Kelvin Open Science Publishers
Connect with Research Community

Research Article *Volume 1 | Issue 1*

KOS Journal of Science and Engineering
https://kelvinpublishers.com/journals/science-and-engineering.php

Networking Challenges in IoT to Deployment of TCP/IP to 6LoWPAN for Next Gen Network System

Vaidehi Shah*

Independent Researcher, India

***Corresponding author:** Vaidehi Shah, Independent Researcher, India, E-mail: shahvaidehi4795@gmail.com

Received: December 02, 2024; **Accepted:** December 18, 2024; **Published:** December 20, 2024

Citation: Vaidehi Shah. (2024) Networking Challenges in IoT to Deployment of TCP/IP to 6LoWPAN for Next Gen Network System. *KOS J Sci and Eng.* 1(1): 1-8.

1. Abstract

The ideas that revolve around the Internet of Things (IoT), include e-health care, self-driving automobiles, smart surroundings, augmented reality, and high-resolution video streaming, are now widely used. These applications demand more capacity, low latency, high throughput, wide bandwidth, and larger data rates. The Internet of Things (IoT) is revolutionizing the digital landscape by tying together a huge number of intelligent devices from industries including industrial automation, smart cities, healthcare, and agriculture. These systems require high efficiency, low latency, and minimal energy usage to operate effectively. Traditional networking protocols like TCP/IP, while foundational to internet communications, are not ideally suited for the specialized needs of IoT environments. This study compares the speed and scalability of traditional protocol stacks and provides an outline of the IoT architecture framework. It is advised to deploy IPv6-based communication using 6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks), a more adaptable choice for nodes with constrained resources. Specifically engineered for IEEE 802.15.4 networks, 6LoWPAN facilitates effective IPv6 communication through mesh routing, lightweight data sharing, and header compression. Additional components such as neighbor discovery, secure routing (RPL), and access control models contribute to its operational efficiency. A detailed comparison of existing models highlights how 6LoWPAN enhances connectivity and system reliability in large-scale deployments. The overall analysis supports the adoption of 6LoWPAN as a scalable and energy-efficient protocol stack for building advanced, next-generation IoT network infrastructures.

2. Keywords

Internet of Things (IoT), IoT Architecture, IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN), challenges in IoT Protocols, TCP/IP.

3. Introduction

In 2016, there were over 30 billion connected devices, as the Internet of Things (IoT) keeps evolving at a fast pace in the digital world, this figure is predicted to quadruple by 2022 [1,2]. The number of IoT devices is increasing every day. Despite this exponential growth, general public awareness regarding IoT services remains limited. The surface area for possible cyberattacks grows as the number of connected devices rises[3,4]. Therefore, ensuring robust security in IoT systems is imperative, as Low-end, resource-constrained devices are frequently found in IoT networks. ranging from sensors to home appliances, the design of these systems is typically governed by minimal power usage and low operational costs, further complicating the challenge of securing them effectively.

The traditional TCP/IP protocol stack, while robust and

extensively deployed across the internet, poses significant inefficiencies when applied to IoT environments [5,6]. Originally developed for general-purpose computing systems, TCP/IP protocols introduce considerable overhead that can drain the limited processing and energy resources of IoT nodes [7]. Past research has investigated the performance of TCP and UDP in constrained settings, suggesting enhancements such as zero-copy and zero-check summing techniques to reduce computational load and improve transmission efficiency. The structural rigidity and resource demands of TCP/IP still make it less than ideal for next-generation IoT networks that require lightweight, adaptive solutions.

6LoWPAN, or Low-Power Wireless Personal Area Networks, can be used to deploy IPv6. IEEE 802.15.4-based networks may communicate over IPv6 to 6LoWPAN [8], specifically designed for applications requiring limited range, low data rates, and minimal power. The protocol introduces an adaptation layer that compresses IPv6 headers, supporting efficient routing and fragmentation, making it suitable for reduced-function devices (RFDs) with limited capabilities. This layer defines four key headers: IPv6 compression using the HC1 Header, Mesh Header, Dispatch Header, and Fragmentation Header, which guarantees efficient packet processing and lower transmission overhead.

The evolution from conventional TCP/IP stacks to 6LoWPAN-based networking represents a strategic advancement in building scalable and interoperable IoT infrastructures. By leveraging lightweight, energy-efficient communication protocols, 6LoWPAN addresses the core networking challenges of IoT, such as constrained memory and processing power, and constrained bandwidth. Its seamless integration with the IPv6 framework further ensures compatibility with global Internet standards, supporting the deployment of resilient and efficient next-generation network systems for smart cities [9], industrial automation, and other critical domains. The transition from conventional TCP/IP to 6LoWPAN signifies a pivotal shift toward building scalable, secure, and efficient next-generation IoT network systems. These networks must not only manage high volumes of real-time traffic across heterogeneous devices but also ensure strong security, privacy, and data integrity. Leveraging lightweight protocol stacks, secure neighbor discovery, and adaptive routing mechanisms, 6LoWPAN addresses key challenges in IoT communication. This paper explores the underlying networking challenges in IoT, limitations of traditional TCP/IP stacks, and the deployment of 6LoWPAN as a forward-looking solution for sustainable IoT networking infrastructure.

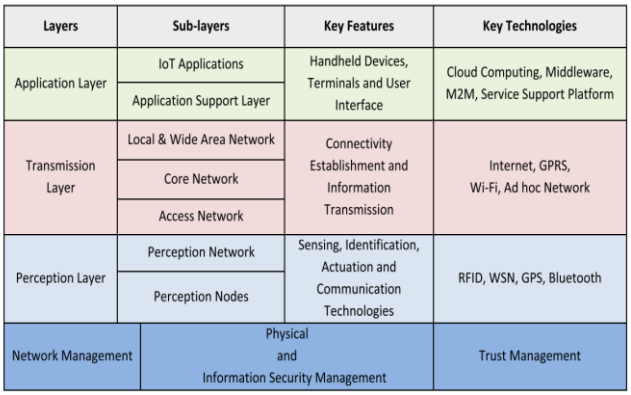
3.1. Structure of the paper

This paper is organized as follows: Section II provides an overview of IoT networking architecture. Section III discusses traditional IoT protocols. Section IV outlines the challenges of TCP/IP in IoT. Section V presents 6LoWPAN as a next-gen solution. Section VI concludes the study by discussing potential future directions.

4. Overview of IoT Networking and Architecture

There will be much more items connected to the Internet than there are humans, and more settings will be connected to the Internet in some way [10,11]. There are several supporting technologies that enable the Internet of Things, such as RFID and wireless sensor networks (WSN), M2M communication, and low-power personal area networks. Careful consideration of security issues is necessary to create dependable systems and applications. The IoT' architecture can handle a variety of issues, such as privacy control, quality of service, dependability, and maintenance of new devices and services. These characteristics support the creation and design of systems that provide dependable and efficient operation. Figure 1 below discusses the three levels that make up the IoT architecture [12].

Figure 1: Architecture of IOT networking.



4.1. Perception layer

A few other names for this layer of perception include the “Device Layer”, “Sensory Layer”, and “Recognition Layer”. It is regarded as the IoT' foundational layer. This category of technologies includes actuation (conducting a mechanical action based on the sensed data), identification (identifying objects based on a unique identity assigned to them), communication (creating connectivity among heterogeneous smart devices), and sensing (gathering data from the environment and sending it to databases, data warehouses, or the cloud). Few human interactions are needed for these technologies. Information from the actual world is captured and represented digitally, which is its defining characteristic. Depending on its function, this layer is composed of two sub-layers: The Perception Network and Perception Nodes (also called Sensory Nodes).

4.2. Transmission layer

The terms "Transportation Layer" and "Network Layer" are other names for the Transmission Layer. It lies in between the levels of perception and application. One way to think about it is as a synthesis of several legacy networks, technologies, and protocols. The information processing unit receives the data collected by the perception nodes over wired or wireless communication links for analysis, data mining, data aggregation, and data encoding. One, it is also in charge of carrying out network administration tasks. It may be separated into three sublayers according to the duties it accomplishes: Access, core, local, and wide area networks.

4.3. Application layer

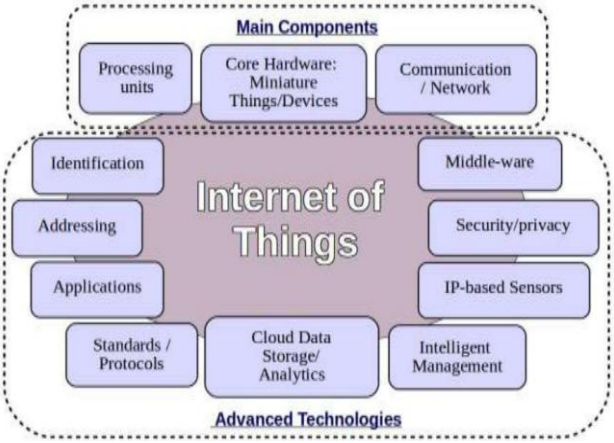
In the architecture of the IoT, this layer is the highest one that the end user may see. The application layer manages and provides applications worldwide by using the data gathered by the perception layer and processed by the information processing unit. Based on their requirements, it provides end customers with network access to bespoke services through a range of portable devices and terminal equipment. Its two sublayers are IoT apps and the Application Support Layer.

4.4. Network management

Topological issues and effective resource management are the main goals of network administration. Recent methods for effective network and resource management in an Internet of Things (IoT) setting include game-theoretical processes, software-defined networking (SDN), and infrastructure built on the Extensible Messaging and Presence Protocol (XMPP). The management of information and physical security is concerned with protecting networked hardware and making sure that data is safely stored and moved between them. As the number of smart devices increases, transparent security management techniques are needed to address the security of software, online interfaces, networks, and mobile services, thereby safeguarding user privacy, information confidentiality, and integrity.

4.4.1. **Element and major technologies for IoT:** The IoT, a fully integrated future Internet, needs key technological components that are combined to create the IoT world (see **Figure 2**). This section discusses the primary enabling technologies [13]. The objective is to provide a concise overview of each component, highlighting its function within the IoT framework.

Figure 2: Key elements and technologies for IoT.



- **Core Hardware: Miniature devices:** Core hardware forms the foundation of IoT systems, made up of small components including embedded processors, sensors, and actuators. These gadgets sense, gather, and send data in order to facilitate automation and real-time monitoring.
- **Processing unit:** Processing units handle local computation and basic decision-making tasks. They reduce latency and minimize reliance on remote cloud servers.
- **Communication/Network:** This element facilitates smooth data transfer across gateways, cloud systems, and devices [14]. It incorporates a number of wired and wireless technologies, including 6LoWPAN, Zigbee, and Wi-Fi.
- **Identification:** Identification mechanisms uniquely recognize each device within the IoT environment. This ensures traceability, authentication, and efficient resource management.
- **Addressing:** Addressing gives every connected device a distinct IP or MAC address. It facilitates accurate routing and device-level communication.
- **Application:** Applications of IoT are found in many fields, including industrial automation, smart homes, healthcare, and agriculture. These applications utilize collected data to offer intelligent services.
- **Standards/protocols:** Standards and protocols ensure interoperability and communication consistency. They define data formats, transmission rules, and system integration methods.
- **Cloud data storage analytics:** Cloud platforms store massive volumes of IoT data and provide tools for analysis. This enables predictive insights and scalable data management.
- **Middleware:** Middleware acts as an interface layer between hardware and applications. It manages services, data abstraction, and device coordination.
- **Security and privacy:** Security mechanisms protect data integrity and user privacy. Techniques like encryption and authentication safeguard against cyber threats [15,16].
- **IP-based sensors:** IP-based sensors are directly connected to the internet and support end-to-end communication. They enable real-time data access and remote control.
- **Intelligent management:** Intelligent management oversees system performance and resource optimization. It supports features like fault detection, system updates, and energy efficiency.
- **Traditional Networking Protocols in IoT:** In the early development of the IoT, traditional networking protocols played a central role in enabling communication among devices. These protocols, originally designed for the broader internet and enterprise networks, were adapted for initial IoT implementations due to their widespread use and existing infrastructure in resource-constrained environments commonly found in IoT systems.

5. TCP/IP and Networking Challenges in IoT Environments

In the initial stages of IoT deployment, conventional internet protocols like File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP) were often used for data sharing and device connection. These protocols, designed for robust computing environments, offered simplicity and interoperability with existing internet infrastructure. The TCP/IP protocol stack has been the foundation of internet communication for decades, offering reliable data transmission, addressing, and routing capabilities it is are some challenges described below:

5.1. Trust and privacy

In medical and assisted-living contexts, where decisions might have dire implications, the action can continue to pose a serious problem. The IoT presents unique challenges, and new compliance frameworks might emerge to address these issues [17]. The adoption of IoT may be hampered by social and political issues in this region.

5.2. Security

The interconnection of so many devices in the IoT network makes it an ideal vector for malware to infiltrate. When technologies are less expensive and less designed to safeguard people, they are also more likely to be tampered with [18]. The integration of middleware, APIs, and M2M connectivity creates a significant amount of complexity and additional security threats.

5.3. Network security monitoring over encrypted traffic

The fast growth of encrypted communication is complicating

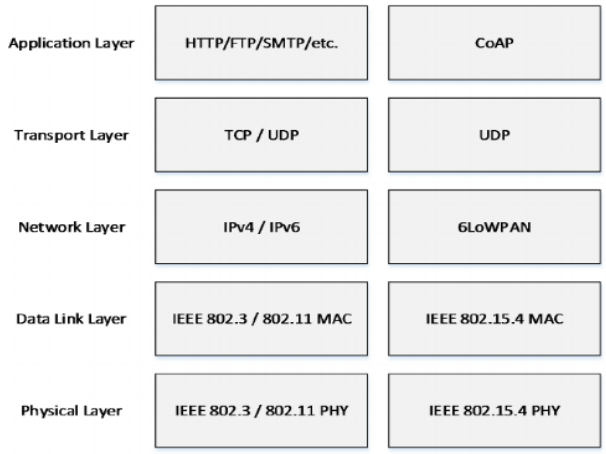
security monitoring and IDS. One of the main tools used by digital business organizations to secure information is encryption. In addition to providing organizations with security, encryption helps attackers avoid discovery [19]. The IoT-specific IDS solutions that are currently available in the literature were created with the presumption that traffic is not encrypted.

- **Real-time network management:** To provide optimal network performance for some IoT applications that need high availability of low-power networks, real-time network management is necessary [20]. Due to the frequent network management procedures, this process may result in an overhead in network traffic.
- **Heterogeneity:** A number of wireless technologies have emerged, increasing the variety of communication links, especially for low-power networks. The development of several standards to facilitate interoperability across various radio technologies has aided in creation of programs for IPv6-centric, or at least IPv6-based, IoT communications [21]. Future studies should concentrate on managing diverse IoT devices while maintaining a high quality of service.
- **Unreliable connectivity:** IoT networks often experience high packet loss, intermittent connectivity, and variable link quality. TCP/IP was not designed for such lossy conditions and fails to maintain efficient communication under these circumstances.
- **Incompatibility with constrained devices:** The conventional TCP/IP protocol stack was not optimized for low-power, memory-constrained IoT devices because it was first created for general-purpose computers. These devices often operate on limited energy budgets and minimal processing capabilities, making the full stack impractical.

5.3.1. Protocol Stack Architecture for IoT: A framework for developing wireless systems' communication protocols has been developed since 2003 by several IEEE and IETF standardization groups. The IEEE standard has been expanded for low-resource networks and devices with IEEE 802.15.4. IEEE 802.15.4 defines wireless personal area networks (WPANs) as networks based on radio frequencies that have a constrained range, low power consumption, and moderate data throughput. However, the higher-layer protocol stack standards needed for sensor nodes to easily interface with the Internet are absent from IEEE 802.15.4.

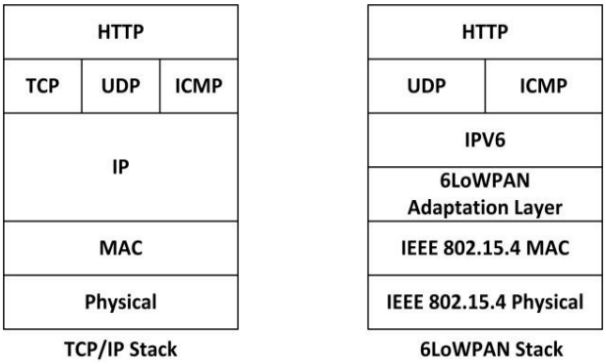
Several studies have been conducted recently to help shift away from proprietary designs and protocols and to make it possible to employ Internet technology on devices with constraints [23]. Two examples of IPv6 transmission networks are IEEE 802.15.4 Networks and Low-Power Wireless Personal Area Networks (RFC 4919 and RFC 4944) [24], The adoption of IPv6 by ZigBee and IETF routing across lossy and low-power networks were the two main advancements in the networking layer. The IoT is made possible by these new rules, which allow end-to-end IP-based network interaction with small devices like sensors and actuators. A stack of IoT communication protocols based on these standardizations is shown in **Figure 3**.

Figure 3: TCP/IP stack and IoT protocol stack [22].



5.3.2. TCP/IP and 6LoWPAN protocol stacks: Only an end-to-end, scalable, and accessible communication infrastructure would allow for interoperability. Devices need to be online in order to activate embedded Web servers (**Figure 4**). There are many different kinds and capacities of things with built-in information that must be a component of a Web-based application. Devices with restricted capabilities should have their IP protocol stack modified. In order to enable IPv6 packet transmission and reception on devices with limited resources, the IETF developed 6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks). This protocol often makes use of IEEE 802.15.4 and other low-power radio communication methodologies.

Figure 4: Comparison between TCP/IP and 6LoWPAN protocol stacks [25].



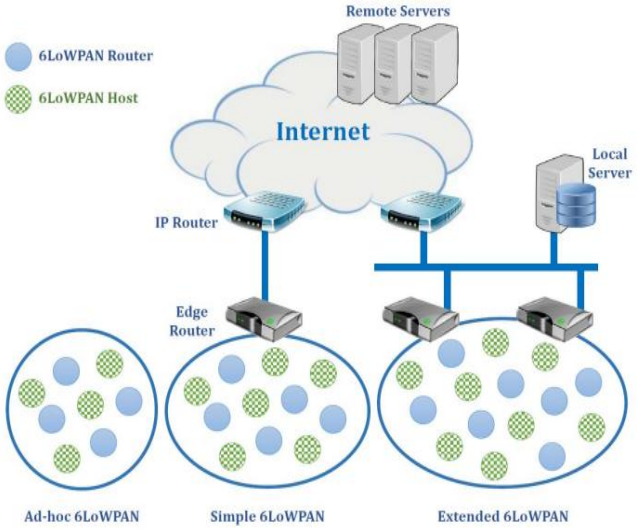
A layer-by-layer comparison is shown in Figure 4, where the TCP/IP and 6LoWPAN stacks are displayed. In their WoT, they point out that the fundamental reason the 6LoWPAN stack needs an adaption layer is to accommodate one MAC (Layer 2) frame of 802.15.4 that contains a single IP packet. In addition, the adaption layer controls edge routing, packet fragmentation, reassembling, and header compression. In order to establish 6LoWPAN, UDP is the best transport protocol to use since it guarantees efficiency while interacting with devices that have Internet connection. Web applications that employ HTTP rather than UDP will be more robust since UDP is unstable. Additionally, 6LoWPAN enables IP layer addressing of items on the Internet.

6. 6LOWPAN Architecture for Next-Gen Solution

The numerous embedded wireless devices that comprise a 6LoWPAN network are characterized by their limited data rate, memory constraints, and power limitations. The method of end-to-end communication that links LoWPANs to the

Internet is shown in Figure 5 and the 6LoWPAN architecture. All of them are IPv6 stub networks since each linked LoWPAN allows IP packets to be transmitted and received, but not from other Internet networks [26]. Three varieties of LoWPANs, ad hoc, simple, and extended, are defined by the architecture. Each type consists of many 6LoWPAN nodes with distinct responsibilities and functions. One well-known infrastructure-less technology that operates independently without an Internet connection is Ad-Hoc LoWPAN.

Figure 5: 6LoWPAN architecture.



The host and the router are two different kinds of linked devices that make up the 6LoWPAN network. The host, sometimes referred to as the end device, does not perform packet routing [27]. In a 6LoWPAN network, the router may send data to hosts and other routers in the network. Both the basic and expanded LoWPANs lack infrastructure. The former connects LoWPAN to external IP networks using a single 6LoWPAN edge router, whereas the latter does it using several edge routers. In the expanded LoWPAN, a backbone link connects the many edge routers. 6LoWPAN network coordination is done via the edge router. The translation between IPv6 and 6LoWPAN networks is its responsibility. A 6LoWPAN typically consists of one or more edge routers and a large number of nodes. By sharing an active connection, through the edge router, the nodes exchange information with one another, and Data is sent to the IP network. Ethernet, Wi-Fi, or communications via standard packet radio services can be used to link the external IP networks to LoWPAN if there are one or more edge routers [28].

6.1. Lightweight secure neighbor discovery for 6LoWPAN

The stateless address auto configuration and neighbor discovery protocol, collectively known as the neighbor discovery protocols (NDP), are used by both nodes and routers in conventional IPv6 networks. These protocols make it possible to: i) find neighborhood routers; ii) learn prefixes and address configuration options; iii) keep track of reachability information on active neighbors; and iv) identify redundant addresses that were suggested by NDP for devices with unmanaged nodes [29].

6.2. IPv6 routing protocol for low power and lossy networks

In order to develop a routing protocol for 6LoWPAN networks that meets the requirements specified in RFCs 5548, 5673, 5826, and 5867, the IETF Routing over Low-Power and Lossy Networks (RoLL) working group was formed. RoLL initially released the IPv6 Routing Protocol for Lossy and Low-power Networks (RPL) in 2010. Due to the fact that most LoWPAN applications only employ a small number of nodes to gather data from sensor nodes and that sensors almost ever connect with one another, multipoint-to-point traffic patterns are now prevalent [30]. To handle traffic, RPL utilizes three ICMPv6 message formats and constructs a Destination-Oriented Directed Acyclic Graph (DODAG): DIO for discovering RPL instances and selecting parents, DIS for requesting DIOs, and DAO for transmitting routing information upward in the DODAG.

6.3. Network access control security framework in 6LoWPAN

In order to regulate node access and guarantee security compliance for authorized nodes, 6LoWPAN networks employ an administrative authorization-based network access control security architecture. There are two modes of operation for the suggested framework: active and listening. There is no security evaluation or enforcement carried out in the listening mode. The ability to collect data on the linked nodes makes this mode helpful for network visibility. A network is safer in active mode than in listening mode since only security-compliant nodes may join.

6.3.1. Node requirements: The LSEND protocol and 6LoWPAN must be supported by every node. To function in active mode, the nodes must have real-time message authentication and a secure reprogramming process in addition to the previously listed requirements for the routing protocol known as RPL. The Rsync size reduction technique, the Maté execution environment, and Seluge may all be used to implement the secure reprogramming process.

6.3.2. Node identification, compliance and data security: Since sensor networks are often utilized for critical sensing measurement tasks in human-unattended settings, Critical issues include the data's authenticity and the data source's authentication. Actually, authentication guarantees may be used to identify sensors and routers, preventing and/or detecting various security threats while safeguarding the integrity and freshness of vital data. The two traditional approaches to authentication are message authentication codes using symmetric keys and digital signatures using public keys.

7. Literature Review

This section reviews prior studies on IoT networking, with an emphasis on the shift from TCP/IP to 6LoWPAN. Table I summarizes key research on protocol performance, limitations, and how 6LoWPAN addresses the challenges in next-gen IoT systems.

Talau, et al. (2023) The home network has already been transformed into a complex composition of many devices, each with unique characteristics in terms of transmission speed, reliability, latency, and TCP protocol variations, thanks to the IoT. IoT is usually used in an IEEE 802.11 context where several devices share a single network. Several variables, such as wireless loss, access point queue saturation, and fairness, affect TCP's performance in this situation. In order to enhance TCP performance in these situations, a revised Early Window Tailoring (EWT) technique [31].

Kim, et al. [32] IoT wireless connection it has been proposed using IPv6-based IoT services over wireless networks, as well as IPv6 via Wireless Personal Area Network with Low Power (6LoWPAN). It hasn't been done yet, though, to investigate IoT systems that use 6LoWPAN over OWC networks. In OWC-based IoT networks, 6LoWPAN is intended for use by both the IoT device and the IoT gateway. Compared to the conventional IPv6 paradigm, the recommended method is easy to deploy and enhances performance in OWC-based IoT networks [32].

Setiawan, Hertiana and Negara (2021) the SDN network architectural model's IoT devices. By using IoT devices that implement TCP/IP overhead, Mininet-IoT is creating a Mininet network emulator. Protocols must also provide smooth device networking and data transfer. IoT protocols need to be secure in order to ensure the availability, confidentiality, and integrity of IoT network devices and communications. The 6LoWPAN device in the IoT network is powered by the SDN paradigm, virtualized IoT devices, and 802.15.4 wireless simulation. It is based on wireless Linux standards the host, Mininet-IoT emulator, switch, and cluster. Increased throughput has reduced in relation to the value of back-traffic traffic [33].

Ooko et al. (2020) IPv6 is introduced via the 6LoWPAN. The edge routers connect to the network architecture. There are several ways to link the IEEE802.15.4 networks to the Internet. The protocol stack offers an adaptability layer between the network and MAC layers in addition to the Internet Protocol's transport and application levels. Numerous applications that support the expanding IoT make use of 6LoWPAN, which has various advantages when linked to IPv6 networks and the Operation of the IEEE802.15.4 network. Concerns about privacy and security were also raised; if the suggestions, which include firewalls, access control, encryption, and 6LoWPsec, are put into practice, the devices will be more secure [34].

Yang and Chang (2019) IoT is the way of the future, and manufacturers and developers of IoT devices are increasingly adopting 6LoWPAN, an open, IPv6-based IoT network standard. IPv6 is replacing more conventional non-IP IoT technologies like BLE and ZigBee. Based on 6LoWPAN, Google, Samsung, and other businesses are creating their Thread IoT solutions. Newer IoT operating systems exploit their support for 6LoWPAN as a selling advantage, and 6LoWPAN is currently being actively investigated. While IP is for the Internet, end-to-end security is still being developed, and other connection layers other than IEEE 802.15.4 are still in their infancy. 6LoWPAN is expected to be a key component of the IoT [35].

Narayana, Sharma and Veeturi (2018) IoT has a lot of commercial potential. 6LoWPAN is a crucial IP (Internet Protocol) layer-based technology for connecting IoT devices. As mandated by IEEE 802.15.4, IP-based networking solutions known as 6LowPAN effectively carry IPV6 packets utilizing short link layer frames. Nevertheless, there are problems with packet sizes and IPv6 header compression that exceed by a large margin the IEEE 802.15.4 maximum packet size. When multicast is utilized extensively on a “low power and lossy network”, 6LoWPAN becomes ineffective and may be unworkable [36].

Table 1: Comparative analysis of TCP/IP to 6lowpan in IoT networks challenges.

Author	Focus Area	Key Findings	Challenges Identified	Key Contribution
Talau, et al. 2023 [31]	TCP performance in home IoT over IEEE 802.11	TCP performance is degraded in shared wireless IoT networks due to losses, queue saturation, and fairness issues	Wireless losses, fairness, and queue saturation in TCP	Proposed an enhanced Early Window Tailoring (EWT) method to improve TCP performance
Kim, et al. 2022 [32]	6LoWPAN over Optical Wireless Communication (OWC)	Proposed architectural model of 6LoWPAN over OWC, demonstrating better performance than traditional IPv6 in such networks	Lack of prior studies on 6LoWPAN over OWC; implementation challenges	Presented a simple, high-performance 6LoWPAN-OWC architecture for IoT
Setiawan et al. 2021 [33]	TCP/IP and 6LoWPAN in SDN-based IoT using Mininet-IoT	Virtualized 6LoWPAN devices using 802.15.4 simulation and evaluated throughput with SDN setup	Throughput degradation; SDN integration complexity	Developed Mininet-IoT to emulate IoT networks with TCP/IP and 6LoWPAN
Ooko, et al. 2020 [34]	6LoWPAN adaptation layer and architecture	IPv6 efficiency is increased in IEEE 802.15.4 by the layer of adaptation that lies between the network layer and the MAC	Privacy and security issues in situations using 6LoWPAN	Emphasized importance of security (e.g., 6LoWPsec, access control) in 6LoWPAN deployments
Yang and Chang 2019 [35]	Industry adoption of 6LoWPAN	6LoWPAN is being adopted by Google, Samsung in Thread-based IoT products; alternative link layers explored	End-to-end security is incomplete; non-802.15.4 support is still immature	Highlighted commercial interest and OS-level integration in 6LoWPAN
Narayana, et al. 2018 [36]	IPv6 header compression in 6LoWPAN	6LoWPAN makes IPv6 possible over IEEE 802.15.4 small frame networks, although it has problems with multicast and compression	Large IPv6 headers, inefficient multicast, low-power link limitations	Analyzed header compression challenges and inefficiencies in lossy IoT networks

8. Conclusion and Future Work

As IoT continues to expand across sectors, enabling real-time applications and large-scale device interconnectivity, addressing the limitations of traditional networking protocols becomes imperative. The TCP/IP stack, while foundational to internet communications, fails to meet the power, memory, and bandwidth constraints of typical IoT nodes. Issues such as high overhead, lack of multicast efficiency, and unreliable performance in lossy wireless environments make TCP/IP unsuitable for next-generation IoT deployment. This study thoroughly examined these drawbacks and presented 6LoWPAN as a game-changing solution that adds IP functionality to low-power IPv6 over IEEE 802.15.4 networks. With mesh routing, header reduction, and fragmentation, 6LoWPAN guarantees scalable, secure, and lightweight communications that are suited for devices with limited resources. Enhancements like secure neighbor discovery, optimized routing protocols such as RPL, and access control frameworks strengthen its suitability for

contemporary IoT applications. Integrating 6LoWPAN with cutting-edge technologies like edge computing, blockchain, and AI-driven network optimization should be the main goal of future research. Additionally, expanding support beyond IEEE 802.15.4 to other physical layers, improving interoperability among heterogeneous devices, and implementing end-to-end security frameworks are crucial research directions. Emphasizing these areas will help address the constantly changing IoT difficulties and open the door to reliable, energy-efficient, and globally networked smart systems.

9. References

1. R. Gurunath, M. Agarwal, A. Nandi, et al. (2018) An Overview: Security Issue in IoT Network. In: 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), IEEE. 104-107.
2. SN Swamy, SR Kota. (2020) An Empirical Study on System Level Aspects of Internet of Things (IoT). IEEE. 8: 188082-188134.
3. E Schiller, A Aidoo, J Fuhrer, et al. (2022) Landscape of IoT Security. Comput. Sci. Rev. 44.
4. A Goyal. (2023) Integrating IoT and Agile Methodologies for Smarter Engineering Solutions. Int. J. Sci. Res. Arch. 8(2): 754-766.
5. H Si, C Sun, B Chen, et al. (2019) Analysis of Socket Communication Technology Based on Machine Learning Algorithms Under TCP/IP Protocol in Network Virtual Laboratory System. IEEE Access. 7: 80453-80464.
6. Y Aslan, B Aslan. (2023) Comparison of IoT Protocols with OSI and TCP/IP Architecture," Int. J. Eng. Res. Dev. UMAGD. 15(1): 333-343.
7. Z Kanmai. (2020) TCP/IP Protocol Security Problems and Defenses. In: 2020 International Conference on Intelligent Computing and Human-Computer Interaction (ICHCI). IEEE. 117-120.
8. K Ee, CK Ng, NK Noordin, et al. (2010) A Review of 6LoWPAN Routing Protocols. Proc. Asia-Pacific Adv. Netw. 30.
9. N Patel. (2021) Sustainable Smart Cities : Leveraging IoT and Data Analytics for Energy Efficiency and Urban Development. J. Emerg. Technol. Innov. Res. 8(3).
10. V Hassija, V Chamola, V Saxena, et al. (2019) A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. IEEE Access. 7: 82721-82743.
11. Stiller E. Schiller, C Schmitt. (2021) An Overview of Network Communication Technologies for IoT. Handb. Internet-of-Things. 1-31.
12. B Gupta. M Quamara. An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. Concurr. Comput. Pract. Exp. 32(21): 1-24.
13. S Abdul-qawy, PJ Pramod, E Magesh, et al. (2015) Internet of Things (IoT): An Overview. In: 3rd International Conference on Advances in Engineering Sciences and Applied Mathematics (ICAESAM'2015), March 23-24, 2015 London (UK), International Institute of Engineers. 71-82.
14. WY Choi. (2021) Energy-efficient MAC protocol for wireless LANs with WiFi sensors. J. Electr. Eng. 72(5): 352-355.
15. VS Thokala. A Comparative Study of Data Integrity and Redundancy in Distributed Databases for Web Applications. Int. J. Res. Anal. Rev. 8(4): 383-390, 2021.
16. SSS Neeli. (2023) Critical Cybersecurity Strategies for Database Protection against Cyber Attacks. J. Artif. Intell. Mach. Learn. Data Sci. 1(1): 2102-2106.
17. W Shang, Y Yu, R Droms, et al. (2016) Challenges in IoT Networking via TCP / IP Architecture. NDN Tech. 1-7.
18. PV Dudhe, NV Kadam, RM Hushangabade, et al. Internet of Things (IOT): An overview and its applications. In: 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS). IEEE. 2650-2653.
19. A Verma, V Ranga. (2020) Security of RPL Based 6LoWPAN Networks in the Internet of Things: A Review. IEEE Sens. J. 20(11): 5666-5690.
20. Z Ullah, S Ahmad, M Ahmad, et al. (2019) A Preview on Internet of Things (IOT) and its Applications. 2019 2nd Int. Conf. Comput. Math. Eng. Technol. iCoMET 1623-1630.
21. M Aboubakar, M Kellil, P Roux. (2022) A review of IoT network management: Current status and perspectives. Journal of King Saud University - Computer and Information Sciences. 34(7): 4163-4176.
22. JW Kim, J Barrado, DK Jeon. An Energy-Efficient Transmission Scheme for Real-Time Data in Wireless Sensor Networks. Sensors. 15(5): 11628-11652.
23. HS Chandu. (2022) A Survey of Memory Controller Architectures: Design Trends and Performance Trade-offs. Int. J. Res. Anal. Rev. 9(4): 930-936.
24. G Montenegro, N Kushalnagar, J Hui, et al. (2007) Transmission of IPv6 Packets over IEEE. 802.15.4 Networks.
25. SS Mathew, Y Atif, QZ Sheng, et al. (2013) The Web of Things - Challenges and Enabling Technologies. In Studies in Computational Intelligence. 1-23.
26. LML Oliveira, JJC Rodrigues, AF De Sousa, et al. (2013) A Network Access Control Framework for 6LoWPAN Networks. Sensors. 13(1): 1210-1230.
27. BR Al-Kaseem, Y Al-Dunainawi, HS Al-Raweshidy. (2019) End-to-End Delay Enhancement in 6LoWPAN Testbed Using Programmable Network Concepts. IEEE Internet Things J. 6(2): 3070-3086.
28. Z Shelby. C Bormann. (2009) 6LoWPAN: The Wireless Embedded Internet. Wiley Telecom. 12-44.
29. M Tanveer, G Abbas, ZH Abbas, et al. LAKE-6SH: Lightweight User Authenticated Key Exchange for 6LoWPAN-Based Smart Homes. IEEE Internet Things J. 9(4): 2578-2591.
30. V Abhinaya, B Sudhakar. (2021) A secure routing protocol for low power and lossy networks based 6LoWPAN networks to mitigate DIS flooding attacks. J. Ambient Intell. Humaniz. Comput.
31. M Talau, TA Herek, M Fonseca, et al. Improving TCP performance over a common IoT scenario using the Early Window Tailoring method. Comput. Networks. 234: 109875.
32. M Kim, SK Lim, JD Jeong, et al. (2022) 6LoWPAN Over Optical Wireless Communications for IPv6 Transport in Internet of Things Networks. IEEE Wirel. Commun. Lett. 11(6): 1142-1145.
33. Y Setiawan, SN Hertiana, RM Negara. (2021) 6LoWPAN Performance Analysis of IoT Software-Defined-Network-Based Using Mininet-Io. In: 2020

IEEE International Conference on Internet of Things and Intelligence System (IoTaIS). IEEE. 60-65.
34. SO Ooko, J Kadammanja, MG Uwizeye, et al. Security Issues in IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN): A Review. In: 2020 21st International Arab Conference on Information Technology (ACIT). IEEE. 1-5.
35. Z Yang, CH Chang. (2019) 6LoWPAN Overview and Implementations. In: Proceedings of the 2019 International Conference on Embedded Wireless Systems and Networks, in EWSN ’19. USA: Junction Publishing. 357-361.
36. Narayana T, Sharma, RC Veeturi. (2018) A comprehensive analysis of 6LoWPAN for IoT. Int. J. Res. Trends Innov. 3(8): 2018.