Demystifying the Internet of Things: A Deep Dive into Protocols, Architectures, Technologies, and Beyond

Dr. J. Gupta, Assistant Professor, Department of ECE, BVCOE, New Delhi

Ms. Shikha, Assistant Professor, Department of ECE, BVCOE, New Delhi

Dr. P. Gupta, Assistant Professor, Department of ECE, BVCOE, New Delhi

Abstract:

The Internet of Things (IoT) is a booming network of interconnected devices, exchanging data and information through various protocols. Recent advancements in wired, wireless, and hybrid technologies connect a vast array of smart devices. To overcome limitations in storage, processing power, and energy in these devices, lightweight IoT protocols emerge as crucial tools. Choosing the optimal protocol is key for system architects, requiring evaluation of next-generation networks with improved connectivity. This paper dives into major wireless and wired IoT technologies with their applications, proposing a new classification for traditional protocols. It analyzes their technical details, limitations, and usage, IoT devices and simulation tools. Finally, it explores current challenges and future directions for the next generation of IoT, aiming to be a comprehensive guide for academics and professionals in this exciting field.

Keywords: IOT, different communication protocols, simulation tools for IOT.

1. Introduction

The Internet of Things (IoT) is has an important role in driving economic growth. It's transforming buildings, workplaces, and even entire cities into self-regulating systems that can collect and exchange data without human intervention [1]. This technology is rapidly becoming integrated into every aspect of our lives, thanks to the development of smart systems powered by wireless technologies like Wi-Fi, Zigbee, and Bluetooth. However, the vast amount of data generated by these interconnected devices necessitates efficient processing, storage, and visualization solutions [2-3]. As the IoT matures, it's moving beyond its initial stages and evolving into a comprehensive network that promises to connect everything at an unprecedented scale. [4-6] This "intelligent environment" presents exciting opportunities, but also challenges due to diverse application requirements and limitations like power consumption and accessibility. The rapid growth of the IoT has spurred the development of numerous protocols, each aiming to address specific needs or dominate the market. This diversity can make it difficult to choose the right protocol for a particular application, especially considering security concerns and the pressure for faster product launches. Additionally, these devices operate in various environments, including homes, hospitals, and transportation systems, highlighting the need for robust and secure communication protocols [7]. With power efficiency being a major concern, researchers are actively exploring ways to optimize communication protocols for IoT devices. Overall, the IoT presents a transformative force with vast potential for economic growth and improved quality of life. However, addressing challenges like protocol selection, security, and power consumption is crucial for its continued success.

Many researchers are actively studying and analysing the IoT from various angles, including its architecture, techniques, and applications. A recent review highlights the diverse areas of interest within the IoT field, categorized into eight key areas: applications, security, data, communication, networking, protocols, and development [8].

1.1 Related Work

This section dives into existing research related to the current work, focusing on relevant surveys and their coverage:

Architectures and Techniques: [9] provides a foundational overview of the IoT model, outlining its core concepts and key advancements. It also explores security considerations and potential applications across various domains.

Applications: Studies like [10] delve into specific applications enabled by IoT technology, while [11] examines various platform designs and proposes a generic standard paradigm for the IoT.

Technologies: [12] offers a broader look at potential conceptual models, communication technologies, and challenges, introducing a new six-layer security design for the IoT infrastructure.

Communication Protocols: [7] provides a comprehensive analysis of application layer protocols, evaluating their suitability for different application categories and communication needs.

Ecosystem and Protocols: [13] reviews the fundamentals of the IoT ecosystem and communication protocols specifically designed for this technology.

Current Landscape: [14] offers an overview of existing IoT models, techniques, and key open-source platforms and applications.

By understanding these existing studies and their coverage, the current work can build upon established knowledge and address potential research gaps within the vast and ever-evolving field of the IOT. Several studies have explored the nuances of wireless technologies and their challenges in the context of IoT integration. Research in [15] examines Bluetooth Low Energy, Zigbee, LoRa, and Wi-Fi variants, highlighting their unique characteristics. Meanwhile, [16] tackles the challenge of selecting the optimal technology for specific applications by comparing standard IoT protocols across various parameters like power consumption, security, and data rate. Additionally, [17] analyzes the limitations of current security techniques, while [18] delves into the link, transport, networking, and session layers of IoT communication protocols, offering insights into security mechanisms for these devices. Focusing specifically on application layer protocols, [19] provides a comprehensive overview of recent developments and lightweight protocols, while [20] describes standardized protocols across various networking levels for resource-constrained devices.

However, it's important to note that both studies might require updates as protocols continue to evolve. By understanding these existing research efforts, we can gain valuable insights into the complexities of IoT protocols and identify potential areas for further exploration and improvement.

1.2 Paper Organization

The study is structured as follows: Section 2 explores the framework and functional components of IoT. Section 3 delves into the stack architecture of IoT. A summary of different application layer protocols is provided in Section 4, while Section 5 discusses the evolving landscape of IoT communication technologies. Section 6 presents a summary of IoT hardware platforms, focusing on their building blocks for connected systems. In Section 7, simulation tools utilized in IoT and Wireless Sensor Networks (WSNs) are discussed. Section 8 outlines the scope of future work in IoT. Finally, Section 9 presents the conclusions drawn from this work.

2 Exploring the IoT Framework

The IoT is a transformative technology rapidly ushering in a new era of interconnectedness. It allows everyday objects to communicate and share data, leading to remarkable discoveries, inventions, and richer interactions between people and their surroundings. These advancements promise to not only enhance our quality of life but also optimize resource utilization, making the most of our finite resources. This section delves into the various definitions of IoT and explores the foundational building blocks that make it all possible [21-22].

2.1 Elements of IoT Infrastructure

Imagine a world where everyday objects communicate and collaborate, sensing their surroundings and acting upon them autonomously. This is the promise of the IoT, and it all comes down to a clever interplay of several key components:

1. Sensing: Like tiny eyes and ears, smart devices use sensors to gather information about their environment. Temperature, pressure, movement, and even sound – no detail is too small! This data becomes the lifeblood of the IoT, feeding insights and fueling actions [23].

2. Actuation: But devices aren't just passive observers. Through actuators like motors, switches, and valves, they can respond to data or commands. Imagine lights adjusting automatically, thermostats responding to your presence, or even complex machinery operating independently – the possibilities are endless [23].

3. Identification: In a network of billions, knowing who's who is crucial. Unique identifiers like serial numbers or tags ensure each device stands out and can be addressed individually. This is like giving each device a name in the digital world [23].

4. Management & Control: The brain behind the brawn, management systems orchestrate communication, analyze data, and make decisions. Whether remotely controlled or programmed to act autonomously, these systems are the conductors of the IoT symphony [24].

5. Networking: Connecting across distances is key. From Bluetooth and Wi-Fi to cellular networks and low-power options like LoRa, various technologies enable devices to share information and collaborate. Just like roads and bridges connect cities, these networks connect the devices in the IoT universe.

6. Services: Beyond basic communication, services add value to the experience. Think data storage, security protocols, analytics tools, and application interfaces – all working together to deliver seamless interaction and functionality. It's like having a team of assistants working behind the scenes to ensure everything runs smoothly [25].

7. Security: With great connectivity comes great responsibility. Securing devices, data, and communication channels is paramount. Robust encryption, authentication, and access control measures act as security guards, protecting privacy and preventing cyberattacks [26].

8. Applications: This is where the magic happens! From smart homes and personal fitness trackers to industrial automation and connected cities, the applications of the IoT are as diverse as our imagination. These applications leverage the building blocks discussed above to solve real-world problems and improve our lives in countless ways.

By understanding these fundamental elements, you gain a deeper appreciation for the intricate yet ingenious workings of the IOT. Remember, these building blocks are constantly evolving, paving the way for even more exciting developments in the future.

3. The Framework of IoT Architecture

The IoT has emerged in environments brimming with diversity, where information flowed from a multitude of sources and was processed by various technologies. This inherent heterogeneity inspired developers to group similar approaches, functionalities, and services into distinct layers within proposed IoT models. This layered approach facilitated the independent development and improvement of each layer, simplifying the overall architecture. While the classic three-layer design provides a good baseline understanding of the IoT, it falls short for deeper research that delves into the intricate details and nuances of this ever-evolving technology.

3.1 The stack architecture of the IoT: A Layer-by-Layer Breakdown

The IoT world operates like a well-oiled machine, with each component playing a crucial role. This intricate system can be visualized as a five-layer stack, each layer responsible for specific tasks:

1. Physical Layer: Sensing the World: Imagine tiny eyes and ears on everyday objects - that's the physical layer's job! Using technologies like RFID chips, wireless sensor networks (WSNs), and GPS, it gathers data about the physical environment – temperature, pressure, movement, and more. Think of it as turning real-world information into digital signals ready for transmission [12].

2. Data Link Layer (Packing and Addressing Dat): This layer acts like a postman, packaging data into manageable packets, addressing them correctly, and ensuring they arrive at their

destination without errors. It also handles tasks like collision avoidance and synchronization. Different protocols in this layer offer diverse features like speed, range, and power consumption, catering to various application needs [27].

3. Network Layer (Finding the Right Route): Think of the network layer as a GPS for data packets. It directs them through the best available routes, utilizing equipment like switches and routers to navigate diverse networks like 3G, 4G, 5G, Wi-Fi, and Bluetooth [28].

4. Transport Layer (Reliable Delivery): This layer focuses on data security and reliability. It ensures error-free transmission by checking data integrity, maintaining delivery order, and managing congestion. Imagine it as a quality control checkpoint for data packets before they reach their final destination [29].

5. Application Layer (Where Magic Happens): This is where the real magic unfolds! The application layer provides the interface for developers to build diverse IoT applications. From smart homes and intelligent transportation systems to healthcare solutions and more, this layer unlocks the limitless potential of the IoT [29].

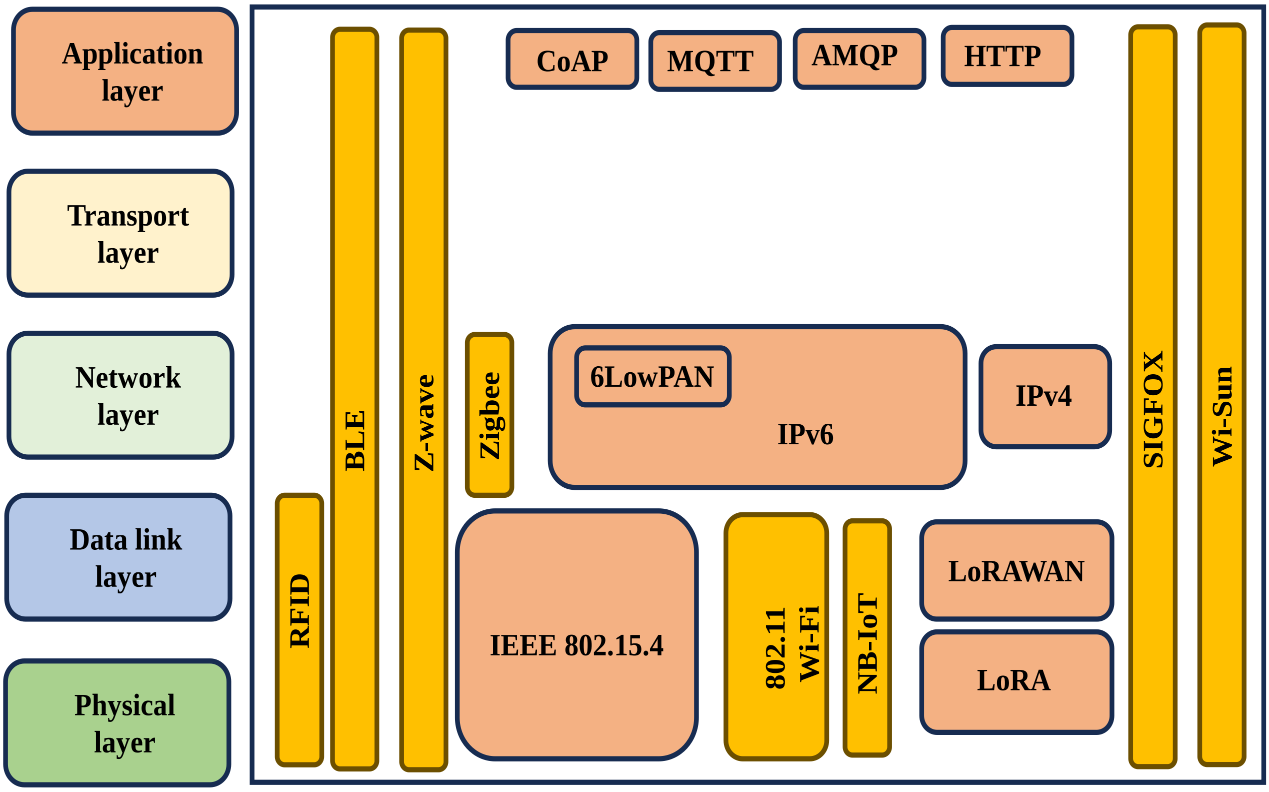

Figure 1. IoT Stack Architecture

By understanding these five layers and their unique functions, you gain a deeper appreciation for the remarkable architecture that powers the interconnected world of the IOT. Remember, this is an ever-evolving landscape, with each layer constantly adapting and improving to deliver even more possibilities in the future.

4 IoT Application Layer Protocols: Enabling Connectivity and Functionality

Navigating the world of IoT messaging protocols can feel like wading through a technical swamp. But fear not Let's shed some light on the top contenders:

1. MQTT: Imagine lightweight runners perfectly suited for marathons. They excel at sending and receiving data efficiently, even with limited resources, making them ideal for sensors and smart home devices [30]. They don't need to know who's sending or receiving, focusing purely on delivering messages through a central "broker [31]."
2. CoAP: Think sprinters built for quick bursts. They inherit some features from HTTP, making them familiar and efficient for small data transfers in smart sensors and wearables. They communicate securely with a central server that relays information further [32].
3. AMQP: Picture robust knights protecting data with advanced security features. They offer reliable message delivery and flexible routing, ideal for demanding applications like healthcare or industrial IoT. They utilize queues and exchanges to ensure messages reach the right recipients [33].
4. HTTP: Consider them friendly neighbors, familiar and widely used for basic data exchange. While simple, they're not the most efficient for resource-constrained devices, requiring multiple small packets that consume network resources [34].
5. XMPP: Think seasoned strategists enabling real-time communication and presence awareness. They excel in dynamic scenarios like smart grids or machine-to-machine communication, allowing devices to "befriend" each other and exchange data based on specific needs [35].

Remember, the ideal protocol depends on your specific needs. Consider your device capabilities, application requirements, complexity preferences, and desired interoperability. By understanding these factors and the strengths of each protocol, you can confidently choose your champion and unlock the full potential of your IoT network!

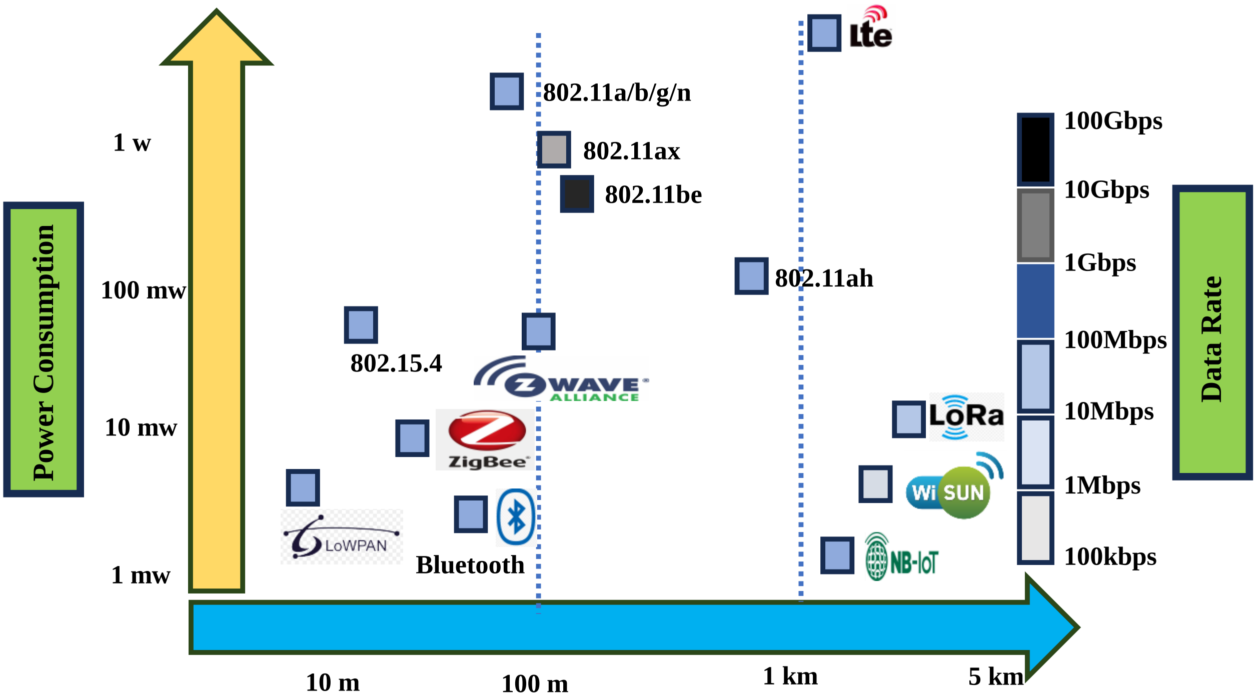

Figure 2 Power consumption, coverage distance, and data rate for the different protocols

5 IoT Communication Technologies: Evolving Landscape

IoT communication technology encompasses the methods and protocols enabling devices to exchange data in IoT applications. It facilitates data collection, analysis, and sharing among connected devices and centralized systems. Various communication technologies are employed:

5.1 Wireless Technologies:

1. Wi-Fi: Offers high-speed data transfer over short to medium distances, suited for devices with continuous power [36].
2. Bluetooth: Facilitates short-range communication between devices like smartphones and smart home gadgets [37-38].
3. Zigbee: A low-power, low-data-rate protocol ideal for applications needing long battery life and mesh networking [39].
4. LoRa: Designed for long-range communication with low power usage, useful for expansive IoT deployments [39].
5. Narrowband IoT (NB-IoT): A cellular technology tailored for low-power IoT devices with intermittent data needs [40].

5.2 Wired Technologies:

1. Ethernet: Commonly used in industrial settings or where high-speed, reliable communication is vital [41-42].
2. Power-line Communication (PLC): Utilizes existing electrical wiring for data transmission, suitable for home automation and smart grid applications [43].

Protocols and Standards:

3. MQTT: A lightweight messaging protocol suitable for low-bandwidth and low-power scenarios [31].
4. CoAP: Designed for constrained devices and networks, providing RESTful communication [32].
5. HTTP/HTTPS: Widely used, especially when interoperability with existing web technologies is essential [34].
6. Mesh Networking: Enables devices to communicate via multiple hops, extending communication range and enhancing network resilience. Examples include Zigbee and Thread [44].

Selection of communication technology depends on factors like power consumption, data requirements, range, cost, and environmental conditions. Different applications may require specific combinations of these technologies to meet their unique needs. Few of the technologies have been summarized in Table.1 for ready reference.

Table 1. Summary of IoT protocols

Characteristics	Standard	Network	Topology	Power	Frequency Bands	Data Rate	Range	Spreading	Security	Comimoni Applications
Bluetooth LE	IEEE 802.15.1	WPAN	Star , mesh	Low	24 GHz	1-2 Mbps	15-30 m Short Range	FHSS	EO stream ,AES - 128	Audio applications and Wireless headsets
Z - Wave	ITU G - 9959	WPAN	Mesh	Low	868 MHz 908 MHz	40 kbps	30 m (indoors) 100 m (outdoor)	-	AES - 128	Home Monitoring and Control
ZigBee	IEEE 802.15.4	WPAN	Star , mesh , tree	Low	24 GHz	250 kbps	10-100 m . Short Range	DSSS	AES - 128	Controlling and Home industry monitoring
LoRa	IEEE 802.15.4g	WAN	Mesh	Ultra - low - power	869/915 MHz	50 kbps	Urban (2-5 km) suburban (15 km)	CSS	AES - 128	Air Pollution Monitoring .Tracking Fire Detection Home Security
6LOWPAN	IEEE 802.15.4	WPAN	Star , Mesh	Low	868 MHz (EU) 915 MHz (USA) , 2.4 GHz (Global)	250 kbps	10-100 m Short Range	DSSS	AES - 128	Monitoringand Control

Wi – Fi	IEEE 802.11	WLAN	Mesh	Medium	24/5/6 GHz	11-9600 Mbps	100m	DSSS	WPA2 / 3	Mobile,Automotive , Browsing
PLC G3 PRIME	ITU - T G - 9903	WAN		Low	3-490 kHz	33.4 kbps	10 m – 100 kms			Smart Grid
	ITU - T G - 9904				3-95 kHz	130 kbps				

6 IoT Hardware Platforms: Building Blocks for Connected Systems

The power and computing capabilities of IoT are exemplified by various processing elements like microcontrollers (MCUs), systems-on-chip (SoCs), systems-in-package (SiPs), and field programmable gate arrays (FPGAs). Educational and evaluation boards such as Arduino, Raspberry Pi, UDOO, FriendlyARM, Intel Galileo , BeagleBone, Gadgeteer, and T-Mote Sky are widely available for running IoT applications.

SoC and SiP technologies play pivotal roles in creating semiconductor options for IoT devices. SoCs integrate analog, digital, mixed-signal, and RF circuitry on a single chip, enhancing system stability and usability while reducing overall expenses. However, there are trade-offs in device performance and energy usage. On the other hand, SiPs combine functional elements independently created into a package, including MCUs, oscillators, and antennas. SiP devices enhance unit speed and power utilization but may incur higher system costs and reduced reliability due to varied materials and fabrication procedures.[45]. Firmware is crucial for computational platforms as it governs device execution throughout its lifecycle. Real-Time Operating Systems (RTOSs) [45] like Contiki, TinyOS, RiotOS, and LiteOS[46] are instrumental in enhancing certain IoT applications.

Cloud platforms are another essential computational aspect of IoT, enabling data transmission, periodic analysis of big data sets, and providing end-users with valuable insights. Numerous cloud platforms and services are available, many of which are free or cater to commercial use, facilitating the deployment of IoT services.

This integration highlights the diverse technological landscape within IoT, spanning hardware platforms, semiconductor technologies, firmware, and cloud-based solutions, all crucial for the development and deployment of IoT applications.

7 Tools for Simulating IoT Environments

With the growing emphasis on IoT and Wireless Sensor Networks (WSNs), there's a rising demand for modern simulators. Choosing the right simulator can be daunting, particularly in the WSN domain, where intricate scenarios and diverse protocols demand specialized functionality. Several simulators, including OpenDSS, Network Simulator-2 (NS-2), NS-3, OMNET++, GridLab-D, and GloMoSim, have emerged to cater to IoT simulation needs.

1. OpenDSS: OpenDSS, developed by Microsoft, is a distributed simulation software tailored for electric distribution systems. It offers a range of functionalities such as AC circuit analysis, load generation simulation, wind power simulation, power flow analysis, and fault analyses [47].

2. NS-2/NS-3: NS-2, a free network simulator, models communication protocols and network topologies for wired and wireless networks[48]. NS-3, an advanced version, supports parallel and emulation simulations, enhancing its capabilities[49].

3. OMNET++: OMNET++, an open-source simulator, supports multiple platforms and is based on unit and simple modules written in C++. Its versatility extends to various areas including ad-hoc networks, peer-to-peer networks, sensor networks, and wireless networks.[50]

4. GridLab-D: GridLab-D integrates end-use models and simulation tools for consumer equipment, retail markets, and power distribution. It also facilitates integration with third-party analysis software and data management tools.[51]

5. MATLAB/Simulink: MATLAB's Simulink offers a visual interface for simulation and modelling, providing features for algorithm development, graphics, application building, parallel computing, and data analysis.[52]

6. GloMoSiM: GloMoSiM focuses on parallel programming software and supports wireless satellite communication systems with heterogeneous connectivity. Its simulation library and Parsec compiler enhance its capabilities.[53]

Figure 3 compares various IoT simulators based on criteria such as availability, programming language, and support for future hardware models. These simulators play a crucial role in testing and simulating IoT setups, offering scalability and diverse functionalities to address various simulation requirements.

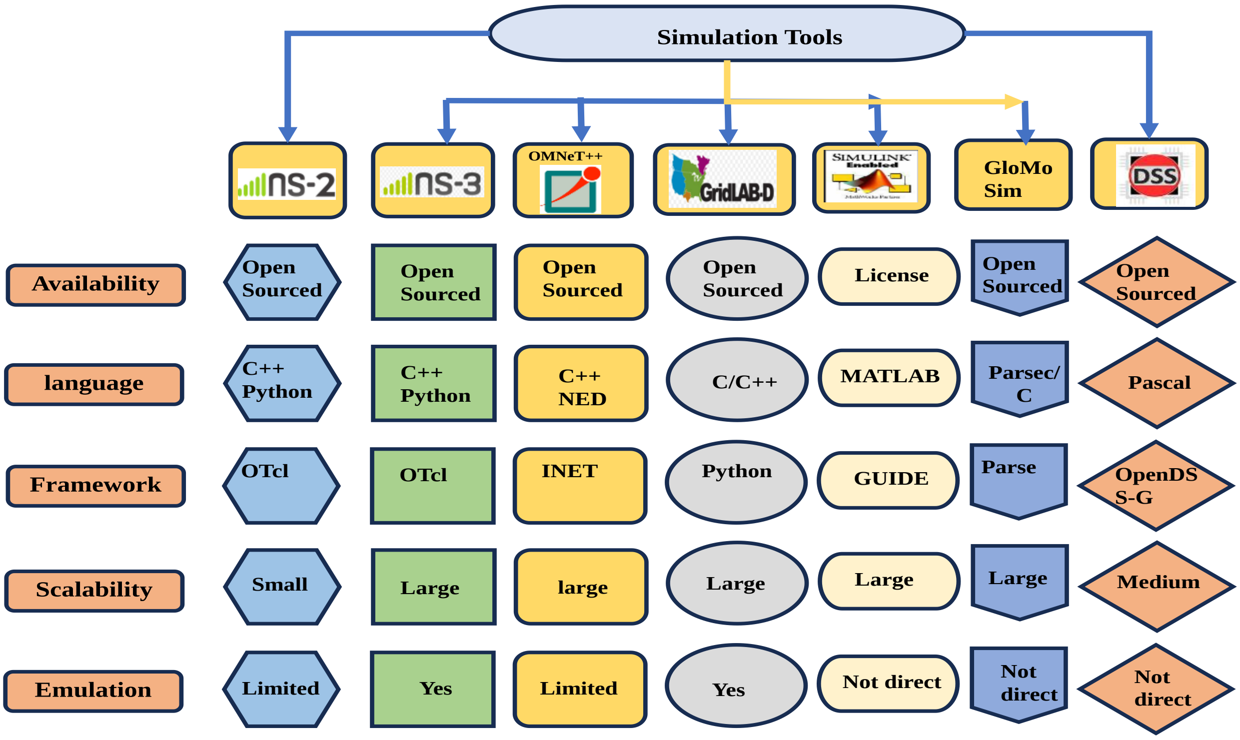

Figure 3 Simulation Tools

8 Prospects for the Future of IoT

In the coming decade, the evolution towards 6G standards promises ubiquitous IoT coverage, especially through satellite-based communications. Geo-location tracking, eco-monitoring, and disaster prediction necessitate seamless coverage everywhere, prompting the integration of satellite systems into 6G networks. Hybrid satellite-terrestrial relay networks (HSTRN) are proposed to enhance reliability, especially in remote areas. 6G communications envision a global network of satellites and aerial platforms powered by AI and big data, addressing scalability, low-power consumption, minimal latency, privacy, and universal coverage. Next-generation multiple access (NGMA) systems[54], such as non-orthogonal multiple access (NOMA)[55] and rate-splitting multiple access (RSMA)[56], are crucial for handling IoT data traffic efficiently. Re-configurable intelligent surfaces (RIS) and unmanned aerial vehicles (UAVs)[57] play significant roles in achieving pervasive IoT connectivity, especially in challenging environments. Fog computing, machine learning, and optimization algorithms are integrated to address low-latency challenges, while Lyapunov optimization and reinforcement learning models optimize resource allocation in heterogeneous Space-Air-Ground IoT (SAG-IoT) [58] networks. Overall, these advancements aim to enhance IoT connectivity, reliability, and efficiency across diverse scenarios and environments

Conclusion

The IoT concept has rapidly permeated modern society, aiming to enhance quality of life by integrating intelligent devices, applications, and technologies to automate various aspects of our surroundings. This paper comprehensively explores key foundations of the IoT, with its protocols, communication technologies, and different applications. Through detailed discussions and examples, it elucidates the operational and efficiency properties of each protocol, serving as a foundational resource for scholars and practitioners seeking to delve deeper into IoT techniques and protocols. Understanding the general structure and functionalities of different parts and protocols equips individuals to select suitable protocols and simulation tools for diverse applications. In conclusion, the forthcoming generation of IoT is poised to be universal in coverage, intelligent in offloading and resource allocation decisions, mindful of Quality of Service (QoS), and more resilient against cyber-attacks. These advancements will facilitate efficient communication between physical and cloud levels, further enriching the IoT landscape.

References:

1. 1. Khorov, E.; Lyakhov, A.; Krotov, A.; Guschin, A. A survey on IEEE 802.11ah: An enabling networking technology for smart cities. Comput. Commun. 2015, 58, 53–69. [CrossRef]
2. 2. Darabkh, K.A.; Alfawares, M.G.; Althunibat, S. MDRMA: Multi-data rate mobility-aware AODV-based protocol for flying ad-hoc networks. Veh. Commun. 2019, 18, 100163. [CrossRef]
3. 3. Michalski, A.; Watral, Z. Problems of Powering End Devices in Wireless Networks of the Internet of Things. Energies 2021, 14, 2417. [CrossRef]
4. 4. Alhasanat, M.; Althunibat, S.; Darabkh, K.A.; Alhasanat, A.; Alsafasfeh, M. A physical-layer key distribution mechanism for IoT networks. Mob. Netw. Appl. 2020, 25, 173–178. [CrossRef]
5. 5. Hendriks, S. Internet of Things: How the World Will Be Connected in 2025. Master's Thesis, Utrecht University, Utrecht, The Netherlands, 2016.
6. 6. Mili´c, D.C.; Toli´c, I.H.; Peko, M. Internet of Things (IoT) solutions in smart transportation management. In Proceedings of the Business Logistics in Modern Management, Osijek, Croatia, 5–6 October 2020.
7. 7. Wytr ˛ebowicz, J.; Cabaj, K.; Krawiec, J. Messaging Protocols for IoT Systems—A Pragmatic Comparison. Sensors 2021, 21, 6904. [CrossRef]
8. 8. Sadeghi-Niaraki, A. Internet of Thing (IoT) review of review: Bibliometric overview since its foundation. Future Gener. Comput. Syst. 2023, 143, 361–377. [CrossRef]
9. 9. Miorandi, D.; Sicari, S.; De Pellegrini, F.; Chlamtac, I. Internet of things: Vision, applications and research challenges. Ad Hoc Networks 2012, 10, 1497–1516. [CrossRef]
10. 10. Said, O.; Masud, M. Towards internet of things: Survey and future vision. Int. J. Comput. Networks 2013, 5, 1–17.
11. 11. Guth, J.; Breitenbücher, U.; Falkenthal, M.; Fremantle, P.; Kopp, O.; Leymann, F.; Reinfurt, L. A Detailed Analysis of IoT Platform Architectures: Concepts, Similarities, and Differences. In Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives; Di Martino, B., Li, K.C., Yang, L.T., Esposito, A., Eds.; Springer Singapore: Singapore, 2018; pp. 81–101. [CrossRef]
12. 12. Colakovi´c, A.; Hadžiali´c, M. Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. ˇ Comput. Networks 2018, 144, 17–39. [CrossRef]
13. 13. Gerodimos, A.; Maglaras, L.; Ferrag, M.A.; Ayres, N.; Kantzavelou, I. IoT: Communication protocols and security threats. Internet Things Cyber-Phys. Syst. 2023, 3, 1–13. [CrossRef]

14. 14. Domínguez-Bolaño, T.; Campos, O.; Barral, V.; Escudero, C.J.; García-Naya, J.A. An overview of IoT architectures, technologies, and existing open-source projects. Internet Things 2022, 20, 100626. [CrossRef]
15. 15. Elkhodr, M.; Shahrestani, S.; Cheung, H. Emerging Wireless Technologies in the Internet of Things: A Comparative Study. Int. J. Wirel. Mob. Networks 2016, 8, 67–82. [CrossRef]
16. 16. Al-Sarawi, S.; Anbar, M.; Alieyan, K.; Alzubaidi, M. Internet of Things (IoT) communication protocols. In Proceedings of the 2017 8th International Conference on Information Technology (ICIT), Amman, Jordan, 17–18 May 2017; pp. 685–690.
17. 17. Burhan, M.; Rehman, R.A.; Khan, B.; Kim, B.S. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Sensors 2018, 18, 2796. [CrossRef]
18. 18. Salman, T.; Jain, R. A Survey of Protocols and Standards for Internet of Things. arXiv 2017, arXiv:1903.11549.
19. 19. Bayılmı¸s, C.; Ebleme, M.A.; Çavu¸so ˘glu, Ü.; Küçük, K.; Sevin, A. A survey on communication protocols and performance evaluations for Internet of Things. Digit. Commun. Networks 2022, 8, 1094–1104. [CrossRef]
20. 20. Florea, I.; Rughinis, R.; Ruse, L.; Dragomir, D. Survey of Standardized Protocols for the Internet of Things. In Proceedings of the 2017 21st International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 19–31 May 2017; pp. 190–196. [CrossRef].
21. Mehta, R.; Sahni, J.; Khanna, K. Internet of things: Vision, applications and challenges. Procedia Comput. Sci. 2018, 132, 1263–1269. [CrossRef]
22. 22. Bonetto, R.; Bui, N.; Lakkundi, V.; Olivereau, A.; Serbanati, A.; Rossi, M. Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples. In Proceedings of the 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), San Francisco, CA, USA, 25–28 June 2012; pp. 1–7.
23. 23. Ray, P.P. A survey on Internet of Things architectures. J. King Saud Univ.-Comput. Inf. Sci. 2018, 30, 291–319. [CrossRef]
24. 24. Rose, K.; Eldridge, S.; Chapin, L. The internet of things: An overview. Internet Soc. 2015, 80, 1–50.
25. 25. Goulart, A.; Chennamaneni, A.; Torre, D.; Hur, B.; Al-Aboosi, F.Y. On Wide-Area IoT Networks, Lightweight Security and Their Applications—A Practical Review. Electronics 2022, 11, 1762. [CrossRef]
26. 26. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet Things J. 2017, 4, 1125–1142. [CrossRef]
27. Oliveira, L.; Rodrigues, J.J.; Kozlov, S.A.; Rabêlo, R.A.; de Albuquerque, V.H.C. MAC layer protocols for internet of things: A survey. Future Internet 2019, 11, 16. [CrossRef]
28. Farooq, M.U.; Waseem, M.; Mazhar, S.; Khairi, A.; Kamal, T. A review on internet of things (IoT). Int. J. Comput. Appl. 2015, 113, 1–7.
29. 33. Vashi, S.; Ram, J.; Modi, J.; Verma, S.; Prakash, C. Internet of Things (IoT): A vision, architectural elements, and security issues. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017; pp. 492–496. [CrossRef]
30. Manowska, A.; Wycisk, A.; Nowrot, A.; Pielot, J. The Use of the MQTT Protocol in Measurement, Monitoring and Control Systems as Part of the Implementation of Energy Management Systems. Electronics 2023, 12, 17. [CrossRef]
31. 51. Yassein, M.B.; Shatnawi, M.Q.; Aljwarneh, S.; Al-Hatmi, R. Internet of Things: Survey and open issues of MQTT protocol. In Proceedings of the 2017 International Conference on engineering & MIS (ICEMIS), Monastir, Tunisia, 8–10 May 2017; pp. 1–6.
32. Arvind, S.; Narayanan, V.A. An overview of security in CoAP: Attack and analysis. In Proceedings of the 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 15–16 March 2019; pp. 655–660
33. Naik, N. Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. In Proceedings of the 2017 IEEE International Systems Engineering Symposium (ISSE), Vienna, Austria, 11–13 October 2017; pp. 1–7
34. Yokotani, T.; Sasaki, Y. Comparison with HTTP and MQTT on required network resources for IoT. In Proceedings of the 2016 International Conference on Control, Electronics, Rrenewable Energy and Ccommunications (ICCEREC), Bandung, Indonesia, 13–15 September 2016; pp. 1–6

35. Nikolov, N. Research of MQTT, CoAP, HTTP and XMPP IoT Communication protocols for Embedded Systems. In Proceedings of the 2020 XXIX International Scientific Conference Electronics (ET), Sozopol, Bulgaria, 16–18 September 2020; pp. 1–4. [CrossRef]
36. Cheruvu, S.; Kumar, A.; Smith, N.; Wheeler, D.M. Demystifying Internet of Things SECURITY: Successful Iot Device/Edge and Platform Security Deployment; Springer: Berlin/Heidelberg, Germany, 2020.
37. Zeadally, S.; Siddiqui, F.; Baig, Z. 25 Years of Bluetooth Technology. Future Internet 2019, 11, 194. [CrossRef]
38. 63. Fatihah, S.N.; Dewa, G.R.R.; Park, C.; Sohn, I. Self-Optimizing Bluetooth Low Energy Networks for Industrial IoT Applications. IEEE Commun. Lett. 2023, 27, 386–390. [CrossRef]
39. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Commun. Surv. Tutorials 2015, 17, 2347–2376. [CrossRef]
40. Sanchez-Gomez, J.; Carrillo, D.G.; Sanchez-Iborra, R.; Hernández-Ramos, J.L.; Granjal, J.; Marin-Perez, R.; Zamora-Izquierdo, M.A. Integrating LPWAN Technologies in the 5G Ecosystem: A Survey on Security Challenges and Solutions. IEEE Access 2020, 8, 216437–216460. [CrossRef]
41. Kenny, J.P.; Wilke, J.J.; Ulmer, C.D.; Baker, G.M.; Knight, S.; Friesen, J.A. An Evaluation of Ethernet Performance for Scientific Workloads. In Proceedings of the 2020 IEEE/ACM Innovating the Network for Data-Intensive Science (INDIS), Atlanta, GA, USA, 12 November 2020; pp. 57–67. [CrossRef]
42. 129. Conti, M.; Donadel, D.; Turrin, F. A survey on industrial control system testbeds and datasets for security research. IEEE Commun. Surv. Tutorials 2021, 23, 2248–2294. [CrossRef]
43. Tonello, A.M.; De Piante, M. Exploring Joint Voltage and Impedance Modulation in Wired Networks. In Proceedings of the 2020 IEEE International Symposium on Power Line Communications and its Applications (ISPLC), Malaga, Spain, 11–13 May 2020; pp. 1–6
44. kumura, R.; Mizutani, K.; Harada, H. A broadcast protocol for IEEE 802.15. 4e RIT based Wi-SUN systems. In Proceedings of the 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, Australia, 4–8 June 2017; pp. 1–5
45. Zhang, Y.; Mao, J. An Overview of the Development of Antenna-in-Package Technology for Highly Integrated Wireless Devices. Proc. IEEE 2019, 107, 2265–2280. [CrossRef]
46. Baccelli, E.; Gündo ˘gan, C.; Hahm, O.; Kietzmann, P.; Lenders, M.S.; Petersen, H.; Schleiser, K.; Schmidt, T.C.; Wählisch, M. RIOT: An open source operating system for low-end embedded devices in the IoT. IEEE Internet Things J. 2018, 5, 4428–4440. [CrossRef]
47. Troiano, G.O.; Ferreira, H.S.; Trindade, F.C.; Ochoa, L.F. Co-simulator of power and communication networks using OpenDSS and OMNeT++. In Proceedings of the 2016 IEEE Innovative Smart Grid Technologies-Asia (ISGT-Asia) IEEE, Melbourne, Australia, 28 November–1 December 2016; pp. 1094–1099.
48. 139. Kumar, S.; Bansal, A. Performance investigation of topology-based routing protocols in flying ad-hoc networks using NS-2. In IoT and Cloud Computing Advancements in Vehicular Ad-Hoc Networks; IGI Global: Hershey, PA, USA, 2020; pp. 243–267.
49. 140. Kim, B.S.; Sung, T.E.; Kim, K.I. An ns-3 implementation and experimental performance analysis of ieee 802.15. 6 standard under different deployment scenarios. Int. J. Environ. Res. Public Health 2020, 17, 4007. [CrossRef]
50. Bautista, P.A.B.; Urquiza-Aguiar, L.F.; Cárdenas, L.L.; Igartua, M.A. Large-scale simulations manager tool for OMNeT++: Expediting simulations and post-processing analysis. IEEE Access 2020, 8, 159291–159306. [CrossRef]
51. Nasiakou, A.; Alamaniotis, M.; Tsoukalas, L.H. MatGridGUI—A toolbox for GridLAB-D simulation platform. In Proceedings of the 2016 7th International Conference on Information, Intelligence, Systems & Applications (IISA) IEEE, Patras, Greece, 11–16 June 2016; pp. 1–5.
52. Chaturvedi, D.K. Modeling and Simulation of Systems Using MATLAB® and Simulink®; CRC Press: Boca Raton, FL, USA, 2017
53. Patel, R.L.; Pathak, M.J.; Nayak, A.J. Survey on network simulators. Int. J. Comput. Appl. 2018, 182, 23–30. [CrossRef]
54. Tegos, S.A.; Diamantoulakis, P.D.; Lioumpas, A.S.; Sarigiannidis, P.G.; Karagiannidis, G.K. Slotted ALOHA with NOMA for the next generation IoT. IEEE Trans. Commun. 2020, 68, 6289–6301. [CrossRef]

55. Lin, Z.; Lin, M.; Wang, J.B.; de Cola, T.; Wang, J. Joint Beamforming and Power Allocation for Satellite-Terrestrial Integrated Networks With Non-Orthogonal Multiple Access. IEEE J. Sel. Top. Signal Process. 2019, 13, 657–670. [CrossRef]
56. Liu, H.; Tsiftsis, T.A.; Kim, K.J.; Kwak, K.S.; Poor, H.V. Rate splitting for uplink NOMA with enhanced fairness and outage performance. IEEE Trans. Wirel. Commun. 2020, 19, 4657–4670. [CrossRef]
57. Li, B.; Fei, Z.; Zhang, Y. UAV Communications for 5G and Beyond: Recent Advances and Future Trends. IEEE Internet Things J. 2019, 6, 2241–2263. [CrossRef]
58. Zhang, Z.; Xiao, Y.; Ma, Z.; Xiao, M.; Ding, Z.; Lei, X.; Karagiannidis, G.K.; Fan, P. 6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies. IEEE Veh. Technol. Mag. 2019, 14, 28–41. [CrossRef]