As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 8(03): 01-08, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0803001
Available online at: http://www.ijmtst.com/vol8issue03.html

Review of Internet of Things (IoT) for Future Generation Wireless Communications

Dr.Nookala Venu[1] | Dr.A.ArunKumar[2] | Karthik Kumar Vaigandla[3*]

[1]Associate Professor, Electronics & Communication Engineering, Balaji Institute of Technology & Science, Narsampet, Warangal, Telangana, India
[2]Associate Professor, Computer Science & Engineering, Balaji Institute of Technology & Science, Narsampet, Warangal, Telangana, India
[3]Assistant Professor, Electronics & Communication Engineering, Balaji Institute of Technology & Science, Narsampet, Warangal, Telangana, India
[1]venunookala@gmail.com, [2]arun.arigala@gmail.com,[3]vkvaigandla@gmail.com

To Cite this Article
Dr.Nookala Venu, Dr.A.ArunKumar and Karthik Kumar Vaigandla. Review of Internet of Things (IoT) for Future Generation Wireless Communications. International Journal for Modern Trends in Science and Technology 2022, 8(03), pp. 01-08. https://doi.org/10.46501/IJMTST0803001

Article Info
Received: 19 January 2022; Accepted: 20 February 2022; Published: 27 February 2022.

ABSTRACT

The Internet of Things(IoT) emerged as a result of technological advancements that enabled efficient wireless tiny devices. This study explores the role of IoT in various fields, identifies technological challenges and examines opportunities offered by the IoT. As the Internet of Things and 5G transform devices into intelligent machines, the future of human life is dependent on them. A complete overview of IoT and 5G technologies is provided in this paper, as well as how these technologies have the potential to change the human perspective about the digital world. Communication requirements for industrial IoT (IIoT) include a high degree of reliability, low latency, flexibility, and security. A 5G mobile technology provides these services instinctively, making it a great candidate to support IIoT scenarios. This paper examines current challenges in IoT research and potential solutions related to 5G-enabled industrial IoT.

KEYWORDS: 5G, 6G, IoT, Communications, Security, Wireless Sensor Network, path loss.

1. INTRODUCTION

Mobile communications are usually characterized by the five-generation (5G) architecture. Various factors have motivated mobile device development, some of them related to communications, such as offering high-speed mobile access to highly populated areas, and others less related to communication, such as battery life of over 10 years, among others. There are several drivers of traffic growth, including the expanding demand for enhanced mobile broadband (eMBB), ultra-reliable and low latency transport modes(URLLC), as well as the requirements associated with massive machine communications (MMTC), massive IoT (MIoT) [1]. Mobile communications will play an increasingly important role in the Industrial Internet of Things thanks to 5G, especially regarding ultra-reliable and low-latency communication requirements.

A multitude of applications built around various types of sensors have revolutionized ubiquitous computing with the IoT [26]. IoT-based products and services are seeing a lot of activity, and this trend is

forecast to continue across the next few years with projections of billions of devices with 6-7 devices per person on average [26]. During the past decade, most of the device and protocol issues were resolved. However, sensors and sensor based systems are now becoming increasingly integrated with cyber physical systems and device-to-device (D2D) communications [9]. IoT is taking center stage as a major component of the 5G network paradigm, which is projected to be a key element of the fifth generation of wireless systems (5G). Several industries will be radically changed by IoT technologies such as machine-to-machine (M2M) communication [11], accompanied by intelligent data analytics. We expect further innovation in IoT to occur due to the emergence of cloud computing and the emergence of the fog paradigm. We are inspired by these developments and intend to survey existing research, design new techniques, and identify new applications of the IoT. The design of IoT-based systems that can be seamlessly integrated with the 5G wireless communication system is a challenge for researchers, scientists, and engineers.

2. INTERNET OF THINGS (IoT)

A recent development in computing that involves device interconnectedness is the IoT [26]. Since the late 1990s, the Internet has become a part of almost every aspect of our lives. Our modern world is filled with objects capable of gathering, processing, and sending data to other objects, servers, and applications [2]. As a leading provider of engineering and medical software, we use a broad range of use cases and sectors [3]. A global networking platform has already become a reality with the creation of smart objects[26]. Wireless sensor networks and nodes are used to form information systems using IoT technology [4] and people and things are connected practically. We will be able to communicate freely and effectively between social media and the internet [2]. This will enable the development of new applications and services [2]. The IoT paradigm is driven by multidimensional technologies such as Bluetooth [2], Wi-Fi, ZigBee [2], Long Term Evolution [25] and Long Term Evolution Advanced. These technologies form the basis of IoT, and the creation of a successful IoT system will be challenging. This system requires identifiers for sensors, as well as interoperability and advanced functions for IoT [6]. Those that are environmentally sustainable should have energy efficient IoT systems as well as efficient data management systems [7].

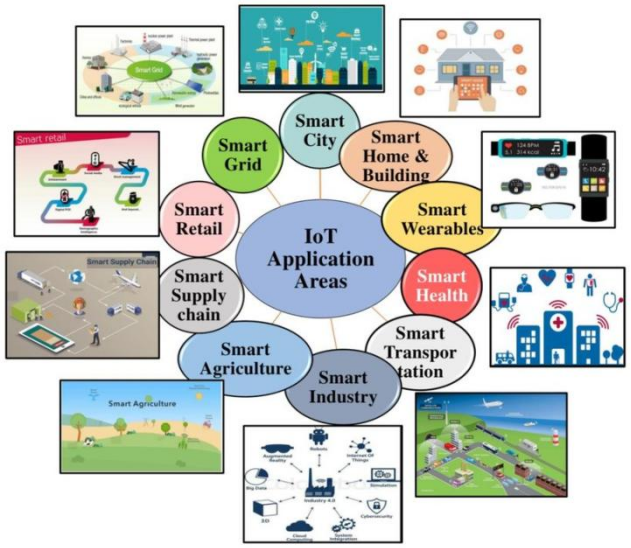

Figure 1. IoT Application areas

Compared to the 3GPP recommendation, the high level expectations of market actors are not as detailed. Even though there were numerous sources of high level requirements, one of the earliest standards on the topic was ITU-R M.2083-0 [8]. This standard defined the three key communication scenarios: eMBB, URLLC, and MMTC for the first time when explaining the importance of key capabilities in different scenarios. Even though there are no high throughput expectations with the mass IoT or MMTC.

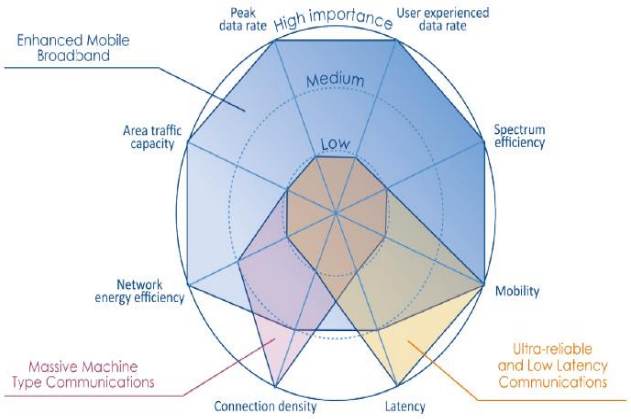

Figure 2. Major requirements for mass IoT or MMTC traffic

3. MOBILE COMMUNICATIONS: THE NEXT GENERATION

A. 5G : Mobile phone bandwidth has greatly increased with 5G technology [9]. The advances in technology are

unprecedented. All of the advanced features of 5G make it a powerful technology that will be widely used and popular [9]. The spacecraft has more power than 5G technology and at least 1000 lunar modules. It is possible to access broadband internet simultaneously with a laptop and a 5G phone using 5G technology. Cameras, MP3 recorders, video players, extensive storage, phone dialing speed, audio players, etc. [10] are examples of 5G technologies.

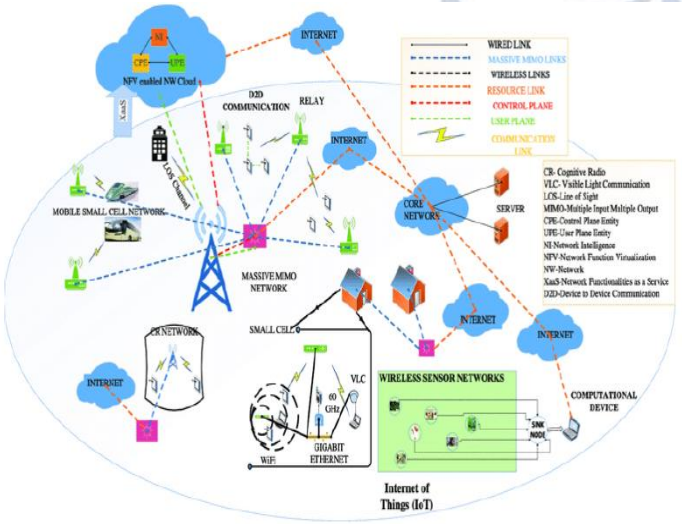

Figure 3. 5G Architecture

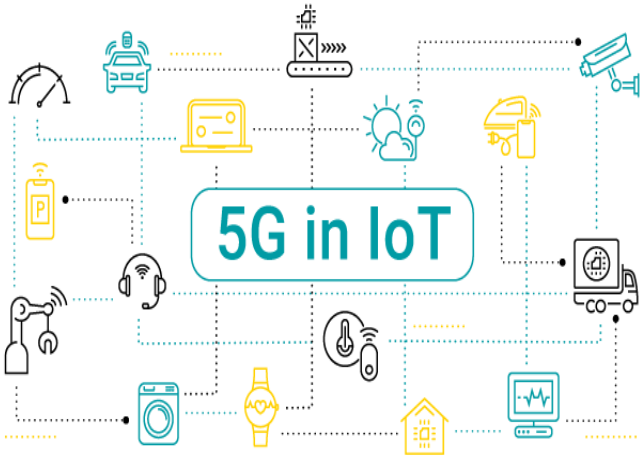

Figure 4. 5G in IoT

Millimeter-wave technology is used in 5G technology for the release of frequency spectrum [11]. A larger channel bandwidth is available as well as more spectrum is available. The 5G device will be universal and will work with existing communication basics and will allow all 5G applications [12]. Integrated radio modulation schemes are used in the technology. Basically, the terminals must access multiple wireless technologies at the same time [13] as it combines different streams of technology.

B. 6G: The sixth-generation (6G) of wireless mobile communication networks will use satellites to provide global coverage [14]. Systems have been developed by four countries to achieve global coverage. GPS was developed by the US, COMPASS by China, Galileo by the EU, and GLONASS by Russia. Each of these developed their own independent systems, making it difficult to roam in space [12]. There will be a unified infrastructure of seventh generation (7G) wireless communication networks. The 6G Internet combines broadband and radio to create a wireless network [14]. Line-of-sight (LOS) transmissions are used to deliver this service. They no longer need the copper cable because speeds are decided by distance from the exchange, and they don't need to rely on the copper cable for data transmission. Additionally, 6G networks are more security and more cost-effective. By integrating satellites and 5G wireless mobile systems, global coverage can be achieved [14].

4. WIRELESS COMMUNICATION IN IoT

In IoT infrastructure, wireless communication systems are crucial because they act as a link for the delivery of data and control messages in dual-direction communication systems. The system can be used for a variety of IoT applications, including those in mission-critical industries like power grids and oil fields, as well as common cases in our modern lives such as smart cities. IBM Research China is leading a worldwide project called Wireless Communication for IoT. Wireless communication in IoT applications presents a number of challenges and issues:

*1)*It is crucial to connect, manage and maintain large numbers of sensors with different types and distributed locations.

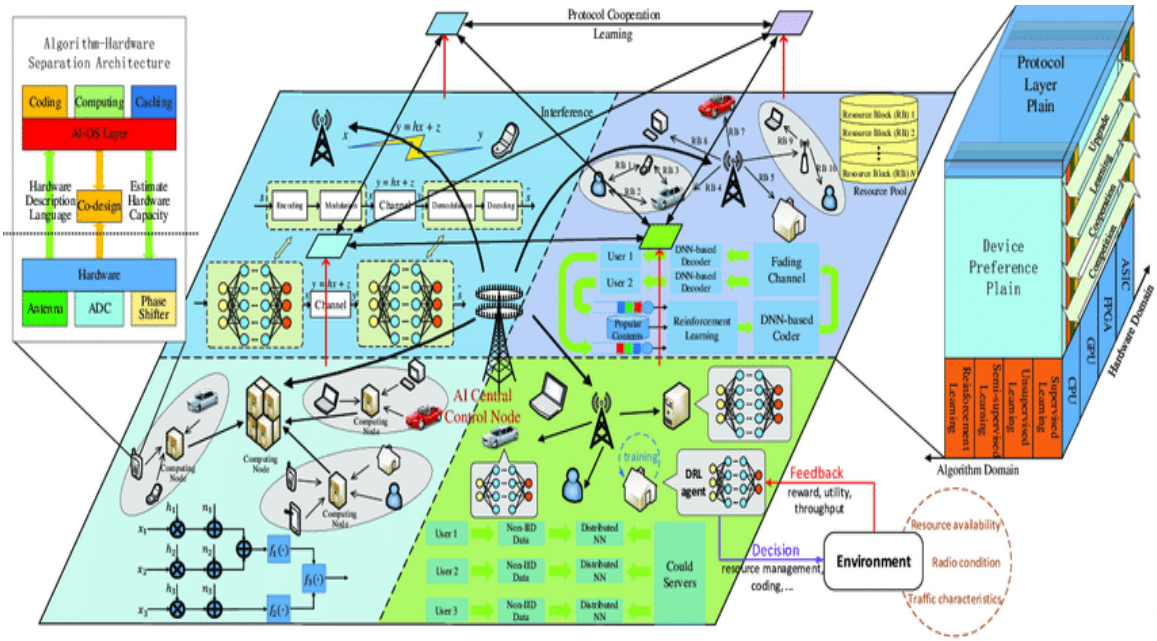

Figure 5. 6G Architecture

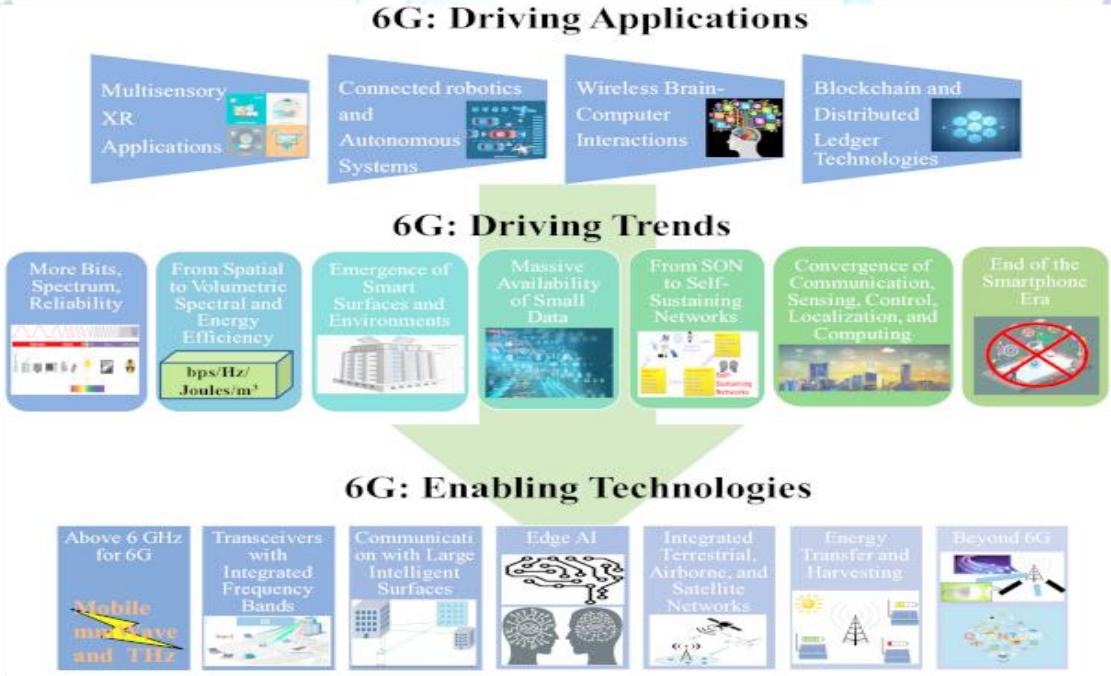

Figure 6. 6G: Applications, Trends, and Technologies

*3)*New IoT wireless networks will have a limited amount of spectrum resources available. *4)*A simple architecture and low power consumption are needed for harsh outdoor areas. *5)*It will be more difficult to install and maintain equipment in harsh outdoor environments. In order to solve those problems, we designed an end-to-end SDR wireless platform for IoT. This platform allowed us to support the optimized communication from the sensor network to the wide area radio network. The base band processing was completed using a general-purpose IT platform with multi-core processors based on software-defined radio (SDR) technology. The whole system is also optimized using wireless optimization technologies, including spectrum allocation, interference mitigation, and energy-saving design.

There are several antennas attached with geometry to the transceivers and receivers for wireless

communication. Signals modulated on the carrier frequency are propagated by the transmitter. It propagates at a speed about equal to the speed of light. There can be obstacles between these two antennas, which can reflect, refract or diffract the signal. Various deployment problems can be rapidly addressed by modeling physical phenomena.

A.Path Loss and Loss of Communication : Communications over wireless networks can be corrupted by various interferences. As a signal travels through space, it suffers path loss, which reduces its power. An energy transmitter produces is determined by the amount of energy that is being provided by an energy source associated with the transmitter. In order for a signal to be successfully received, the receiver sensitivity must be low. At the receiving end, the signal power must be higher than the sensitivity of the receiving device for a successful communication. Physical environment is the primary cause of path loss. A number of factors contribute to path loss including antenna gain and height, distance between the transmitter and receiver, communication frequency range, obstacles, user mobility, and environmental conditions [15].

B.Propagation Space and Environment : IoT devices and users are mobile, hence a variety of environmental conditions must be taken into account in order to create an accurate model of wireless communication. Because propagation space affects signal characteristics, communication models must be accurate in describing the environment. Prorogation characteristics and network parameters are significantly affected by three factors: location, population, and flora. Generally speaking, urban and rural environments can be classified according to their populations. Mobile users are more common in urban areas. When the device is placed indoors or outdoors, under a tree or in an open space, different weather conditions and locations significantly affect parameters such as attenuation.

C.Q-Theory for Wireless Communication in IoT : In the literature, Q-theory is quite popular from the perspective of performance. IoT does not sufficiently consider the energy efficiency or the mean energy consumption of the wireless communications. This is because IoT base stations are not typically equipped with unlimited power supply [16], contrary to conventional base stations. Increasing the efficiency of data traffic and handheld devices can help operators reduce CO2 emissions and operating costs as energy makes up an important portion of their costs [17-18]. The most popular approach in this field is queuing theory, which measures energy consumption and identifies ways to conserve power.

5. SECURITY OF IoT IN 5G

A. IoT Security Requirements

IoT security concerns have always been one of the biggest challenges to solve. Considering that the number of IoT devices, not only in the civil/residential sector, but also in industrial sectors, is increasing rapidly, it is becoming critically important to handle privacy and security issues. Since IoT is an implementation and integration of different technologies and infrastructures, the IoT system that relies on them inherits the threats and security challenges from those technologies. IoT security risks are therefore present at all layers of its architecture [19]. Additionally, IoT systems present unique challenges in terms of security that don't exist in conventional networks. IoT sensors/physical devices have limited computational and storage capabilities and operate in the sensor/physical layer of an IoT system. Thus, standard security solutions such as public key encryption and spread-spectrum methods cannot be made available to all endpoints [20]. Moreover, these systems contain separate subsystems that have varying defense capabilities. By determining the vulnerability of the most vulnerable node, the overall security level is determined.

B. Security Issues of a Layered IoT Architecture

In order to better taxonomize the IoT, it is necessary to create new categories of application domains, architectural domains, communication channels, and data domains [21]. 5G-IoT architecture taxonomy [22] should provide the essential information for designing and analyzing protected systems by providing a security analysis, services, and attacks. The taxonomy consists of five layers: each layer interacts with the other layer to make 5G-IoT a secure and private architecture; each layer covers some parts of 5G-IoT.

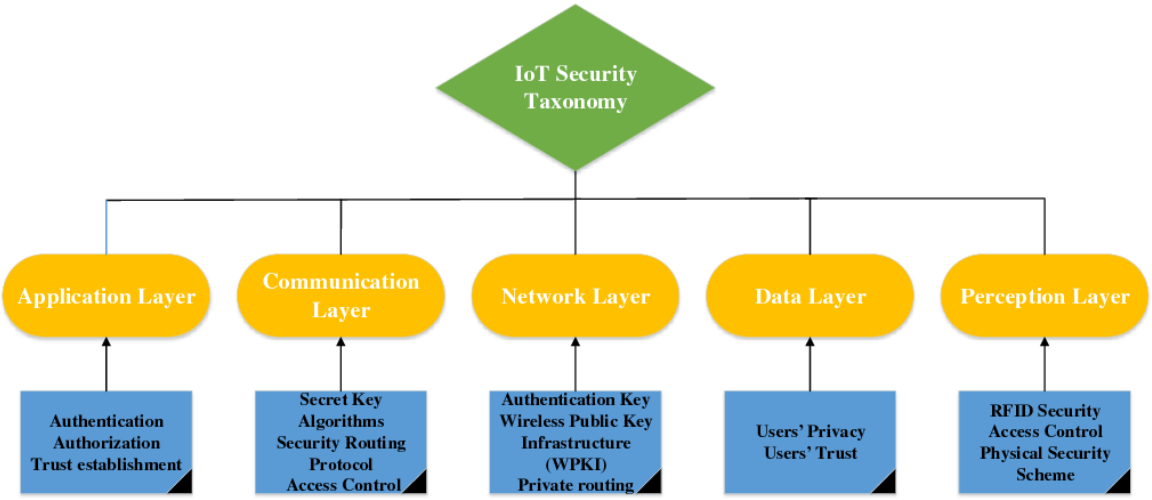

Figure 7. 5G-IoT security taxonomy

Application Layer : The IoT is affecting a wide range of applications. Because of this, IoT systems would need an application layer that is heterogeneous and unpredictable. Different applications have very different requirements for protection. Applications are categorized according to the degrees to which they are open to the network, how heterogeneous they are, and how closely they are associated with specific users [24]. Many security methods exist (such as authentication, authorization, exhaustion of resources, and trust establishing).

Network Layer : 5G-IoT architectures use the Internet and 5G networks for the network layer. Data security is threatened on the Internet, which damages IoT services. The common routing of networks is often simple, and these networks' security and safety are not considered. Due to the aforementioned device arrangement, the autonomy, the unreliability of energy, and the lack of dynamic topology, the current IoT systems are based on a common architecture. As a result, devices can easily be threatened by the attacker. It is required for each network architecture to establish a specific method of authentication, key adjustment, Wireless Public Key Infrastructure (WPKI), private routing, interference detection, etc. The network layer also needs to improve authentication at the domain and network levels. 5G-IoT architectures are often characterized as using network virtualization technology (NFV). Therefore, there is a significant reduction in the complexity of network management and the probability of a mistake [24].

Data Layer : As applications are deployed at this layer in shared-resource conditions, confidentiality and trust of users are important considerations. The protection of personal information of users may require the provision of secret encryption.

Communication Layer : Wireless Sensor Networks, as an integral part of the IoT, enables broadcasting of information in the free space. Attackers can easily intercept and analyze the information. So we should employ several means of attack so that we can utilize the most appropriate protection techniques.

Perception Layer : IoT perception layer is primarily composed of RFID and WSN [23].

6. CONCLUSION

Researchers are focusing on the IoT as an important research topic, and these systems are changing people's daily lives. Communication paradigm is provided by being able to integrate numerous sensors, actuators, and data into meaningful information. Moreover, IoT deployments have increased requirements for security, which are driving the need for wide-spread deployment. A review of 5G IoT security was presented in this paper. A number of the fundamental concepts of IoT are addressed here, including path loss, terrain, environment, routing, heterogeneous networks, and radio frequency identity. By allowing smart objects to be directly connected to the Internet, they can act as sensors and share continuous data about their surroundings. The IoT can bring new perspectives to the field of automation. 5G will improve communication for IoT devices, making human life

better and more efficient. The paper will helpful for researchers interested in studying these technologies.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Pal Varga , Jozsef Peto, Attila Franko, David Balla, David Haja, Ferenc Janky, Gabor Soos ,Daniel Ficzere, Markosz Maliosz and Laszlo Toka, "5G Support for Industrial IoT Applications—Challenges, Solutions, and Research Gaps," Sensors 2020, 20, 828; doi:10.3390/s20030828

[2] Karthik Kumar Vaigandla , Radha Krishna Karne , Allanki Sanyasi Rao, "A Study on IoT Technologies, Standards and Protocols," IBM RD's Journal of Management & Research Volume 10, Issue 2, September 2021, pp.7-14, DOI: 10.17697/ibmrd/2021/v10i2/166798

[3] Pallavi Gupta and Usha Tiwari(2020) " Review on Internet of Things Network Protocols", Journal Of Critical Reviews, VOL 7, ISSUE 3, pp.790-794.

[4] Anna Triantafyllou ,Panagiotis Sarigiannidis and Thomas D. Lagkas (2018) "Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges, and Trends", Wireless Communications and Mobile Computing, https://doi.org/10.1155/2018/5349894

[5] D. Miorandi, S. Sicari, F. de Pellegrini, and I. Chlamtac(2012) "Internet of things: vision, applications and research challenges," AdHoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012.

[6] O. Mavropoulos, H. Mouratidis, A. Fish, and E. Panaousis(2017) "ASTo: a tool for security analysis of IoT systems," in Proceedings of the 15th IEEE/ACIS International Conference on Software Engineering Research, Management and Applications, pp.395–400.

[7] R. Khan, S. U. Khan, and R. Zaheer(2012) "Future internet: the internetof things architecture, possible applications and key challenges,"in Proceedings of the 10th International Conference on Frontiers of Information Technology (FIT' 12), pp. 257–260.

[8] ITU-R. IMT Vision—Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond. Available online: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDFE.pdf (accessed on 23 January 2020).

[9] Karthik Kumar Vaigandla and Dr.N.Venu, "A Survey on Future Generation Wireless Communications - 5G : Multiple Access Techniques, Physical Layer Security, Beamforming Approach", Journal of Information and Computational Science, Volume 11 Issue 9, 2021, pp.449-474.

[10] Shrikant R Tripathi and Sushil Khaparde, " Analysis and Survey on Past, Present and Future Generation in Mobile communication", National Conference on Recent Trends in Computer Science and Information Technology (NCRTCSIT-2016) , IOSR Journal of Computer Engineering (IOSR-JCE), pp.30-36.

[11] Karthik Kumar Vaigandla, Bolla Sandhya Rani, Kallepelli Srikanth, Thippani Mounika, RadhaKrishna Karne, " Millimeter Wave Communications: Propagation Characteristics, Beamforming, Architecture, Standardization, Challenges and Applications," Design Engineering, 2021 Issue: 9 ,Pages: 10144-10169

[12] Karthik Kumar Vaigandla, Nilofar Azmi, Podila Ramya, Radhakrishna Karne, "A Survey On Wireless Communications : 6g And 7g," International Journal Of Science, Technology & Management, Vol. 2 No. 6 (2021): November 2021, pp. 2018-2025. https://doi.org/10.46729/ijstm.v2i6.379

[13] Mishra, Ajay K. "Fundamentals of Cellular Network Planning and Optimization, 2G/2.5G/3G…Evolution of 4G", John Wiley and Sons, 2004

[14] Karthik Kumar Vaigandla, SandyaRani Bolla , RadhaKrishna Karne, "A Survey on Future Generation Wireless Communications-6G: Requirements, Technologies, Challenges and Applications", International Journal of Advanced Trends in Computer Science and Engineering, Volume 10, No.5, September - October 2021, pp.3067-3076, https://doi.org/10.30534/ijatcse/2021/211052021

[15] Umit Deniz Ulusar, Fadi Al-Turjman, Gurkan Celik, "An Overview of Internet of Things and Wireless Communications," 2017 IEEE, pp.506-508

[16] S. Misra, I. Woungang, and S. C. Misra, "Guide to Wireless Ad Hoc Networks", Springer, 2009.

[17] Y. S. Soh, T. Q. S. Quek, M. Kountouris, and H. Shin, "Energy Efficient Heterogeneous Cellular Networks", IEEE Journal on selected areas in communications, Vol. 31, No. 5, May 2013, pp. 840-850

[18] T. Zhang, J. Zhao, L. An, and D. Liu, "Energy Efficiency of Base Station Deployment in Ultra Dense HetNets: A Stochastic Geometry Analysis", IEEE Wireless Communication Letters, Vol. 5, No. 2, April 2016, pp. 184-187

[19] Andrea, I.; Chrysostomou, C.; Hadjichristofi, G. Internet of Things: Security vulnerabilities and challenges. In Proceedings of the IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, 6–9 July 2015.

[20] Fadele, A.; Othman, M.; Hashem, I.; Alotaibi, F. Internet of things Security: A Survey. J. Netw. Comput. Appl. 2017, 88, 10–28. [CrossRef]

[21] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," J. Netw. Comput. Appl., vol. 88, pp. 10–28, 2017.

[22] H. Rahimi, A. Zibaeenejad, and A. A. Safavi, "A Novel IoT Architecture based on 5G-IoT and Next Generation Technologies," to be presented at IEEE IEMCON conference, Vancouver, BC, Canada, Nov. 2018, available at https://arxiv.org/abs/1807.03065.

[23] K. Zhao and L. Ge, "A survey on the internet of things security," in Computational Intelligence and Security (CIS), 2013 9th International Conference on, 2013, pp. 663–667.

[24] Hamed Rahimi, Ali Zibaeenejad, Parsa Rajabzadeh, Ali Akbar Safavi, " On the Security of the 5G-IoT Architecture," SCIOT, September 26–27, 2018, ttps://doi.org/10.1145/3269961.3269968

[25] Karthik Kumar Vaigandla , Dr.N.Venu, " Survey on Massive MIMO: Technology, Challenges, Opportunities and

Benefits,"YMER, VOLUME 20 : ISSUE 11 (Nov) - 2021, Page No:271-282.

[26] Dr.Nookala Venu, Dr.A.ArunKumar, Karthik Kumar Vaigandla, "Investigation on Internet of Things(IoT) : Technologies, Challenges and Applications in Healthcare," International Journal of Research, Volume XI, Issue II, February/2022, Page No: 143-153.