IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

STUDY ON WIRELESS TECHNIQUES IN NETWORKING

[1]J. Joselin, [2]C. Aishwarya, [3]V. Prateeksha, [4]A. Robin Anto, [5]S. Kiruthick
[1]Associate Professor, [2,3,4,5]BCA Students
[1,2,3,4,5]Dept. of Computer Applications, Sri Krishna Arts and Science College, Coimbatore, India.

Abstract: In an era defined by connectivity, the significance of networking technologies, both wired and wireless, has become paramount. The seamless transmission of data has transcended mere convenience to become a fundamental necessity across various domains. Recognizing this evolving landscape, our study delves into the intricate realm of wireless communication technologies, offering a comprehensive analysis of their characteristics, functionalities, and applications. Wireless networking factors in consideration such as range, mobility, and the diverse array of hardware components required to establish a functional wireless network. Wireless technology facilitates the transmission of information through free space, utilizing electromagnetic waves such as radio frequencies, infrared, and satellite signals to propagate data from one point to another. Data transmission is integral to virtually every application or system, necessitating efficient processing and evaluation. Various wireless technologies fulfill this fundamental purpose, each offering unique characteristics and advantages. Our research aims to dissect these technologies, exploring their unique features, strengths, and limitations. By providing a comparative analysis, we seek to empower decision-makers with the knowledge necessary to select the most suitable wireless solution for their specific needs. Moreover, we underscore the critical importance of security in wireless networks, offering practical recommendations to fortify against potential threats and vulnerabilities.

Keywords - WLAN, Wi-fi, Security, Zig bee, Bluetooth.

1. INTRODUCTION

Wireless communication technology has evolved since its introduction in the 19th century, becoming one of the most vital means of transmitting information between devices. This technology allows for the transmission of data through the air, utilizing electromagnetic waves like IR, RF, and satellite signals, eliminating the need for cables or wires. Today, wireless communication encompasses a diverse range of devices and technologies, including smartphones, computers, tablets, laptops, Bluetooth, and printers. Telecommunication has become an integral part of daily life, contributing significantly to advancements in various fields. An emerging mode in wireless communication is Wireless broadband technology, which transmits multiplexed information across a wide band of frequencies. The deployment of Wireless broadband services considers factors such as geographical population density and bandwidth limitations. Designed to overcome the limitations and obstacles posed by cables, wireless technologies offer greater convenience compared to wired networking. Wi-Fi technology has made significant strides in providing faster wireless access to internet applications and data across radio networks, surpassing conventional modem speeds. Utilizing radio bands such as 2.4GHz and 5GHz, Wi-Fi technology relies on wireless hardware such as Ethernet protocol and CSMA for operation. Like other communication networks, Wi-Fi involves a transmitter (Wireless Router/Hotspot) and receiver, which can be any Wi-Fi-enabled device such as a laptop, mobile phone, or tablet.

2. CHARACTERISTICS OF WIRELESS TECHNOLOGY

Wireless technology encompasses a range of characteristics that distinguish it from traditional wired communication methods. Here are some key characteristics of wireless technology.

1. **Mobility:** Wireless technology enables users to access communication networks and services without being physically tethered to a fixed location. This mobility allows for greater flexibility and convenience in accessing information and resources.
2. **Flexibility:** Wireless networks can be deployed in various environments and configurations, adapting to different spatial constraints and user requirements. This flexibility facilitates the implementation of diverse applications and services.
3. **Scalability:** Wireless networks can easily accommodate changes in network size and capacity, allowing for seamless expansion or contraction based on evolving demands. This scalability is particularly beneficial in dynamic environments with fluctuating user populations or data traffic.
4. **Accessibility**: Wireless technology enhances accessibility by extending network coverage to remote or hard-to-reach areas where wired infrastructure may be impractical or cost-prohibitive. This accessibility promotes digital inclusion and connectivity for underserved populations.
5. **Reliability:** Despite potential challenges such as signal interference or environmental factors, wireless networks strive to maintain reliable communication services. Advanced protocols and technologies are employed to mitigate disruptions and ensure consistent performance.
6. **Security:** Ensuring the security of wireless communication is paramount to protect sensitive data and prevent unauthorized access. Encryption, authentication mechanisms, and other security protocols are implemented to safeguard wireless networks against potential threats and vulnerabilities.
7. **Speed and Bandwidth:** Wireless technology continues to advance, offering higher data transmission speeds and increased bandwidth capacity. This enables the delivery of bandwidth-intensive applications such as streaming media, online gaming, and cloud-based services.

2.1 Objective

The objective of this paper is to provide a comprehensive comparative analysis of various wireless communication technologies, exploring their characteristics, functionalities, and applications. By examining the strengths and weaknesses of each technology, this paper aims to assist readers in selecting the most suitable wireless solution based on specific requirements. Additionally, the paper seeks to offer recommendations for securing wireless networks, highlighting essential practices and protocols to mitigate potential risks and vulnerabilities.

3. METHODS AND TECHNOLOGY ITS TYPES

1. Bluetooth

Bluetooth technology facilitates wireless connectivity between a diverse range of electronic devices, enabling seamless data transfer and sharing. Its primary function revolves around establishing connections for the exchange of information between devices. For instance, Bluetooth enables the linkage of cell phones to hands-free earpieces, wireless keyboards, mice, and microphones with laptops, facilitating efficient communication and interaction as shown in figure 1. With its versatility, Bluetooth serves numerous functions and holds a prominent position in the wireless communications market. Bluetooth is standardized under the IEEE 802.15.1 standard, primarily utilized for short-range communication purposes. Operating within the frequency range of 2.4 to 2.485 GHz in the ISM band, it allocates 79 channels separated by 1 MHz each. Data transmission occurs in packet form, employing Frequency Hopping Spread Spectrum (FHSS) for efficient communication [1]. Notably, Bluetooth technology boasts low power consumption, affordability, and straightforward functionality. Functioning on a "Master-Slave" principle, communication initiation relies on the Master device. Each device possesses a unique Global ID exchanged during connection establishment. The latest iterations, Bluetooth Low Energy (BLE) and Bluetooth 4.0, significantly reduce power

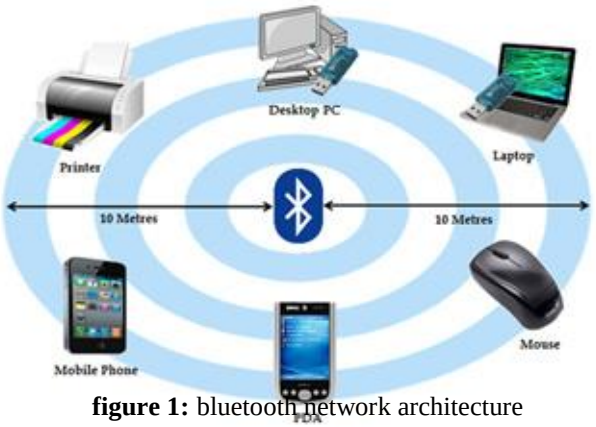


figure 1: bluetooth network architecture

consumption. These advancements have led to the integration of Bluetooth technology in diverse applications such as healthcare, security, and fitness. Although occasional pairing errors may occur, Bluetooth technology continues to find extensive application in wireless networking between devices and peripherals such as mice, keyboards, headsets, media transfer, wireless control, and data logging equipment [8].

2. **ZigBee**

ZigBee stands out as a wireless communication standard tailored specifically to cater to the distinctive requirements of low-power, cost-effective wireless sensor, and control networks. Its versatility allows for implementation in a wide array of environments, owing to its straightforward integration and minimal power consumption. Developed with a focus on facilitating data communication, particularly from sensors, ZigBee boasts a simple, yet efficient structure tailored to meet these communication demands. In industrial and medical applications, there arises a requirement for a medium capable of low data transfer rates. To address this need, the Zigbee alliance introduced the IEEE 802.15.4 standard. Unlike Bluetooth and Wi-Fi, which excel in transferring large data files such as media, Zigbee is ideally suited for scenarios where communication occurs sporadically, involves smaller packet sizes, and emphasizes minimal power consumption [5]. Zigbee operates within unlicensed bands at frequencies of 2.4 GHz, 900 MHz, and 868 MHz, relying on radio standards. However, its range is limited to 10 to 100 meters due to its low power and data rate capabilities, which stand at 250 kbps. Nonetheless, its energy efficiency translates to prolonged battery life [9]. Employing Direct Sequence Spread Spectrum (DSSS), Zigbee ensures minimal latency, a notable feature enhanced by its support for mesh networking. In this topology, every node can self-locate, and a routing table enables nodes to select the most optimal communication path. Through ad-hoc routing and mesh topology, Zigbee enhances stability, supporting up to 65,000 nodes in network topology. It offers various network configurations, including point-to-point, point-to-multipoint, mesh, and "Personal Area Network" (PAN). Moreover, Zigbee provides robust security features, employing 128-bit encryption to safeguard against data collision, interference, and unauthorized access. Widely utilized in automated meter reading (AMR), industrial sensor networking, medical devices, lighting control, and building automation, Zigbee's affordability and prolonged battery life make it a preferred choice for diverse applications.

3. **Wireless Fidelity**

Wireless networking technologies facilitate the connection of multiple computers. Wireless local area network (WLAN), which falls under the category of Wi-Fi. Wireless Fidelity (Wi-Fi), governed by the IEEE 802.11 standard, is commonly referred to as Wireless Local Area Network (WLAN). It serves as a protocol facilitating wireless connectivity, enabling devices to access the internet and connect to wired networks. Operating with a range typically exceeding 100 meters, Wi-Fi operates on either the 2.4 GHz or 5 GHz frequency bands, both of which fall within the freely available ISM band. Utilizing radio waves, Wi-Fi facilitates wireless communication and internet access among devices. Establishing Wi-Fi communication requires two essential devices: a Wireless adapter and a Wireless router. Notably [8], identified three key security standards employed in Wi-Fi networks: Wireless Equivalent Privacy (WEP), which utilizes 40- or 104-bit encryption, WPA (Wi-Fi Protected Access), and WPA-2 (Wi-Fi Protected Access-2), employing 128-bit encryption methods. The utilization of high-frequency 2.4 or 5 GHz bands allows Wi-Fi to accommodate larger data transmissions. Wi-Fi technology serves various purposes, including internet sharing, file sharing, and resource sharing among devices, making it a versatile solution for connectivity needs. It facilitates WLAN integration with other network components such as LAN, MAN, WAN, and

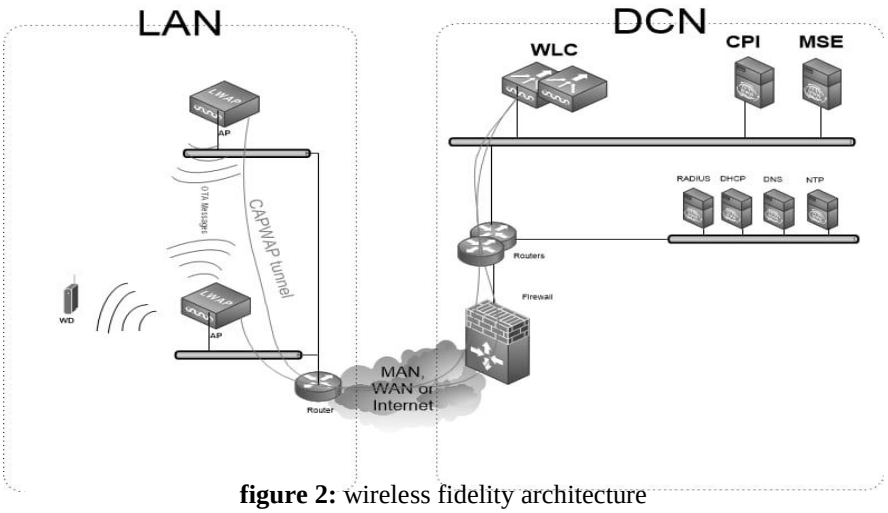


figure 2: wireless fidelity architecture

DCN, ensuring adherence to end-to-end application QoS and Security Service Level Agreements (SLAs). Figure 2 illustrates an example of this architecture.

4. Near Field Communication

Near Field Communication (NFC) represents a wireless technology enabling seamless interaction between mobile devices. Operating within an extremely short range, NFC facilitates data exchange between devices situated within 4 cm of each other. Functioning at a frequency of 13.56 MHz within the unlicensed ISM radio frequency band, NFC provides data transfer speeds that vary between 106 and 424 kbps. This technology serves as an ideal platform for recognition protocols that authenticate secure data transfer. NFC operates in three modes: Card emulation allows a smartphone to replicate the functionality of a smart card for conducting payment transactions; Reader/writer mode, enabling smartphones to read or write NFC tags as shown in figure 3 and Peer-to-peer mode, facilitating direct interaction and data exchange between two NFC-enabled devices.

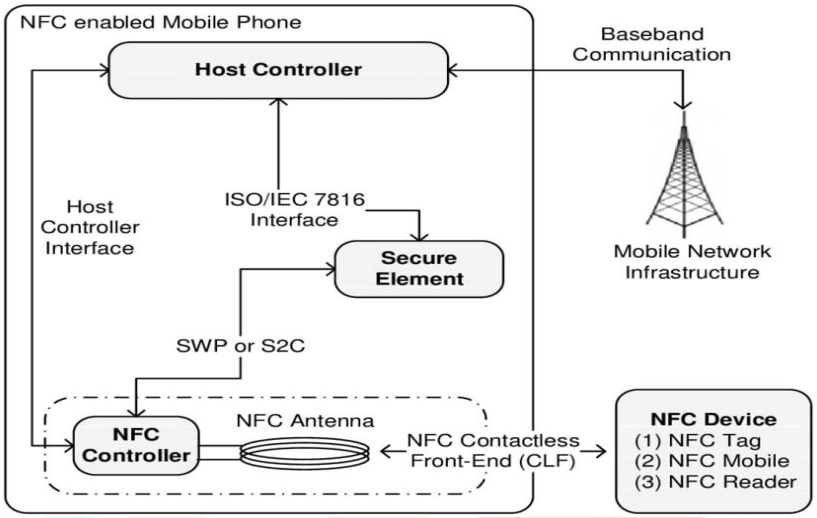


figure 3: near field communication

Figure 3: Near Field Communication Architecture

5. Ultra-Wideband

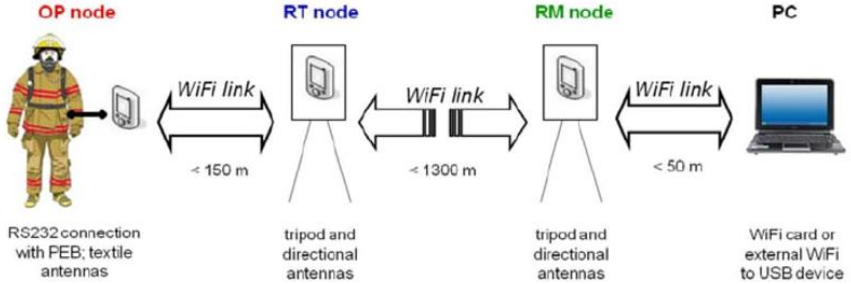
Ultra-Wideband (UWB) technology, with its extensive bandwidth and low power spectral density, enables the transmission of data across a wide spectrum. Operating within the frequency range of 3.1 to 10.6 GHz, UWB facilitates spectrum sharing and serves as a high-rate personal area network (PAN). Known as pulse radio, UWB modulates amplitude, frequency, or phase to transmit data in discrete time intervals. Its spatial capacity, estimated at approximately 10^13 bits per square meter, makes it particularly suitable for radar imaging techniques, while also proving useful in short-range indoor applications [3].

6. Wireless Body Area Network

Wireless Body Area Network (WBAN), standardized under IEEE 802.15.6, is primarily designed for low-power, short-range, and highly reliable applications in the medical and healthcare sectors. Utilizing the ISM band (Industrial, scientific and medical) and other frequency bands allocated for medical purposes, WBAN ensures data transfer rates of approximately 10 Mbps. Operating within a range of 2-5 meters, WBAN supports up to 256 nodes and adopts a star network topology for communication. A crucial layer utilized in WBAN for data communication is the MAC layer. This technology enables the timely transmission of notifications before the occurrence of a heart attack, based on changes in vital signs, and facilitates insulin injection for diabetic patients. WBAN integrates three tiers of security: unencrypted communication (level 0), authentication without encryption (level 1), and authentication with encryption (level 2). For communication to commence, both the host and node must align at the same security level, generating a temporary key for each session to guarantee one-time functionality.

7. Long Range

Long Range (LoRa) represents a wireless communications system with an emphasis on extended range. It targets applications involving long-lasting battery-powered devices, prioritizing energy efficiency. LoRa



consists of two separate layers: one is a physical layer utilizing the Chirp Spread Spectrum (CSS) radio modulation technique, and the other is a MAC layer protocol called LoRaWAN. The LoRa physical layer facilitates long-range, low-power, and low-throughput communications. Operating on the 433-, 868-, or 915-MHz ISM bands, its frequency varies depending on the deployment region. Each transmission can carry a payload ranging from 2 to 255 octets, with data rates reaching up to 50 Kbps through channel aggregation. The modulation technique is proprietary and developed by Semtech. LoRaWAN serves as a medium access control mechanism, enabling numerous end-devices to communicate with a gateway utilizing the LoRa modulation. Although the LoRa modulation remains proprietary, the development of LoRaWAN is being undertaken as an open standard by the LoRa Alliance [4]. An outline of the nodes' configuration is depicted in Figure 4. All three nodes utilize identical hardware platforms, consisting of an ALIX3c2 single-board computer featuring a 500 MHz AMD Geode LX CPU, 256 Megabytes of RAM, 2 mini-PCI slots, one RS232 serial port, and a 1 Gb compact flash.

8. **Infrared**

This technology utilizes infrared radiation for communication, requiring an infrared port for transmitting data and reception. Offering bi-directional communication, it operates within a range of approximately 1 to 10 meters and delivers data rates of about 4 Mbps. Notably, infrared technology is characterized by its cost-effectiveness, low power consumption, high security, portability, immunity to noise, and simple circuitry. However, it also possesses limitations; line of sight communication is essential, with obstacles potentially causing interference and communication failure. Furthermore, it's restricted to short-range communication and susceptible to environmental factors such as light, climate, and atmospheric conditions. Typically employed in TV remote controls and budget-friendly mobile handsets.

9. **Light Fidelity**

Light Fidelity (Li-Fi) operates on Visible Light Communication (VLC) principles, utilizing LED light bulbs whose intensity rapidly fluctuates to transmit data. VLC employs visible light wavelengths ranging from 400 THz (780 nm) and 800 THz (375 nm) for both data transmission and illumination purposes. By employing high-speed LEDs with efficient multiplexing techniques, data rates exceeding achieving 100 Mbps is possible. Additionally, parallel data transmission via LED arrays, where each LED transmits independently data stream, can further enhance the Visible Light Communication data rate. Despite requiring the lights to remain on for data transmission, dimming them is possible to a level imperceptible to humans while still capable of data transmission. This technology provides a broad unlicensed bandwidth, making it suitable for a range of applications such as video and music streaming, internet connectivity for both mobile and stationary devices, and more [6]. All this process is implemented in Li – Fi as shown in figure 5.

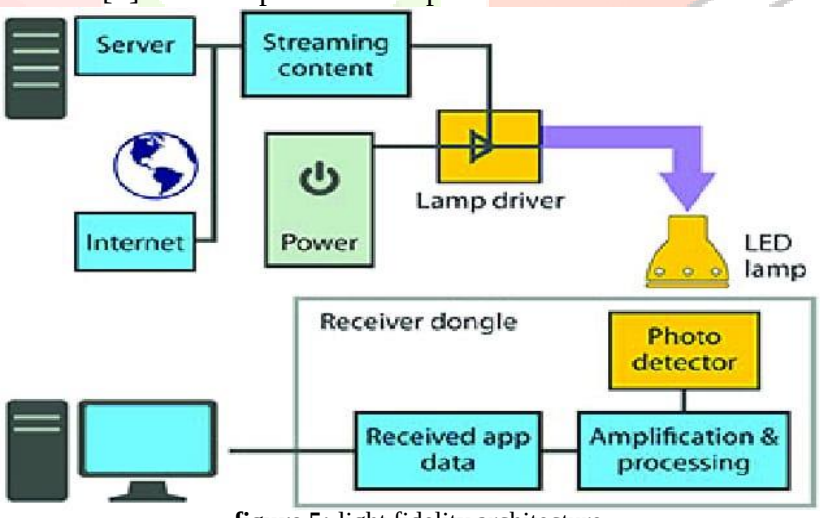


figure 5: light fidelity architecture

10. **Dedicated Short-Range Communication**

The Dedicated Short-Range Communication (DSRC), developed and functions as a multi-channel wireless protocol operating within a 75MHz licensed spectrum, spanning from 5.850 to 5.925 GHz. Originally intended for indoor WLAN with limited mobility, DSRC based on 802.11p is gaining traction as a potential wireless technology to enhance transportation safety and highway efficiency. Its operation within a rigorous environment demands fast communication to sustain connections with rapidly moving vehicles in real-time, thereby upholding stringent quality of service requirements. DSRC prioritizes minimal transmission power usage while ensuring privacy and anonymity. Its applications span various domains, including IntelliDrive, cooperative intersection collision avoidance systems (CICAS), electronic toll collection, and transit or emergency vehicle signal priority, among others [10].

11. Long-Term Evolution

Long-Term Evolution (LTE), as standardized by the 3rd Generation Partnership Project (3GPP), represents a highly adaptable radio interface. The initial release of LTE delivers peak rates of 300 Mbps, with a radio-network delay of less than 5 ms, marking a substantial improvement in spectrum efficiency over preceding cellular systems. It introduces a novel flat radio-network architecture aimed at streamlining operations and reducing costs. LTE accommodates both frequency-division duplex (FDD) and time-division duplex (TDD), supporting a diverse Range of bandwidths within the system to operate across various spectrum allocations. The radio link control (RLC) and medium access control (MAC) layers manage retransmission handling and data flow multiplexing, among other functions. At the physical layer, data to be transmitted undergoes turbo coding and modulation employing one of three methods: quadrature-phase shift keying (QPSK), 16-Quadrature Amplitude Modulation, or 64- Quadrature Amplitude Modulation, orthogonal frequency-division multiplexing (OFDM) modulation. The subcarrier spacing is set at 15 kHz, with provisions for two cyclic-prefix lengths in both uplink and downlink transmissions: a standard cyclic prefix of 4.7 μs, suitable for most scenarios, and an extended cyclic prefix of 16.7 μs, designed for highly dispersive environments [7].

4. SOLUTIONS BASED ON RESEARCH

4.1 Recommendations for Secured Wireless Networks

Maintain a comprehensive understanding of the wireless network's topology. Properly label and maintain inventories of deployed wireless and handheld devices. Regularly back up data to mitigate potential loss. Conduct routine security testing, audits, and assessments of the wireless network. Before acquiring wireless technologies, conduct a thorough risk assessment, develop a security policy, and establish security requirements. Implement security management practices and controls to ensure the secure operation of wireless networks following meticulous installation. Ensure that the information system security policy explicitly addresses the utilization of 802.11, Bluetooth, and other wireless technologies. Utilize configuration/change control and management practices to ensure that all equipment is updated with the latest software releases, including security enhancements and patches for identified vulnerabilities. Enforce standardized configurations to align with security policies and promote consistency in operations while ensuring the alteration of default values. Provide security training to enhance awareness of potential threats and vulnerabilities associated with wireless technologies. Employ robust cryptography to safeguard data transmitted over the radio channel, considering equipment theft as a significant concern.

5. CONCLUSION

This paper thoroughly examines various wireless communication technologies, detailing their functionalities and applications. It emphasizes the significance of robust security measures to protect against potential threats, offering practical recommendations for network administrators. By providing insights into the strengths and limitations of each technology, the paper serves as a valuable resource for decision-makers seeking to optimize wireless solutions effectively.

6. REFERENCE

[1] Rajeev, S., & Brent, A. M. (2000). The Bluetooth Technology: Merits and Limitations. ICPWC, 80-84.

[2] Agrawal, P., & Sharad, B. (2016). Near field communication. SETLabs Bridfings, 67-74.

[3] Aiello, G. R., & Gerald, D. R. (2003). Ultra-wideband wireless systems. Microwave Magazine, 36-47.

[4] Aloÿs, A., Jiazi, Y., Thomas, C., & William, M. T. (2016). A Study of LoRa: Long Range & Low Power Networks for the Internet of Things. Sensors, 1-18. doi:10.3390/s16091466

[5] Andreas, W., Kirsten, M., & Adam, W. (2005). Wireless Technology in Industrial Networks. IEEE, 93(6), 1130-1151.

[6] Anurag, S., Shalabh, A. (., & Asoke, N. (. (2015). Li-Fi Technology: Data Transmission through Visible Light. International Journal of Advance Research in Computer Science and Management Studies, 3(6), 1-12.

[7] David, A., Erik, D., Anders, F., Ylva, J., Magnus, L., & Stefan, P. (2009). LTE: The Evolution of Mobile Broadband. IEEE Communications Magazine, 44-51.

[8] Deepan, B., Himanshu, P., & Hardik, M. (2016). Emerging Wireless Technologies: A Comparative Analysis. Journal of Emerging Technologies and Innovative Research (JETIR), 3(4), 300-304

[9] Fotouhi, G. M., Vahabi, M., Rasid, M. F., & Raja, A. R. (2008). Energy Efficiency in MAC 802.15.4 for Wireless Sensor Networks. IEEE 2008 6th National Conference on Telecommunication Technologies (pp. 289- 294). IEEE.

[10] Habib, S., Hanna, M. A., Javadi, M. S., Samad, S. A., Muad, A. M., & Hussain, A. (2013). Intervehicle wireless communication technologies, issues and challenges. Information Technology Journal, 12(4), 558-568. doi:10.3923/itj.2013.558.568