Mobile Networks and Applications manuscript No.
(will be inserted by the editor)

Standards, Security and Business Models: Key Challenges for the IoT Scenario

Armir Bujari · Marco Furini · Federica Mandreoli · Riccardo Martoglia · Manuela Montangero · Daniele Ronzani

Received: date / Accepted: date

Abstract The number of physical objects connected to the Internet constantly grows and a common thought says the IoT scenario will change the way we live and work. Since IoT technologies have the potential to be pervasive in almost every aspect of a human life, in this paper, we deeply analyze the IoT scenario. First, we describe IoT in simple terms and then we investigate what current technologies can achieve. Our analysis shows four major issues that may limit the use of IoT (i.e., interoperability, security, privacy, and business models) and it highlights possible solutions to solve these problems. Finally, we provide a simulation analysis that emphasizes issues and suggests practical research directions.

Keywords Internet of Things; Communication Protocols; Interoperability; Security; Privacy; Business Model.

1 The IoT Scenario

In recent years, the term Internet of Things (IoT) has received considerable attention by both academia and industry, with governments making the first regulatory steps enabling their deployment [1,2]. In the IoT scenario, people

A. Bujari and D. Ronzani
Dipartimento di Matematica
Universtà di Padova, Via Trieste 63, Padova, Italy,
E-mail: {abujari, dronzani}@math.unipd.it

M. Furini
Dipartimento di Comunicazione ed Economia
Universtà di Modena and Reggio Emilia, Viale Allegri 9, Reggio Emilia, 42121, Italy,
E-mail: marco.furini@unimore.it

M. Montangero, F. Mandreoli and R. Martoglia
Dipartimento di Scienze Fisiche, Informatiche e Matematiche
Universtà di Modena and Reggio Emilia, Via Campi 213/a, Modena, 41125, Italy,
E-mail: {manuela.montangero, federica.mandreoli, riccardo.martoglia}@unimore.it

and physical objects are connected and are able to communicate with each other, to improve life quality [3–9]. Vehicles, home appliances, smartphones, home and wearable sensors, personal and public devices are examples of objects that can become smart in order to be part of an IoT scenario. Indeed, by providing the ability to communicate, even through non conventional paradigms [10,11], these objects can share captured data. This data might be the base of an integrated analysis that aims to produce intelligent services [12].

Probably one of the most known IoT applications is home automation, for which many systems are already available on the marketplace. Nevertheless, the IoT scenario is definitely wider: a city may become smart by using sensors and devices to monitor and manage traffic, to improve the efficiency of waste management, to plan urban and transportation changes, etc.; health-care may become smart by using sensors and devices to improve emergency services, to provide elderly home assistance and medical aids, etc.; industries may use IoT to improve security in automotive transportation, to make logistics more efficient, to enhance industrial automation, etc.; energy providers may use IoT to intelligently manage energy distribution [3,13]. There is no doubt in saying that the IoT scenario has the potential to be pervasive in almost every aspect of human life [3–7].

Technically speaking, the IoT can be thought of as the interconnection of objects with the Internet, as shown in Figure 1. At *objects* level we have sensors that perform actions like "feel", "ear", "measure", "check" and we have actuators that perform actions through electrical, hydraulic, pneumatic or mechanical movements. All these objects *communicate* with each other through sensor networks [14–16] that use data link protocols like NFC, RFID, LTE, Wi-Fi, Zigbee, etc., and interact with the *platform* and with the *application* levels through Internet communication technologies.

Millions of physical objects are currently connected to the Internet [14] and several research reports agree that by 2020 the IoT scenario will include more than 20 billion of smart objects. These objects are enabled by several technological changes that caused, among others, a lowering of the production costs of sensors and devices, an increase of computational capacity and an ubiquitous networking coverage. For these reasons, different ICT consulting firms foresee an exponential growth of the IoT over the next few years. For instance, Gartner[1] forecasts that the IoT will generate revenue exceeding $300 billion in 2020, resulting in $1.9 trillion in global economic value-add through sales into diverse end markets. Moreover, also public governments are reserving large fundings to IoT research: in 2015, the UK government committed around €50 million to IoT research; Germany has earmarked up to €200 million to projects related to internet-based manufacturing; France reserves €50 million to digital development projects related to embedded software and connected objects [17].

[1] https://www.gartner.com/doc/2625419/forecast-internet-things-worldwide-

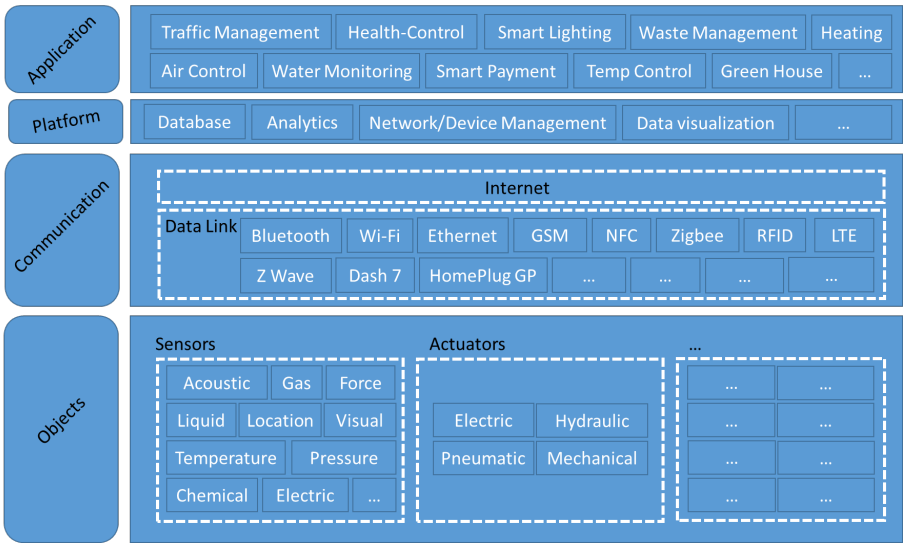


Fig. 1: The IoT architecture [18].

However, although many research studies state that IoT technologies will affect several domains, there are some critical open issues, including interoperability, security and privacy, that need to be addressed.

The remainder of the paper is organized as follows: In Section 2, we describe the most promising application domains for the IoT; in Section 3 we analyze the IoT scenario, highlighting open issues and possible directions that might help removing these burdens. Section 4 presents an original experimental assessment of state-of-the-art IoT internetworking approaches, whereas conclusions are drawn in Section 5.

2 Fields of Applications

In recent years, academic and private researches have proposed many different fields of application for the IoT. In the following, we will first briefly describe two well-known IoT fields of application and then we will focus on four most promising ones.

Smart Home. Smart home is a firm and important field of application with a market expected to reach $121 billion by 2022 [19]. Comfort, security and energy efficiency are among the main benefits that a smart home can bring [20]. For instance, house owners might use their smartphone to control Wi-Fi enabled home electronics (*e.g.*, appliances, heaters, air conditioning, coffee machines, etc.) from anywhere, might increase home security (*e.g.*, by using Wi-Fi connected cameras, sensors, and alarms) and might manage energy more efficiently (*e.g.*, by using Wi-Fi outlets to turn off electronics when not in use).

Smart City. Smart cities market is estimated to grow from $52 billion in 2015 to $147 billion by 2020 [21]. Smarter utilization and deployment of public resources (*e.g.*, lights, roads, parkings), better efficiency of services (*e.g.*, waste management, public transportation)[22,23], better quality life (*e.g.*, pollution and traffic control) and, in general, a reduction of wastes and costs for the public administration are among the main benefits of smart cities [4,24]. For instance, simple objects equipped with LoRaWAN and Sigfox communication technologies can transform the act of parking, allowing citizens to detect available parking spots in an easy way. This would not only save citizens time, but it would also help to reduce pollution, thus improving the lives of citizens.

Smart Mobility. The market for smart mobility infrastructure and services is expected to exceed $25 billion in 2024 [25]. The key advantages of smart mobility are automation, safety, and comfort. For instance, modern vehicle connection interfaces, exploiting the cars' OBD2 connectors and Bluetooth technologies, can automatically record routes and refueling stops on smartphones, keeping an eye on data such as odometer reading and tank fill level; intelligent streets, digital railways, Vehicular Ad Hoc Networks (VANETS) and advances in cognitive ability are transforming the way autonomous vehicles react to hazards and traffic. Furthermore, it is predicted that, in the next 20 years, most vehicles will be fully automated, transforming current drivers into simple passengers [26].

Health-care. Medical and health-care are very attractive fields for the IoT [3] and this market is expected to create about $1.1 - $2.5 trillion in value by 2025 [27]. Cost efficiency, reliability and safety are among the main benefits that smart health-care can bring: patients monitoring might be done in remote and in real-time through the use of smart objects and sensors, smart objects might be used to replace human regular checks of patients vital signs, home health might be improved by issuing alerts if some irregularity is detected. For example, smart prescription bottles[2] have sensors that register actions on bottles (as opening, or reducing their content) and are rechargeable using a standard micro-USB port. Bottles use the cellular communication technology to (world wide) interact with the service provider that checks on the patient activity in real time and promptly reacts if needed.

Retail Industry. The IoT retail market size is expected to reach $54 billion by 2022 [28]. Better customer experience, more efficient and secure supply chain, and the development of new channels and revenue streams are among the main benefits that smart retail industry can bring. For instance, sensors can be used to track customers' behaviors in order to better organize products placements; RFID can be used to track products in the supply chain [29, 30] and to update in real time inventories information from off-the-shelves products; smart price tags, smart codes and sensors can be used to automate many functions that are currently manually performed [31].

[2] https://adheretech.com/

Smart Factory. The smart factory market size is expected to reach $75 billion by 2020 [32]. In a Smart Factory [33], the manufacturing solutions exploit flexible and adaptive production processes, where the actors are equipped with enough computing and communication capabilities to give them an ability to act independently, without direct human intervention. For example, BMW has developed a tracking system based on RFIDs to enhance motor production and client customization: an RFID tag attached to each engine enhances the performance of the assembly line. This brings to higher levels of automation, but also to reduction of unnecessary labor and waste of resources. The benefits could also go beyond the actual production of goods. For instance, in a food supply chain scenario, IoT can enhance the whole process, from farms to processing plants, from processing plants to stores and from stores to consumers [29].

Although at first sight the above examples may look like a successful realization of IoT technologies, to a closer look they are just independent IoT applications and do not implement a global IoT scenario. Indeed, such examples also show one of the main limitations for a successful employment of IoT technologies: the lack of interoperability between objects of the same scenario. For instance, a city using many independent IoT applications, cannot be addressed as a *real* smart city. Analogously, health-care companies are proposing a large variety of interesting sensor-based applications, but what is lacking is a systematic and smart integration of the collected data, potentially together with personal information records. The current IoT scenario reminds the ICT scenario of the 70s, composed of many networks (*e.g.*, milnet, nsf-net, cs-net, etc.) unable to communicate with each other and many applications and operating systems that were unfortunately unable to interact with the others. The fragmented scenario of the 70s was virtually unified by the standardization of protocols and services provided by TCP/IP. As discussed in the following section, we suggest to follow a similar path to make the IoT a successful scenario.

3 Open Issues and Future Directions

The IoT might open a wide new world of opportunities, but for an actual large-scale employment it is still necessary to address important open issues.

3.1 Interoperability

IoT objects and devices are produced by different vendors, have different technical characteristics and specifications (*e.g.*, smartphones vs. simple RFID tags), use different communication protocols (Zigbee, Bluetooth, Bluetooth Low Energy, Wi-Fi, GSM, 3G and LTE, just to name few), and are often integrated with other heterogeneous sources of information. This is a big issue:

on the one side, producers that want to invest do not have clear indications on standards to adopt when developing IoT products and, when adopting specific IoT technologies for their products, they do not know for how long these technologies will be supported in the IoT market; on the other side, users who want to buy IoT products do not know for how long these will be compatible with the upcoming IoT scenario.

Open standards seem to be the right answer to these problems, as they can provide clear guidelines for companies to deliver quality products. Private companies (*e.g.*, AllSeen Alliance), as well as third-party institutions (*e.g.*, the IEEE Standards Association[3]), are working on producing communication standards for IoT objects with the goal of allowing different devices and sensors to communicate between themselves, regardless of their brand, category and technical equipment. Needless to say, once open standards are defined, producers should be enforced to apply them.

In addition, the traditional Internet architecture needs to adapt to IoT challenges, both at low and high level. One main reason is the tremendous increasing number of objects willing to connect to the Internet: 2010 has seen the surpass of the number of objects connected to the Internet over the earth's human population [14]. We have to expect a great increase of the traffic on the Internet, incurring into possible delays and in an increase of bandwidth request. Therefore, to allow IoT scalability, IPv6 and new generation of communication protocols seem to be mandatory.

Finally, there are also platform level interoperability issues concerning the need of integrating raw data coming from IoT objects with static and historical data stored in databases or accessible through Web services [22]. Indeed, information integration is a key (and costly) challenge [34] that needs to address many different interrelated problems like data extraction and cleaning, data transformation into data conforming with the unified format. A possible answer to these problems is the dataspace paradigm [35], an emerging approach in the information integration agenda. In a dataspace, data coexist while the actual integration efforts are faced when needed. This paradigm might represent a good answer to the problem of interoperability for IoT because of the high level of heterogeneity of the involved information sources and the need of a large scale deployment. To this end, the use of open source platforms might facilitate the development of IoT applications through plug-in services for push/pull data connection and integrated view creation and maintenance.

3.2 Security and privacy

IoT takes advantage of the possibility to gather large sets of data that, properly analyzed, give information that can be used to provide better services. However, as any other device connected to the Internet, IoT objects are possible target to a wide range of security attacks that can lead to data leakage

[3] http://standards.ieee.org/innovate/iot/projects.html

and/or data manipulation. Some recent examples of security issues include: a smart doorbell receiving the video feed from someone else house, people taking unauthorized control of the security system of specific buildings (*e.g.*, houses, banks, factories, etc.), attackers compromising on-line car systems and stopping/speeding up cars with malicious intent. If customers are expected to use IoT technologies and products, they must be assured that no accidental and/or malicious behavior might loose, steal or manipulate their data.

In the IoT scenario, security solutions cannot be limited to the single object or device, but they must be end-to-end solutions, going from the application level to the object level and vice-versa. Again, the heterogeneity of IoT interacting objects further complicates matters as different objects require different security levels (*e.g.*, fitness wearables vs. health-care applications). Nevertheless, it is fundamental to provide security solutions at least for the following problems: *authentication* (any object involved in a communication must be clearly and uniquely identified); *confidentiality* (data must be secure and available only to authorized entities); *integrity* (data must not be altered by anyone when traveling from one point to another, or while stored in some database); *fault-tolerance* (even in the presence of a fault, security services must be continuously provided).

Another issue strictly related to security is privacy. In the Internet scenario, consumers are becoming more and more aware that data are now trading currencies for services (*e.g.*, personal information in exchange of an email account), and they are increasingly interested in their privacy [36,37]; the lack of clarity about who has access to data may limit the growth of the IoT scenario. For instance, what if personal sensitive data collected with wearable devices (*e.g.*, heart rate, blood pressure, etc.) will be available also to health insurance companies? And what if these companies exploit users' personal data to tune the insurance policy cost or even to deny the policy? Possible solutions to these privacy issues are new policies reassuring customers that data do not concern individuals but aggregates, clarifying the use of data, for how long these data are stored, and who has access to them.

3.3 Business

The IoT scenario suffers from the lack of clear, widely accepted, and successful business models, of use cases and of return of investment examples [38].

Although there are some early players that successfully invested in IoT (*e.g.*, companies in the fitness and/or smart home scenarios), most companies are still thinking whether joining the IoT, because the scenario has characteristics that limit the development of a solid business model: i) diversity of objects, ii) immaturity of innovation, and iii) unstructured ecosystem [39]. The diversity of objects and the immaturity of innovation cause the employment of several different proprietary platforms and of proprietary end-to-end IoT solutions, whereas the unstructured ecosystem causes doubts to investors because the scenario is too chaotic, just like the Internet was in the mid-90s.

The solution to these problems is closely dependent on the solution of the problems highlighted above. In particular, it is fundamental to first address the problems related to interoperability and security, as this would make available IoT communication standards and IoT end-to-end security solutions. These solutions could be the blocks on which to build solid business models for the IoT scenario.

4 Internetworking in the IoT Environment

As highlighted in the previous section, one of the main issues in the development of an effective IoT scenario is the interoperability of objects and devices. A similar problem was approached and solved within the well-known and well studied Mobile Ad-hoc NETwork (MANET) paradigm, where distinct pervasive and ubiquitous sensors and devices are connected to the Internet. Therefore, one may think to employ specific MANET communication techniques to manage interactions among objects and devices in the IoT scenario. However, the IoT networking environment also shows differences with the MANET scenario. Indeed, IoT exhibits peculiar features such as 3D topologies and mobility conditions that change greatly from scenario to scenario. In particular, there are environments where objects and devices keep moving, others where they seldom move, or where just a small percentage of them move whereas the majority is static or move nomadically. With the goal to investigate whether the adoption of MANET solutions is efficient or not for the IoT environment, in this section, we present a simulation study that uses some representative MANET protocols in a 3D scenario, which is a typical representation of an IoT environment. However, since MANET protocols are generally designed for 2D scenarios, we employ well known techniques to address 3D ones.

Generally speaking, MANET protocols are either topology-based or position-based. The former approach relies on topological information to route packets between a source and a destination, whereas the latter relies on node locations to determine the suitable next hop. It is noteworthy to mention that position-based approaches were introduced to address some limitations of topology-based protocols. For instance, position-based protocols exploit the Global Positioning System (GPS) to maintain, at node level, an up-to-date view of the positional information of its neighborhood. Conversely, topology-based protocols incur in large overheads due to the need to maintain up-to-date routes of path disruptions caused by node mobility.

We consider two topology-based protocols (*i.e.*, the Ad hoc On-Demand Distance Vector (AODV [40]) and the Destination Sequenced Distance Vector (DSDV [41])) and two position-based protocols (*i.e.*, the Greedy-Face-Greedy (GFG [42]) and the Greedy-Random-Greedy (GRG [43])).

In particular, AODV considers a reactive approach to routing, and it builds routes on-demand whenever they are needed, whereas DSDV considers a proactive approach where route changes are propagated to the entire network in order to have an up-to-date view of the network paths. Another inherent property

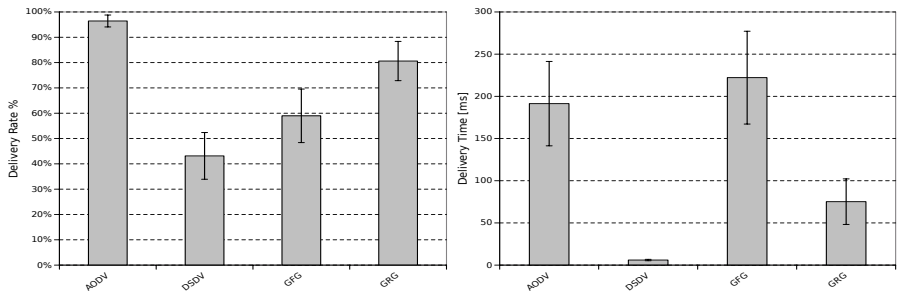
Table 1: Simulation parameters.

Parameter	**Value**
MAC type	IEEE 802.11g
Simulation area	1000 m x 1000 m x 1000 m
Transmission range	250 m
Node max speed	10 m/s
Number of data flows	10
Packet size	64 Bytes
Packet rate	2 pckt/s
Queue type	Drop Tail
Pause time	5s

of both protocols is the employment of routing tables necessary to identify the next-hop towards a destination. State-of-the-art position-based strategies rely on the Face algorithm, where packets are forwarded on a planar graph following the right-hand rule [42]. The algorithm does guarantee packet delivery to the destination in the context of planar (2D) networks, addressing the issue of local *minima* to which a greedy approach to routing is subject to. Porting the concept of planarization in 3D environments is not so straightforward, nevertheless studies like [44, 45] investigate the issue and proposed projection techniques whereby nodes of interest are projected over a 2D plane in order to create a planar sub-graph where the Face technique can be applied. In our simulation study, we consider the Face projection algorithm described in [45], as different studies agree that it achieves the best performance in terms of packet delivery ratio. GFG and GRG interleave operational phases whenever packet delivery is stuck in a local *minima*. In specifics, both approaches start with a greedy operational phase whereby packets are greedily forwarded close to the destination and, whenever packet advancement is not possible (i.e., stuck in a local *minima*), the next node is chosen either randomly or according to the Face strategy.

4.1 Experimental Scenario and Results

The simulation scenario consists of a set of nodes randomly positioned inside a cube of length 1000 units and a transmission range of 250 units. To asses the protocols, we consider a mixed scenario comprised of 20 mobile and 80 static nodes. In particular, mobile nodes are randomly positioned inside the scenario boundaries, move in a 3D space and follow a Random Way Point mobility mode. In order to increase the confidence of the outcome, we perform 40 runs of each configuration scenario and report the average values. Moreover, the simulation duration is set to 100s and the traffic consists of 10 flows (different sources and destinations) of CBR traffic. Table 1 summarizes the considered mobility parameters. It is noteworthy to point out that position-based protocols are equipped with a beaconing mechanism, whereby nodes announce their presence every 0.5s in the neighborhood.



(a) Delivery rate (b) Delivery time

Fig. 2: Delivery profiles comparison of topology and position-based approaches.

In Fig. 2a we can observe that DSDV and GFG achieve the lowest performance, with AODV having the best performance in terms of delivery rate. When analyzing the delivery time (Fig. 2b), DSDV outperforms the other protocols, however at the cost of achieving the lowest delivery rate. Focusing on the position-based approaches, GFG has the worst performance when compared to GRG and this can be explained thinking to the protocol *modus operandi*, whereby packets end up traversing long paths in projected faces in order to reach the destination.

Since most IoT application scenarios require a certain level of data delivery, DSDV and GFG are not worth using due to their low data delivery rates. On the other hand, even if AODV achieves a good level of data delivery, it unfortunately experiences high delivery delays (*e.g.*, on average, few hundreds of milliseconds could be spent to deliver a packet), as shown in Figure 2b. Therefore, it is unable to support real time and interactive traffic (*e.g.*, road safety, on-line games/chat, distributed control). These performances are affected by the necessity of establishing a route towards the destination before beginning the transmission of the data.

Since the ability to support real-time and interactive traffic is crucial for IoT applications (*e.g.*, to support safety and distributed control for automated vehicles, or just for entertainment applications), it is necessary to develop routing solutions specifically tailored to IoT. Needless to say, these solutions should be released as open standards and should be secured to malicious attacks.

5 Conclusions

In this paper, we analyzed the IoT scenario: we observed a very fragmented scenario that might compromise the successful employment of IoT. Major issues regard the proliferation of communication technologies, the absence of end-to-end security solutions and the lack of solid business models. To this aim, we provided a simulation analysis that emphasized issues and suggested

practical research directions. Finally, we highlighted some future research directions that might help addressing the identified issues, thus making the IoT a real pervasive and successful scenario.

References

1. Federal Aviation Administration. Unmanned Aircraft Systems Registration, 2016.
2. European Parliament and Council. General Data Protection Regulation, 2016.
3. S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak. The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access*, 3:678–708, 2015.
4. A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi. Internet of Things for Smart Cities. *IEEE Internet of Things Journal*, 1(1):22–32, Feb 2014.
5. M. Roccetti, S. Ferretti, C.E. Palazzi, P. Salomoni, and M. Furini. Riding the Web Evolution: From Egoism to Altruism. In *Proceedings of the IEEE Consumer Communications and Networking Conference (CCNC)*, pages 1123–1127, Jan 2008.
6. S. Ferretti, M. Furini, C.E. Palazzi, M. Roccetti, and P. Salomoni. WWW Recycling for a Better World. *Communications of the ACM*, 53(4):139–143, 2010.
7. M. Montangero and M. Furini. TRank: Ranking Twitter Users According to Specific Topics. In *Proceedings of the IEEE Consumer Communications and Networking Conference (CCNC)*, pages 767–772, Jan 2015.
8. Marco Furini and Manuela Montangero. TSentiment: On gamifying Twitter sentiment analysis. In *Proceedings of the IEEE Symposium on Computers and Communication (ISCC)*, pages 91–96, June 2016.
9. Armir Bujari, Marco Furini, and Nicolas Lainà. On Using Cashtags to Predict Companies Stock Trends. In *Proceedings of the IEEE Consumer Communications and Networking Conference (CCNC)*, Jan 2017.
10. C. E. Palazzi, A. Bujari, S. Bonetta, G. Marfia, M. Roccetti, and A. Amoroso. MDTN: Mobile Delay/Disruption Tolerant Network. In *Proceedings of the International Conference on Computer Communications and Networks (ICCCN)*, pages 1–6, July 2011.
11. C. E. Palazzi, A. Bujari, G. Marfia, and M. Roccetti. An overview of opportunistic ad hoc communication in urban scenarios. In *Proceedings of the Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET)*, pages 146–149, June 2014.
12. R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan. Internet of Things (IoT) Security: Current status, Challenges and Prospective Measures. In *Proceedings of the International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 336–341, Dec 2015.
13. P. Bellavista, G. Cardone, A. Corradi, and L. Foschini. Convergence of MANET and WSN in IoT Urban Scenarios. *IEEE Sensors Journal*, 13(10):3558–3567, Oct 2013.
14. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys Tutorials*, 17(4):2347–2376, Fourthquarter 2015.
15. L. Bononi, L. Donatiello, and M. Furini. Real-Time Traffic in Ad-Hoc Sensor Networks. In *Proceedings of IEEE International Conference on Communications (ICC)*, June 2009.
16. L. Donatiello and M. Furini. Ad Hoc Networks: A Protocol for Supporting QoS Applications. In *Proceedings of the IEEE International Parallel & Distributed Processing Symposium (IPDPS)*, April 2003.
17. R. Davis. The Internet of Things. *European Parliamentary Research*, May 2015.
18. M. Furini, F. Mandreoli, R. Martoglia, and M. Montangero. IoT: Science Fiction or Real Revolution? In *Proceedings of the Conference on Smart Objects and Technologies for Social Good (GoodTechs)*, November-December 2016.
19. Markets and Markets. Smart Home Market by Product, Security & Access Control, HVAC, Entertainment, Home Healthcare and Smart Kitchen, Software & Service and Geography - Global Forecast to 2022. Technical report, 2016.
20. M. Alam, B. Reaz, and M. Ali. A Review of Smart Homes - Past, Present, and Future. *IEEE Transactions on Systems, Man, and Cybernetics*, 2012.

21. Markets and Markets. Internet of Things (IoT) in Smart Cities Market by Solutions Platform Application - Global Forecast to 2020. Technical report, 2016.
22. L. Carafoli, F. Mandreoli, R. Martoglia, and W. Penzo. A Data Management Middleware for ITS Services in Smart Cities. *J. UCS*, 22(2):228–246, 2016.
23. Luca Carafoli, Federica Mandreoli, Riccardo Martoglia, and Wilma Penzo. A framework for ITS data management in a smart city scenario. In *Proceedings of the International Conference on Smart Grids and Green IT Systems*, pages 215–221, 2013.
24. R. De Michele and M. Furini. Understanding the City to make it Smart. In *Internet of Things*, volume 169, pages 239–244. Springer International Publishing, 2016.
25. Navigant Research. Urban Mobility in Smart Cities. Technical report, 2015.
26. Deloitte. Transport in the Digital Age - Disruptive Trends for Smart Mobility. Technical report, 2015.
27. J. Manyika, M. Chui, J. Bughin, R. Dobbs, P. Bisson, and A. Marrs. Disruptive Technologies: Advances that will transform life, business, and the global economy. Technical report, 2013.
28. Inc. Grand View Research. Gypsum Board Market Analysis By Product (Wallboard, Ceiling Board, Pre-Decorated Board), By Application (Residential, Corporate, Commercial, Institutional) And Segment Forecasts To 2022. Technical report, 2016.
29. Zh. Xiaorong, F. Honghui, Zh. Hongjin, F. Zhongjun, and F. Hanyu. The Design of the Internet of Things Solution for Food Supply Chain. In *Proc. of EMIM*, 2015.
30. Razia Haider, Federica Mandreoli, and Riccardo Martoglia. RPDM: A system for RFID probabilistic data management. *JAISE*, 6(6):707–722, 2014.
31. M. Furini and C. Pitzalis. Smart Cart: when Food enters the IoT Scenario. In *Internet of Things*, volume 169, pages 284–289. Springer International Publishing, 2016.
32. marketsandmarkets.com. Smart Factory Market by Technology (PLM, MES, PLC, SCADA, ERP, DCS, HMI), Component (Sensors & Actuators, Communication Technologies, Industrial Robotics, Machine Vision), Industry (Process, Discrete), and Geography - Global Forecast to 2022 . Technical report, 2016.
33. B. Katalinic, A. Radziwon, A. Bilberg, M. Bogers, and E.S. Madsen. The Smart Factory: Exploring Adaptive and Flexible Manufacturing Solutions. *Procedia Engineering*, 69:1184–1190, 2014.
34. P.A. Bernstein and L.M. Haas. Information Integration in Ehe enterprise. *Communication of the ACM*, 51(9):72–79, 2008.
35. M.J. Franklin, A.Y. Halevy, and D. Maier. A first tutorial on dataspaces. *PVLDB*, 1(2):1516–1517, 2008.
36. M. Furini and V. Tamanini. Location Privacy and Public Metadata in Social Media Platforms: Attitudes, Behaviors and Opinions. *Multimedia Tools and Applications*, 74(21):9795–9825, 2015.
37. M. Furini. Users Behavior in Location-aware Services: Digital Natives vs Digital Immigrants. *Advances in Human-Computer Interaction*, 2014, 2014.
38. A. Laya, V. Bratu, and J. Markendahl. Who is Investing in Machine-to-Machine Communications? In *Proceedings of ITS*, 2013.
39. M. Westerlund, S. Leminen, and M. Rajahonka. Designing Business Models for the Internet of Things. *Technology Innovation Management Review*, 4:5–14, Jun 2014.
40. C. Perkins, E. Belding-Royer, and S. Das. Ad hoc on-demand distance vector (AODV) routing, 2003.
41. Hemanth Narra, Yufei Cheng, Egemen K. Çetinkaya, Justin P. Rohrer, and James P. G. Sterbenz. Destination-sequenced distance vector (dsdv) routing protocol implementation in ns-3. In *Proceedings of the ICST Conference on Simulation Tools and Techniques*, pages 439–446, 2011.
42. P. Bose, P. Morin, and I. Stojmenovic. Routing with Guaranteed Delivery in Ad hoc Wireless Networks. *Proceedings of ACM DIAL-M/Mobicom Workshop*, 1999.
43. R. Flury and R. Wattenhofer. Randomized 3D Geographic Routing. *Proceedings of INFOCOM*, 2008.
44. A.E. Abdallah, T. Fevens, and J. Opatrny. Randomized 3D Position-based Routing Algorithms for Ad hoc Networks. *Proceedings of MOBIQUITOUS*, pages 1–8, 2006.
45. G. Kao, T. Fevens, and J. Opatrny. 3D Localized Position-based Routing with Nearly Certain Delivery in Mobile Ad hoc Networks. *Proceedings of the International Symposium on Wireless Pervasive Computing (ISWPC)*, 2007.