2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)

Contrasting Internet of Things and Wireless Sensor Network from a conceptual overview

Johana A. Manrique, Johan S. Rueda-Rueda, Jesús M.T. Portocarrero
Centro de Excelencia y Apropiación en Internet de las Cosas (CEA IoT)
Universidad Autónoma de Bucaramanga (UNAB), Colombia
(jmanrique4, jrueda526, jtalavera)@unab.edu.co

***Abstract*—The number of Internet-connected everyday objects grows thanks to the Internet of Things (IoT). The trend with this new paradigm where smart embedded devices, people, and systems are connected, is that over the next few years we could see a shift in the notion of what it means to be "on the Internet". In this context, Wireless Sensor Network (WSN) technology is an essential component of IoT because it consists of a collection of sensor nodes connected through wireless channels, capable of providing digital interfaces to the real-world things. Moreover, as it occurs in IoT, specific WSN applications can be applied to a wide variety of domains like health, agriculture, logistics, wearable computing and others. However, recent works considered as WSN applications are being called as IoT applications without distinguishing the new features that characterize this denomination. Hence, in this paper we propose to contrast IoT and WSN from a conceptual overview, aiming to find out the relationship between them and to highlight their differences in terms of (i) the thesaurus proposed by IEEE, ACM and UNESCO; (ii) by performing a chronological review of the concepts since these terms appeared; (iii) the definition issued by reference organizations and researchers; and (iv) the main application requirements addressed by reference architectures proposed for both fields of study.**

***Index Terms*—Conceptual overview, Internet of things, Wireless Sensor Network**

I. Introduction

In recent years, the term Internet of Things (IoT) has been widely used to describe solutions developed with different devices with computational capacity and connected to the Internet [1]. These solutions can be applied in domains like health [2], agriculture [3], smart cities [4], industry [5], logistics [6], among others domains. Despite the term IoT is relatively new, the idea of monitoring and controlling devices through computers and networks has been around for decades.

The first artificial satellite "Sputnik I" was launched in 1957 for performing telemetry from space. This fact marked the history of telecommunications around the world. In 1970 the network surveillance systems for remote monitoring of electricity meters appeared. In the 80's decade, the Supervisory control and data acquisition (SCADA) networks were considered as the first generation of Machine-to-Machine (M2M) communications [7]. M2M refers to the direct communication between two devices through a wireless or cabling communication channel. This technology provides interconnection of devices such as sensors and actuators for the remote control of industrial processes [8]. In 1995 the international corporation Siemens[1] developed the first cell phone to be used in M2M industrial applications allowing the wireless communication between machines.

This progressive research in Computer networks and M2M communications began an emerging field of tiny-networked sensors, offering an opportunity for a wide array of real-time applications with the capacity to provide a digital interface to the real-world things known as Wireless Sensor Network (WSN). The International Organization for Standardization (ISO) [9] defines a sensor network as a system of distributed sensor nodes interacting with each other and others environments in order to acquire, process, transfer, and provide information extracted from the physical world.

However, many of these early solutions were based on closed purpose-built networks and industry-specific standards. Through the establishment of the Open System Interconnection (OSI) protocol [10] began the development of communication services for the interconnection of computer networks in an open way with global in a scope known as the Internet. The first connection of computers called ARPANET was developed in United State of America (USA) in 1969, and it was used as a means of communication for academic and state institutions. By the early 1990s, Tim Berners-Lee [11] developed a distribution system of hypertext documents which was interconnected with the Internet architecture, initiating the World Wide Web. Since its creation, the Web and Internet both have been evolving.

The third age of Internet is currently being developed like a new paradigm known as the Internet of Things. The first two ages were characterized by the connection of people to Internet through personal computers and mobile devices respectively. Nowadays, the challenge is to connect not only people but also things to the Internet in such a way that can be linked the real world to cyberspace [12]. These things, which belong to the real/physical world, will make use of existing and future technologies to create a digital/virtual space, where they will interact with each other and other entities (e.g. tangible like human beings and intangible like software) through well-defined interfaces [13]. This means that things will have the ability to maintain their identity in the virtual world and at the same time have access to real-world information such as its physical location, state of the environment, and others. This new technological paradigm conceived as a global network of

[1] Web page https://www.siemens.com/global/en/home.html

978-1-5090-5880-8/16 $31.00 © 2016 IEEE
DOI 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.66

devices has five IoT technologies that are widely used for the deployment of successful IoT-based applications for different domains [14]:

- Radio-Frequency Identification (RFID) uses track tags attached to objects that allow their automatic identification.
- WSN allows different network topologies and multihop communication between low-cost and low-power miniature devices known as sensor nodes.
- Middleware is a software artifact that provides services to software applications to make it easier for application developers to perform communication and Input/output.
- Cloud Computing refers to hardware and systems software in the data centers that provide those services over Internet.
- IoT Applications enable device-to-device (M2M) and Human-Computer Interaction (HCI).

In this sense, WSN can be considered an integral part of the IoT paradigm in the process of connecting everyday things. Based on the above, we present an analysis from a conceptual overview between the characteristics of IoT and WSN, and between their requirements.

The remaining of this paper is organized as follow. In Section 2, we introduce some works that have ambiguity in how the concepts of both terms are addressed. In Section 3, we highlighted the main differences between IoT and WSN from a conceptual point of view. Finally, the conclusions are presented in Section 4.

II. LITERATURE REVIEW

WSN can be applied in multiple domains. Rawat et al. [15] present a summary of some applications for different domains which make use of WSN such as process control and automation [16], and manufacturing monitoring [17] for the Industrial domain; surveillance [18] and sensing disaster [19], [20] for the smart cities domain, monitoring peoples health conditions [21], [22] for the health domain; and monitoring agricultural production [23] for agriculture domain. According to Borgia [12], IoT can also be applied in these domains by proposing a WSN-based solution.

In addition, Wang et al. [24] presented in 2008 a comprehensive review of works related to middleware systems for WSN. This survey shows an overview of almost thirty existing projects where features as process communication, context, application, network, and node sensors were compared. Furthermore, the authors discuss the challenges related to the contexts of distributed computing and the embedded sensor devices, the tradeoffs between the degree of application specificity and middleware generality, and the context of Quality of Service (QoS). On the other hand in 2016, Razzaque et al. [25] outline a set of requirements for IoT middleware systems, and present a survey of the existing middleware solutions. This survey is organized by functional, non-functional and architectural requirements. However, it is important to note that some of the middleware systems described in [25], such as: MagnetOS [26], Mate, MiLAN [27], SINA, TinyDB [28], COUGAR [29], Impala [30], Agilla [31], AutoSec [32] were also described in [24] as WSN middleware systems, eight years ago.

In this context, a question arises: considering that WSN applications can also connect things to the Internet, What is the difference between the self-denominated WSN and IoT applications? What are the implications if in an IoT project that implements a WSN, the word IoT is changed by WSN?. For instance, ”A WSN solution for agriculture” instead of ”An IoT solution for agriculture”. Are these terms different or just complement each other? In the next sections, we intend to answer these questions.

III. CONCEPTUAL OVERVIEW

Although the terms IoT and WSN are closely related, from a conceptual overview there are some remarkable differences. We organized this section into four perspectives. The first is a list of thesauri organized hierarchically linking both terms, the second shows the relationship over the time of both concepts, the third is related to the behavior of scientific publications from 1990, and the fourth perspective compares IoT and WSN with respect to their applications requirements.

A. Thesaurus Search

This perspective aims to place IoT and WSN into the scientific terms proposed by some of the main academic organizations, in order to find out the relationship between these two concepts that allow us to understand their origin from a etymological point of view. We analyzed the thesaurus proposed by the IEEE* [33], ACM^{-} [34], and UNESCO^{+} [35] to find out the relationship between IoT and WSN. For this purpose we developed a concept map, depicted in Figure 1.

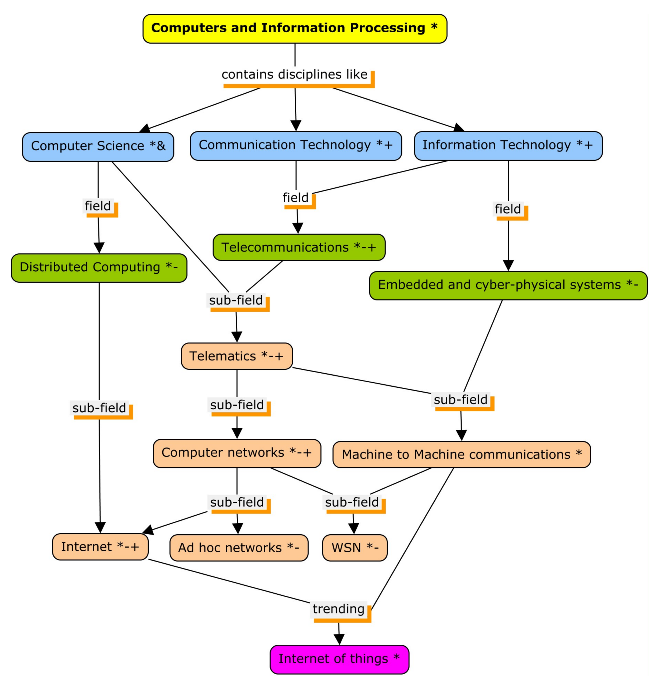

Fig. 1. Thesaurus relationship between IoT and WSN

The map was hierarchically organized based on the analysis of the broader terms and their respective narrow terms. The broader term Computers and Information Processing *(yellow)* contains disciplines as Computer Science, Communication Technology and Information Technology *(blue)*. These disciplines handle digitized information obtained from communication channel networks. From there, fields of research as Distributed Computing, Telecommunications and Embedded and Cyber-physical systems were born. Distributed Computing is a model for solving massive computing in cluster way. Telecommunications make use of information and communications technology to transmit different types of data. Cyber-physical Systems (CPS) [36] refers to the next generation of embedded Information and Communication Technology (ICT) systems for to be more adaptable, efficient, reliable and secure systems. These fields are the foundation of Internet, M2M Communications and Computer Networks.

By analyzing the Thesaurus relationship between IoT and WSN, +we can conclude at one end, the WSN term is derived as a sub-field from Computer Networks and M2M Communications and on the other hand, IoT is a trend that comes up from the Internet like as a particular type of Computer Networks and the M2M communications. From the perspective of thesauri, both terms are influenced by M2M for sending telemetry from one machine to another. Nevertheless, IoT uses the Internet Protocol (IPv6) to ensure that every "thing" has an identifiable Internet address [37]. WSN could use the Internet but not required.

B. Timeline concepts

This perspective aims to create a graphical representation by displaying when the terms WSN, IoT and their related terms sequentially appear along the time as shown in Figure 2. Institutions and researchers around the world have proposed definitions about what IoT and WSN are. Among all, they try to define the meaning of what these terms represent and what are the most important features to achieve the standardization.

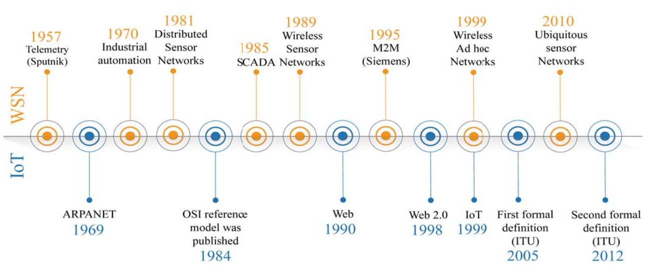

Fig. 2. Timeline of concepts

In the mid-80s, sensor networks were called as Distributed Sensor Network. For Akyildiz et al. [38], a sensor network is composed of a large number of sensor nodes interconnected with the ability to perform sensing and data collection. At the end of the 80s, the WSN concept began to be used. Wang et al. [24] describe that WSNs connect sensor nodes wirelessly, facilitating the construction of distributed system for collecting data giving coverage of large geographic areas. For the year 2010, The International Telecommunication Union (ITU) defines the term Ubiquitous Sensor Network (USN) as a conceptual network built through existing physical networks that use the detected data and provides services for extracting knowledge that can be used by anyone, anywhere and anytime where information is generated from the context awareness.

On the other hand, the IoT term came out about two decades after WSN. The origin of IoT has been attributed to members of the Auto-ID Center at Massachusetts Institute of Technology (MIT) [39] around 2000. They developed a network of objects with Electronic Product Code (EPC) for identifying and monitoring the flow in a supply chain automatically. This code was stored in an integrated circuit in the form of tag to be read by Radio Frequency Identification (RFID) [40]. RFID technology is regarded as one of the driving of IoT like M2M communication.

The ITU [41] published the IoT first formal definition in 2005, describing IoT as a new dimension added to the world of ICT. Anyone is going to have connectivity with anything from anytime and anywhere. In 2012, the ITU published the second formal definition [42] describing IoT as the global infrastructure for the information society that promotes the provision of advanced services through the interconnection of physical/virtual things for interoperability of present and future ICT.

The concepts described above define the IoT as the Internet of the future. A global network infrastructure, linking physical and virtual objects which have their own identity, with autonomy to collect data, communicate with each other, process and visualize the results of that process. In contrast to IoT, WSN does not specify a direct connection of the sensor nodes to the Internet for sensing and data collection.

C. Academic Publications search

In this perspective, we perform a search in Scopus, the online bibliographic database for academic publications. We defined two terms "Internet of things" and "Wireless Sensor Network" for searching in the title, abstract or keywords. From the results obtained in both searches, we extracted the number of publications and the years in which they were published as shown in Figure 3.

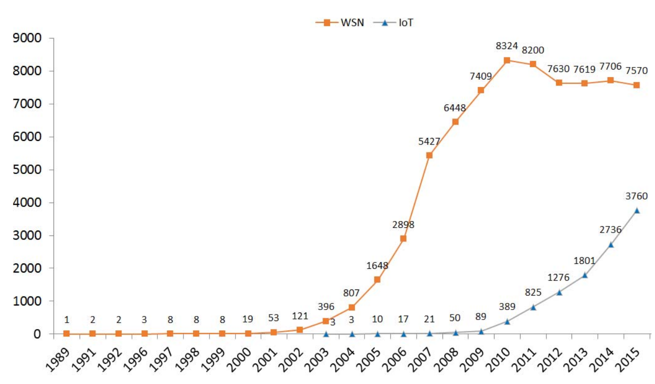

Fig. 3. Literature search of IoT and WSN

According to the graphic, in the early 80's were published the first scientific publications related to sensor networks.

The contributions of these works were about to the solution of problems in network design, distribution nodes and data aggregation made by the sensors [43]–[45].

Over time, scientific research and technological development about WSN grew thanks to the efforts of researchers to troubleshoot related with: (i) size reduction of sensor nodes, (ii) implementation of sensor networks in multiple domains [46]–[48], (iii) the increasing of data transmission range [49], (iv) more computing power, (v) low-power consumption of the sensor nodes [50], (vi) reliability in the connection between sensor nodes [51].

IoT related publications appear after 2000. From a broader perspective, this is due to the proliferation of technologies (HW and SW) and the trends of companies to start in the IoT market with smaller, easy to use and economical devices, according to the specific domains. Since 2010, IoT publications have increased considerably, and the trend of this paradigm is to grow more. At the same time, WSN publications began to descend. However, this does not mean that researchers in this area to stop completely, but being WSN considered as an integral component of the ecosystem of IoT, WSN research is redirected as a technology that is part of IoT. Alcaraz et al. [52] describe that WSN reaches its full potential when once it is connected to the Internet, becoming part of IoT.

D. Application Requirements

The application requirements are guidelines that any development in a determined field of study must fulfill, in this case, WSN and IoT. For contrasting this point of view, we reviewed the application requirements of reference models, the Sensor Network Reference Architecture (SNRA) from the ISO [53] and reference model for IoT from ITU [54]. The common application requirements for WSN and IoT are described below:

- **Security and Privacy:** In WSN, the security level varies according to the application. Usually, it has a mid-high security level, but other applications must have a high-security level (e.g. Theft prevention system for high-value goods or critical infrastructure monitoring). In IoT, the security level due to its complexity is higher because all things are connected which results in significant security treatment of confidentiality, authenticity, and integrity of both data and services. Another reason is the need to integrate different security policies and techniques related to the variety of devices and user networks in the IoT.
- **Robustness:** Sensor networks must provide and maintain operational robustness though some sensor nodes die or leave the sensor network. In IoT, the state of devices change dynamically (e.g., sleeping and waking up, connected and disconnected as well as the context of devices including location and speed).
- **Scalability:** The sensor network must adapt itself dynamically to provide scalability for various sensor network applications and number of sensor nodes. In IoT, the number of devices that need to be managed and that communicates with each other is a greater amount than in WSN. The IoT Applications must support scalability, it includes the number of devices, the volume of data to be handled, and the data traffic that needs to be communicated.
- **Quality of Service (QoS)** A WSN needs to address QoS requirements, such as data accuracy, reliability, and latency. In IoT, the QoS requirements are more complex than WSN due to the diversity of IoT services like information services, infrastructure services, ubiquitous network, reliable transmission technologies, and easy to set up or auto-configurable. These QoS requirements are required in IoT solutions to provide ubiquitous and intelligent services, and people with rich real-world information.
- **Heterogeneity:** In WSN, the heterogeneity consists in to support the interoperability among different sensor networks. In IoT, the heterogeneity consists in to support different devices, hardware platforms, and networks.
- **Deployment and Coverage:** The WSN manages information about deployment and coverage for ensuring the correct functionality of the network. This requirement is one of the most important requirements for a WSN implementation.
- **Mobility:** In WSN, the node mobility occurs when a sensor node moves within the sensor network. In IoT, the mobility no only consist of a device that moves within a network, but also in service mobility between different service providers at the network level.
- **Power/Energy Management:** The sensor nodes have limited resources, for this reason, a WSN application must provide an energy management scheme to optimize the sensor networks operation lifetime.
- **Identification of Things:** IoT requires a unique identification of the thing for ensuring the communication. For this reason, IPv6 is relevance. In WSN applications, the things identification is not required; its scope is the coordinated collection of data [55].
- **Autonomy:** The WSN must be autonomous, in others words, it should address self-configuration, self-healing, self-protection and self-optimization.
- **Data Processing:** In WSN, the data processing consist in data aggregation to reduce network congestion. In IoT, the data are not only the data processing from a physical/device layer but they are also the data analytics by applying Big Data techniques to get new information from collected data. In IoT, data becomes information, information transform in knowledge and knowledge transform in wisdom.
- **Communication and Internet Connection:** Sensor networks must have communication capabilities between each component (sensor nodes and gateway) and other sensor networks. Communication in IoT is IP-based, and it is considered by several organizations like a global network. In WSN, Internet connection is not required, and it is interconnected through wireless connection channel. The sink node receives data from sensor nodes, and this, in turn, sends data toward WSN to a server. Some WSN application uses Internet as a communication channel, but this is not an essential characteristic to be considered in

WSN. In IoT, Internet connection is a mandatory feature.

- According to [54], other IoT application requirements are interoperability, autonomic networking, autonomic services provisioning, location-based capabilities, plug and play, manageability, compliance with laws and regulations and awareness of service.

The application requirements between WSN and IoT are very similar. The difference lies in the degree of relevance of each of them, as shown in table I. To this end, four degrees of relevance were established: High, Medium, Low and Null.

TABLE I
APPLICATION REQUIREMENTS BETWEEN IoT AND WSN

Requirement	**WSN**	**IoT**
Security and Privacy	Medium	High
Robustness	High	High
Scalability	Medium	High
Quality of Service	Medium	High
Heterogeneity	Medium	High
Deployment and Coverage	High	Null
Mobility	Medium	High
Power/Energy Management	High	Medium
Identification of Things	Null	High
Autonomy	High	High
Data Processing	Null	High
Communication and Internet Connection	High	High

IV. CONCLUSIONS

WSN and IoT are two fields of study with origins in common, computer networks and M2M. This is reflected in their features, application requirements and application domains. However, both of them have different approaches that we addressed along this work, allowing us to conclude the following.

At first, IoT is a new paradigm that integrates several technologies that already existed, such as WSN, RFID, Cloud Computing, Middleware systems and end-user applications.

Second, the number of scientific publications related to WSN has been declining in recent years, and this declining is not due to WSN is losing importance in nowadays, on the contrary, researchers are beginning to treat WSN as a technology integrated into the IoT ecosystem.

Third, although WSN was originally conceived for local networks, WSN applications may take advantage of Internet, even without being an essential requirement for WSN. Unlike of WSN, the Internet is an essential requirement for IoT applications, and this is the major difference between IoT and WSN.

Finally, IoT and WSN have similar application requirements. However, both of them share these requirements in different degrees of relevance. On one hand, WSN prioritizes the management of limited resources. On the other hand, the assurance security, scalability, heterogeneity and QoS attributes are more complex activities in IoT than WSN, mainly due to IoT integrates several hardware and software technologies, communication protocols, and others features that increase the risks associated with these technologies.

As future work, we will intent to compare IoT and WSN from an architectural point of view, by analyzing their reference architectures, technologies, and protocols in order to offer a deeper and more detailed comparison between these fields of study.

ACKNOWLEDGMENT

The authors would like acknowledge the cooperation of all partners within the *Centro de Excelencia y Apropiación en Internet de las Cosas (CEA-IoT)* project. The authors would also like to thank all the institutions that supported this work: the Colombian Ministry for the Information and Communications Technology (*Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC*) and the Colombian Administrative Department of Science, Technology and Innovation (*Departamento Administrativo de Ciencia, Tecnología e Innovación - Colciencias*) through the *Fondo Nacional de Financiamiento para la Ciencia, la Tecnología y la Innovación Francisco José de Caldas* (Project ID: FP44842-502-2015).

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[2] F. Hu, D. Xie, and S. Shen, "On the application of the internet of things in the field of medical and health care," in *Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing*. IEEE, 2013, pp. 2053–2058.

[3] F. Zhang, "Research on applications of internet of things in agriculture," in *Informatics and Management Science VI*. Springer, 2013, pp. 69–75.

[4] L. Sanchez, L. Muñoz, J. A. Galache, P. Sotres, J. R. Santana, V. Gutierrez, R. Ramdhany, A. Gluhak, S. Krco, E. Theodoridis *et al.*, "Smartsantander: Iot experimentation over a smart city testbed," *Computer Networks*, vol. 61, pp. 217–238, 2014.

[5] C. Kruger and G. P. Hancke, "Implementing the internet of things vision in industrial wireless sensor networks," in *2014 12th IEEE International Conference on Industrial Informatics (INDIN)*. IEEE, 2014, pp. 627–632.

[6] J. Jiang and K. Su, "Management platform architecture of modern tobacco logistics based on internet of things technologies," in *LISS 2012*. Springer, 2013, pp. 1403–1409.

[7] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in scada networks," *Computers & Security*, vol. 25, no. 7, pp. 498–506, 2006.

[8] J. Kim, J. Lee, J. Kim, and J. Yun, "M2m service platforms: survey, issues, and enabling technologies," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 61–76, 2014.

[9] I. J. 1, "Study on Sensor Networks (Version 3)," Tech. Rep., 2009.

[10] G. V. Bochmann, "Protocol specification for osi," *Computer Networks and ISDN Systems*, vol. 18, no. 3, pp. 167–184, 1990.

[11] T. Berners-Lee, R. Cailliau, J.-F. Groff, and B. Pollermann, "World-wide web: the information universe," *Electronic Networking: Research, Applications and Policy*, vol. 2, no. 1, pp. 52–58, 1992.

[12] E. Borgia, "The internet of things vision: Key features, applications and open issues," *Computer Communications*, vol. 54, pp. 1–31, 2014.

[13] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, "Key management systems for sensor networks in the context of the internet of things," *Computers & Electrical Engineering*, vol. 37, no. 2, pp. 147–159, 2011.

[14] I. Lee and K. Lee, "The internet of things (iot): Applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431–440, 2015.

[15] P. Rawat, K. D. Singh, H. Chaouchi, and J. M. Bonnin, "Wireless sensor networks: a survey on recent developments and potential synergies," *The Journal of supercomputing*, vol. 68, no. 1, pp. 1–48, 2014.

[16] C.-C. Shen, C. Srisathapornphat, and C. Jaikaeo, "Sensor information networking architecture and applications," *IEEE Personal communications*, vol. 8, no. 4, pp. 52–59, 2001.

[17] E. Shi and A. Perrig, “Designing secure sensor networks,” *IEEE Wireless Communications*, vol. 11, no. 6, pp. 38–43, 2004.

[18] M. Dunbabin, P. Corke, I. Vasilescu, and D. Rus, “Data muling over underwater wireless sensor networks using an autonomous underwater vehicle,” in *Proceedings 2006 IEEE International Conference on Robotics and Automation, 2006. ICRA 2006.* IEEE, 2006, pp. 2091–2098.

[19] M. Castillo-Effer, D. H. Quintela, W. Moreno, R. Jordan, and W. Westhoff, “Wireless sensor networks for flash-flood alerting,” in *Devices, Circuits and Systems, 2004. Proceedings of the Fifth IEEE International Caracas Conference on*, vol. 1. IEEE, 2004, pp. 142–146.

[20] J. Heidemann, Y. Li, A. Syed, J. Wills, and W. Ye, “Underwater sensor networking: Research challenges and potential applications,” *Proceedings of the Technical Report ISI-TR-2005-603, USC/Information Sciences Institute*, 2005.

[21] Y. Zatout, E. Campo, and J.-F. Llibre, “Wsn-hm: Energy-efficient wireless sensor network for home monitoring,” in *Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2009 5th International Conference on*. IEEE, 2009, pp. 367–372.

[22] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, “A survey on wireless body area networks,” *Wireless Networks*, vol. 17, no. 1, pp. 1–18, 2011.

[23] S. E. Díaz, J. C. Pérez, A. C. Mateos, M.-C. Marinescu, and B. B. Guerra, “A novel methodology for the monitoring of the agricultural production process based on wireless sensor networks,” *Computers and Electronics in Agriculture*, vol. 76, no. 2, pp. 252–265, 2011.

[24] M.-M. Wang, J.-N. Cao, J. Li, and S. K. Dasi, “Middleware for wireless sensor networks: A survey,” *Journal of computer science and technology*, vol. 23, no. 3, pp. 305–326, 2008.

[25] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, “Middleware for internet of things: a survey,” *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 70–95, 2016.

[26] C. M. Kirsch, M. A. Sanvido, and T. A. Henzinger, “A programmable microkernel for real-time systems,” in *Proceedings of the 1st ACM/USENIX international conference on Virtual execution environments*. ACM, 2005, pp. 35–45.

[27] W. B. Heinzelman, A. L. Murphy, H. S. Carvalho, and M. A. Perillo, “Middleware to support sensor network applications,” *IEEE network*, vol. 18, no. 1, pp. 6–14, 2004.

[28] S. R. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, “Tinydb: an acquisitional query processing system for sensor networks,” *ACM Transactions on database systems (TODS)*, vol. 30, no. 1, pp. 122–173, 2005.

[29] P. Bonnet, J. Gehrke, and P. Seshadri, “Towards sensor database systems,” in *International Conference on Mobile Data Management*. Springer, 2001, pp. 3–14.

[30] T. Liu and M. Martonosi, “Impala: A middleware system for managing autonomic, parallel sensor systems,” in *ACM SIGPLAN Notices*, vol. 38, no. 10. ACM, 2003, pp. 107–118.

[31] C.-L. Fok, G.-C. Roman, and C. Lu, “Agilla: A mobile agent middleware for self-adaptive wireless sensor networks,” *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, vol. 4, no. 3, p. 16, 2009.

[32] Q. Han and N. Venkatasubramanian, “Autosec: An integrated middleware framework for dynamic service brokering,” *IEEE distributed systems online*, vol. 2, no. 7, pp. 22–31, 2001.

[33] T. I. of Electrical and E. Engineers, “2014 ieee thesaurus,” Tech. Rep., 2014. [Online]. Available: http://www.ieee.org/documents/ieee_thesaurus_2013.pdf

[34] Association for computing machinery ACM, “CCS 2012,” Tech. Rep., 2012.

[35] United Nations Educational Scientific and Cultural Organization, “UNESCO Thesaurus,” 2016. [Online]. Available: http://vocabularies.unesco.org/

[36] K.-J. Park, R. Zheng, and X. Liu, “Cyber-physical systems: Milestones and research challenges,” *Computer Communications*, vol. 36, no. 1, pp. 1–7, 2012.

[37] S. Deering and R. Hinden, “Internet protocol, version 6 (ipv6) specification,” The Internet Engineering Task Force (IETF), Tech. Rep., 1998.

[38] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” *Computer networks*, vol. 38, no. 4, pp. 393–422, 2002.

[39] D. L. Brock, “The electronic product code (epc) naming scheme for physical objectsc,” *Auto-ID Center White Paper MIT-AUTOID-WH-002*, p. 21, 2001.

[40] S. Sarma, D. Brock, and D. Engels, “Radio Frequency Identification and the Electronic Product Code,” *IEEE Micro*, vol. 21, no. 6, pp. 50–54, 2001.

[41] International Telecomunication Union - ITU, “The Internet of Things,” Tech. Rep., 2005.

[42] International Telecommunication Union, “Overview of the Internet of things,” Tech. Rep., 2012.

[43] R. Wesson, F. Hayes-Roth, J. W. Burge, C. Stasz, and C. A. Sunshine, “Network structures for distributed situation assessment,” *IEEE Transactions on systems, man, and cybernetics*, vol. 11, no. 1, pp. 5–23, 1981.

[44] C.-Y. Chong, S. Mori, and K.-C. Chang, “Information fusion in distributed sensor networks,” in *1985 American Control Conference*, vol. 1, 1985, pp. 830–835.

[45] C.-Y. Chong, K.-C. Chang, and S. Mori, “Distributed tracking in distributed sensor networks,” in *American Control Conference, 1986*. IEEE, 1986, pp. 1863–1868.

[46] S. M. A. El-Kader and B. M. M. El-Basioni, “Precision farming solution in egypt using the wireless sensor network technology,” *Egyptian Informatics Journal*, vol. 14, no. 3, pp. 221–233, 2013.

[47] B. M. M. El-Basioni, S. M. A. El-kader, and M. Abdelmonim, “Smart home design using wireless sensor network and biometric technologies,” *information technology*, vol. 1, p. 2, 2013.

[48] J. Yang, J. Zhou, Z. Lv, W. Wei, and H. Song, “A real-time monitoring system of industry carbon monoxide based on wireless sensor networks,” *Sensors*, vol. 15, no. 11, pp. 29 535–29 546, 2015.

[49] H. Z. Abidin, N. M. Din, and Y. E. Jalil, “Multi-objective optimization (moo) approach for sensor node placement in wsn,” in *Signal Processing and Communication Systems (ICSPCS), 2013 7th International Conference on*. IEEE, 2013, pp. 1–5.

[50] X. Chen, X. Wang, and X. Chen, “Energy-efficient optimization for wireless information and power transfer in large-scale mimo systems employing energy beamforming,” *IEEE Wireless Communications Letters*, vol. 2, no. 6, pp. 667–670, 2013.

[51] Y. K. Joshi and M. Younis, “Restoring connectivity in a resource constrained wsn,” *Journal of Network and Computer Applications*, vol. 66, pp. 151–165, 2016.

[52] C. Alcaraz, P. Najera, J. Lopez, and R. Roman, “Wireless sensor networks and the internet of things: Do we need a complete integration?” in *1st International Workshop on the Security of the Internet of Things (SecIoT10)*, 2010.

[53] S. G. on Sensor Networks (SGSN), “Study on sensor networks (version 3),” ISO/IEC JTC 1, Tech. Rep., 2009.

[54] ITU-T, “F.748.0: Common requirements for internet of things (iot) applications,” International Telecommunication Union, Tech. Rep., 2014.

[55] I. I. Initiative, “Towards a definition of the internet of things (iot),” Tech. Rep., 2015.