www.ijaceeonline.com ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 3, Issue 1, January 2018, pp. 10–15

Secured Friendship Selection to Increase Navigability in Social Internet of Things

Dr.S.Malliga
Professor, Department of Computer Science and Engineering,
Kongu Engineering College, Erode, Tamil Nadu, India
Email: mallinishanth72@gmail.com

Dr.SV.Kogilavani
Associate Professor, Department of Computer Science and Engineering,
Kongu Engineering College, Erode, Tamil Nadu, India
Email: kogilavani@kongu.ac.in

Dr.C.S.Kanimozhiselvi
Professor, Department of Computer Science and Engineering,
Kongu Engineering College, Erode, Tamil Nadu, India
Email: kanimozhi@kongu.ac.in

Abstract: *A new paradigm of being "Always Connected" is what our society is now steadily moving towards. This is due to the advent of smart devices. Communication now involves 'things' (device of various sorts) in addition to persons thus bringing about the 'Internet of Things' (IoT) environment in which objects will have virtual counterparts on the Internet. IoT has a large number of smart objects which automatically interact with each other through various communication protocols and unique addressing schemes for the search of services. They also collaborate with their neighbors to achieve common goals. As the number of devices on the Internet increases, searching for the right device for the required service is of chief importance. Social networking concepts are incorporated into IoT called Social Internet of Things (SIoT). Smart objects can find the desired services through their friends in a de-centralized manner using only local information. However, a node may have many friends, and each friend node, in turn may have many more new friends, and so on. High computational and memory demands are required for processing all the links. Hence it is important to thoughtfully reduce the friends of a node by applying some strategies in order to reduce computational load and at the same time preserve network navigability. A remarkable work in this area has been done. This work adds trustworthiness to the already proposed strategies. An analysis is also performed based on metrics like average clustering coefficient, average path length and average degree of connections.*

Keyword: *Internet of Things (IoT), Social Internet of Things (SIoT), Network Navigability, Trustworthiness.*

1. INTRODUCTION

IoT is a world-wide network of interconnected objects [1] which are uniquely addressable based on standard communication protocols. The objects could be anything ranging from small sensors devices to large multi-purpose computers. There is no doubt that the IoT will make its pervasive presence in every aspect of our world and it is bound to make a huge impact in our everyday life as stated by the US National Intelligence Council (NIC) [2], "by 2025 Internet nodes may reside in everyday things − food packages, furniture, paper documents, and more". It is estimated that the IoT will be composed of trillions of objects interacting in an extremely heterogeneous way in terms of requirements, behavior and capabilities [3].

One of the biggest challenges posed to the research community is how to organize such a huge collection of devices so as to facilitate efficient discovery of objects and services, and provide scalability to the growing demands. Recently, there have been quite a number of independent research activities into investigating the possibilities of integrating social networking concepts into IoT. The motivation behind the idea of integrating social networks paradigm into IoT can be traced back to a seminal idea proposed by Stanley Milgram during 1969 [4]. The idea is based on the fact that if someone belongs to a global friendship network, then not only he/she does have paths of friends connecting one to a large fraction of the

Cite this paper:

S. Malliga, SV.Kogilavani, C. S. Kanimozhiselvi, "Secured Friendship Selection to Increase Navigability in Social Internet of Things", International Journal of Advances in Computer and Electronics Engineering, Vol. 3, No. 1, pp. 10-15, January 2018.

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 3, Issue 1, January 2018, pp. 10–15

world's population, but these paths are, in fact, surprisingly short.

IoT can be generalized as things that talk with other devices. Since the objects collaborate to accomplish a common goal, they need to use the services offered by other objects. With the advancement of technologies, devices on the Internet are getting smarter and are proliferating rapidly. With this increasing number of objects, the selection of service becomes a tedious task as a device can have enormous number of connections with other entities of heterogeneous nature. The convergence of Social Networks and IoT is now called as Social Internet of Things (SIoT).

The term 'Social Networking' not only revolves around the online social networking websites but also the natural social relations among people. Social networking involves the use of dedicated websites and applications to interact with other users, or to find people with similar interests to one's own. The communication between the objects is governed by the relationship with other objects. The objects that are closely related to other objects and can directly communicate without any intermediate agent are called neighbors or friends. The smart objects can communicate with their friends directly and the process continues resulting in communication with devices which are not friends in a de-centralized manner. Thus it makes the smart objects more a social entity, giving rise to the term Social Objects [5].

The article is orchestrated as follows: Section 2 deals with the work already done in friendship selection. The present and proposed strategies are discussed in Section 3. The simulation details and results of the simulation are explained in Section 4. Section 5 concludes the study and provides guide for future work.

2. LITERATURE REVIEW

Service in IoT is looked in such a way that the object which needs a service will first search among its friends. If the desired service is not available with its friends, then the search proceeds to the next level i.e. friends of friends, thereby initiating a de-centralized searching process. Service searching is one of the major research activities in IoT. The various research challenges in locating the desired service in an efficient way is addressed in [6]. This section presents the recent researches on searching for services in brief.

Atzori [7] has addressed the IoT with a view to identify and track technologies using enhanced communication protocols and distributed intelligence for smart objects. Different versions of IoT paradigms are reported and enabling technologies are reviewed. The issues faced by research community of IoT and most relevant among them are discussed in this paper and the basic IoT scenario is also explained. He also proposed techniques in IoT using social networking concepts. The techniques enhance the level of trust between objects that are friends with each other. This paper also analyzes major opportunities arising from the interaction of social networking concepts with the IoT, presents the major ongoing research activities and points out the most critical technical challenges in the existing IoT environments. The objects are enhanced with social networking concepts thus transforming the smart objects in the IoT into social objects.

Michele Nitti [8] proposed a SIoT wherein the social networking concepts are integrated into IoT. The basic idea is to search for service in a de-centralized manner through the friends considering only the local network properties. As the scalability of devices connected increases, there is an increase in number of friends. This ultimately slows down the searching process. This paper attempted to increase the overall network navigability by adopting several five strategies to select efficient neighbors to get the required services. But, this work did not consider one fundamental aspect (i.e) it did not consider node similarity for the discovery operations. The nodes try to reach the destination using only information about the degree of their neighbors. However, external properties could also be used to select the right nodes (among the available friends) to which ask for the desired service. One of these properties is the profile of the friend involved, its trustworthiness [9], and the type of relationship that links it to the requester.

This paper extends the above work by considering the trustworthiness of the nodes for providing the services. It is important to understand how the information provided by members of the social IoT has to be processed so as to build a reliable system on the basis of the behavior of the objects. According to [9], there are two models for trustworthiness management from the solutions proposed for P2P and social networks. In the subjective model, each node computes the trustworthiness of its friends on the basis of its own experience and on the opinion of the friends in common with the potential service providers. In the objective model, the information about each node is distributed and stored making use of a distributed hash table structure so that any node can make use of the same information. This work uses subjective trustworthy computation to determine the nodes that can provide services.

3 PRESENT AND PROPOSED STRATEGIES

3.1 An Example Scenario

In the scenario depicted in Figure 1, the IoT environment is visualized as a graph, where each node represents a device and the edge between any node to any other nodes is depicted as the friendship link of the nodes under consideration irrespective of the physical distance. The nodes with higher degree are

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 3, Issue 1, January 2018, pp. 10–15

shown bigger in size than the nodes with lower degrees.

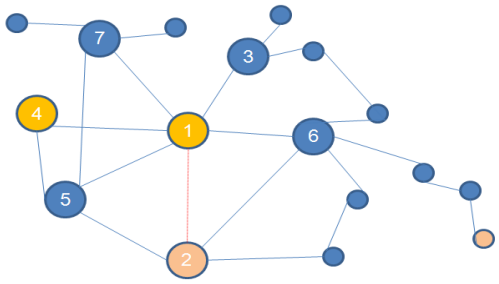

Figure 1 Example IoT scenario implementing de-centralized search

Consider that the node6 searches for a service that can be offered by node4. Now node6 initiates the search by searching its first hop friends namely, node1, node 2 etc. If the desired service is not found, the search is propagated through its friends by searching its 'friends of friends. Eventually the search terminates in the node that provides the desired service. The path found is through node-1 and node-13.

3.2 Existing Strategies

The friendship selection has already been illustrated in [1] by Nitti et al. wherein 5 heuristics are proposed for selecting efficient friendship links.

The heuristics proposed in [1] are given below.

Reject after Nmax: A threshold value named Nmax is assigned and any new request after Nmax friends will be rejected by the device. This makes the device to have static friends.

Maximize Neighborhood: After reaching Nmax friends, if a new device sends a request, then thenode deletes a friend node with minimum degree to make room for requesting one. This strategy is to increase the reachability of the node.

Minimize Neighborhood: After reaching Nmax friends, to accept any new request the node with maximum degree is deleted.

Maximize clustering: On a new request after Nmax connections, a friend node with minimum number of mutual friends is eliminated.

Minimize clustering: In the event of a new request after Nmax connections, then a friend node with maximum number of mutual friends is eliminated.

For instance, strategy-4 achieves a maximum local clustering but suffers from low percentage of giant component. Since the existence of giant component is essential for network navigability, lower giant component entails reduction in the overall search efficiency even though it guarantees high local clustering co-efficient.

But these strategies still lack in some aspects such as understanding how the information provided by the other members have to be processed so as to build a reliable system on the basis of the behavior of the objects. Indeed, without effective trust management foundations, attacks and malfunctions in the IoT will outweigh any of its benefits [10]. Hence, in this work, trustworthiness is calculated for the nodes and it is used to decide upon the strategy to be followed. This is explained in following section.

3.3 Computation of Trustworthiness

By using the above connectivity is formed. Since the network is subjected to various security issues to ensure the trustworthiness among the nodes, trustworthiness concept is implemented. In the work [9], two models for trustworthiness management from the solutions proposed for P2P and social networks are defined. In the subjective model, each node computes the trustworthiness of its friends on the basis of its own experience and on the opinion of the friends in common with the potential service providers. In the objective model, the information about each node is distributed and stored making use of a distributed hash table structure so that any node can make use of the same information. This work uses subjective trustworthy computation to determine the nodes that can provide services in a secured manner.

4. SIMULATION AND ANALYSIS

4.1 Simulation

Things with sensing and communication capabilities are called smart objects. In the IoT environment, every object is supposed to be a smart one. Since IoT is not completely deployed till date, experimentation on IoT environment is generally simulated using a tool, for instance, Gephi [11]. For simulation of objects and its friendship, Barabasi–Albert model (BA) [12] is used. BA algorithm generates random scale-free network. SIoT is expected to follow scale-free network, since the online social network analysis reports that online social network of human follows a complex scale-free network. An object entering into IoT network should have a least a number of friends; this can be modeled using BA model. BA model follows the power law for generating degrees for nodes at each step.

The idea of using subjective model to compute trustworthiness has been borrowed and used from [9]. According to the subjective model, each node stores and manages the feedback needed to calculate the trustworthiness level locally. This is intended to avoid a single point of failure and infringement of the values of trustworthiness. Consider the scenario where pi and pj are adjacent nodes, i.e., they are linked by a social relationship. The other scenario where they are farer each other in the social network is also considered. Tij is the trustworthiness of pj seen by pi and is computed as shown in Equation 1.

$$T_{ij} = (1-\alpha-\beta)\, R_{ij} + \alpha\, O^{dir}{}_{ij} + \beta\, O^{ind}{}_{ij} \qquad (1)$$

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 3, Issue 1, January 2018, pp. 10–15

pi computes the trustworthiness of its friends on the basis of their centrality Rij of its own direct experience Odirij and of the opinion Oindij of the friends in common with node pj (Kij). The centrality of direct experience and opinion is calculated as given in [9]. For the simulation, the parameters are set as given in [9] and shown below in Table I.

TABLE I SETTING OF PARAMETERS

Parameters	Description	Default values
M	Number of nodes in SIoT	800
mp	% of malicious nodes	25%
mr	% of transaction a malicious node acts as malicious	100%
res	% of nodes respond to a transaction request	5%
L_{lon}	Number of transaction in the long term opinion	50
L_{rec}	Number of transaction in the short term opinion	5
N	Number of run for each experiment	4
α	Weight of the direct opinion	0.4
β	Weight of the indirect opinion	0.3
γ	Weight of the long-term opinion	0.5
δ	Weight of the relationship factor	0.5

If pi and pj are not friends, then the trustworthiness is calculated by word of mouth through a chain of friendships. That is, if pi, that requests the service, and pj ,that provides it, are not adjacent, i.e., are not linked by a direct social relationship, the computation of all the trustworthiness values is carried out by considering the sequence of friends that link indirectly pi to pj.

4.2 Analysis of Results

Analysis is made using the following metrics in the formulation of the heuristics along with trustworthiness:

Average Degree: Degree refers to the number of friends of a node. Average degree is calculated as the ratio of number of degrees of each node to the total number of nodes. The average degree increases with the increase in number of relationships among nodes.

Average clustering Co-efficient: It refers to the closeness of the nodes to form a complete graph. It defines how the nodes are embedded in the neighborhood. Clustering coefficient is calculated for each node and it ranges from 0 to 1. The expression for clustering coefficient differs for undirected and directed network, which are presented in Equation 2 and Equation 3.

For undirected network,

$$C_n = \frac{2e_n}{(k_n(k_n-1))} \quad (2)$$

Whereas for directed network,

$$C_n = \frac{e_n}{(k_n(k_n-1))} \quad (3)$$

Where kn is the number of neighbors of n and en is the number of connected pairs between all neighbors of n. The average clustering co-efficient for all the nodes is calculated as given in Equation 4.

$$\overline{C} = \frac{1}{n}\sum_{i=1}^{n} C_i \quad (4)$$

where n is the total number of nodes in the network. Ci is the local clustering co-efficient of each node.

Average path length: The shortest distance between any two nodes in the network is averaged as average path length. The efficient strategy should intend towards reducing the average path length.

All these strategies are applied to the network shown in Figure 1 and the statistics are taken after implementing each strategy with established network structure. The final results are analyzed in terms of average degree, average clustering coefficient, giant component and average path length.

4.2.1 Average Clustering Coefficient

Clustering coefficient is calculated for each node and it ranges from 0 to 1. Average local clustering is the mean value of individual coefficients and is calculated based on main-memory triangle computations for very large graphs. The average clustering coefficient for example graph: 0.422

After implementing these strategies, Average Clustering Coefficient for all the strategies are shown in the Table II.

TABLE II AVERAGE CLUSTERING COEFFICIENT

Strategy	Average Clustering Coefficient
Reject after Nmax	0.422
Maximize Neighborhood	0.21
Minimize Neighborhood	0.21
Maximize Clustering	0.44
Minimize Clustering	0.1

The above table shows that if we follow the strategy4, there will be more reachability of nodes.

4.2.2. Average degree

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 3, Issue 1, January 2018, pp. 10–15

The average degree is computed to find the relationships since the average degree and the numbers of relationship are directly proportional. The average Degree for the example graph is calculated. After implementing strategies average degree for all the strategies are shown in Table III.

TABLE III AVERAGE DEGREE

Strategy	Average Degree
Reject after Nmax	2.57
Maximize Neighborhood	2.33
Minimize Neighborhood	1.33
Maximize Clustering	1.97
Minimize Clustering	1.33

The average degree for strategy 1 and 2 is found to be more that other nodes. This means these nodes will improve the reachability to other nodes.

4.2.3 Average Path Length

The shortest distance between any two nodes in the network is averaged as average path length. It should be kept as low as possible so that the fast reachability of a node from another node increases. After implementing strategies, Average Path length for all these strategies are shown in the Table IV.

TABLE IV AVERAGE PATH LENGTH

Strategy	Average Path length
Reject after Nmax	1.61
Maximize Neighborhood	1.63
Minimize Neighborhood	1.63
Maximize Clustering	1.46
Minimize Clustering	1.81

The above table shows that strategy 4 will be a better one than others for the sample graph.

4.2.4 Trustworthiness

The requested node requests for the trust value from the requesting node and these values are obtained through opinion from the past transactions between the neighbors through the social relationship. In subjective model, each node stores and manages the feedback and all the information needed to calculate the trustworthiness level. Trustworthiness for example graphs are calculated. After implementing these strategies, trustworthiness value for all these strategies are shown in the Table V.

From the above table, it can be understood that strategy 4 provides a better trustworthiness that other strategies. That is, the opinion about the neighbor in other strategies is not as good as the strategy 4.

Even though this work can suggest a strategy to be followed while requesting service, it is found that no on strategy is good in all situations. The strategy depends on the network structure and opinion of a node about its friends. ence, this work concludes that based on dataset a strategy which gives better reachability can be used for selecting the node for receiving a service.

TABLE V TRUSTWORTHINESS

Strategy	Average Path length
Reject after Nmax	0.89
Maximize Neighborhood	0.71
Minimize Neighborhood	0.73
Maximize Clustering	0.91
Minimize Clustering	0.86

5. CONCLUSIONS AND FUTURE WORK

This paper has addressed the challenges imposed on service selection in the IoT network. It has extended the methodologies of incorporating the social networking concepts in IoT by selecting efficient friends that makes the total network more navigable which in turn makes the service discovery more efficient. Heuristics or strategies addressed in earlier work for friendship selection which impacts the overall network parameters such as average degree, giant component, average local clustering coefficient and average path length have been analyzed. The strategies are found to have a better network navigability with a large giant component. But these strategies lack in some aspects such as understanding how the information provided by the other members have to be processed so as to build a reliable system on the basis of the behavior of the objects. This work extends the basic strategies by considering the trustworthiness. Indeed, without effective trust management foundations, attacks and malfunctions in the IoT will outweigh any of its benefits. Hence, in this work, trustworthiness is calculated for the nodes and it is used to decide upon the strategy to be followed.

The other aspects which could further improve the proposed work include the consideration of profile of the friend involved and the type of relationship that links the requesting node to the requested node. The work has also not focused on delivery of the service. Depending on how the SIoT model is implemented, the service can be delivered either directly relying on the communication network or through the friends that discovered the service. These issues will be considered as future scope of the proposed work.

REFERENCES

[1] Michele Nitti, Luigi Atzori, and Irena Pletikosa Cvijikj. (2015), “Friendship Selection in the Social Internet of Things: Challenges and Possible Strategies” IEEE Internet of Things Journal, Vol. 2, No. 3, pp. 240-247.

[2] National Intelligence Council, Disruptive Civil Technologies — Six Technologies with Potential Impacts on US Interests Out to 2025 — Conference Report CR 2008–07, April 2008, Online: www.dni.gov/nic/NIC_home.html

[3] LuigiAtzori, AntonioIera, GiacomoMorabito, MicheleNitti. (2012), “The Social Internet of Things (SIoT)—When social

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 3, Issue 1, January 2018, pp. 10–15

networks meet the Internet of Things: Concept, architecture, and network characterization" Computer. Network, Vol. 56, No. 16, pp. 3594–3608.
[4] Jeffrey Travers and Stanley Milgram,(1969), "An experimental study of the small world problem" Sociometry, Vol. 32, No. 4, pp. 425-443.
[5] Luigi Atzori, Antonio Iera, and Giacomo Morabito. (2014), "From Smart Objects to Social Objects: the next evolutionary step of the Internet of Things" IEEE Communication Magazine.
[6] Daqiang Zhang, Laurence T. Yang_; Hongyu Huang. (2011), "Searching in Internet of Things: Vision and Challenges" *Proceedings of IEEE 9th International Symposium on Parallel Distributed Processing Applications (ISPA)*, pp. 201–206.
[7] Luigi Atzori, Antonio Iera, and Giacomo Morabito. (2010), "The Internet of things: a survey" Computer Networks, Vol. 54, No. 15, pp. 2787–2805
[8] Michele Nitti, Luigi Atzori, and Irena Pletikosa Cvijikj. (2014), "Network navigability in the Social Internet of Things" *Proceedings of IEEE World Forum Internet Things (WFIoT)*, pp. 405–410.
[9] Michele Nitti, Roberto Girau, Luigi Atzori. (2014), "Trustworthiness management in the social Internet of Things. Knowledge and Data Engineering" IEEE Transactions on Knowledge and Data Engineering, Vol. 26, No. 5, pp. 1253–1266.
[10] Rodrigo Roman, Pablo Najer, Javier Lopez. (2011), "Securing the Internet of things" Computer, Vol. 44, No. 9, pp. 51–58
[11] http://www.gephi.org
[12] Sun Tie-li, Deng Jing-wei, Deng Kai-ying. (2008), "Scale-free network model with evolving local-world" *Proceeding of 4th Int. Nat. Comput. Conf.*, pp.237–240

Authors Biography

Dr. S.Malliga is working as a Professor in the Department of Computer Science and Engineering, Kongu Engineering College, Tamil Nadu, India. She has completed PhD in the year 2010 from Anna University, Chennai. Her main research area is Network and Information Security. She has done consultancy project for BPL and offered several courses on latest technology. Currently she is guiding three research scholars. She has also guided many UG and PG projects. She has published 12 articles in international journals and presented more than 25 papers in national and international conferences in her research and other technical areas.. She is also interested in cloud and virtualization technolgies.

Dr. S.V.Kogilavani is associated with the Department of Computer Science and Engineering as an Associate Professor at Kongu Engineering College, Tamil Nadu, India. Her research is in information retrieval and summarization. She got her Ph.D from Anna Unviesity, Chennai in the year 2013. She has presented many papers in national and international conferences and published 6 papers in national and international journals. She conducted many courses for the benefits of students.

Dr. C.S.Kanimozhi Selvi, professor, Department of Computer Science and Engineering. Kongu Engineering College, Erode, Tamil Nadu, India, is interested in Data Mining and has received her PhD in association rule mining and classification from Anna University, Chennai. Her current research interests are security issues in Cloud and Data Mining. Her research articles are published in national and international journals. She has involved herself in big data analytics.

Cite this paper:

S. Malliga, SV.Kogilavani, C. S. Kanimozhiselvi, "Secured Friendship Selection to Increase Navigability in Social Internet of Things", International Journal of Advances in Computer and Electronics Engineering, Vol. 3, No. 1, pp. 10-15, January 2018.