Quest Journals
Journal of Electronics and Communication Engineering Research
Volume 7 ~ Issue 7 (2021) pp: 01-06
ISSN(Online) : 2321-5941
www.questjournals.org

Research Paper

Radar based Sensors for Internet of Things (IoT) Application: A Feasibility Study

Surajo A. Musa[1]*, Sahanunu Dahiru[2], Aminu Maigari[3]
[1]*Electrical Engineering Dept., Federal Polytechnic Daura, Katsina-Nigeria*
[2]*Computer Engineering Dept., Jigawa State Institute of Information Technology (JSIIT) Kazaure-Nigeria*
[3]*Computer Science Dept., Jigawa State Institute of Information Technology (JSIIT) Kazaure, Jigawa-Nigeria*

ABSTRACT: *The Internet of Things (IoT) is an attempt of providing a virtual platform for intelligent interactions between physical devices, vehicles, home appliances (smart homes) and other objects embedded with sensors and actuators thus communicating over an internet protocol (IP). Apart from radio frequency identification (RFID) sensors, a radar-based sensor for IoT applicatioin is introduced. It is a proposed technology that is capable of providing not only information to the IoT system but in addition helps to secure the smart environment from relatively intending stealth objects vulnerable to the environment. This paper verified the feasibility of integrating radar system as a sensor device to serve as a source of information for a successful IoT deployment. The paper further highlights some IoT architectures presented by various researchers, given preference to sensor layer of the IoT architecture.*

KEYWORDS: *Internet of Things (IoT), Radio Frequency Identification Device (RFID), Radar*

Received 24 July, 2021; Revised: 07 August, 2021; Accepted 09 August, 2021 *© The author(s) 2021. Published with open access at* www.questjournals.org

I. INTRODUCTION

Internet is continuously evolving from a human-to-machine (H2M) base communication to machine-to-machine (M2M) communication system [1] and [2]. It was estimated that by the year 2020, about 30 billion devices were expected to be deployed across the world [3]. Internet of things (IoT) is a synergetic approach of cascading telecommunication, hardware and software engineering, informatics as well as social sciences to work as one entity [2], for interoperability of heterogeneous devices. In the face of wireless communication systems, tremendous achievements were recorded with smart homes, which can be seen as the advent of IoT when multihop network interconnecting a smart environment was extended to represent a virtual world [4]. In spite of the foreseen IoT benefits like learning enhancement, e-health among others, there exist a posing threats like trust guarantee, compromise of security and privacy and other challenging factors derailing the acceptance of the emerging worldwide network [5].

IoT creates a platform for intelligent interaction between real time activities [6], and making the Internet more immersive and pervasive [7]. Smart algorithms execution for intelligent interactions with other things in the Internet is one basic IoT feature achievable via information consumption. IoT involved transforming a real life activity into virtual or rather digital world. The IoT emerges among the hot topics focused by both researchers, industries [8], and government agencies. [1] reported how European and American organizations with other multinational companies were involved in the design and development of IoT for achieving multiple benefits. Very powerful automated services in the field of security, e-health and e-governance were among the various services that can be achieved through a successful implementation of the IoT.

Objects connected to IoT environment usually provides a M2M communication platform through sensors and actuators. Information retrieved from the connected objects can be through either or a combination of RFID, wireless sensor networks (WSN), gateway server, middleware, internet protocols (IPs). M2M connectivity can also be achieved via global positioning system (GPS), geographical information system (GIS), smart objects and RFID. Through IoT, objects can be sensed and controlled remotely via the existing network facilities [7]. Identification and tracking technologies as a function of IoT [8] is performed by RFID, barcode

and intelligent sensors thus, radar can therefore serves as a good candidate for such application as well due to its similar characteristics.

Radio frequency identification device (RFID) is among the wireless sensors used for information retrieval about an object that is already stored in an electronic form. In a smart environment, RFID serves as the major source information. In this regard, radar sensors can also be adopted due to some features capable of providing not only information to the IoT system but also help in securing the smart environment from harmful or stealth objects. This paper therefore tends to verify the feasibility of implementing the radar system as one of the sensor device that can be integrated into the intending IoT technology.

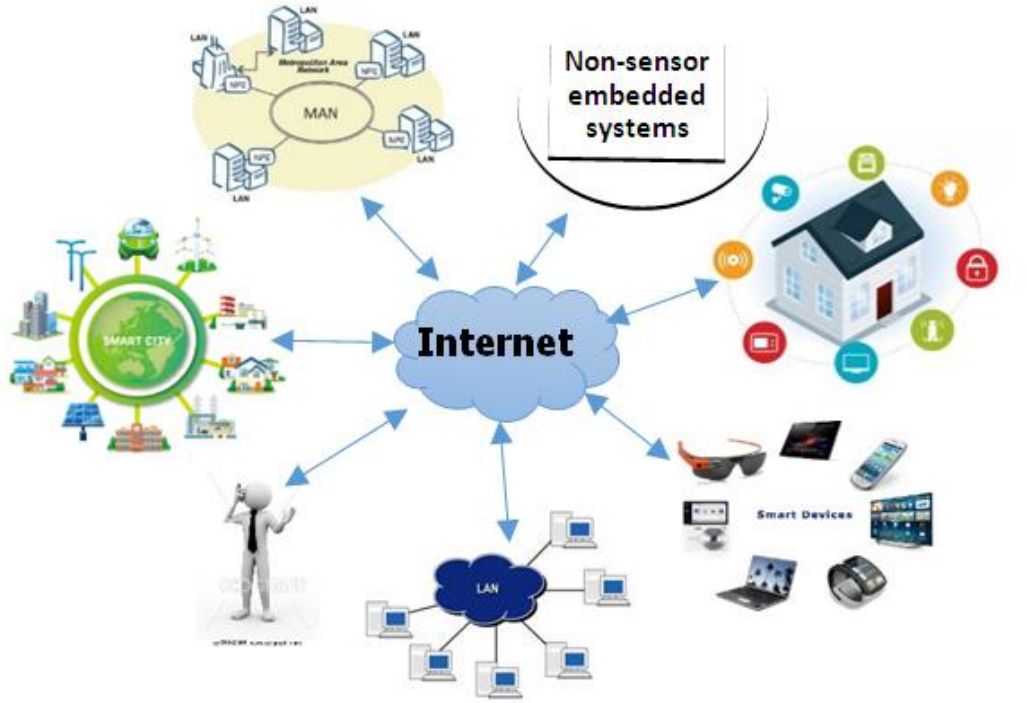

Figure 1. Typical IoT components

Figure 1 shows a typical IoT platform involving smart devices, smart homes, local area network (LAN), metropolitan area network (MAN) and other non-sensor embedded things/systems, directly connected to Internet via their respective sensors. Non-sensor objects or thing can be humans, birds, airplane or object with stealth technology. Implementation of radar sensors may therefore be of help in getting this types of objects to be detected. The remain of the paper is presented follows: Section II describes an overview of the IoT. Section III presents an introduction of radar system and its features. Prospects and challenges was discussed in IV while section V concludes the paper and provides a summary of some achievements in the radar system.

II. IOT ARCHITECHTURE OVERVIEW

This section briefly discussed how different researchers viewed the IoT architecture describing the important components necessary for successful IoT implementation. Different views and perspectives do exist toward the concept and formation of Internet of things. The international telecommunication union (ITU) in [9] sees IoT as the interconnection of physical and virtual things base on their existing and evolving interoperability that give rise to a global infrastructure meant for informative society enabling environment. Others have seen it as an extension of smart community [4] categorized as home domain (smart home), community domain (smart community) and service domain (IoT). It also be characterized as either an 'internet based' or "things based" [5]. Any time, any place and any things connection are considered the three basic dimensions of IoT by [6]. The technology involved according to [9] are the things or object layer, connectivity layer and IoT cloud layer.

Efforts have been made by many international organization to develop various IoT standards [8] to coordinate it with local standard for optimal benefit. [2] described how a wireless sensor networks (WSN) can be integrated into the IoT architecture. The sensor despite its one-way communication protocol, is able to receive information and send it to the sensor device in form of command and react on behalf of the user. The proposed system architecture for this integration involves the wireless sensor networks (WSN), Gateway server, middleware and the mobile client.

Perception, network, middleware, application and business layer are the 5-layers architecture model according to [1]. 4-layer structures was identified by [8] such as Sensing, Networking, Service and Interface layer necessary to implement an IoT platform. The ITU considered Sensing, Networking, Application, Middleware and Accessing layers to be necessary for a successful IoT implementation. Radio environment map (REM) repository, multiple radar operators, measurement capable device (MCD) and the IoT network entities are the 4-layered architecture proposed by [10] for a successful IoT implementation.

Based on the proposed architectures in [5], [1], there is need to address some challenges such as interoperability, reliability, scalability, quality of service (QoS) among others. This is as a result of what was involved in the IoT communication between H2M and M2M intelligent interactions hence, induce traffic and storage limitation in the network facility. IoT may therefore depends on advancement in its technological design to improve application and business models. Irrespective of the number of layers involve in IoT design model, it is pertinent to note that most researchers considered sensor layer as one basic requirement for successful IoT deployment. In contrast, IoT can be represented as a 3-layered architecture involving Object-, Interface- and Internet layer as shown in figure 2a. All other facilities involved in other architectures can be resolved or inclined to either of these 3 layers.

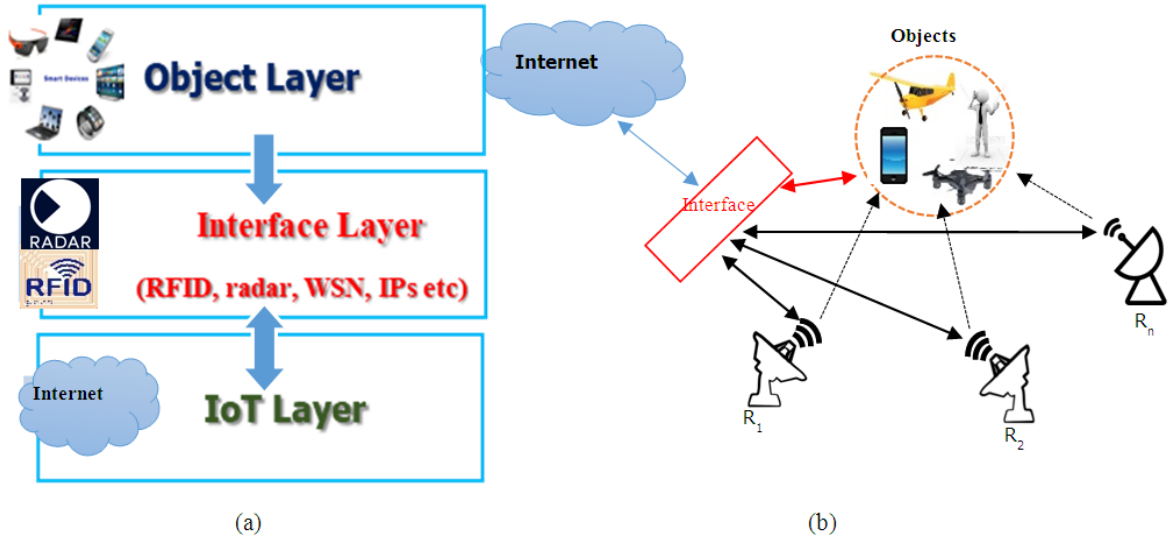

Figure 2. IoT Architecture (a) Radar or RFID-based sensor (b) Radar-based IoT objects monitoring

The Figure 2a shows how the 3 layers are related to one another. The interface layer of involved an onboard signal and/or data processing capabilities like sensor devices, WSN, transceiver, micro-processor, radar etc. In figure 2b, a representation of the proposed radar-based objects monitoring capable of monitoring all objects connected to the IoT platform. The architecture comprises of multiple radar nodes with different characteristics and capabilities, observing all connected objects, devices, people before given access to connect into the IoT environs for surveillance purpose. The interface of figure 2b may also involve an auto correlation between information received from an object seeking connection access and that of the radar. Although this may require further processing yet, decision as to whether an object be given access to connect to IoT platform or not may be based on information provided by the radar.

III. RADAR ENABLE SENSORS

Radar is an acronym that stands for Radio Detection And Ranging. It is an electronic device designed for detecting an object usually called a target at a predefined distance [11]. The basic principle of radar operation is the transmission of a radio frequency at a speed of light and echoed a reflection from the referenced target. The reflected signal contains information about an object and its target location at a distance that an unaided eye cannot see or rather estimate its distance [12]. In the year 1800, Michael Faraday's experiment proved that an electric current produced a magnetic field which returns the energy contained in this field to the circuit even if the current is absent [13].

In the recent years, the use of various illuminators of opportunities (passive) for target detection and classification has become popular and is explored by many scholars for both monostatic to bistatic approaches. Illuminators used in passive bistatic approach (PBR) such as global navigation satellite system (GNSS) in [14], Long Term Evolution (LTE) signal [15], WIFI [16], digital video terrestrial broadcast (DVT-B) [17], digital

audio broadcast (DAB) [18], FM based [19] became a boosting tool for radar worldwide, thereby becoming a prominent tool for both military and common applications.

Active radars like forward scatter radar (FSR) formed another breakthrough as to how best the target radar cross section (RCS) could be minimized [20]. Furthermore, radar system was explored for many applications via different techniques which can be implemented for integrating its capability, as well as serving as a sensor device in the emerging IoT technology. Radar detects the presence of an object via the reflected signal resulting from initial emitted radio wave. While a continuous wave radar detects objects in path of the radiated signal, the frequency modulated continuous wave can be used to measure the range of the detected object [22]. Radar was popularly known to be used for maritime and aerospace industries, until recently that advanced driver assisted systems (ADAS) was added to the variety radar application.

According to [23], next generation sensors are the developmental factor of providing qualitative data for building more applications and capabilities which serves as the key enabler of IoT. Features like low cost, low power consumption, high reliability and adaptability may be a motivating factor for multiple devices integration easily into the IoT platform. Proximity detection, speed estimation and detection and ranging (DAR) are the three categories of remote sensing [23] with DAR been the most complex. In comparison between passive and active sensors, [23] further described radar as rugged, matured and widely deployed technology across the globe. Although radar suffers bad weather condition yet, can penetrate through buildings. Unlike its non-suitability to detect objects with non-reflective profile, recent radars can detect objects with stealth technology.

IoT as a sensor based networks, can implement echo-acoustic based radars that are able to provide information about object's distance and azimuth, shape, material, size and motion [24]. Until now, implant sensors to human activities are at its infancy [25] hence, human gaits system, automatic object detections and many more are the common application of today's radar system. While RFID locate and track in real-time sensor-embedded objects [6], radar has similar capability of detecting and tracking a non-sensor-embedded object at distance. As IoT is pervasive over variety of objects apart from computers (i.e. internet of computers), for security reasons many posing threats with stealth technology do exist upon which may be countered by the use of radar system devices.

Irrespective of any software agent system, radar based IoT security for real time connected device was introduced by [3]. For future IoT related capabilities, Portnox company introduces into its product an IoT radar capable of addressing the growing concern over IoT security issues. Although infrared has been used for motion detection and proximity yet a typical infrared sensors can only detect motion over a small distance and unable to determine the object speed, infrared radar became the advance capabilities [22]. It was then further suggested that the use of unlicensed 246Hz ISM band to avoid interference with surrounding frequencies like WiFi, GSM, LTE or any other equipment within the range. Another possibility of incorporating radar technology into IoT in an attempt to curtail the suffers by different IoT protocols and looking at the huge generated data that cannot be handled by the already congested licensed/unlicensed spectrum, [10] proposed a zone-based shared access frame work with rotating radar.

IV. **PROSPECTS AND CHALLENGES**

In this section, we discussed some benefits of integrating radar into IoT as a sensor and the deployment IoT are cited with some emerging challenges. A recent intending drone weaponry deadlier than the nuclear weapons that only requires a target's biodata to execute its command is alarming. In the verge of developing the autonomous weapon that can kill without human help called slaughter-bots or smart weapons in an attempt to get rid of bad guys is horrifying [26]. The smart weapon is deadlier than an atomic weapon, as it only needs a target's profile like age, sex, fitness, uniform and ethnicity to get a mission done. Within it, are wide field cameras, tactical sensors, face recognition and shaped explosive [27] (figure 3). The initiation may be for good yet, some users may take advantage and act negatively. Hence, for IoT to provide a secured environment, radar-based systems can be adopted for surveillance purpose to this and other similar objects before causing the menace. Although there may be challenges while integrating radar into IoT such as multiple sensors required to support the REM and complex algorithm, there are other benefits that can be derive by this attempt [10].

Figure 3. Drone weaponry: [26]

IoT apart from environmental monitoring [1], it also find application in industries [8], healthcare aided services, inventory and production management, food supply chain among others. To an urban perspectives, IoT finds application in public service optimization problems that involves surveillance, lighting cultural heritage preservation, parking services, transportation, collection of garbage, health and school services [28]. It also applies to disaster prediction and water scarcity monitoring [1]. Unlike a passive infrared (PIR), the radar based system can detect objects in multiple of meters as compared to ten meters range of PIR [22] in addition to speed estimation, non-moving object detection and it also is not affected by environmental changes or ambient temperature.

Companies like Mint Controls are already into customized cost effective infrared radar based systems IoT solutions for broader applications in industrial, commercial and aerospace [22]. The IoT management involving IT and network administrators iterated some important benefits resulting from IoT radar that includes:
a) Instant visibility in a way that all connected gadgets or devices such as smart phones, printers etc. especially for objects with stealth technology can be instantly seen as soon as they are connected.
b) It provides easy management for all connected objects because by seeing the connected objects, managing such device become easier and simplified. A single management dash board may be implemented to enable users distill network security threats.
c) It gives the network managers an absolute control by been aware of potential security risk in order to alleviate the immediate risk involved.
d) With immediate knowledge of all connected devices, an automated decision making policy is improved thereby avoiding wrong decision making that may risk or compromise the network or the entire business [3].
In addition to personal security and location privacy, IoT suffers other challenges like identity management, standardization, objects safety, interoperability and power demand management [1].

V. CONCLUSION

This paper so far presented some proposed IoT architectures based on researchers' perspectives. An introduction of radar systems, how it works and some common applications was also presented. The paper proposed the feasibility of integrating radar into IoT, highlighting the key benefits and challenges thus, providing a step forward for further study. Based on the findings, it can be seen that radar can be incorporated into IoT system not only as a sensor device (i.e input layer) but rather as a measure for securing the entire system. This study therefore may open up a basis for counter measures to minimizing or curtailing threats posed by surrounding objects that are either part of the IoT or otherwise.

REFERENCES

[1] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: The internet of things architecture, possible applications and key challenges," *Proc. - 10th Int. Conf. Front. Inf. Technol. FIT 2012*, pp. 257–260, 2012, doi: 10.1109/FIT.2012.53.

[2] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Ad Hoc Networks Internet of Things : Vision , Applications and Research Challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012, doi: 10.1016/j.adhoc.2012.02.016.

[3] O. Amitai, "IoT Radar for Real-Time Connected Device Security and Management," *Business Wire, A Berkshire Hathaway Company*, 2017. https://www.businesswire.com/news/home/20170503005126/en (accessed Mar. 22, 2018).

[4] X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin, "Smart Community: An Internet of Things Application," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 68–75, 2011, doi: 10.1109/MCOM.2011.6069711.

[5] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," *Comput. Networks*, vol. 54, no. 2, pp. 2787–2805, 2010, doi: 10.1007/s10796-014-9492-7.

[6] B. Khoo, "RFID - From Tracking to the Internet of Things: A Review of Developments," *IEEE/ACM Int. Conf. Green Comput. Commun. GreenCom Proc.*, pp. 533–538, 2010, doi: 10.1109/GreenCom-CPSCom.2010.22.

[7] Harvard Business Review, "Internet of Things: Science Fiction or Business Fact?," *Harv. Bus. Rev.*, vol. Analytics, p. 8, 2014,

[Online]. Available: https://www.google.at/url?sa.
[8] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Trans. Ind. Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014, doi: 10.1109/TII.2014.2300753.
[9] F. Wortmann and K. Flüchter, "Internet of Things: Technology and Value Added," *Bus. Inf. Syst. Eng.*, vol. 57, no. 3, pp. 221–224, 2015, doi: 10.1007/s12599-015-0383-3.
[10] Z. Khan, J. J. Lehtomaki, S. I. Iellamo, R. Vuohtoniemi, E. Hossain, and Z. Han, "IoT Connectivity in Radar Bands: A Shared Access Model Based on Spectrum Measurements," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 88–96, 2017, doi: 10.1109/MCOM.2017.1600444CM.
[11] M. A. Richards, J. A. Scheer, and W. A. Hom, *Principle of Modern Radar: Basic Principles*, vol. I. SciTech Publishing Inc., Georgia USA, 2010.
[12] L. N. Ridenour, "Radar System Engineering," in *Dover Publications.*, vol. 1, 1965, pp. 1–748.
[13] N. J. Willis, *Bistatic Radar*. USA: SciTech Publishing Inc., Georgia USA, 2005.
[14] M. Golabi, A. Sheikhi, and M. Biguesh, "A New Approach for Sea Target Detection in Satellite Based Passive Radar," in *21st Iranian Conference on Electrical Engineering (ICEE), IEEE Conference Publication*, 2013, pp. 1–5, doi: 10.1109/IranianCEE.2013.6599599.
[15] A. Salah, R. Raja Abdullah, A. Ismail, F. Hashim, and N. Abdul Aziz, "Experimental study of LTE signals as illuminators of opportunity for passive bistatic radar applications," *IET Journals Mag.*, vol. 50, no. 7, pp. 545–547, 2014, doi: 10.1049/el.2014.0237.
[16] S. A. Hassan and H. Mazhar, "Analysis of target multipaths in WiFi-based passive radars," *IET Radar, Sonar Navig.*, vol. 10, no. 1, pp. 140–145, 2016, doi: 10.1049/iet-rsn.2015.0075.
[17] T. Peto and R. Seller, "Quad Channel DVB-T Based Passive Radar," in *17th International Radar Symposium (IRS), 2016*, 2016, no. 1, pp. 1–4, doi: 10.1109/IRS.2016.7497383.
[18] M. Weiß, "Compressive Sensing for Passive Surveillance Radar using DAB Signals," in *International Radar Conference*, 2014, pp. 1–6.
[19] N. V. K. Rao, "A Cross-Correlation Approach to Determine Target Range in Passive Radar Using FM Broadcast Signals," in *IEEE WISPNET Conference*, 2016, pp. 524–529.
[20] N. H. Abdul Aziz and R. S. A. Raja Abdullah, "RCS classification on ground moving target using LTE passive bistatic radar," *J. Sci. Res. Dev.*, vol. 3, no. 2, pp. 57–61, 2016.
[21] R. S. A. Raja Abdullah, N. Abdul Aziz, N. Abdul Rashid, A. Ahmad Salah, and F. Hashim, "Analysis on target detection and classification in LTE based passive forward scattering radar," *Sensors*, vol. 16, no. 10, p. 1607, 2016, doi: 10.3390/s16101607.
[22] M. Controls, "IoT and Infrared Radar Sensors.pdf," *Mint Controls*, 2018. http://mintcontrols.com/iot-infrared-radar/ (accessed Mar. 22, 2018).
[23] S. Duquet, "Enabling Detection And Ranging For The Internet Of Things And Beyond," *German magazine elektronik Praxis*, German, Apr. 2015.
[24] X. Zhang *et al.*, "Human echolocation : waveform analysis of tongue clicks," *Electron. Lett.*, vol. 53, no. 9, pp. 9–10, 2017, doi: 10.1002/wcs.1408.
[25] A. Nallanathan and C. Science, "Molecular Communications : Unleashing the Internet of Nano-Things," vol. 2018, 2018.
[26] D. Nield, "Campaign to stop Killer Robots," *https://www.sciencealert.com/chilling-drone-video-shows-a-disturbing-vision-of-an-ai-controlled-future*, 2017. https://www.sciencealert.com/chilling-drone-video-shows-a-disturbing-vision-of-an-ai-controlled-future (accessed Mar. 02, 2018).
[27] B. Campaign, "Ban Lethal Autonomous Weapons Campaign Increase," *autonomousweapons.org/slaughtaerbots/*, 2018. autonomousweapons.org/slaughtaerbots/ (accessed Mar. 02, 2018).
[28] a Zanella, N. Bui, a Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, 2014, doi: 10.1109/JIOT.2014.2306328.