Trust Management in Social Internet of Thing

Preeti Patil
M.E. Computer Network Student,
G.H.R.C.E.M. Wagholi, Pune
Savitribai Phule Pune University, PUNE, India

Mansi Bhonsle
Assistant Prof. (Comp.Engg.)
G.H.R.C.E.M. Wagholi, Pune Savitribai Phule Pune
University, PUNE, India

ABSTRACT
Internet of Things allows the interconnection of smart objects, such as mobile robots, wireless sensors, etc., and of human beings, by using various communication protocols and by developing a dynamic multi-modal heterogeneous network. The Internet of Things is expected to be overpopulated by a very huge number of objects, with intensive interactions, heterogeneous communications and millions of services. Consequently, scalability issues will arise from the search of the right object that can provide the desired service. A new paradigm known as Social Internet of Things has been introduced and proposes the integration of social networking concepts into the Internet of Things. The underneath idea is that every object can look for the desired service using its friendships, in a distributed manner. The cluster between Internet of Things (IoT) and social networks (SNs) enables the connection of people to the ubiquitous computing universe.[1]

Keywords
Internet of things, social networks, SIOT, trustworthiness management

1. INTRODUCTION
The Internet of Things (IoT) is the network of physical objects or "things" embedded[1] with electronics, software, sensors[2] and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Thus IoT is the network connectivity between objects allowing them to send and receive data. The Social Internet of Things (SIoT) is based on the notion of social relationships among objects. It is like creating a social network like facebook or twitter among smart objects and humans.[2] Through the SIoT paradigm, the capability of humans and devices to discover, select, and use objects with their services in the IoT is augmented. Besides, a level of trustworthiness is enabled to steer the interaction among the billions of objects which will crowd the future IoT.

2. RELATED WORK
Smart objects are conveyed into usage, all things considered,by people. There are around 7 billion people in world consequently expected number of brilliant articles is trillions. We have informal organizations set up so that 7 billion individuals could connect admirably and offer the information safely. Henceforth idea of long range interpersonal communication is being connected to web of items with the goal to discover right protest, approve information and oversee information created by trillions of articles.[2] Give us a chance to consider the accompanying case of execution of SIoT in the field of pharmaceutical to get the fundamental thought.

3. EXISTING SYSTEM
The Internet of Things (IoT) is the network of physical objects or "things" embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications.[3]

Things, in the IoT, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, or field operation devices that assist fire-fighters in search and rescue. These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices. Current market examples include smart thermostat systems and washer/dryers that utilize Wi-Fi for remote monitoring.

4. PROPOSED SYSTEM
Humans usually interact with others in a wide variety of relationships during their everyday life. Also, they would utilize many smart services and applications from IoT improve their life quality. In IoT, as mentioned above, an individual user connects to the other(s) via legacy networks; on the other hand, sets of things collaborate with each other via the Internet for offering information to smart services and applications, while each user uses them. In order to practically integrate the ubiquitous computing in our future daily life with high Quality of Experience (QoE), we need to improve the connectivity of all the relationships between users and things, and to enhance the availability of computational power via sets of things surrounding us.[2] Therefore, we take into consideration social networks (SNs) of all entities (i.e., humans and things) for ubiquitous computing as an evolution beyond the IoT. In other words, things should be socialized for allowing humans to establish relationships with them in an easy way.

4.1 Social Internet of Things
Future ubiquitous computing will usher in a wide range of smart services and applications to cope with many challenges that individuals and organizations face in their everyday lives via allowing humans and things to be connected with either anyone or anything, in any place, at any time.[4] While IoT studies have typically mentioned communication to physical world by sensing or actuating through many of different

devices to be the biggest novelty, SIoT paradigm, however, raises important concerns about why and how to utilize these services and applications. For this objective, there are two considerations as shown in Fig. 1:

1) Increasing sociality (or connectivity) and

2) Improving pervasiveness (or availability)

4.2 The Architecture

In this section we provide an overview of a possible implementation of the SIoT. Here the major functions required to run the SIoT are illustrated. To describe the proposed system we resort on the simple three-layer architectural model for IoT presented in.[1] It consists of:

i. The sensing layer, which is devoted to the data acquisition and node collaboration in short- range and local networks;

ii. The network layer, which is aimed at transferring data across different networks; and

iii. The application layer, where the IoT applications are deployed together with the middleware functionalities.

Figure 1 shows the resulting three-layer architecture. The three basic elements of the proposed system are: the SIoT Server, the Gateway, and the Object

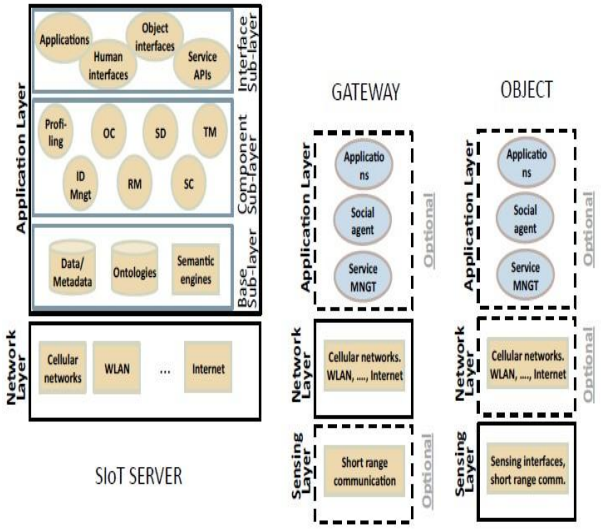

Figure 1: System architecture

Following the three- layer model made of the sensing, network, and application layer. The main SIoT components belongs to the application layer, wherein the relationship management (RM), service discovery (SD), service composition (SC), and trustworthiness management (TM) functionalities are located. The lines represent the optional layers in both the object and the gateway architecture.[1]

The basic elements of SIoT are: Application Layer

i) Base sub-layer: Includes the database for the storage and the management of the data and the relevant descriptors. Record the social member profiles and their relationships. Record the activities carried out by the objects in the real and virtual worlds. Data about humans (object owners as well as visitors) are also managed.

ii) Component sub-layer : Includes the tools that implement the core functionality of the SIoT system. ID management assigns an ID that universally identifies all the possible categories of objects. Profiling configures manually and automatically a (static or dynamic) information about the objects.

a) Owner control (OC) define activities performed object, information that can be shared, set of objects which can access such information and type of relationships that can be setup.

b) Relationship management (RM) allow objects to start, update, and terminate their relationships with other objects.

c) Service discovery (SD) finds which objects can provide the required service.

d) Trustworthiness management (TM) defines how the information provided by the other members shall be processed.

e) The service composition (SC) component enables the interaction between objects. Most of the time, the interaction is related to an object that wishes either to retrieve an information about the real world or to find a specific service provided by another object.

iii) Interface sub-layer: Here the third-part interfaces to objects, humans, and services are located. This sub-layer may be mapped onto a single site. It can be deployed in a federated way by different sites, or deployed in a cloud.

4.3 Gateway and Objects

As to the Gateway and Objects systems, the combination of layers may vary mainly depending on the device characteristics. The following three scenarios can be foreseen.

I. In a simple one, a dummy Object (e.g., either a RFID tag or a presence sensing device) that is equipped with a functionality of the lowest layer, is only enabled to send simple signals to another element (the Gateway). The Gateway is equipped with the whole set of functionalities of the three layers.

II. In another scenario, a device (e.g., a video camera) is able to sense the physical world information and to send the related data over an IP network.The object would then be set with the functionality of the Network Layer other than that of the Application one. Accordingly, there is no need for a Gateway with Application Layer functionality. An Application Layer in a server, somewhere in the Internet, with the gateway application layer functionality would be enough.

III. According to a third scenario, a smart object (e.g., a smartphone) may implement the functionality of the three layers so that the Gateway is not needed, but for some communication facilities targeted to maintain the Internet connectivity of the object. This is the case of a smartphone, which has enough computational power to perform all the three-layer operations and that may need a Gateway for ubiquitous network connectivity.[1]

5. ALGORITHM

Below algorithm can be implemented to deal with malicious node in order to increase the trustworthiness factor.

If malicious node belongs to Class 1 then switch (relationship factor)

case OOR, CLOR, CWOR:

act benevolent
case SOR:

act benevolent only with close friends case POR:

act maliciously
default:

act maliciously end switch

end if

if malicious node belongs to Class 2 then act malicious with everyone

end if

6. MATHEMATICAL MODEL

Mathematical model using finite automata. A finite automata consist of five parts

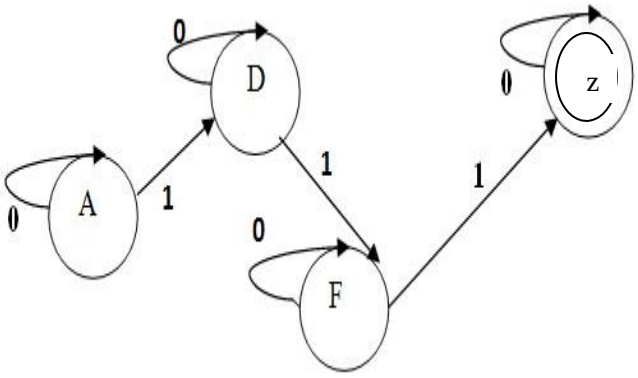

Figure 2: Mathematical model of trustworthiness

Q = {A, D, F, Z} = {Set of nodes in SIoT}.

Σ = {0,1} = {malicious, benevolent}.

A = initial state

F = final state/accepting state

δ(A,0) = A δ(A,1) = D δ(F,0) = F δ(F,1) = Z δ(D,0) = D δ(D,1) = F δ(Z,0) = Z

7. RESULT

SIoT network navigability is one the example to showcase the advantage of SIoT over any random network.

In Table 1 we show the probability distribution of the minimum path length between a pair of randomly selected objects of the SIoT. We show the distribution of the minimum path length between a pair of randomly selected nodes for a random network with the same number of nodes and edges as the SIoT. We observe that the average path length is 3.03 (almost equal to the one we found for the SIoT), however, the network diameter is 11 and 4% of the nodes are isolated.

Table 1: probability distribution of the minimum path length between a pair of randomly selected objects of the SIoT

Parameter	SIoT	Random Network
Average path length	2.85	3.03
Diameter	6	11
Isolated nodes (%)	0	4%

The average value of the minimum path length has been evaluated by considering pairs of randomly selected objects.

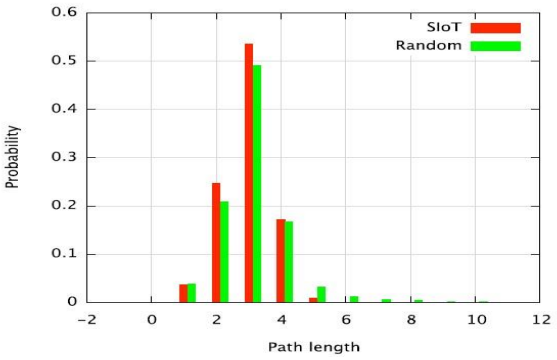

Figure 3: Probability distributions of the minimum path length between a pair of randomly selected objects in SIoT and random network cases.[1]

8. CONCLUSION

The IoTs concept aims at connecting anything, to be accessed at anytime from anywhere. Illustrating the evolution from IoT

to SIoT, and providing a detailed description of this new model from several point of views, constitutes the content of this report. The Social Internet of Things could be implemented faster than the average person would think. Most of the necessary technological advances needed for it have already been made but its impact on the legal, ethical, security and social fields would delay the implementation. Efforts are made to overcome these challenges. Study has been performed here on the methods to improve the security in SIoT by implementing the different phenomena to compute the trustworthiness factor. By bringing up such answers to the above mentioned challenges, practical implementation of SIoT over a global level is not far to serve for the development and betterment of people worldwide.

9. ACKNOWLEDGEMENT

I express my sincere thanks to M.E. Coordinator Prof. Mansi Bhonsle for her constant support and experienced guidance and providing me precious help and advice without which the successful completion of this seminar would not have been possible. I am also thankful to Prof. Dr. Shah (Principal, GHRCEM) for giving me necessary resources and support to complete my seminar. Last but not the least, I thank all others, and especially my classmates and my family members who in one way or another helped me.

10. REFERENCES

[1] Luigi Atzori*, Antonio Iera**, Giacomo Morabito***, and Michele Nitti: The Social Internet of Things (SIoT) - When Social Networks meet the Internet of Things:Concept: Architecture and Network CharacterizationI: Paper submitted and published in Computer Networks, Volume 56, Issue 16,14 November 2012, Pages 3594–3608.

[2] Michele Nitti, Roberto Girau, and Luigi Atzori, SeniorMember,IEEE Trustworthiness Management in the Social Internet of Things :IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 26, NO. 5, MAY 2014

[3] Antonio M. Ortiz, Member, IEEE, Dina Hussein, Soochang Park, Member, IEEE, Son N. Han, Student Member, IEEE, and Noel Crespi, Senior Member, IEEE.Cluster Between Internet of Things and Social Networks: Review and ResearchChallenges : IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 3, JUNE2014

[4] Kazi Masudul Alam_, Mukesh Sainiy, and Abdulmotaleb El Saddik; Multimedia Computing Research Laboratory, University of Ottawa, Ottawa, ON, Canada; Division of Engineering, New York University, Abu Dhabi, UAETowards Social Internet of Vehicles: Concept, Architecture and Applications: DOI10.1109/ACCESS.2015.2416657, IEEE Access

[5] Michele Nitti*, Luigi Atzori*, Irena Pletikosa Cvijikj; University of Cagliari, Italy, michele.nitti, l.atzori@diee.unica.it ETH Zurich, Switzerland, ipletikosa@ethz.chFriendship selection in the Social Internet of Things: challenges and possible strategies; DOI10.1109/JIOT.2014.2384734, IEEE Internet of Things Journal

[6] Google Images on Internet of Things and Social Internet ofThings.

[7] Wikipedia on Social Internet of Things and Internet ofThings.

[8] L. Atzori, A. Iera, and G. Morabito, "The Internet of things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2010.

[9] P. Mendes, "Social-driven Internet of connected objects," in Proc. Interconn. Smart Objects with the Internet Workshop, Lisbon, Portugal, 2011.

[10] L. Ding, P. Shi, and B. Liu, "The clustering of Internet, Internet of things and social network," in Proc. 3rd Int. Symp. KAM, Wuhan, China, 2010.

[11] D. Guinard, M. Fischer, and V. Trifa, "Sharing using social networks in a composable web of things," in Proc. 8th IEEE Int. Conf. PERCOM Workshops, Mannheim, Germany,2010.

[12] E. A. K. amd, N. D. Tselikas, and A. C. Boucouvalas, "Integrating RFIDs and smart objects into a unified Internet of things architecture," Adv. Internet Things, vol. 1, no. 1, pp. 5–12, 2011.

[13] L. Atzori, A. Iera, and G. Morabito, "SIoT: Giving a social structure to the Internet of things," IEEE Commun. Lett., vol. 15, no. 11, pp. 1193–1195, Nov. 2011.

[14] J. Surowiecki, The Wisdom of Crowds, New York, NY, USA: Doubleday, 2004. [8] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of things," Computer, vol. 44, no. 9, pp. 51–58, 2011.

[15] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, "A subjective model for trustworthiness evaluation in the social Internet of things," in Proc.IEEE 23rd Int. Symp. PIMRC, Sydney, NSW, Australia, 2012, pp. 18–23.

[16] 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," Comput. Netw., vol. 56, no. 16, pp. 3594–3608, Nov. 2012.

[17] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "TRM-IoT: A trust management model based on fuzzy reputation for Internet of things." Comput. Sci. Inf. Syst., vol.8, no. 4, pp. 1207–1228, 2011.

[18] R. Sherwood, S. Lee, and B. Bhattacharjee, "Cooperative peer groups in NICE," Comput. Netw., vol. 50, no. 4, pp.523–544, 2006.

[19] E. Adar and B. A. Huberman, "Free riding on Gnutella,"First Monday, vol. 5, no. 10, 2000.

[20] M. Feldman, K. Lai, and J. Chuang, "Quantifying disincentives in peer-to-peer networks," in Proc. 1st Workshop Economics of Peer-toPeer Systems, Berkeley, CA, USA, 2003.

[21] R. Jurca and B. Faltings, "An incentive compatible reputation mechanism," in Proc. 2nd Int. joint Conf. Autonomous Agents and Multiagent Systems, 2003, pp.1026–1027.

[22] S. Marti and H. Garcia-Molina, "Identity crisis: Anonymity vs. reputation in P2P systems," in Proc. 3rd Int. Conf. Peer-to-Peer Computing, Linköping, Sweden, 2003, p.134.

[23] R. Zhou, K. Hwang, and M. Cai, "Gossiptrust for fast reputation aggregation in peer-to-peer networks," IEEE Trans. Knowl. Data Eng., vol. 20, no. 9, pp. 1282–1295, Sept. 2008.