Governance of the *Internet of Things*

Avri Doria, Markus Fiedler, Ralph Herkenhöner, Wolfgang Kleinwächter, Giannis F. Marias, George C. Polyzos[1]

Abstract

As an attempt to increase the understanding of popular notions and concepts, this paper reflects upon the interrelationship between the *Internet of Things* (IoT), the Internet, and the Future Internet (FI). This paper discusses the coexistence, correlation, links, mutual impacts, similarities and differences between these internets through a review of the related design principles. The central issue of governance is highlighted. Furthermore, various technical and in particular security and privacy challenges are discussed. A set of use cases is presented as a motivating and introductory example to highlight relationships between the IoT and the Internet as we know it and as it may develop in the future.

Introduction

The 'Internet of Things'[2] is an expression of ubiquitous computing and communication as described by the late Mark Weiser in his seminal vision of future technological ubiquity, where increasing 'availability' of processing power would be accompanied by its decreasing 'visibility.' As he observed, 'the most profound technologies are those that disappear…they weave themselves into the fabric of everyday life until they are indistinguishable from it.'

While the term 'Internet of Things' is ill defined, there is a general understanding that an 'Internet of Things' (IoT) means the linkage of objects, equipped with near field (radio) communications, often a Radio Frequency Identification (RFID) chip, in a network within an 'Object Naming System' (ONS). At the moment, such services are offered and standardised by companies and organizations like *GS1* and *EPCGlobal* on top of the '.com' domain within the existing Internet. Efforts are undertaken to offer alternative, more general and competitive services on top of other domains, or with entirely different internetworking philosophies and, maybe more importantly, different governance models.

The emergence of the IoT is seen by the European Commission as one of the key areas in the evolution towards next generation networks. The linkage of objects to networks and through them to themselves and the ability to communicate with these objects, open doors for new economic developments with great market potential and wide-ranging political, legal, and socio-economic (and in particular privacy) implications.

Research has been concentrated so far on the technical and economic aspects, in particular on the development of RFID technology, the design of an ONS and the possible commercial applications and services. But while there is a general agreement that an IoT has also far reaching political, legal, and social implications, there is only little research with regard to public policy issues such as governance and privacy with regard to the IoT and in particular the ONS service.

In this paper, we start with the presentation of a scenario involving the IoT in order to motivate our discussion and demonstrate aspects of the issues under consideration. (Most of these technologies exist today, some are already in wide use, but in general they are still deployed as separate, isolated systems with very limited advances towards addressing governance and socio-economic issues.) Then we look at each of these three correlated entities, IoT, Internet, and FI separately and, finally, we move on to exploring the links between them and then present and discuss some of the challenges that arise.

---

[1] Avri Doria is with the Luleå University of Technology; Markus Fiedler is with the Blekinge Institute of Technology; Ralph Herkenhöner is with the University of Passau; Wolfgang Kleinwächter is with the University of Aarhus; and Giannis F. Marias and George C. Polyzos (corresponding author, polyzos@aueb.gr) are with the Athens University of Economics and Business.

[2] ITU Internet Reports: The Internet of Things, 2005 (http://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf)

A Scenario

Sofia, a young Greek seismologist must leave early from home. Her task is to go to the *UniLab*, pick some modern measurement equipment and then go to the airport to fly to the island of Santorini in order to replace some equipment and carry out some measurements related to the recent seismic activity next to the volcano. She uses her RFID-enabled mobile phone in order to unlock her new car[3]. Once the engine is on, internal car sensors record and report to remote agents, using mobile network services, the car's actions, responses, and statistics.[4] In addition, Sofia's new car uses an advanced car-to-car warning and control system that monitors and controls the distances between vehicles and manages the car speed to avoid car accidents.[5]

Sofia reaches the lab and uses her university ID-card to be authenticated at the gate and to be allowed to use a particular parking spot in the garage. The same ID-card is used to open the inner door of the main building and allow Sofia to access the lab premises.[6] Finally, Sofia picks up and loads the equipment into her car, leaves the university, and enters the freeway on her way to the Athens International Airport (AIA). The toll system recognizes the RFID on Sofia's car and charges her bank account with the time-sensitive price for the tolls (since it is very early in the morning and she does not contribute to congestion the price is rather low…).[7] On the freeway she is careful to avoid speeding since police has announced the launch of a new monitoring network that uses advanced sensor cameras in freeways.[8] The parking system at the AIA reads the RFID signal from Sofia's car, opens the gate to allow her to enter into the garage, whilst there is a hold put on her bank account for the parking charge for the maximum time period permitted (she will be charged when she picks the car on her return).

At the airport, Sofia uses a 'soft' boarding pass on her mobile to enter through the gate and she is authenticated by airport security through her passport/ID-card which was recently upgraded and equipped with an RFID chip.[9] The measurement instrument she carries along as a carry-on passes easily and quickly through security even though it resembles a weapon because it has been previously certified in a secure way acceptable to most airport security administrations. Sofia passed quickly through all the access control phases and now enjoys the short journey over the Aegean Sea. Upon her arrival in Santorini she rents a SUV using her credit card[10] and signs the contract without the need for her to fill-in any personal details or even to decide on all the alternative offered services—her professional default choices are enforced immediately, even without a previous reservation.

Sofia manages to get to the measurement field where several sensors have been installed and self-configured to monitor the seismic activity near the volcano. She opens her new, more accurate and reliable *episensor* and replaces an older one, making sure it has been properly

---

[3] This is an example of machine-to-machine use of the IoT paradigm. The actual Internet, as infrastructure, is not involved. This mainly happens when dedicated short range communication occur.

[4] This is an example of machine-to-intranet use of the IoT paradigm, whereas mobility should be supported. The measurement 'thing,' i.e., the car, is on the move. The Internet is used as a bearer service to convey information from/to the car.

[5] This provides an example of machine-to-machine use of the IoT paradigm. The Internet infrastructure is not involved.

[6] In this example, the usage of the IoT is within a local, private domain, i.e., the access control system in the campus.

[7] This is an example of a usage of the IoT using an inter-domain approach. The tolls system domain and the bank/credit card domain are bridged via the Internet.

[8] An example of surveillance network of things that might use the Internet to build private networks of remotely managed things. In this case, fast and reliable connections are required.

[9] This is an example of an IoT deployment that involves secured, private communication and not an intranet-based service.

[10] This is another example of an IoT deployment that involves secured, private, probably not intranet-based service (such as SWIFT).

initialized and works reliably; this takes less than an hour and then she bridges it to the local sensor-sink and takes a look at the collected and aggregated data of last week.[11]

Sofia now feels exhausted; she needs a warm bath and a good dinner with view over the volcano and under the moon. She uses a new mobile service on her smart phone that locates nearby friends, using either GPS data or triangulations, and discovers that Lina, a UniLab PhD student, is on the island.[12] They talk and decide to have dinner at '1820,' a marvellous restaurant of modern Greek gastronomy. After this excellent dinner, Sofia decided to leave geolocated recommendation to rank this restaurant. She uses augmented reality software that enables her to place an opinion on locations, sightseeing places, restaurants, and other notable objects and places.[13]

The aforementioned every-day life snapshots illustrate that when deployed, the 'things' might be a part, an extension, or run separately from the (Future) Internet. If we consider the Internet as public infrastructure (meaning that the networking stack up to the transport layer is considered as a social asset), then each of the aforementioned parts of the scenario places different requirements for connecting, associating, integrating, interoperating, or embedding objects ('things') on the globe:

- Reliability, when critical services, such as passport/ID-card verification, are based on robust IoT
- Security and privacy, at several layers, such as for information, transaction privacy and security, personal security and privacy, etc.
- Quality of Experience and Quality of Service, e.g., when high-capacity connections (for high-resolution multimedia information), or error-free links are required
- Inter-domain connections (i.e., when the objects of one domain trigger multi-domain transactions)
- Accountability at various levels, from human actions to network choices and decisions
- Mobility and roaming of devices (i.e., when mobile objects are associated with different internet domains or Autonomous Systems)
- Resource constraints, since dense deployment of objects will stress the use of (the common, limited) spectrum (and wireless resources in general)
- Management of private scopes (i.e., private 'networks of things' over the Internet)
- Addressing, i.e., when RFID-based addresses should be routable over or traversable through IPv4 or IPv6 (inter-)networks
- And many others…

The Future and Governance of the Internet of Things

In order to address pro-actively the many governance and privacy issues raised by IoT technologies and mostly by the interconnection and combination of information obtained by very many different sources, many that not even the designers of the systems that provide it could imagine ahead of time, we believe that it is important to begin at the heart of the issue. I.e., start the conversation with the thought that this topic involves a correlation—a term used in statistics to indicate a relationship where a change in one variable relates to changes in others. In this paper our starting point is our belief that any change in either the IoT or the Internet and in particular with the introduction of a Future Internet (FI) with potentially different architecture and governance model, will have a concomitant effect on the other. When it comes to the topic of governance, it is expected that the governance of the Internet will serve

[11] In this example, 'things' (i.e., sensors) are deployed in a separate field and are self-organized to produce, aggregate, and process local data. A sink might be present whereas in some cases it is connected via the Internet with the lab facilities (via satellite or other wireless or mobile links).

[12] In this example Global Positioning System (GPS) receivers on smart phones (or the smart phone through other technologies) act as location identification 'things.' They are linked to the Internet to report the current position on a Web service using some kind of subscription and authentication of friends.

[13] This example is used to identify the 'virtual thing,' i.e., identification of place, or object in the virtual world, i.e., using a specific service (and not a small device). This offers annotation capabilities of eventually every item in the planet, without the use of RFID. But it still needs the Internet/Web to be recorded, stored, discovered, and manipulated.

as a base that will shape or at least inform governance of the IoT and the FI. And it is anticipated that the European research on the Network of the Future, including an emphasis on Socio-Economic aspects (amongst others through the European Network of Excellence *Euro-NF*[14]) will be a force behind these correlated changes.

The correlated entities

The Internet

The Internet can be explained in many ways. It is first and foremost a network of networks, it runs IP based protocols developed in the IETF, it is built according to a certain set of design principles[15] and it is nearly ubiquitous in the developed world and critical for business and for society in general. However, none of these aspects seems to be the most critical, but rather the fact that the Internet works on a single global set of numbers,[16] numbering rules, naming rules and names.

The Internet of Things

Those envisioning an Internet of Things (IoT) see the possibility of interconnecting objects of common use to each other and other network entities. It is a network where an object and its subcomponents can be tracked and communicate for their entire lifecycle from manufacture to distribution, through use, to the end of their life and disposal. It is envisioned as a global network of networks, with many individual private segments and a strong focus on security and privacy. The key idea and difference with the Internet is that communication among those objects is mainly in order to better enable their main function (the thing they are made for) and they are not primarily devices facilitating (end-)user communication (even though of course, there are no black-and-white boundaries). Of course, in order to get user commands or specifications, the Internet, and users through it, will need to communicate with the IoT (and particular networks or even devices belonging to the IoT, or maybe, according to some, a particular IoT).

The word *Internet* in 'Internet of Things,' does not refer to a network infrastructure, but rather to the (inter-)network built up by the interaction of the objects that participate in a multitude of networks. For the most part, it is expected that the IoT will use the existing Internet as a communication substructure, though it will not be restricted to using only the Internet substructure and in some cases may be implemented on a new, yet to be developed, infrastructure, possibly with a new architecture. The IOT is expected to be opportunistic in that it could use the network infrastructures that are available without prejudice.

What is important is that the term Internet in IoT is used in a different way than it is when speaking of the Internet qua Internet. Some consider this overloading of the nomenclature to be unfortunate, but it is the name that is in use. One element that remains similar is that the IoT currently uses the naming system of the Internet with its names being a sub-tree of the '.com' registry. As entities are using the Internet for communication, they are also using Internet addresses. While there is no mandate that the names and number used by the IoT, remain numbers from the sets controlled by the *Internet Assigned Numbers Authority* (IANA), and managed by the *Internet Corporation for Assigned Names and Numbers* (ICANN) and the Regional Internet Registries (RIRs), it is difficult to see how this would stop being the case. There is also no reason why the naming needs to remain in a sub-tree in the '.com' registry. It could be rooted in various registries or, if the architecture warranted it, control its own Top Level Domain (TLD).[17]

---

[14] http://www.euronf.org/

[15] Among these principles are: packet-switching, layered architectures, the end-to-end principle, the hourglass model with the Internet Protocol (IP) at the narrow waist, the Postel robustness principle (be conservative in what you send; be liberal in what you accept), and shared fate and creative anarchy.

[16] More precisely two sets, IPv4 and IPv6 addresses, but who is counting…

[16] For example, some consortium of IoT concerned entities could apply for a ".iot" domain.

On the Network of the Future or the Future Internet

Euro-NF is a European project on the Network of the Future, formed by 35 institutions (from the academia and industry) from 16 countries. Its main target is to integrate the research effort of the partners to be a source of innovation and a think tank on possible scientific, technological and socio-economic trajectories towards the network of the future.[18]

The goal of the Euro-NF Network of Excellence is to provide a forum for dialog among European network researchers and to lead to integration of research on new networking technology, with focus on the Network(s) of the Future, or the FI, the IoT etc. The vision of Euro-NF[19] states amongst others:

> In the future networked society the physical and the digital worlds will merge based on the massive usage of wireless sensor networks. Objects will be able to identify and locate themselves and to communicate through radio interfaces. Self-organized edge networks will become more and more common. Virtualisation and programmability will allow for providing different networking environments over the same infrastructure. Autonomic networking will deal with the increasing complexity of instrumentation and control systems. End-user empowerment will increase with their capacity of providing services and content, as well as connectivity support.

The links between the correlated entities

The question 'Is the Internet of Things a part of the Internet?' has been debated extensively. In one respect the IoT is something other than the Internet because it is based on the associations between the elements and not on the definitions of the Internet. Yet at the same time, it is part of the Internet, because it relies on what is fundamental about the Internet, its addressing and naming (and for now because it is and may continue to be attached, or be an extension of it…). Of course, this does not always need to be so, but it is difficult to see what path might be taken to result in something fundamentally different, as that would require the IoT to create its own (global?) infrastructure. This seems improbable given that so much infrastructure already exists and the difficulty and expense of rolling out new infrastructure in the near term.

Two arguments have been made by proponents of considering the IoT as (somehow) separate from the Internet:

- The IoT can use any form of (wireless) network, including but not limited to cellular wireless (2,5G, 3G, 4G), IEEE 802.11, IEEE 802.15 etc. For cellular networks, even though it is true that the UMTS network used in Europe has not yet fully converged with the Internet, in many ways it has and the goal is certainly in that direction for 3G and towards 4G. Even the work being done by the ITU on its next generation network is based on IETF MPLS technology, a technology that relies on an Internet Protocol (IP) control plane. The IEEE 802.11 and .15 protocols are mostly link and lower layers and even though can be used to run IP on top of them, they do not necessarily point in that direction.
- That the IoT may not use global addressing, using private networks, or private addressing instead. Even if this is often the case, as it is for many SOHO and business networks, it does not really mean that the IoT is separate from the Internet, as the Internet will often be used to transit from one private network to another. It is also worth noting that all private networking stubs on the Internet use addresses based on RFC 1918 and RFC 4193 on private addressing allocation.

Given this duality, the IoT would be part of the Internet, while also being separate from it. Understanding the IoT as a collection of interconnected but local and private networks—let's call them *Private Networks* (PNs)—such PN would be in a very similar relation to the Internet like current (private) LANs/WLANs. From this point of view, the PN could be understood as a part of the Internet, having one or more Internet Protocol (IP) addresses. These addresses could be used to address the PN or components of it. Its members may be visible in the

[18] http://euronf.enst.fr/en_accueil.html
[19] http://www.euronf.org/

Internet or not. If they are visible, they would have their own Internet address (resolved by NAT/PAT[20]). But from the logical point of view, it is the PN that is part of the Internet, not the members of the PN. Nevertheless, inside the PN, common Internet protocols may be used. Assuming that a PN is able to route Internet traffic, one PN node should also operate as a core node (not only as an edge node). On the other hand a PN can be considered as a (small) communication network, not being part of the Internet, but connected to it at the edge. Internal nodes will not be able to be addressed directly by Internet nodes and it will not be using Internet protocols internally. Nevertheless, a PN may be able to transport Internet traffic inside and abroad (via overlay or border gateways).

The Challenges

Technical challenges

A suitable architecture needs to be identified. Typically, the physical arrangement of the 'things' and the capabilities of potential radio interfaces will have an impact on the type of appropriate network (multi-hop/chain, tree, mesh, etc.). Suitable roles of nodes and resources need to be defined, which may range from traditional client-server setups, to peer-to-peer relationships, or even to publish/subscribe arrangements.

The communication facilities of the objects ('things') need to be self-organised and smoothly self-managed. Typically, the 'things' neither have advanced user interfaces, nor processing capabilities, nor are their users willing to spend large efforts in setting them up. 'Things' need to be able to make themselves (i.e. their information and services) available to each other and to the outer world. This implies the need for lightweight self-organising and self-managing functionalities and, depending on the level, service discovery and execution facilities.

Security and privacy challenges

The 'things' are envisioned as anywhere and anytime information publishers (producers) or subscribers (consumers). Information is normally linked to persons, activities, places, time and other everyday habits. It is essential to define scopes of information. Scopes will provide rules and policies for information reachability and limiting information dissemination. A private scope would define a PN where information is limited in that 'private' domain. A confidential scope may define access privileges on information transferred between two virtually interconnected PNs. A public scope would publish information to all (the public).

Because hard security and privacy countermeasures might be inappropriate to be used by or embedded in the 'things,' security and privacy should probably be enforced at the service level, i.e., where the ONS or DNS are used and when names and addresses are resolved and linked to everyday habits.

A real challenge seems to be how to contain information disseminated that was obtained from or produced by the combination of (legally) available information from various sources (that seems inconsequential) and deduction and leading to the revelation of personal and maybe sensitive information. This is becomes a real challenge in this environment because for the first time in human history events and information will be recorded at such large scales globally and will be tagged with time and location information and many times in ways completely hidden to humans (realizing Mark Weiser's dream of technologies that disappear, which however, if this challenge is not effectively addressed, may turn into a nightmare…).

One approach to address this challenge, since limiting access to widely or publically available

[20] Network Address Translation (NAT) is the process of modifying network address information in datagram (IP) packet headers while in transit across a traffic routing device for the purpose of remapping one IP address space into another. NAT is often used to hide an entire IP address space, usually consisting of private network IP addresses, behind a single IP address in another, often public address space. Port Address Translation (PAT) is the process of modifying TCP streams or UDP packets to enable communications made between hosts on a private network and hosts on a public network. It allows a single public IP address to be used by many hosts on a private network.

information is not realistic, is to consider approaches of *information accountability*.[21]

Governance challenges

When it comes to governance of the IoT, given its self-organizing nature, we need to understand how it fits into the existing governance regimes and whether it needs a different form of governance altogether. For example, since the IoT is using the Internet addressing scheme and naming system, which is governed by ICANN, one must ask to what extent will the IoT be governed by ICANN principles. Some experts on the subject of IoT governance have gone so far as to state: Governance of the IoT will not/should not replicate the ICANN model or the ICANN debate.[22] Yet, when looking at the IoT, there is not yet sufficient evidence to let us know in what ways the governance would/should differ. One industry group, EPCGlobal[23] which has a focus on the RFID technology that makes up an integral part of the current concept of IoT, has already shown an interest in having a role in the governance of the IoT, but have not given a well-formed plan of a new governance model.

The European Commission has been concerned about the shape IoT governance will take for over a year. They have started to look into the needs for IoT governance, specifically[24]:

> According to the European Commission, policymakers should also participate in the development of IoT alongside the private sector. Some challenges are indeed policy-related, as highlighted by the World Summit on the Information Society, which encourages IoT governance designed and exercised in a coherent manner with all the public policy activities related to Internet Governance.

Many questions concerning the implementation of the connection of objects arise such as:

- object naming;
- the authority responsible for assigning the identifier;
- ways to find information about the object;
- how information security is ensured;
- the ethical and legal framework of the IoT;
- control mechanisms.

The European Commission also released an action plan for Europe on the IoT[25] indicating the need for 'promoting a shared and decentralised network governance,' committing to follow *World Summit on the Information Society* (WSIS) principles in the governance of the IoT. The European commission set the following as its goal:

> **Line of action 1 — Governance[26]**
>
> The Commission will initiate and promote, in all relevant fora, discussions and decisions on:
>
> – defining a set of principles underlying the governance of IoT;
>
> – setting up an 'architecture' with a sufficient level of decentralised management, so that public authorities throughout the world can exercise their responsibilities as regards transparency, competition and accountability.

---

[21] Weitzner, D.J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., and Sussman, G.J. 2008. Information accountability. *Commun. ACM* 51, 6 (Jun. 2008), 82-87.

[22] http://twitter.com/bcute17/status/2189966433

[23] http://www.epcglobalinc.org/home/

[24] http://europa.eu/legislation_summaries/research_innovation/research_in_support_of_other_policies/ si0009_en.htm

[25] http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf

[26] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009DC0278:EN:NOT

Conclusions

In this paper, we have reviewed the relationship between the Internet of Things (IoT), the Internet, and the Future Internet (FI). Due to natural similarities between those, originating amongst others from common roots and common original design principles, and due to the fact that all of them will have to interwork at least to some extent, challenges known from one domain re-appear in another one. The latter implies that valuable solutions from one domain might be considered in another domain. For instance, the IoT copes with addressing and energy issues that need to be taken into account for the FI and even for the current Internet and its applications. On the other hand, research on the FI focusing on future-proof architectures, composition and management principles is expected to point directions for the IoT. A detailed inventory of such issues of mutual interest and potential approaches within the European Network of Excellence Euro-NF is currently carried out by its Joint Specific Research Project 'GOVPIMIT.' Currently governments, industry, the Internet community, and civil society stand at the starting point of creating a WSIS-principle based multi-stakeholder debate on the future of IoT governance.