIoT. The obtained results are reported in Figure 2. From the analysis of this figure, we can conclude that the scope presents a trend similar to the one of the largest IoTs of Figure 1. In particular, it is very high for $t = 1$; it is high for $t = 2$; it has an intermediate value for $t = 3$, whereas it is very low for $t > 5$.

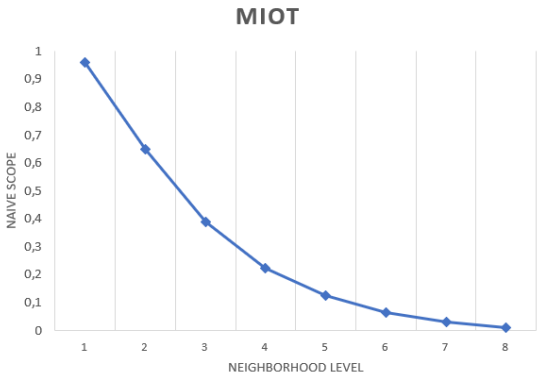


**Fig. 2.** Variation of the average scope for the whole MIoT against the neighborhood level

As a final task, we subdivided all the instances of the MIoT in two groups containing i-nodes and c-nodes, respectively. Then, we computed the variation of the average values of the scope for the two groups. The final goal of this task was to verify if i-nodes and c-nodes showed different behaviors as far as their scope

is concerned. The obtained results are reported in Figure 3. From the analysis of this figure, we can observe that the scope decreases for both i-nodes and c-nodes. However, the trends are different. Indeed, the decrease is much smother for i-nodes than for c-nodes. In particular, for c-nodes, the decrease is very steep because the scope is less than 0.2 already for $t = 3$. This 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 3 represent a confirmation) 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.

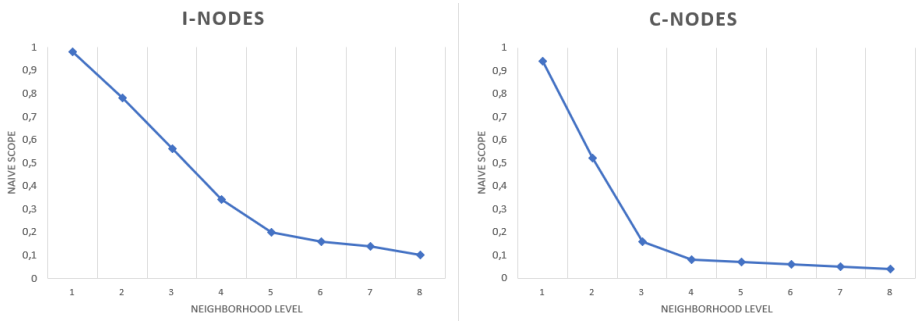


**Fig. 3.** Variation of the average scope for the i-nodes and the c-nodes of the MIoT against the neighborhood level

As for the investigation of the values of the scope for objects, we observe that they are obtained by averaging the values of the scope 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 the scope of objects for the whole MIoT is reported in Figure 4. As we could have expected, this trend is very similar (or, better almost identical) to the one of Figure 2.

## 6 Conclusion

In this paper, we have seen that social internetworking and the Internet of Things are becoming more and more contiguous and are giving rise to several social and/or multiple IoTs paradigms. In this new scenario, we have introduced the concept of scope of a thing in a MIoT, along with a formalization allowing the computation of the corresponding values. Then we have illustrated one possible application along with some experiments aiming at evaluating the variation of scope against the value of the neighborhood level.

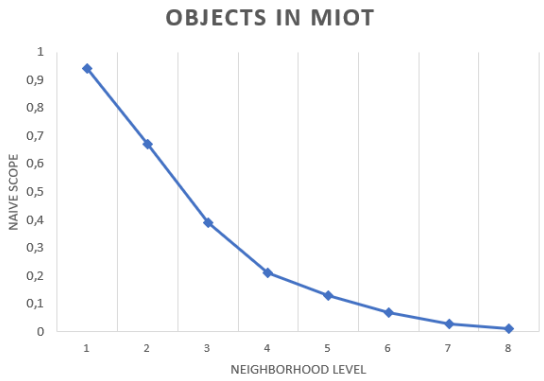


**Fig. 4.** Variation of the average scope for the objects of the MIoT against the neighborhood level

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 on 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, for understanding the extension and the importance of the damage caused by them. Finally, we would like to analyze the exploitation of scope in predictive maintenance, that is currently one of the most important research issues in the manufacturing industry.

## References

1. Concise Oxford Dictionary. *https://en.oxforddictionaries.com/*, 2019.
2. IPSO Alliance. *https://www.ipso-alliance.org/*, 2019.
3. 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.
4. 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.
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. 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.
8. 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.

9. A. Forestiero. Multi-agent recommendation system in internet of things. In *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, CCGRID 2017, Madrid, Spain, May 14-17, 2017*, pages 772–775. IEEE Computer Society / ACM, 2017.
10. 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.
11. R. Lea and M. Blackstock. Smart cities: an iot-centric approach. In *Proceedings of the 2014 International Workshop on Web Intelligence and Smart Sensing, IWWISS '14, Saint Etienne, France, September 1-2, 2014*, pages 12:1–12:2. ACM, 2014.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.
21. Z. Zhou, C. Gao, C. Xu, Y. Zhang, S. Mumtaz, and J. Rodriguez. Social big-data-based content dissemination in internet of vehicles. *IEEE Transaction on Industrial Informatics*, 14(2):768–777, 2018.