Wireless IoT Protocol Report

Purpose of the Report

This report aims to guide in selecting wireless communication protocols for IoT devices, focusing on efficiency, cost, scalability, and reliability. We compare WiFi, Bluetooth, Bluetooth LE, Zigbee, Z-Wave, and NFC across various parameters such as range, data rate, power consumption, and security, to aid stakeholders in making informed decisions for IoT applications.

Areas to Investigate

- Protocol Overwiev
- Range
- Power Consumption
- Security
- Other Considerations for IoT

Authors

Simon Thorell, Erik Pettersson, Nathan Tewelde Bahta, Milad Isho Saeb and Abdihakim Abdisamad Roble.

WIFI

Here is some text...

Protocol Overview

- Here is also some variant.
- Here is also some variant.
- Here is also some variant.

Range

Some text...

Power Consumption

Some text...

Security

- Here is also some variant.
- Here is also some variant.

- Here is also some variant.

Other Considerations for IoT

1. List item
2. List item
3. List item

Bluetooth

Here is some text...

Protocol Overview

- Here is also some variant.
- Here is also some variant.
- Here is also some variant.

Range

Some text...

Power Consumption

Some text...

Security

- Here is also some variant.
- Here is also some variant.
- Here is also some variant.

Other Considerations for IoT

1. List item
2. List item
3. List item

Bluetooth LE

Bluetooth Low Energy (Bluetooth LE, colloquially BLE, formerly marketed as Bluetooth Smart) is a wireless personal area network technology designed and marketed by the Bluetooth Special Interest Group (Bluetooth SIG) aimed at novel applications in the healthcare, fitness, beacons, security, and home entertainment industries. Compared to Classic Bluetooth, Bluetooth LE is intended to provide considerably reduced power consumption and cost while maintaining a similar communication range.

Protocol Overview

- Bluetooth LE is renowned for its low power consumption, making it an ideal choice for battery-operated devices. Key features include:

- Low Energy Operation: BLE is optimized for low power use at a reduced data rate. Adaptive Frequency Hopping: Increases the robustness of communication by avoiding channels with interference.

Range

Bluetooth LE can achieve a communication range of up to 100 meters (328 feet) in open space, though this is highly dependent on environmental factors and the capabilities of the specific devices being used.

Power Consumption

BLE's power efficiency is one of its most significant advantages:

- Devices can operate for months or even years on a tiny battery by efficiently managing sleep and active modes.
- The actual power consumption depends on usage patterns, broadcast frequency, and data volume.

Security

Bluetooth LE provides several security features to protect against eavesdropping and man-in-the-middle attacks:

1. Encryption: AES-128 bit encryption for securing data transmission.
2. Authentication: Features to verify the identity of connected devices.
3. Privacy: Random address techniques prevent tracking of devices.

Other Considerations for IoT

Bluetooth LE is highly suitable for Internet of Things (IoT) applications due to:

1. Low Cost: BLE devices are relatively inexpensive to manufacture.
2. Ubiquity: BLE is supported by a vast array of modern smartphones, tablets, and PCs, facilitating easy interactions with IoT devices.
3. Community and Support: A broad community and robust ecosystem of tools and libraries support BLE development.

This technology's combination of low power consumption, robust security features, and widespread support makes Bluetooth LE an excellent choice for developing a wide range of IoT applications.

Zigbee

Zigbee is a short-range protocol with high scaleability for use of upwards to 65000 units. The protocol is typically used for cases where you have multiple devices with low range that sends low data-rate and low-power consumption applications and is an open standard.

The criterias for comparison were choosen to make it clearer wether or not a certain protocol is right for your specific use case. Or more likely a brief introduction to the different protocols and their capabilities.

Protocol Overview

As mentioned before the most common use case for Zigbee is indoors, why? Because the most effective range for Zigbee is 1-10m indoors. So what does this mean? Well Zigbee can be a great protocol for home automation, industrial automation aswell as smart metering system.

Because of it's low data rate and power consumption you can use Zigbee for devices like garage doors, locks, lights, motion sensors and much more. Think of all the things you have home such as smoke alarms etc connected that sends data to for example your smart phone for you to monitor. All of this can be acheieved with Zigbee, at a lower power consumption than Bluetooth and Wifi, 20-50% cheaper than for example Z-Wave devices. Zigbee is also backed as a protocol by Philips, Samsung, Siemens & Whirlpool.

It also recently started to being used by Amazon, Apple and Google where they integrate it into their smart speakers and smart screens. Zigbee also uses the 2.4 GHz band as WiFi does. Which makes Zigbee protocol available to all around the world so you can use the devices anywhere you want.

Range

Indoors up to 10-100 meters Outdoors up to 250 meters

Depends on interference with the signal, by that it means if obstacles in the environment and the power output from the devices. Zigbee devices in some cases also uses a mesh networking feature which extends the signal by make the signal "bounce" off of or through multiple devices.

Power Consumption

Since Zigbee uses a low power consumption compared to other wireless protocols like WiFi, it is great suited for devices that is powered by battery. Zigbee is designed to consume a minimal power in idle mode or "sleep" mode. Which means it consumes in the range of microwatts or minimalwatts. It is hard to say what the lifetime is for different batteries inside Zigbee devices, but in devices that sends low data rate the battery can last months or years on a single charge.

Security

Network:

Key Establishment: Devices with zigbee protocol, uses network keys to make communication between devices secure on a Zigbee network.

Link key Encryption: You can also use link keys or encrypted keys which makes communcation between devices confidential.

Frame Counter: Frame counters are for to prevent replay attacks. Which makes each message unique so there wont be replays of other messages sent before.

Application:

Application-Level Encryption: The Zigbee protocol also support encryption on the application layer. It is a symmetric encryption that is being used AES (Advanced Encryption Standard). This is to ensure that sensitive data exchange between devices are being protected inside the network.

Message Authentication Codes(MACs): "MACs" Media Access Control are also used in the Zigbee protocol. Which means that the integrity is ensured so unauthorized modification is not made to the data during transmission. This makes all the messages tracable back to the device, which makes it easy to see if a specific device "belongs" on the network or not.

Key Transport: Within the network it also securly transports keys between devices which makes the distribution of keys effecient and secure.

Trust center: Within Zigbee there is also a "trust center" which is responsible for management of keys. It distributes and facilitates key establishment. The trust center is also responsible for the authentication process. It authenticates devices joining the network and establish each devices privileges.

Cryptographic Techniques: As mentioned before it primarily uses AES for encryption and decryption of data in both the network layer and application layer. Zigbee uses hash functions aswell for example SHA-256 to ensure the generation of message authentication, that ensures data integrity. Random number generations is also used to prevent patterns that are predictable inside security protcols. How? they generate cryptographic keys.

Security settings: Zigbee has configurable security settings that can be specified to your certain use case. This let's network admins to make changes to the security settings for their application. The typical settings are encryption length of keys and the rotation intervals for the keys. This is changed through the trust center settings.

Pros & Cons

Pros:

- low power consumption
- high scaleability upwards to 60000 units.
- backed by big companies and used by big companies
- secure connections (CIA)
- costs less than other devices using for example Z-Wave

Cons:

- low data rate transfer
- short range
- interupted signal if there are obstacles
- latency with more devices
- may need complex knowledge to use to it full potential

Conclusion

Zigbee as a protocol should mainly be used for low data rate transmissions such as home automation for garage doors, lamps, smoke alarms, monitoring water usage and such. That doesn't require more than 10 meters in distance between the devices and as little as possible obstacles between the devices for the best signal. It can also be used for industrial automation and monitoring different sensors outside. But be aware that it needs to be some kind of amplifier to make the signal reach longer outside. Also to take in to consideration is that you need a pretty good understanding in IT to use the protocol to it's full potential. Over all the protocol is very secure to use in the sense that the protocol is both backed and used by companies such as Amazon, Google, Philips, Siemens etc. The protocol uses "CIA" in different layers and can be configure to suit the specific use case for the admin or admins on the network.

Z-Wave

Z-Wave is a wireless communications protocol used primarily for home automation. It is designed to allow smart devices to communicate with each other within the home via low-energy radio waves. Developed by Zensys, a Danish company, it is now managed by the Z-Wave Alliance, a consortium of over 700 companies dedicated to the development of Z-Wave technology.

Protocol Overview

- Z-Wave operates on a mesh network topology, enabling devices to communicate with each other by forwarding messages across the network. Key features include:
- Low Energy Operation: Z-Wave is designed for low power consumption, extending the battery life of devices.
- Mesh Networking: Devices can act as repeaters, extending the range and reliability of the network.

Range

Z-Wave networks can cover a typical home, with a range of approximately 30 meters (98 feet) indoors. The mesh network architecture allows devices to work together to extend coverage and overcome obstacles.

Power Consumption

Z-Wave's power efficiency ensures that battery-operated devices, such as sensors and locks, can last for years on a single battery charge:

- Devices are designed to minimize energy use, entering sleep mode when not actively communicating.
- The actual power consumption varies based on device activity and network configuration.

Security

Z-Wave includes several layers of security to safeguard against unauthorized access and ensure secure communication:

1. AES-128 Encryption: Provides strong encryption for data transmission.
2. S2 Security Framework: Enhances security with secure key exchange and device pairing procedures.
3. Device Authentication: Ensures that only authorized devices can join the network.

Other Considerations for IoT

Z-Wave is particularly well-suited for smart home and IoT applications due to:

1. Interoperability: Z-Wave ensures that devices from different manufacturers can work together seamlessly.
2. Wide Adoption: Over 2,600 certified products available, making it easy to find devices that fit specific needs.
3. Dedicated Frequency: Operates on a dedicated frequency band (typically 908.42 MHz in the US, varying by country), reducing interference from other wireless devices.

Z-Wave's combination of low power consumption, strong security measures, and extensive interoperability makes it a preferred choice for smart home automation and IoT ecosystems.

NFC (Near Field Communication)

NFC is a short-range wireless communication technology operating at 13.56 MHz, and the NFC Forum has helped to both define and promote the technology commonly used in access pairing, contactless transactions, device pairing, mobile payments, and ticketing. This is because it facilitates communication between devices when those are brought within proximity of each other, typically a few centimeters.

NFC operates through electromagnetic induction, providing a secure and convenient method for data transfer, device authentication, and transactions by supporting two modes:

1. Active, where both devices generate radio frequency (RF) field.
2. Passive, where one device generates an RF field while the other modulates data onto it.

Protocol Overview

- NFC is known for its short-range communication capabilities, typically within a few centimeters, making it suitable for secure transactions and data exchange at near proximity.
- Low Power Consumption: NFC technology is designed to operate with minimal power, making it efficient for battery-operated devices.
- Secure Communication: NFC provides secure data transmission through encryption algorithms, ensuring confidentiality and integrity of transmitted information.
- Ease of Use: NFC-enabled devices can establish connections simply by bringing them close together, without the need for complex setup procedures.

Range

NFC operates within a short range, typically a few centimeters, facilitating secure data transfer and interaction between devices.

Power Consumption

NFC technology is known for its relatively low power consumption:

- NFC-enabled devices operate efficiently on a single charge or battery, thanks to their effective power management.

- Power usage depends on factors like NFC interaction frequency, activation duration, and communication complexity.
- These devices are passive and don't need their own battery; they draw power from the active device they're connected to, like a smartphone or NFC reader.

Security

- Encryption: NFC uses different encryption algorithms depending on the protocol used. The most common encryption algorithms within NFC are AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), and ECC (Elliptic Curve Cryptography). The choice of algorithm depends on the security requirements of the task.

- Authentication: It includes features to verify the identity of connected devices, ensuring a secure connection between them.

- Privacy: NFC employs random address techniques to prevent device tracking, enhancing user privacy.

- Short Range: NFC's short-range communication limits the risk of interception, making it more secure for sensitive transactions.

- Secure Element: Some NFC-enabled devices have a secure element, a tamper-resistant area for storing sensitive information like payment credentials, further enhancing security.

- Trusted Execution Environment (TEE): TEE provides a secure environment for executing sensitive operations, adding an extra layer of protection against malicious attacks.

Other Considerations for IoT

NFC technology brings numerous benefits and factors to consider for its integration into IoT applications:

1. Cost-effectiveness: NFC devices are cost-effective to produce.
2. Contactless Communication: By bringing devices close together, NFC enables fast and convenient transactions.
3. User-Friendly: NFC is known for its user-friendliness and requires minimal installation or configuration.

The combination of short-range, contactless communication, low power consumption, security, and user-friendliness makes NFC a suitable choice for specific IoT applications.

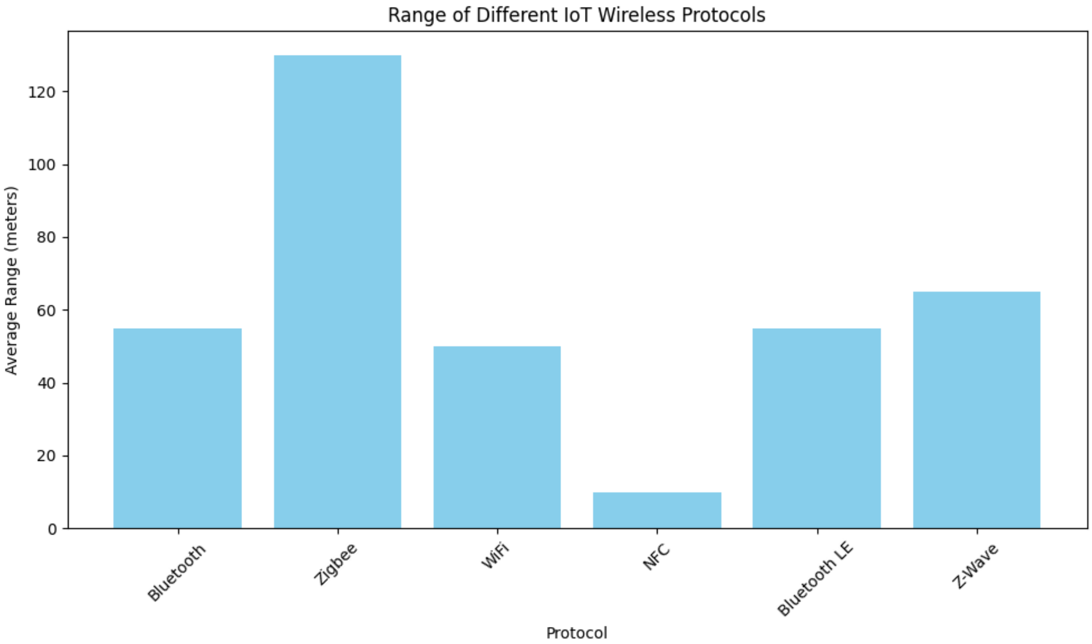
Protocol Summary

- **WiFi** emerges as the go-to choice for high-bandwidth applications requiring internet access, although at the cost of higher power consumption.
- **Bluetooth** and **Bluetooth LE** offer versatility, with BLE being particularly advantageous for battery-operated devices due to its low energy profile.
- **Zigbee** and **Z-Wave** stand out in creating extensive, low-power mesh networks, ideal for home automation and sensor networks.
- **NFC** offers a unique niche in close-proximity, secure transactions and data exchange.

The diversity in wireless communication protocols is highlighted by their range, data rate, and frequency utilization, each catering to specific application needs within the IoT ecosystem.

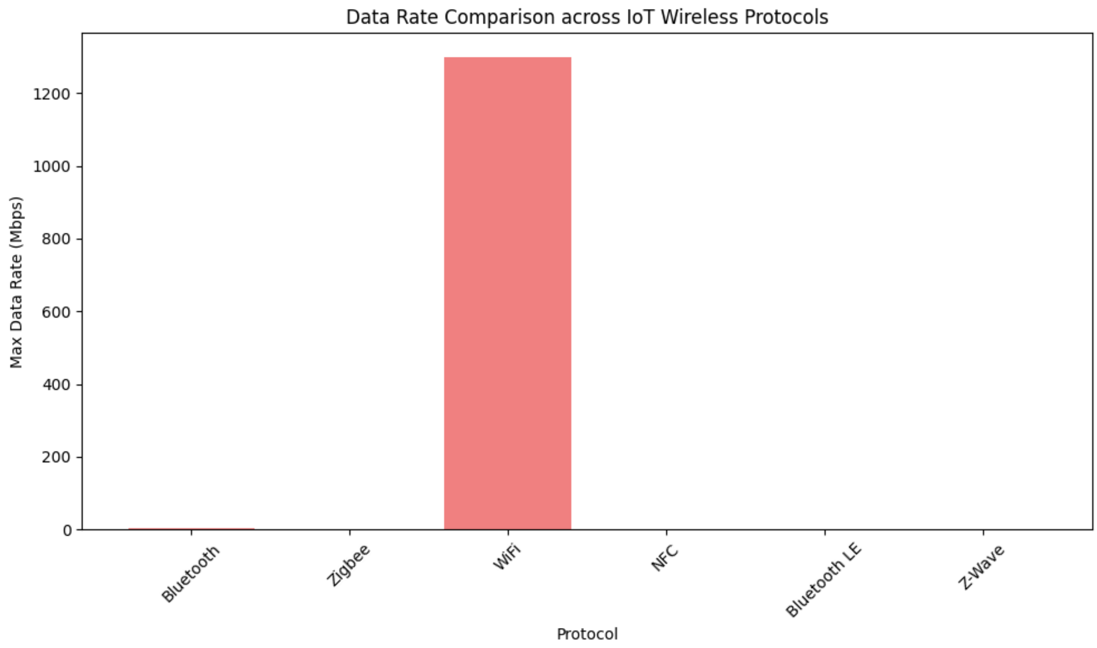
Range Insights

The range of a protocol determines its effectiveness across different environments. WiFi, with its capability for substantial coverage, is well-suited for a variety of applications, both indoors and outdoors. Zigbee also offers a wide coverage area, making it ideal for sensor networks spread across a large area. In contrast, NFC is designed for very short-range interactions, typically a few centimeters, making it perfect for secure, close-proximity tasks such as payments and quick data exchanges.



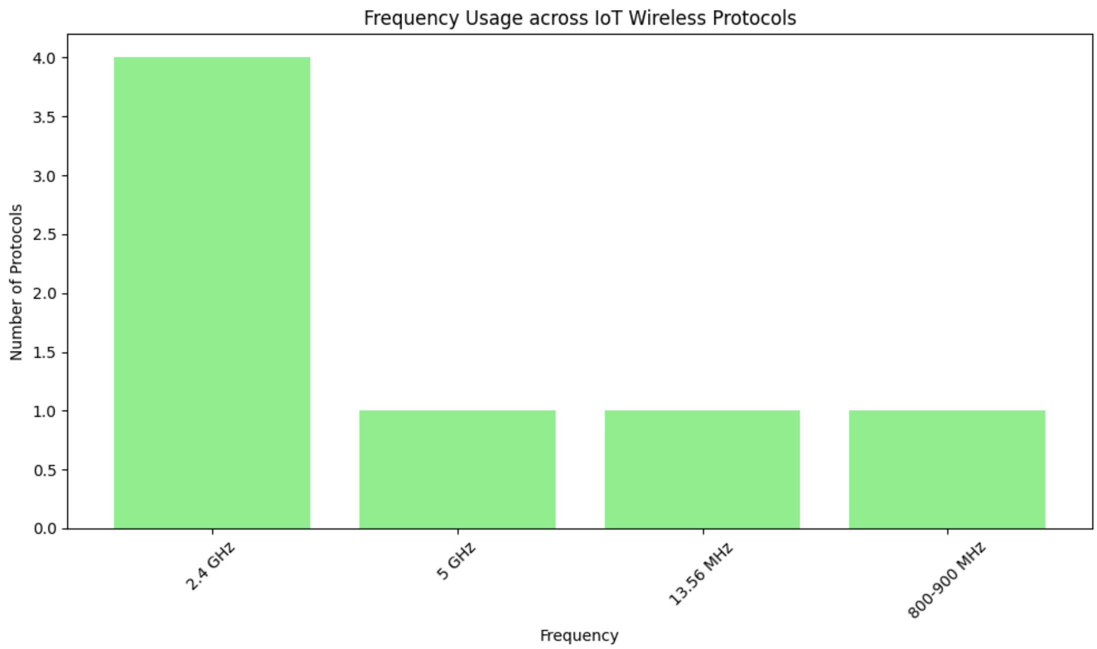
Data Rate Capabilities

Data rate is a crucial factor for applications requiring fast data transmission. WiFi excels in this area, supporting high data rates that are ideal for streaming and other data-intensive applications. On the other hand, Bluetooth LE is designed to provide a balance between efficient power consumption and adequate data rates, making it suitable for IoT devices that prioritize energy efficiency. Zigbee, with its focus on low-power sensor networks, offers lower data rates, which is sufficient for the transmission of small amounts of data over a network designed for efficiency and longevity.



Frequency Utilization

The choice of frequency band impacts a protocol's susceptibility to interference and its ability to coexist with other wireless technologies. Both WiFi and Bluetooth predominantly operate in the 2.4 GHz band, a common frequency that is shared by many devices, leading to a higher potential for interference. Zigbee also operates in the 2.4 GHz band but is designed to efficiently manage coexistence with other technologies in this crowded space. Z-Wave, by contrast, utilizes the 800-900 MHz frequency band, which is generally less congested, offering advantages in terms of reduced interference and improved reliability for home automation systems.



Security Considerations

Security is a paramount concern in IoT applications, where the integrity and confidentiality of data must be safeguarded. Each wireless protocol incorporates distinct security features tailored to its use cases.

- **WiFi** employs WPA3 encryption, providing comprehensive security with complex cipher suites for data protection and user authentication, suitable for bandwidth-intensive environments.
- **Bluetooth** incorporates Adaptive Frequency Hopping and ECDH key exchange for enhanced security, facilitating encrypted communications in personal and commercial settings.
- **Bluetooth LE** extends Bluetooth's security features with LE Secure Connections, including FIPS-approved algorithms for encryption and secure key distribution, optimizing for power efficiency.
- **Zigbee** uses network and link key encryption, frame counters to prevent replay attacks, and AES for application-level encryption. It employs MACs for data integrity and a trust center for key management and device authentication, ensuring comprehensive security.
- **Z-Wave** uses AES-128 encryption and Secure S2 framework for advanced network security, ensuring encrypted communication in smart home applications with minimal power usage.
- **NFC** utilizes advanced encryption (AES, RSA, ECC) tailored to specific security needs, with authentication to ensure secure device connections. It enhances privacy through random addressing, reducing trackability. The inherent short range limits interception risks, while a secure element and TEE offer additional protection for sensitive transactions and operations, ensuring robust security

Security in wireless communication protocols is continuously evolving to address emerging threats and vulnerabilities. Choosing a protocol with adequate security features is essential for building trustworthy IoT systems that users can rely on.

Conclusion: Choosing the Right Wireless Protocol for IoT

Selecting a wireless protocol is crucial, with each serving specific IoT needs. The choice hinges on application, range, throughput, power, and interoperability. This report aims to help IoT developers in making protocol choices, the key to efficient and scalable IoT solutions. Embracing the right protocol is strategic, essential for IoT innovation and advancement.

About This PDF

This PDF was generated using a Continuous Integration (CI) pipeline, leveraging Python scripts for merging markdown files and creating diagrams, followed by a markdown-to-PDF conversion process. This automated workflow ensures the report is always up-to-date with the latest contributions from all authors. For more information and to contribute to this report, visit the GitHub repository: https://github.com/simonthorell/wl-iot-protocols-report.