A Conceptual Trust Model for the Internet of Things Interactions

Abouzar Arabsorkhi
Iran Telecommunication Research Center and the
University of Tehran
Tehran, Iran
abouzar_arab@itrc.ac.ir

Mohammad Sayad Haghighi
School of Electrical and Computer Engineering,
University of Tehran
Tehran, Iran
sayad@ut.ac.ir

Roghayeh Ghorbanloo
Nooretouba Institution of Higher Education
and Iran Telecommunication Research Center
Tehran, Iran
roghayeh_ghorbanloo92@student.nooretouba.ac.ir

***Abstract*—In the new world that is called the Internet of Things (IoT), people, machines and products communicate with each other via the internet. Trust plays an important role in communications and interactions of objects in this world and is considered as a key factor in the success of online transactions. In this paper, we fist review different definitions of trust and go through the models presented for trust management in this new internet. Inspired by how people put trust to work in everyday social life, we propose a conceptual model that caters for the needs of IoT. The proposed model is capable of working in highly dynamic and decentralized networks. It has multiple parameters which can be tuned to satisfy the level of trust requirements in a specific application.**

Keywords— Internet of Things; Distributed Networks; Trust Model

I. Introduction

The Internet of Things (IoT) [1] is a network of networks in which a massive number of objects, sensors and devices are connected through a communications infrastructure to provide value-added services. IoT allows people and things to be connected anytime, anyplace, with anything and anyone, ideally via any network or service [2].

IoT is a rapidly emerging ecosystem in which all devices connect to the Internet, either directly or indirectly. These devices are not just typical desktop PCs, laptops, or cell phones. The concept is much broader and includes almost every object around us, like what we wear, what we drive or what we use to communicate with. IoT is turning everything smart. For example, cars now have navigation systems which receive traffic jam and weather condition reports via internet and also update their maps or software occasionally. Moreover, they are equipped with vehicular network modules to talk to other cars and let the driver know of any invisible danger. They can park themselves and even react to an imminent accident. Homes are getting smarter and so are manufacturing stations, oil and gas controls, power line transformers, jet planes, medical implants and even x-ray machines.

Since IoT integrates many objects of different kinds (which also belong to different players), a serious question arises on whether we should trust these things or not, both as an individual or as a federation of entities. Note that the idea of IoT has brought new issues in security, privacy and reliability which are reflected in the common term “trust”. For example, exposure of communication channels due to the extensive usage of wireless media can lead to the leakage of user data and jeopardize his privacy. In addition, the devices or things upon which services are built, can be stolen for ill-intentioned purposes by unauthorized individuals and their confidential data such as cryptographic keys be extracted.

Everyone knows what trust is, but no one really knows how to define it to everyone’s satisfaction [3]. Trust is a feature in human relationships which can hardly be formulated. In the context of IoT, it gets even more complicated since services rely upon each other as a chain. Therefore, you do not necessarily deal with a single thing to get service from. You might contact one at the front-end, but it is actually a network of things that is providing you the service. Trust to the provided service could be quantized if we had a measure to find the trust between two things. For this, we have to generalize the concept of trust in the human’s world and bring it to the world of objects.

In this research, our main effort is to model the trust among things/objects, to study the trust models and to find how objects can trust each other. The results can help us ensure the reliability and usability of services in IoT interactions. Then, objects can establish trustworthy relationships with each other and as a result, the user will have a more reliable and trustful experience at the network front-end.

After reviewing the current models of trust in the Internet of Things, we present a new one which has been adopted from the humans’ social world. It takes into account both personal experience and a mechanism similar to word of mouth. The presented model is thoroughly distributed in contrast to some of the previous centralized solutions. It has multiple parameters which can be tuned to satisfy the level of trust requirements in an IoT application. The rest of the paper is organized as follows:

In Section II, a review of the previous efforts in the area of internet of things is presented. The main focus will be on IoT trust issues and models, however, initially, the basic definitions of IoT and trust are also given. The proposed model is presented in Section III accompanied by a descriptive discussion. Finally, Section IV concludes the paper.

II. RELATED WORK

A. *Definitions of Internet of Things*

The Internet of Things refers to uniquely identifiable objects (things) and their virtual representations in an Internet like structure. This term was first used in 1999 by Ashton [1]. Later, other definitions of IoT appeared. In Table I, we have quoted the definitions of IoT from a few accredited sources. According to this table, it can generally be said that IoT is a collection of objects that are connected to each other via the Internet and with ability of communicating and sharing information among each other in a smart manner.

B. *Definitions of Trust*

There are different views to the concept of trust itself. Regardless of the context, some tried to define the concept of trust independently. In this subsection, we have collected all such definitions and summarized them in a table. Table II presents these different views to trust given in the literature. The next subsection specifically focuses on the works done on trust in the context of IoT.

C. *Trust in the Internet of Things*

According to [4], trust can be decomposed into device trust, entity trust, and data trust. Device trust in the IoT is a challenge, as a priori trust in devices cannot always be established, e.g., due to high dynamics and cross domain relations. Hence, approaches such as trusted computing [5] as well as computational trust [6] are required to establish device trust. Moreover, every entity may assess trust in a device differently, hence IoT architectures have to deal with different views of trust. Entity trust in the IoT refers to the expected behavior of participants such as persons or services. While device trust can be established via trusted computing, mapping such approaches to device trust is claimed to be more challenging and experimental. The authors argue that data trust occurs in the IoT in a twofold manner. First, trusted data may be derived from untrusted sources by aggregation. Second, IoT services themselves can create data for which trust assessment is required.

TABLE I. INTERNET OF THINGS DEFINITIONS

source	Definition
ITU [24]	A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies.
IETF [21]	A world-wide network of interconnected objects uniquely addressable, based on standard communication protocols.
Compose [22]	A global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities.

TABLE II. TRUST DEFINITIONS

source	Definition
Kimery & McCard [17]	Online trust is a customer's willingness and enables to accept an online transaction according to their positive and negative expectations on future online shopping behavior.
Mayer et al. [18]	Trust is the willingness of a party to be vulnerable to the action of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective to the ability to monitor or control that other party.
Corritore et al. [19]	An attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited.
Chang et al. [20]	the belief that the Trusting Agent has in the Trusted Agent's willingness and capability to deliver a quality of service in a given context and in a given Timeslot.
Buttyan et al. [21]	Trust is about the ability to predict the behavior of another Party.

Gligor and Wing [7] present a theory of trust in the network of humans and computers that consists of elements of computational trust and behavioral trust. They propose a simple communication model of entities and channels. The participants of this model can be human beings, network hosts, or network applications. For human users, behavioral trust following a game-theoretical approach is used. In order to trust the received information, the value of information must be higher than the costs of trusting. Trust can be achieved by verifying whether the sender can be trusted, e.g., by second opinions. However, such a second opinion might never arrive. Therefore, the receiver might be forced to use information without validation in some situations. Gligor and Wing use the concept of isolation that can be achieved by direct receiver verification, second opinion, etc.

Leister and Schulz [8] explored the different meanings of trust and strategies that can be used to determine if something is trustworthy and proposed a model for trust that takes into account people, devices, and their connections. The model uses `a priori and `a posteriori trust to give an indication of how much a user can trust or distrust the information provided by things. This trust indicator can inform users' decisions on whether or not to use a device or service.

Køien et al. [9] reviewed and identified different aspects of trust in software, hardware, devices and services in the internet of things environment and tried to answer the question of how we can trust devices and objects. Some aspects of human trust and what impact it may have on our confidence in this area has also been analyzed. The authors investigated trust in an IoT setting in considerable depth, and came to the conclusion that while it is obvious that one cannot fully trust any of the IoT components (software, hardware, communications, etc.), it does not mean that humans cannot or should not trust IoT services at all.

The IoT systems encounter more serious issues of security, reliability and availability. For this purpose, an autonomic agent trust model to decrease security concerns, increase reliability and credibility and ensure information collecting, sharing and processing in dynamic IoT environments has been proposed by Xu et al. [10]. In their model, in order to build the credibility protection model for IoT systems, agents and agent platforms have to be implemented on all nodes.

Similar to most security schemes, trust establishment methods themselves can be vulnerable to attacks. Sun [11] sought to examine the benefits of trust in distributed networks, the vulnerabilities in trust establishment methods and the defense techniques against attacks in these networks. However, the authors mainly had mobile ad hoc and sensor networks in mind while developing the defense mechanisms.

Yan et al. [12] proposed a research model for trust management in the internet of things and analyzed trust characteristics, issues and challenges in this field. In their view, an IoT system contains three layers: a physical perception layer, a network layer and an application layer. Each layer is intrinsically connected to other layers through cyber-physical links. A trustworthy IoT system or service relies on not only reliable cooperation among layers, but also the performance of each system layer with respect to security, privacy and other trust-related properties.

Bao and Chen [13] [14] proposed a trust management protocol considering both social trust and QoS trust metrics. They took both direct observations and indirect recommendations into account while updating the trust values. Their trust management protocol considers a social IoT environment whose conditions are dynamically changing, e.g., increasing misbehaving node population/activity, rapid membership changes, and interaction pattern changes.

Chen et al. [15] proposed another trust management model based on fuzzy reputation for IoT. However, their trust management model considers a specific IoT environment consisting of only wireless sensors with QoS trust metrics such as packet forwarding/delivery ratio and energy consumption. Compared to the previous work, it does not take into account the social relationships which are crucially important in IoT interactions.

III. The Proposed Model

A. Modelling Process

IoT has somewhat unique characteristics that differentiates it from the previous networks. In terms of size and scale, it is enormous, and heterogeneous as well. It is a highly dynamic network in which things enter, make connections and leave the network anytime. We aim to propose a model that captures these characteristics, especially the enormity of scale as well as the dynamic changes.

We take the modelling process depicted in Fig. 1. In an IoT trust model, a thing has to collect information about the candidates it wants to get service from (or sometimes provide service to, depending on the scenario). If there are multiple candidates, there should be a ranking mechanism to prioritize them. Once the entity is selected and the transaction happens, the thing has to update its database according to the experience and punish/reward the service provider, either locally in its database or globally in the network.

In this section, we provide a decentralized model for trust provisioning in IoT based on the concept of trust in human societies. We do not focus on the details such as the ranking mechanism or how the opinions should be combined, but rather concentrate on how one should evaluate the trust to a thing. This is a generic framework to which any ranking system or method of opinion mixing can be applied.

B. The Proposed Trust Model

The proposed trust model has been depicted as a flow chart in Fig. 2. It starts when the node X tries to evaluate a potential service provider (Y). Initially, X looks up into the entries of its past experiences database to see if there is enough information to judge about Y's trustworthiness. If there is, it checks whether the quantified trust to Y is greater than a predefined threshold TH_0. This is a threshold set by each service seeker depending on the sensitivity of the application it is running. It can be a dynamic threshold which changes per service request at X's discretion. In highly sensitive applications, the threshold is higher, but in normal applications it can be lowered. If Y satisfies the minimum level of the trust required, X gets the service from it and after the transaction finishes, updates its database accordingly.

If the evidences in the database are enough but are against Y's trustworthiness assumption, X simply ignores Y and starts the algorithm for the next candidate in the ranked list. However, if there are not enough pieces of evidence, X queries the (IoT) network to see if there are other objects that have prior experiences of working with Y. This can be done by broadcasting to all or a subset of network nodes. No specific algorithm is specified in this model, however, priority shall be given to the nodes X trusts more. This is very similar to the well-known notion of Web of Trust [16].

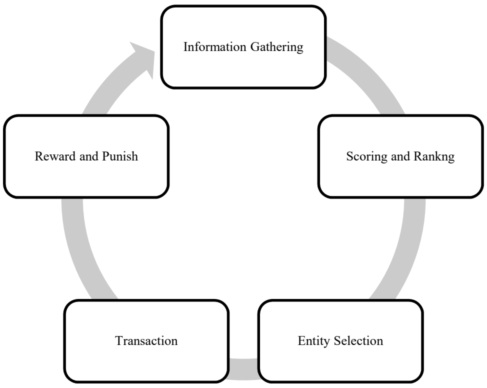

Fig. 1. The trust modeling process

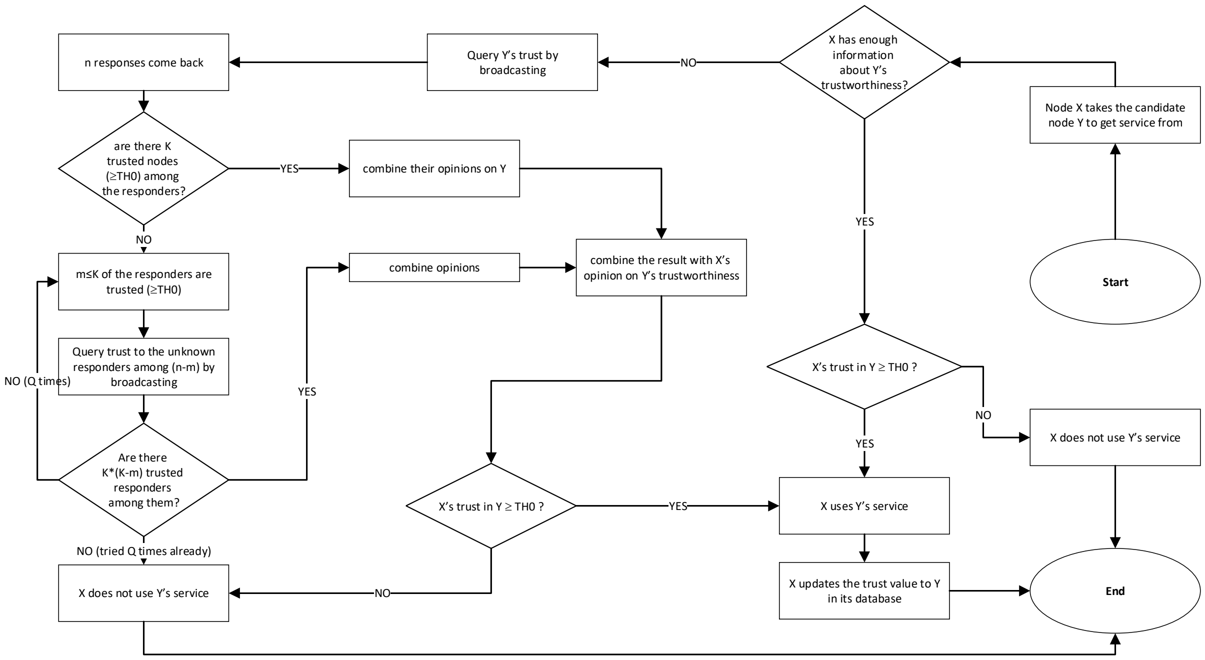
n responses come back
Query Y's trust by broadcasting
NO
X has enough information about Y's trustworthiness?
Node X takes the candidate node Y to get service from
are there K trusted nodes (≥TH0) among the responders?
YES
combine their opinions on Y
YES
NO
Start
m≤K of the responders are trusted (≥TH0)
combine opinions
combine the result with X's opinion on Y's trustworthiness
Query trust to the unknown responders among (n-m) by broadcasting
NO (Q times)
YES
X's trust in Y ≥ TH0 ?
NO
X does not use Y's service
YES
Are there K*(K-m) trusted responders among them?
X's trust in Y ≥ TH0 ?
YES
X uses Y's service
NO (tried Q times already)
X does not use Y's service
NO
X updates the trust value to Y in its database
End

Fig. 2. The proposed IoT trust model

Let us say, out of the queries X sent, n have come back with responses. However, X does not necessarily trust all of the responders. X looks for K pieces of evidence collected from K responders to complete his judgment about Y's trustworthiness. If there are K trusted responders among them, X combines their opinions and compares the resultant trust value against TH_0. Just like before, if Y is trusted enough, X asks for the service, otherwise, X ignores Y and takes the next candidate in the list. In this specific case, X can optionally update its database to keep this record for future references.

If there are less than K trusted responses, X cannot come to a solid conclusion, not at least instantly. Among n responders, let us assume X only trusts $m \leq K$ and does not know (or even distrusts some of) the $n - m$ remaining sources. Since we said the preference was given to the X's trusted peers in querying, we do not subtract any number from $n - m$. Otherwise the number of distrusted responders should have been subtracted from this quantity.

Now, X has to find the trust value to at least $K - m$ of those unknown responders. This is the number of evidence pieces which are missing from X's perspective. We assume if K trusted peers could tell X that one of those unknown sources is trusted, it would rely on that unknown node's opinion about Y. Here, for the sake of simplicity, we have used the same K as before though in general, a different parameter could be used.

In order to find the trustworthiness of the unknown responders, this time X queries the network for them hoping that for each of at least $K - m$ unknown responders, it can get K trusted evidences supporting its trustworthiness. This can go on and on, and each time, X has to ask the network about the trustworthiness of the unknown responders to the last query.

If X succeeds in collecting enough information, it combines the opinions and compares the resultant trust value against TH_0 to decide whether it should get the service from Y or not. If enough evidences cannot be collected after iterating the above algorithm for Q times, or the evidences work against Y's trustworthiness hypothesis, X simply decides not to use Y's services and takes the next candidate in the list.

Note that the above algorithm is an adoption of what humans do in real social life. People tend to work with and get services from those they trust more. If they do not know about the service provider much, they tend to ask somebody who knows and they trust. This goes on and on till it gets to the point that the chain is broken or people rely on references from unknown sources. Judging a job applicant based on the reference letters provided by his former employers is the most one can do if the applicant is not recommended by a trusted friend or company.

In the above model, Q determines how long we want to go along this chain and K determines how conservative we want to be. This model can cope with the decentralized architecture of IoT and works well in dynamic environments too. One can easily tailor the proposed model to his needs by choosing a proper ranking mechanism and tuning the thresholds and variables given in the model.

IV. Conclusion

In this paper, we studied the trust issues in the future internet of things. We reviewed different definitions of trust and went through the models presented for trust management in the IoT literature. Inspired by how people put trust to work in everyday social life, we proposed a general model to show how a thing can trust another thing in IoT. The model is capable of working in even highly dynamic and decentralized networks. It has multiple parameters which can be tuned to cater for the needs of any specific application, whether sensitive or insensitive.

As the future work, we tend to analyze the model on a real large-scale graph by means of simulation and show how it performs under different application settings. We believe that evolutionary algorithms can be employed to choose better references and to optimize the model parameters.

V. References

[1] L. Atzori, A. Iera and G. Morabito, "The internet of Things: A survey," *Computer Network,* vol. 54, no. 15, pp. 2787-2805, 2010.

[2] C. Perera, A. Zaslavsky, P. Christen and D. Georgakopoulos, "Context Aware Computing for The Intenet of Things: A Survey," *Communications Surveys Tutorials, IEEE,* vol. 16, no. 1, pp. 414-454, 2013.

[3] A. Patrick, P. Briggs and S. Marsh, "Designing Systems that People Will Trust," in *Security and Usability: Designing Secure Systems that People Can Use*, O'Reilly Media, 2005.

[4] J. Daubert, A. Wiesmaier and P. Kikiras, "A review on privacy and trust in iot," in *In IOT/CPS-Security Workshop, IEEE International Conference on Communications, ICC 2015*, London, 2015.

[5] I. Alexander and W. Sean, "Protecting client privacy with trusted computing at the server," in *IEEE Security & Privacy*, 2005.

[6] J. Audun, I. Roslan and B. Colin, "A survey of trust and reputation systems for online service provision," *Decision Support Systems,* vol. 43, no. 2, pp. 618-644, 2007.

[7] V. Gligor and J. Wing, "Towards a theory of trust in networks of humans and computers," in *the 19th international workshop on security protocols, ser. LNCS*, 2011.

[8] W. Leister and T. Schulz, "Ideas for a Trust Indicator in the Internet of Things," in *The First International Conference on Smart Systems, Devices and Technologies*, 2012.

[9] G. Køien, "Reflections on Trust in Devices: An Informal Survey of Human Trust in an Internet of Things Context," *Wireless Personal Communications,* vol. 61, pp. 495-510, 2011.

[10] X. Xu, N. Bessis and J. Cao, "An Autonomic Agent Trust Model for IoT systems," *Procedia Computer Science,* vol. 21, pp. 107-113, 2013.

[11] Y. Sun, Z. Han and K. Liu, "Defence of Trust Management Vulnerabilities in Distributed Networks," in *Security in Mobile AD HOC and Sensor Networks*, 2008.

[12] Z. Yan, P. Zhang and A. Vasilakos, "A Survey on Trust Management for Internet of Things," *Journal of Network and Computer Applications,* vol. 42, pp. 120-134, 2014.

[13] F. Bao and I. Chen, "Dynamic Trust Management for Internet of Things Applications," in *International Workshop on Self-Aware Internet of Things*, California, USA, 2012.

[14] F. Bao and I. Chen, "Trust Management for the Internet of Things and Its Applications to service Composition," in *IEEE WoWMoM 2012 Workshop on the Internet of Things: Smart Objects and Services*, 2012.

[15] D. Chen, G. Chang, D. Sun, J. Li, J. Lia and X. Wang, "TRM-IoT: A Trust Management Model Based on Fuzzy Reputation for Internet of Things," *Computer Science and Information Systems,* vol. 8, no. 4, pp. 1207-1228, 2011.

[16] R. Guha, R. Kumar, P. Raghavan and A. Tomkins, "Propagation of trust and distrust," in *the 13th international conference on World Wide Web*, 2004.

[17] K. Kimery and M. McCard, "Third-party assurances: Mapping the road to trust in e-retailing," *Journal of Informationa Technology Theory adn Application,* vol. 4, no. 2, pp. 63-82, 2002.

[18] R. Mayer, J. Davis and F. Schoorman, "An integrative model of organizational trust," *The Academy of Management Review,* vol. 20, no. 3, pp. 709-734, 1995.

[19] C. Corritore, B. Kracher and S. Wiedenbeck, "On-line trust: concepts, evolving themes, a model," *Int.J. Human-Computer Studies,* vol. 58, no. 6, pp. 737-758, 2003.

[20] L. Buttyan and J. Hubaux, Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing, New York, NY, USA: Cambridge University Press, 2007.

[21] A. Bassi, G. H. Sintef and E. Hitachi, "Internet of Things in 2020: A Roadmap for the future," European Commission/ EPoSS Expert workshop on RFID/ Internet of Things, Brussels, 2008.

[22] CASAGRAS, "Final Report, RFID and Inclusive Model for the Internet of Things," Coordination and support action for global RFID-related activities and standardization (EU Framework 7 Project), 2009.

[23] E. Chang, T. Dillon and F. Hussain, "Trust and reputation relationships in service-oriented environments," *ICITA 2005. Third International Conference on Information Technology and Applications,* vol. 1, pp. 4-14, 2005.

[24] ITU Telecommunication Standardization, "ITU-T Recommendation database," 15 06 2012. [Online].