Study on wireless techniques in networking

Mr. Ayan Mukherjee
Assistant Professor
Department of Computer Science & Engineering
NSHM Knowledge Campus, Durgapur, West Bengal, India

I) Abstract:

In a time when connectivity is king, networking technologies—wired and wireless—have become critical. Data transmission that is seamless is now essential in many fields and goes beyond simple convenience. Given this dynamic environment, our research explores the complex world of wireless communication technologies, providing a thorough examination of their features, capabilities, and uses. considerations for wireless networking, including mobility, range, and the wide variety of hardware needed to set up a working network. Using electromagnetic waves like radio frequencies, infrared, and satellite signals, wireless technology makes it easier to send data across open space. Almost all systems and applications rely on data transmission, which calls for effective processing and analysis. different wireless technologies.

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

II) OVERVIEW

Since its inception in the 19th century, wireless communication technology has developed into one of the most important forms of information transfer between devices. Without the use of cables or wires, this technology enables data transmission through the air using electromagnetic waves such as infrared, radio frequency, and satellite signals. These days, a wide variety of gadgets and technologies fall under the umbrella of wireless communication, such as printers, smartphones, laptops, tablets, PCs, and Bluetooth. Since it has become a necessary component of everyday life, telecommunication has greatly advanced many different fields. Wireless broadband technology is a new wireless communication mode that sends multiplexed data over a broad frequency range. When implementing wireless broadband services, variables like geographic population density and bandwidth constraints are taken into account. Wireless is intended to get around the restrictions and challenges that come with cables.

III) CHARACTERISTICS OF WIRELESS TECHNOLOGY: -

The various features that set wireless technology apart from conventional wired communication techniques are as follows. Key features of wireless technology include the following.

1. **Mobility:** Without being physically tied to a single place, wireless technology allows users to access communication networks and services. Access to resources and information is made more flexible and convenient by this mobility.

2. **Flexibility:** Depending on the user's needs and the available space, wireless networks can be set up in a variety of settings. Diverse applications and services can be implemented more easily thanks to this flexibility.

3.**Scalability:** Wireless networks can readily adapt to variations in network capacity and size, enabling seamless growth or shrinkage in response to changing needs. When user populations or data traffic fluctuate in dynamic environments, this scalability is especially advantageous.

4.**Enhancement of Accessibility:** Wireless technology expands network coverage to hard-to-reach or remote locations where wired infrastructure might be prohibitively expensive or impractical. For underserved populations, this accessibility encourages digital inclusion and connectedness.

5.**Reliability:** Wireless networks work to maintain dependable communication services in spite of possible obstacles like environmental factors or signal interference. Advanced technologies and protocols are used to guarantee consistent performance and minimize interruptions.

6.**Security:** Wireless communication security must be guaranteed in order to safeguard private information and stop illegal access. Security protocols such as encryption and authentication are used to protect wireless networks from possible dangers and weaknesses.

7. **Bandwidth and Speed:** As wireless technology develops, it can transmit data at faster rates and with more bandwidth. This makes it possible for bandwidth-demanding applications like cloud-based services, online gaming, and streaming media to be delivered.

IV) Objective: -

In order to better understand the features, capabilities, and applications of different wireless communication technologies, this paper will compare and contrast them in detail. In order to help readers, choose the best wireless solution based on particular needs, this paper will analyse the advantages and disadvantages of each technology. Furthermore, by emphasizing crucial procedures and guidelines to reduce potential risks and vulnerabilities, the paper aims to provide suggestions for safeguarding wireless networks.

V) METHODS AND TECHNOLOGY ITS TYPES:

1. Bluetooth:

Bluetooth technology makes it possible for a wide variety of electronic devices to connect wirelessly, allowing for seamless data sharing and transfer. The establishment of connections for the purpose of information exchange between devices is its main function. As illustrated in figure 1, Bluetooth, for example, makes it possible to connect cell phones to wireless keyboards, mice, microphones, and hands-free earpieces with laptops, promoting effective communication and interaction. Due to its adaptability, Bluetooth has many uses and is widely used in the wireless communications industry. The IEEE 802.15 standard governs Bluetooth. 1 standard, which is mostly used for close-quarters communication. It allots 79 channels, each separated by 1 MHz, and operates in the ISM band between 2.4 and 2.485 GHz. Utilizing Frequency Hopping Spread Spectrum (FHSS) for effective communication, data is transmitted in packet form. Bluetooth technology is notable for its low cost.

2. ZigBee:

ZigBee is a wireless communication protocol designed to meet the specific demands of low-power and cost-efficient wireless sensor and control systems. Its adaptability and low energy usage make it suitable for diverse applications across different environments. Built primarily for sensor-based data exchange, ZigBee features a simple yet powerful architecture optimized for such communication tasks.

In industrial and healthcare domains, where low data rate transmission is essential, the ZigBee Alliance introduced the IEEE 802.15.4 standard to meet these requirements. Unlike Bluetooth and Wi-Fi—technologies optimized for transmitting large media files—ZigBee focuses on low-speed, low-power communication involving small data packets and intermittent transmissions [5]. It functions in unlicensed frequency bands such as 2.4 GHz, 900 MHz, and 868 MHz. Although its range is limited to around 10–100 meters and its maximum data rate is 250 kbps, its high energy efficiency contributes to extended battery life.

ZigBee utilizes Direct Sequence Spread Spectrum (DSSS) technology, which minimizes latency and improves communication reliability. Its mesh networking capability allows each node to determine its location autonomously, while routing tables enable nodes to select optimal communication paths. This ad-hoc routing approach enhances network resilience, allowing support for up to 65,000 nodes. The network can be configured in multiple topologies, such as point-to-point, point-to-multipoint, mesh, or Personal Area Network (PAN).

Security is another strong aspect of ZigBee, as it employs 128-bit encryption to prevent data collisions, interference, and unauthorized access. Due to its low cost, scalability, and energy-efficient operation, ZigBee has become a popular choice for a wide range of applications, including automated meter reading (AMR), industrial sensor networks, medical monitoring devices, lighting systems, and building automation.

3. Wireless Fidelity:

Several computers can be connected more easily thanks to wireless networking technologies. One subset of Wi-Fi is wireless local area networks, or WLANs. The IEEE802.11 standard governs Wireless Fidelity (Wi-Fi), which is also known as Wireless Local Area Network (WLAN). It functions as a protocol that makes wireless connectivity possible, allowing devices to connect to wired networks and the internet. Wi-Fi operates on either the 2 GHz or 4 GHz frequency bands, both of which are part of the open ISM band, and has a range of usually more than 100 meters. Wi-Fi enables wireless internet access and communication between devices by using radio waves. Two key components are needed to establish Wi-Fi communication: a wireless router and an adapter. Notably, [8] identified three important security standards used in Wi-Fi networks: WPA (Wi-Fi Protected Access), WPA-2 (Wi-Fi Prote), and Wireless Equivalent Privacy (WEP), which uses 40- or 104-bit encryption.

4. Near Field Communication:

One wireless technology that makes it possible for mobile devices to interact with each other seamlessly is called near field communication, or NFC. With its incredibly short operating range, NFC allows data transfer between devices that are only 4 cm apart. NFC offers data transfer rates ranging from 106 to 424 kbps and operates at a frequency of 13.56 MHz in the unlicensed ISM radiofrequency band. The recognition protocols that authenticate secure data transfer are perfectly suited to this technology. NFC functions in three ways: reader/writer mode, which enables smartphones to read or write NFC tags as illustrated in Figure 3; card emulation, which enables a smartphone to mimic the functionality of a smart card for payment transactions; and peer-to-peer mode, which enables direct communication and data exchange between two NFC-enabled devices.

5. Ultra-Wideband:

With its large bandwidth and low power spectral density, Ultra-Wideband (UWB) technology makes it possible to send data over a broad spectrum. Operating between 3.1 and 10.6 GHz, UWB functions as a high-rate personal area network (PAN) and makes spectrum sharing easier. In order to send data in distinct time intervals, UWB modulates amplitude, frequency, or phase. This technique is called pulse radio. Because of its spatial capacity, which is estimated to be around 10^13 bits per square meter, it is especially well-suited for radar imaging techniques and also works well for short-range indoor applications.

6. Wireless Body Area Network:

An IEEE 802.15 standard is the Wireless Body Area Network (WBAN). 6. is mainly made for reliable, short-range, low-power applications in the healthcare and medical industries. With WBAN, data transfer rates of roughly 10 Mbps are guaranteed by using the ISM band (Industrial, Scientific and Medical) and additional frequency bands designated for medical applications. Working within a 2–5 m range, WBAN uses a star network topology for communication and supports up to 256 nodes. The MAC layer is an essential layer used for data communication in WBAN. This technology helps diabetic patients receive insulin injections and allows timely notifications to be sent before a heart attack occurs based on changes in vital signs. WBAN incorporates three security tiers: level 0 (unencrypted communication), level 1 (unencrypted authentication), and level 2 (encrypted authentication). Both the node and the host must line up at the same time for communication to begin.

7. Long Range:

Long Range (LoRa) is a wireless communications system that prioritizes long-range communication. It prioritizes energy efficiency and targets applications involving devices that run on long-lasting batteries. Two distinct layers make up LoRa: a MAC layer protocol known as LoraWAN and a physical layer that uses the Chirp Spread Spectrum (CSS) radio modulation technique. Low-power, low-throughput, long-range communications are made possible by the LoRa physical layer. It operates on the ISM bands at 433, 868, or 915 MHz; the frequency varies based on the deployment region. Data rates can reach up to 50 Kbps through channel aggregation, and each transmission can carry a payload of 2–255 octets. The modulation method was created by Semtech and is proprietary. By acting as a medium access control mechanism, LoRaWAN allows a large number of end devices to connect to a gateway that uses the LoRa module. However, the development of LoRa modulation is still proprietary.

8. Infrared:

This technology requires an infrared port in order to transmit and receive data because it uses infrared radiation for communication. It provides data rates of roughly 4 Mbps, operates within a range of roughly 1 to 10 meters, and allows bi-directional communication. The cost-effectiveness, low power consumption, high security, portability, noise immunity, and straightforward circuitry of infrared technology are noteworthy features. It does have certain drawbacks, though; communication must be in line of sight, and obstructions may result in interference and poor communication. In addition, it can only communicate over short distances and is influenced by atmospheric conditions, light, and climate. often found in inexpensive mobile phones and TV remote controls.

9. Light Fidelity:

Light Fidelity (Li-Fi) uses LED light bulbs with rapidly changing intensities to transmit data, based on the principles of Visible Light Communication (VLC). For data transmission and illumination, VLC uses visible light wavelengths between 400 THz (780 nm) and 800 THz (375 nm). It is possible to achieve data rates higher than 100 Mbps by using high-speed LEDs with effective multiplexing techniques. Further increasing the Visible Light Communication data rate is possible through parallel data transmission using LED arrays, in which each LED sends a separate data stream. It is possible to dim the lights to a level that is undetectable to humans while still enabling data transmission, even though data transmission requires the lights to stay on. This technology's wide unlicensed bandwidth makes it appropriate for a variety of uses, including streaming music and video, providing internet connectivity for stationary and mobile devices, and more [6]. Every step of this procedure is carried out.

10. Dedicated Short-Range Communication:

Dedicated Short-Range Communication (DSRC) is a multi-channel wireless protocol that operates in a 75MHz licensed spectrum between 5point 850 and 5point 925 GHz. DSRC, which is based on 802.11p, was initially designed for indoor WLANs with restricted mobility. However, it is becoming more and more popular as a possible wireless technology to improve travel safety and highway efficiency. Its operation in a demanding environment necessitates quick communication in order to maintain connections with swiftly moving vehicles in real-time and meet strict quality of service standards. DSRC prioritizes anonymity and privacy while using the least amount of transmission power. Among its many uses are IntelliDrive, electronic toll collection, cooperative intersection collision avoidance systems (CICAS), transit or emergency vehicle signal priority, and more.

11. Long-Term Evolution:

A very flexible radio interface is Long-Term Evolution (LTE), which was standardized by the Third Generation Partnership Project (3GPP). Compared to earlier cellular systems, LTE's initial release offers a significant increase in spectrum efficiency, with peak speeds of 300 Mbps and a radio network delay of less than 5 ms. It presents a cutting-edge flat radio-network architecture designed to simplify operations and cut expenses. Both frequency-division duplex (FDD) and time-division duplex (TDD) are supported by LTE, allowing the system to serve a wide range of bandwidths across different spectrum allocations. The medium access control (MAC) and radio link control (RLC) layers oversee data flow multiplexing and retransmission handling, among other tasks. Using one of three techniques—64-Quadrature Amplitude Modulation, 16-Quadrature Amplitude Modulation, or quadrature-phase shift keying (QPSK)—the data to be transmitted is turbo coded and modulated at the physical layer.

VI) SOLUTIONS BASED ON RESEARCH:

Recommendations for Secured Wireless Networks:

Continue to have a thorough understanding of the topology of the wireless network. Ensure that deployed wireless and handheld devices are appropriately labelled and listed. Make regular data backups to reduce the chance of loss. Perform regular wireless network audits, assessments, and security testing. Do a comprehensive risk assessment, create a security policy, and set security requirements prior to purchasing wireless technologies. Once wireless networks have been installed carefully, put security management procedures and controls in place to guarantee their safe operation. Make sure the information system security policy specifically mentions using Bluetooth, 802.11, and other wireless technologies. Make sure that every piece of equipment has the most recent software updates, including security patches and security enhancements, by using configuration/change control and management procedures. Enforce uniform configurations to support and comply with security guidelines.

Detailed recommendations & how to implement them: -

1) Use modern encryption & authentication

- **What:** Deploy WPA3-Personal (SAE) for homes/small networks and WPA3-Enterprise or 802.1X + AES (CCMP) for corporate networks. Use Opportunistic Wireless Encryption (OWE) for open networks that need privacy.
- **Why:** WPA3 fixes key-recovery and handshake weaknesses present in WPA2 and introduces stronger key exchange (SAE).
- **How:** Upgrade AP firmware and client OSes; avoid transition/dual SSIDs unless required; if using transition mode, plan for staged migration and risk acceptance.

2) Strong authentication & authorization

- **What:** Prefer 802.1X with EAP-TLS (certificate-based) or other strong EAP methods for enterprise access. Use per-device credentials or certificates for IoT/OT where possible.
- **Why:** PSKs are easy to leak and rotate poorly; 802.1X enables per-user/device control and revocation.
- **How:** Deploy a RADIUS server (hardened, redundant), issue device/user certificates or unique credentials, and integrate with identity systems (AD/IdP).

3) Network segmentation & least privilege

- **What:** Put guest Wi-Fi, corporate clients, IoT/OT devices, and management interfaces on separate logical networks (VLANs) with strict firewall rules and ACLs.
- **Why:** Segmentation reduces attack surface and lateral movement if one segment is compromised.
- **How:** Use NAC (Network Access Control) to restrict device posture; enforce inter-VLAN firewalling and micro segmentation for sensitive assets.

4) Harden APs, controllers, and endpoints

- **What:** Disable unused services (e.g., WPS, Telnet), change default admin credentials, enable secure management (HTTPS/SSH), and restrict management plane access to management VLANs.
- **Why:** Default settings are common vectors for compromise; hardening reduces exploitable surface.
- **How:** Apply vendor hardening guides/CIS Benchmarks, remove unnecessary packages, enforce MFA for management accounts.

5) Patch management & device lifecycle

- **What:** Maintain a firmware/OS update program for APs, controllers, and wireless clients; retire unsupported hardware.
- **Why:** Many vulnerabilities are fixed via vendor updates; unsupported devices are persistent risks.

- **How:** Inventory wireless assets, schedule regular updates, test updates in staging, and document rollback plans.

6) Protect IoT & constrained devices

- **What:** Treat IoT/medical/industrial devices as high risk: isolate them, use proxied access to backend systems, avoid default credentials, and apply OWASP IoT guidance for secure development and deployment.
- **How:** Use device gateways that provide protocol translation and security controls, apply strict ACLs, and enforce minimum crypto where supported.

7) Visibility, monitoring & detection

- **What**: Deploy Wireless IDS/IPS, RF spectrum monitoring, and centralized logging for all APs and controllers. Collect 802.11 management frames, authentication events, and RADIUS logs.
- **Why:** Wireless attacks often start with reconnaissance (rogue APs, evil-twin, deauth); detection shortens dwell time.
- How: Use SIEM integration, alarms for rogue APs or abnormal association rates, and periodic RF surveys.

8) Policy, training & incident readiness

- **What:** Define acceptable use, access provisioning/deprovisioning, guest onboarding, and BYOD policies; provide staff training and run incident response drills that include wireless scenarios.
- **Why:** Technology alone won’t stop social engineering or misconfigurations. Policies and rehearsed processes reduce human error and speed response.

VII) Conclusion: -

Data transmission, sharing, and utilization across various domains have been transformed by wireless communication technologies, which have emerged as the foundation of contemporary digital connectivity. This study has looked at the development, traits, and uses of a number of wireless technologies, including Wi-Fi, Bluetooth, ZigBee, NFC, Li-Fi, LoRa, WBAN, DSRC, UWB, and LTE. Each of these technologies has special benefits in terms of energy efficiency, range, bandwidth, and environmental suitability. Low-power solutions like ZigBee, LoRa, and WBAN serve sensor-driven and Internet of Things applications, while Wi-Fi and LTE dominate high-speed, wide-area communication, according to the comparative analysis. Li-Fi and UWB, meanwhile, offer cutting-edge techniques that make use of light and ultra-wide bandwidths to provide faster and more secure transmissions. But as wireless connectivity grows, maintaining security and dependability continues to be a top priority. In order to reduce related risks, this paper highlights.

VIII) Future Scope: -

As wireless technologies advance, more research will be done to achieve greater data throughput, energy efficiency, and seamless interoperability among heterogeneous networks. Wireless systems will be able to achieve optimal performance in real time by integrating machine learning (ML) and artificial intelligence (AI). This will enable dynamic spectrum allocation, automated fault detection, and predictive network management. Emerging paradigms such as 6G communication, Cognitive Radio Networks (CRNs), and Quantum Communication promise to revolutionize wireless connectivity by introducing ultra-low latency, enhanced security, and unprecedented data rates. In order to minimize energy consumption and environmental impact, sustainable wireless communication will prioritize green networking. The convergence of Internet of Things (IoT), Edge Computing, and Cloud Networking will further strengthen automation, smart infrastructure, and personalized user experiences. In the future, studies may also focus on secure IoT frameworks, blockchain-based network authentication, and privacy-preserving data transmission mechanisms. Finally, the continued exploration of hybrid wireless models—combining radio frequency, optical, and satellite-based systems—will drive innovation toward building intelligent, resilient, and universally accessible communication networks.

IX) References: -

[1] wireless channel, modulation, spread-spectrum etc. Useful for understanding basics like FHSS, DSSS, bandwidth, speed trade-offs. Wireless Communications by Andrea Goldsmith.

[2] Bluetooth, WLAN, cellular, mobility, MAC, network/transport layers. *Mobile Communications* (2nd Ed.) by Jochen H. Schiller.

[3] Relevant for ZigBee, WBAN, sensor nodes, energy consumption, routing, topology. Wireless Sensor Networks by Ian F. Akyildiz, Mehmet Can Vuran.

[4] Deep dive specifically on ZigBee: architecture, routing, security, applications. ZigBee Wireless Sensor and Control Network by Elahi, Gschwender.

[5] LoRa/LoraWAN – long range, low power, use cases and limitations. Useful for comparing with Bluetooth/ZigBee etc LoRa Communication Technology for IoT Applications by Luca Leonardi.

[6] data security/privacy in WBAN in IoT contexts. Relevant for your "Security" considerations, "Systematic survey on data security in wireless body area networks in IoT healthcare system" (Frontiers in Medicine, 2024.

[7] protocols and vulnerabilities in WBANs, "Security Analysis of Wireless Body Area Network Protocols: A Survey" (2023).

[8] Bluetooth, WiFi, LiFi, ZigBee etc. in industrial contexts – helps in comparing trade-offs (range, speed, interference etc.), "Survey on Wireless Technologies in Industrial Application" (IJERT, 2017).

[9] Deals with challenges: power, privacy, QoS, MAC, channel models etc, "Technological Requirements and Challenges in Wireless Body Area Networks for Health Monitoring: A Comprehensive Survey".