Long Range Communication Protocols

Maximizing the unknown capabilities of radio protocols

Andrea Paloschavez
Computer Science
George Mason
University

Fairfax, VA USA
apalosch@gmu.com

Adrian Meneses
Computer Science
George Mason
University

Fairfax, VA USA
amenes@gmu.com

Siddarth Patel
Computer Science
George Mason
University

Fairfax, VA USA
spatel53@gmu.com

Andres Reyes
Computer Science
George Mason
University

Fairfax, VA USA
areyes24@gmu.com

ABSTRACT

Today, nearly everything is connected to Wi-Fi, a wireless technology in the form of a radio signal. Wi-Fi sends a signal from a router to a computer which enables computers to communicate and connect to the internet by translating the signal waves to data. To start, the transmission of data is determined by current protocols that try to ensure data is sent and received by implementing a minimum requirement in the protocol. Next, the range of Wi-Fi is another issue that can be affected by the location of the router, access point, and the physical surroundings. Most of the time, it is not easy to change physical locations of the router, but range, and more importantly data, can be improved by changing the software to a new wireless standard protocol.

When we first approached the problems of long-range communications we had to research some of the most commonly used wireless communications on the market. We considered seven types of wireless communications our team could apply to the On-Off Noise Power Communication approach we chose to research from the ACM article written by Philip Lundrigan et al.

CCS CONCEPTS

• Networking • Radio range • Network range • Network design • Network protocols • Network Performance Evaluation • Protocol designs • Wi-Fi • Long-range signals

KEYWORDS

Long-range signals; Wi-Fi range; Radio range; Designing network protocols

1 Types of Wireless Communication

First we looked at satellite communication but saw the difficulty was sending signals to other countries due to the spherical nature of the Earth. This posed a problem that could not be solved simply by changing networking protocols so we then considered infrared communication.

Infrared communication receives light through a photoreceiver and sends it through a transmitter. This type of communication is often used in the home to connect TVs with remote controllers by using a ray of light that is invisible. We found this form of wireless connection to be unusable if there was an object blocking the light. However, networking protocols could not be applied to infrared communications because a blockage of light would mean absolutely no connection was being made. Our approach focused on maintaining at least a low connection to ensure communication so the binary aspect of light removed infrared communication from our potential form of communication.

We considered microwave communication due to its widespread use across first world countries. Upon further research we discovered terrestrial and satellite versions of microwave communication. This form of communication uses antennas similar to how a radio would to send waves back and forth. It was ideal for long-range communications involving satellites. While this was interesting as our focus was regarding long range communications, we could not implement an effective protocol because physical blockage problems such as weather patterns posed a major threat to establishing secure connections.

Satellite microwave communication was quite similar to infrared in that both required an unblocked beam of light in order to operate. Because of the same binary nature of light and microwaves we decided not to use microwave satellite communications in our design.

Another type of microwave communication is terrestrial microwave communication. This method requires a signal to be passed between two antennas similar to a radio connection. It also meant the signal could simply be sent internally in a network but this form of microwave communication still did not correctly meet our goal for long-range communications.

Moving on to research mobile communication systems we quickly found that it was quite similar to Wi-Fi since it uses satellite to transmit between local networks. The same barriers that presented in satellite microwave communications arose in terms of physical barriers blocking the signals. In addition to physical barriers such as buildings and weather we also had the issue of heavy cellular traffic. There were a whole host of issues with mobile connections; location, physical surroundings, certain materials, distance, trees, weather and even cosmic events. It is not surprising when you consider how often we lose cellular connection. Even more problems arose when you consider the nature of mobile connections which rely entirely on battery operated portable devices. After a battery dies the connection is effectively closed and cannot be reestablished until power is applied. We realized we could only apply the On-Off Noise Power Communication protocol to devices that were capable of maintaining a constant connection so we turned our focus on machines that stay plugged in and operable at all times. After considering mobile communication systems we naturally began looking into Bluetooth connections.

Bluetooth technology was very briefly considered since it is commonly used to connect devices and would ideally need to maintain a constant connection for a seamless user experience. We considered applying the idea of maintaining a constant connection but ultimately decided it would be more beneficial to improve on long-range connections as it would have more impact. Bluetooth is a very new technology but the lack of range and ability to be blocked by physical objects discouraged us from applying a new long-range networking protocol to improve it.

After researching a multitude of wireless connections we went back to the basics and decided to try to implement the On-Off protocol on a simple broadcast radio. Since it was the very first type of wireless network the design is quite simple and involves radio waves passed between two antennas by using a transmitter and receiver. There can be a multitude of frequencies so it is easy to send signals especially since they are narrow (unlike wide range signals). The data is passed along these radio waves in electromagnetic signals so the range of a radio broadcast can vary greatly. This means we can easily extend the range and apply the On-Off protocol to a radio system. The idea works by sending a long range communication at a slow rate to maintain a constant connection. The transmitter can send the packet at any specified time. The receiver of a radio already naturally measures interference so it can be modified to constantly and consistently check for a live connection.

Verifying the On-Off protocol can be applied to basic broadcast radios was not satisfactory for the team because it was a very old and basic technology. Combining our knowledge of networking and experience with general protocols we attempted to apply the logic of On-Off to Wi-Fi. Wi-Fi is the supreme wireless technology used in this day and age because it serves to connect all devices such as computers, phones, printers, etc. It also uses a radio signal to achieve this massive connectivity. In very general terms, Wi-Fi functions because the radio signal is sent from a router and translated into data displayed on a user's device. Because Wi-Fi basically functions off the idea of a broadcast radio it was a natural conclusion that On-Off Power Communications would also function over Wi-Fi and could be implemented on Wi-Fi hardwares.

Wireless Communication Type	**Drawbacks**	**Application to On-Off Protocol**
Satellite communication	Curvature of Earth	Long-range
Infrared communication	Physical barriers, short-range	Constant connection
Microwave communication	Physical barriers	Long-range
Mobile communication	Physical barriers, battery-operated	Long-range
Bluetooth technology	Short-range, battery-operated	Constant connection
Radio broadcast communication	Simplistic, outdated	Long-range, constant connection
Wi-Fi connection	Still expanding technology	Long-range, constant connection

Table 1: **Summary of research conducted on common wireless communications with applications to On-Off protocol.**

The table above provides a brief summary of the analysis discussed in the section above. We summarized the factors preventing the full application of the On-Off protocol in the "Drawbacks" column and noted the aspects of the wireless communication type that supported the implementation in the "Application to On-Off Protocol" column. As shown, it is clear that the On-Off protocol can only be applied to radio broadcast communication and Wi-Fi connections. This is not particularly surprising since our research shows Wi-Fi is modeled after the original broadcast radio. The next section will discuss the main aspects of On-Off Power Communication as applied to radio and Wi-Fi hardwares.

1.1 Research on On-Off Power Communication

The main idea is to maximize the lower bandwidth spectrum in which no data is sent between devices. Currently, the 802.11 protocol only allows sending data as long as the link speed is at least one megabit per second. As it stands, this means that a device can be connected to a router but because the transmission rate is lower than one megabit per second, there is no actual data being sent or received. In other words, if a device is connected to a router but the data rate is say, half a megabit, the protocol will simply block the transmission of data.

To circumvent this issue, one solution can be to implement a new protocol or maybe extend the current one to allow transmission that is lower that one megabit per second. The reasoning behind this is that some devices do not need to send data that fast back to the router. To illustrate, a device that takes a small air sample to measure pollution only needs to send a report in the form of a small text file back to the router which would be only a few kilobytes in size. However, since the protocol only allows an active connection that is one megabit per second in order to transmit data, the router might refuse the transmission. Granted, there might be obstacles between the router and the air sampling device which will of course obstruct the signal between the router and the device but this should not prevent the connection from being dropped.

Therefore, the proposed protocol can solve this issue by alerting the router that the device is still transmitting by sending noise instead of actual data. Specifically, the transmission of a single digit such as a 1 to let the router know that the air sampling device is still transmitting. Of course, to send a single digit should not require an active connection of one megabit per second.

1.2 Comparing Wireless Connectivity Protocols

We decided to research other types of wireless connectivity protocols to compare and see if LoRa was the correct approach and whether other protocols could be applied in the proposed On-Off protocol. Choosing the correct protocol can optimize device connectivity.

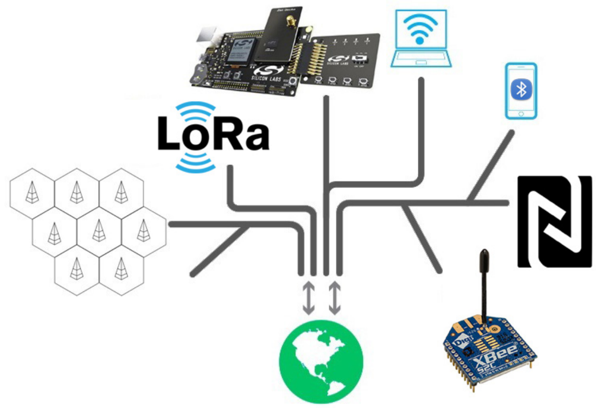

Figure 1: **Different types of wireless internet communication protocols in Internet of Things.**

We mainly focused on the comparison of Wi-Fi and Long Range, Lower Data Rates, Extended Battery Life (LoRaWan).

Wi-Fi falls under the LAN/PAN category as it is a local area network or a wide area network. It connects billions of devices to the internet and each other on a broadband wireless system. Wi-Fi has a very high data rate capability but its range is still long enough to satisfy consumers.

LoRa is a protocol focused on a longer range that transmits with low data rates (when compared to Wi-Fi). It accomplishes this because it uses radio frequencies on the physical layer.

Similar to LoRa, LoRaWAN is a revised approach that helps to define the upper networking layers such as the MAC layer. These two connectivity protocols work in separate spaces; LoRa assists the physical layer with long range connections while LoRaWAN defines the actual system architecture of the network as well as the communication protocol. Another benefit to using LoRaWAN is that battery consumption is lowered making it very practical for personal devices considering the portable nature in this era.

Protocol	Optimized for Extended Battery Life	Nominal Range Limit	Typical Data Rate	Spectrum
NFC	✓	Personal (<10m)	2Mbps	ISM 2.4GHz unlicensed
Bluetooth	✓	Contact (<4cm)	100kbps	ISM 13.56MHz unlicensed
WiFi	✗	Local (<100m)	>100Mbps	ISM 2.4GHz/5GHz unlicensed
LoRaWAN	✓	Metro (>10km)	<50kpbs	ISM 900Mhz, 868MHz, 433MHz unlicensed
NB-IoT	✓	Metro (>10km)	200kbps	Licensed cellular
2G | 3G	✗	Metro (>30km)	<2Mbps	Licensed cellular
4G LTE	✗	Metro (>30km)	>100Mbps	Licensed cellular
5G	✗	Metro (>30km)	>10Gbps	Licensed cellular

Table 2: **Comparison of wireless connectivity protocols to determine the benefits of each as applied to the On-Off protocol.**

A brief comparison of LoRaWAN in perspective with other common wireless protocols shows the benefits and why we ultimately need to use LoRaWAN to accomplish the On-Off Protocol.

1.3 External Factors that Affect Signal

Signals can easily be disrupted as seen in Section 1 after a thorough analysis of commonly used wireless connections. A variety of factors ranging from physical barriers to location can weaken or drop the connection. Fortunately, not all of these factors discussed would have an effect on the On-Off Noise Power Communication protocol. In this section we discuss the factors that would affect the signal produced in the On-Off protocol.

The most common factors seen today that affect signals can be simple everyday objects: walls, desks, windows, doors, and furniture to name a few. For this reason, signals will deteriorate over time which will result in some devices suffering to transmit data properly. Rearranging some of the objects might fix the issue but the same issue is bound to happen again.

Magnets can cause signal interference when close to a device that is trying to send a signal. The electromagnetic field can create noise that can produce an incorrect interpretation. This can be flipping bits while transmitting data, partial or total corruption of a datagram, or possibly a complete blockage of the transmission in its entirety. This is because any electrical device produces small amounts of magnetism.

Another factor that can influence the wireless signal considerably is crosstalk. Nowadays, a home is plagued with wireless devices ranging from small gadgets such as baby monitors, cell phones, and security cameras to microwaves, printers, and laptops. As one can assume, every device is in a constant battle to have priority over the radio signals that are emitting from the router. This is assuming that the router is fully capable of handling multiple transmissions at the same time. To eliminate a bad experience for the user, or at least to minimize it, the new protocol would ensure that all devices are still actively trying to transmit some data back to the router. This of course would mean that no connection would be dropped. A side effect, and a welcomed one, would be that devices would avoid reloading applications from scratch therefore saving some energy in the process.

1.4 The Power of Noise

We have touched upon noise in the previous sections and realized we needed to explicitly address it because energy interferences can affect the wireless signal quality. There are many types; external noise arises from outside factors that can disrupt a signal whereas internal noise is actually generated in the network itself. We can address the most common ones and how they will affect the On-Off protocol as well as how we can counter these interferences.

Thermal noise arises when the temperature of the system is affected. We can counteract this by adding fans to our hardware system when it overheats. Another form of noise is crosstalk in which the electromagnetic field experiences interference. The signals become confused and cross over each other. This disturbance is more difficult to protect against.

The most important type of noise we need to consider in the On-Off protocol is the noise power ratio. This ratio measures intermodulation noise. We can account for this by using a quiet slot to find out how much noise has been introduced by intermodulation.

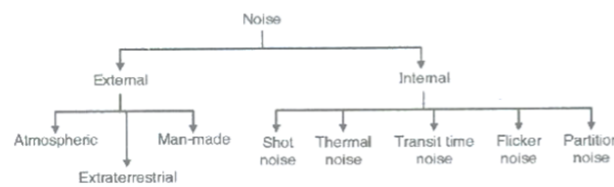

Figure 2: **Flow chart explaining the different types of noise and how they fall under External/Internal branches.**

As shown in the flow chart above these are the different types of noise we need to consider in our On-Off protocol implementation. We need to establish methods to counteract physical noise such as the external examples of atmospheric and man-made disturbances as well as develop our hardware to be resistant to internal noises.

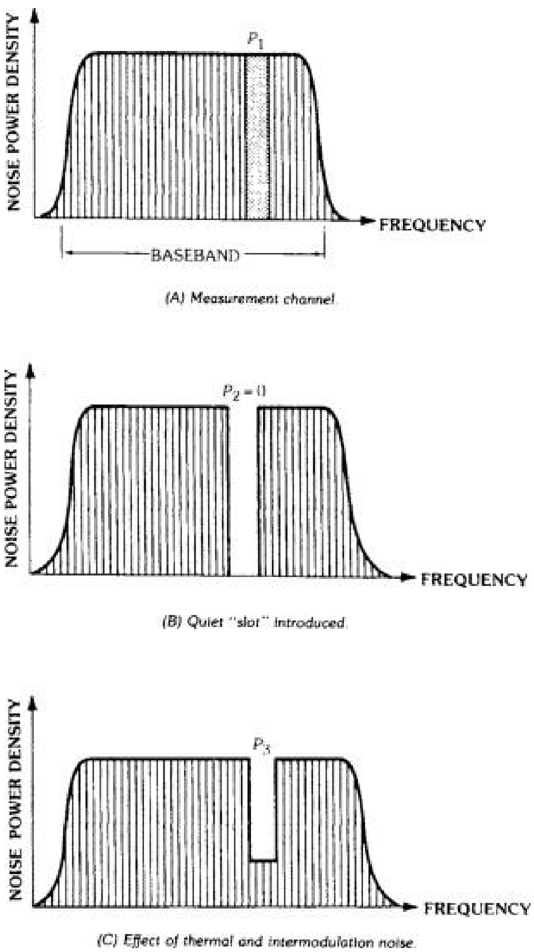

Figure 2: **Comparison of the power in the measurement channels.**

Using the formula provided in the noise power ratio we can determine exactly how much intermodulation has been added. Based on the plots above we can clearly see that NPR can be calculated as the power in the measurement channel divided by the effect of the noise components.

$$NPR = \frac{P_1}{P_3}$$

Formula 1: **The ratio of power measurement as determined by applying a quiet slot.**

We determined that the use of this formula can help us perform a Noise-Power Ratio Test to see multiplexed communication systems.

2 Practical Use Cases of a Long-Range Protocol

The main benefit from the new protocol would expand new possibilities that otherwise would be restricted. Not only would devices be able to send data at very low frequency rates but the transmission rate would also be unrestricted in the sense that it would not require a minimum. This should in theory also increase the range since devices can now listen and transmit data back to the router at distances that are currently not allowed.

Other areas of interest would be in the router space for example. The new protocol can be used to validate that a device that is orbiting in outer space or on another planet is still active and trying to transmit.

Moreover, residents in rural areas will be able to know that cellular towers are still transmitting some type of data even though the transmission rate is not optimal. In the medical sector, people that depend on small devices that alert paramedics when a person has fallen can greatly benefit from the new protocol. This will simply open up possibilities in every major professional sector.

2.1 Example of Long-Range Communications

What is Sigfox? One can define Sigfox as a French global network operator that supports long-range coverage. It is fit for small amounts of packets as it transmits data very slowly. Since, we are sending data for a long-range while preventing packet loss, our data must be in small chunks which is one of the down sides of long-range coverage. Due to this reason, Sigfox is suited for small amounts of data such as IoT applications.

So how do Sigfox accomplish such data transfer? Sigfox accomplished this by setting up antenna towers quite identical to cell phone towers through a one-way system. An example of a one-way system is basic alarm systems and location monitoring.

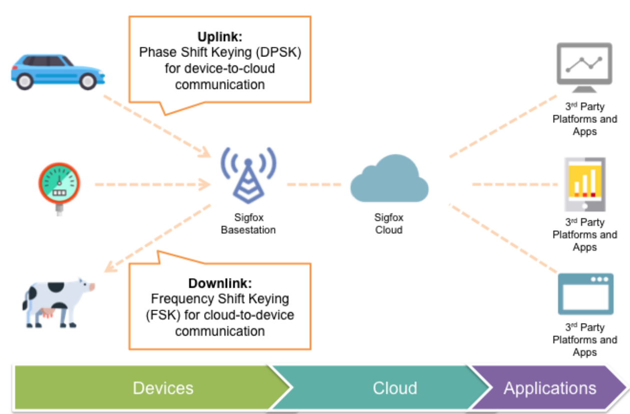

Figure 3: **This depicts the basic functionality of Sigfox and how it connects Uplinks and Downlinks to provide connectivity to applications.**

2.2 Implementing On-Off NPC

ONPC is a protocol which modifies the software in commodity packet radios to allow communication, independent of their standard protocol, at a very slow rate at long range. In order to achieve this, a transmitter is used as an RF power source which can be on or off if it does or does not send a packet, respectively, and a receiver that repeatedly measures the noise and interference power level.

To overcome interference from other devices' channel access to provide long ranges at much lower data rate, spread spectrum techniques are used on top of the basic on/off mechanism.

The protocol is implemented on top of commodity WiFi hardware. To ensure the implementation of ONPC works correctly, a synthetic wireless trace generator is used. The transmitter of the protocol is built using a Wemos D1 mini pro which is based on the ESP8266. The call wifi_send_pkt_freedom is used to transmit packets when the hardware timer fires.

For the access point a router is used which runs DD-WRT. This provides ssh access so that management commands can be run. With the use of a router, access to packets is easier to control. This gives testing and implementation a better visual on what is going on.

The receiver is implemented as a Python application. The main purpose of this application is to log onto the AP through ssh, and collect samples. Then it transfers the sample file for processing. The ONPC receiver is connected by ethernet connection to the access point [1].

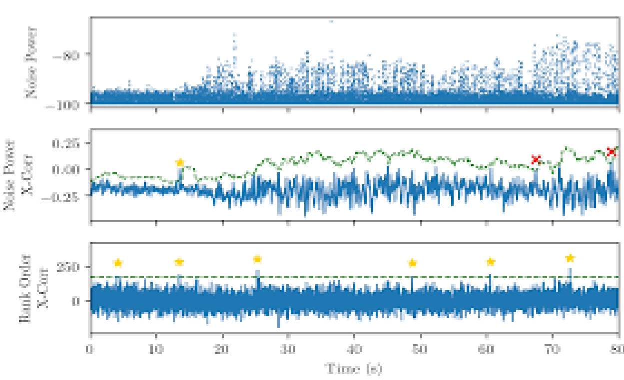

Figure 4: **This depicts the noise in transmissions.**

2.3 Analysis of Short-Range Communications

Li-Fi stands for Light Fidelity technology. I am sure you have found the name similar to Wi-Fi, so how are they similar? Li-Fi refers to a wireless connection environment without the need for routers. Let me explain in detail! It uses technology that uses light emitting diodes to transmit data wirelessly which was first demonstrated in 2011. It has been a decade since the technology came out, but it still is not mainstream or replaced with Wi-Fi.

Li-Fi is cheaper to begin with compared to Wi-Fi. But there is a theoretical limit to it of about 10-15 GB data. It also cannot run without lights off which would limit the locations where you could use it. The real issue that needs to be addressed is its incapability to transmit light through thick material walls or heavy cardboards. Moreover, any other light such as sunlight or moonlight may significantly interfere with the diodes that are being sent by the lights.

With this analysis it is better to conclude that long-range technology works best in close proximity than a modern technology that recently got released.

ACKNOWLEDGMENTS

We would like to thank our Networking professor at George Mason University for providing us a framework of networking which has fostered our creativity and desire to explore new networking concepts. We would also like to thank our senior team leader, Andres Reyes, for providing encouragement, support, and his proven knowledge of IT to the junior members of the team. Lastly, we would like to thank George Mason University for offering the chance to delve into senior topics of interest and providing a robust course in networking.

REFERENCES

[1] Philip Lundrigan, Neal Patwari, and Sneha K. Kasera. 2019. On-off Noise Power Communication. *The 25th Annual International Conference on Mobile Computing and Networking* (2019). DOI:http://dx.doi.org/10.1145/3300061.3345436

[2] Mahmood Abdulsattar and Zahir A. Hussein. 2012. Energy Detection Technique for Spectrum Sensing in Cognitive Radio: A Survey. International journal of Computer Networks and Communications , Vol. 4 (09 2012), 223--242. https://doi.org/10.5121/ijcnc.2012.4514

[3] Anon. 2020. The different types of wireless communication. (January 2020). Retrieved December 13, 2021 from https://www.rantecantennas.com/blog/the-different-types-of-wireless-communication

[4] Wilson Amplifiers. 2021. 9 reasons why cell phone signals suddenly go bad. (December 2021). Retrieved December 13, 2021 from https://www.wilsonamplifiers.com/blog/reasons-why-cell-phone-signals-suddenly-go-bad/

[5] Anon. Choose the right IOT Wireless Connectivity Protocol. Retrieved December 13, 2021 from https://abracon.com/news/choose-the-right-iot-wireless-connectivity-protocol

[6] Anon. Noise power. Retrieved December 13, 2021 from https://www.sciencedirect.com/topics/engineering/noise-power