ACCESSIBLE LONG-RANGE COMMUNICATION WITHOUT INTERNET

We are happy to answer any questions about the project. You can reach us at either of the email addresses below.

Erling Mathias Staff – erlingstaff@gmail.com

Kristian Smedsrød – krissmed@hotmail.com

GitHub: https://github.com/erlingstaff/the-freedom-forum

Table of contents

Abstract

Authoritarian governments are increasingly using the internet as a strategic method of hindering pro-democracy movements. This is done by spreading propaganda or shutting it down to prevent information from coming in or going out. In this paper, we will propose a solution that uses existing Bluetooth-mesh technology and pairs it with LoRa radio communication-enabled microcontrollers to build a resilient, accessible, long-range network without the internet. We also address some security concerns with Bluetooth mesh communication. We have created a prototype as a proof of concept for both a chat application using this network and the LoRa microcontrollers that extend the range of the network. We have additionally assessed what needs to be done to further test the proposed solution's possibilities.

Introduction

The internet is a great way of sharing information and communicating. However, it is increasingly being used strategically by governments and government leaders to spread fake news and propaganda. Internet shutdowns have also been used as a strategic element for cracking down on pro-democracy movements, such as the one in Myanmar (Ratcliffe, 2021). Freedom House calls it "the rise of digital authoritarianism" (Shahbaz, 2018). Hence, we need a platform for communication that cannot be hindered by an internet shutdown.

Current solutions

Today, most secure communication is done online. Applications like Session, Signal, and Telegram are all communication platforms that focus on secure and private communication. However, these do not work without an internet connection, so if the internet were shut down or partially shut down, these platforms would no longer be available.

Calling or texting is still an option as long as the GSM (2G, 3G, 4G, and 5G) network is still available, however, the GSM network is susceptible to both physical attacks against infrastructure or eavesdropping (van den Broek, 2011). The GSM network relies heavily on a few, very large, centralized antennas that cover a large geographical area. Hence, they are very easy to disable.

When both the internet and GSM are down, there are very few options for remote communication. The most practical one is Bluetooth mesh networks.

A mesh network is a flexible network structure where the devices on the network are connected to each other, instead of all devices connected to a central server. This makes the network very resilient because if one or more devices disconnect from the network, the connection stays intact as there are most likely several routes from one device to another. Another benefit of a mesh network is that users can communicate with each other without being directly connected together. A mesh network is depicted in figure 1.

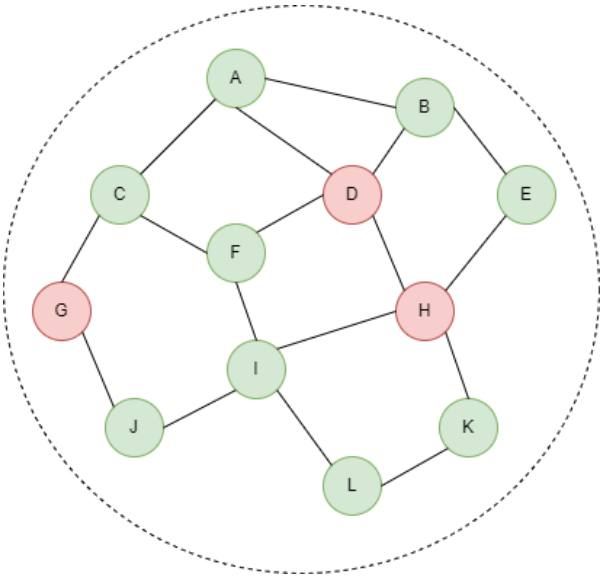

Figure 1: Mesh network in practice

Even when device D, G, and H are disconnected, all connected devices can still reach each other.

Problem motivation

Freedom House states that over the past 16 years, each year the freedom in the world overall has declined. 8 out of 10 people lived in non-free countries in 2021 (Repucci & Slipowitz, 2021; Repucci, S. & Slipowitz 2022). One of their recommendations for solving this issue is to let the internet remain open and free for everyone. This is not the case at this time. A way to achieve this is to combat internet shutdowns with alternative methods of wireless communication, an example of this is with the aforementioned Bluetooth mesh network.

Bridgefy is an example of an app that uses a Bluetooth mesh network to create a chat. The app transfers data

wirelessly to everyone nearby who also has the app installed. However, this specific app has been criticized for its lack of security features (Albrecht, Blasco, Jensen & Marekova, 2021; Albrecht, Eikenberg, Paterson, 2022).

Bluetooth communication like Bridgefy can be a partial replacement in case of an internet shutdown, however, Bluetooth is severely lacking when it comes to one very key aspect: long-distance communication. This makes it very difficult for a group of individuals to communicate remotely with each other as you could potentially end up with several separated networks, where e.g. a person in network 1 can not communicate with a person in network 2. In practice, this means that you are limited to communicating with the people who are very close to you in proximity. Communication over long distances is impossible with only Bluetooth, as depicted in figure 2 below.

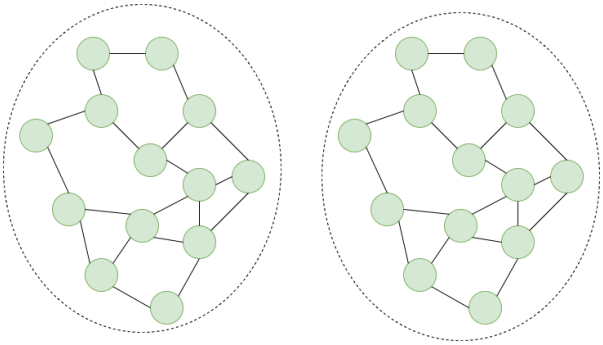

Figure 2: Separate mesh networks

Two separate mesh networks. This is a result of Bluetooth having a short range.

Therefore, we need an accessible platform for communication that allows for long-range communication without needing internet access or access to GSM.

Solution

To solve this problem we created *The Freedom Forum*. *The Freedom Forum* is an app and a protocol that uses Bluetooth mesh technology paired with cheap, small, and easy to manufacture microcontrollers that increase the range of the network to be upwards of 1500 times longer than a normal Bluetooth mesh network can provide.

With our solution, we use the flexibility and the availability of Bluetooth-enabled smart devices, such as smartphones, together with microcontrollers that utilize LoRa radio communication to expand the network's range drastically. These microcontrollers are small computers that receive signals from the Bluetooth mesh network and broadcast the message over LoRa to other microcontrollers, which then give the messages to Bluetooth devices close to them. The microcontrollers are meant to be used to relay all the messages from one Bluetooth-mesh to every other Bluetooth-mesh in a large area, effectively combining them. Therefore, only a handful of them is needed to connect a vast amount of people.

The first part of our solution is the protocol for both Bluetooth and LoRa communication. This protocol has been open-sourced in the GitHub repository linked above and made available for people to make their own implementations on the network. By open-sourcing the protocol, we ensure that even during an internet shutdown, people can participate in the chat by using the protocol to build their own app. The final result is an ecosystem of Bluetooth and LoRa devices that work together to relay messages and create a vast chatroom.

The other part of the solution is the proof-of-concept. We created both an app for android, *The Freedom Forum*, and multiple LoRa microcontrollers that in their current state work well. Both *The Freedom Forum* app and microcontroller code are also open-sourced in the GitHub repository.

It is important to stress that in our solution, every user is *not* supposed to have a microcontroller with them. Users connect to each other over Bluetooth by using the app and as long as one microcontroller is in the vicinity, everyone's messages are relayed to every other microcontroller, which then in turn relays them even further. Our solution relies on either a small number of people creating their own microcontrollers with our code or an entity creating a couple dozen and spreading them all over a city or landscape. But even without these microcontrollers, the network is fully operational. The network will then just be using Bluetooth mesh communication. An example of how this would work in practice is depicted below, in figure 3.

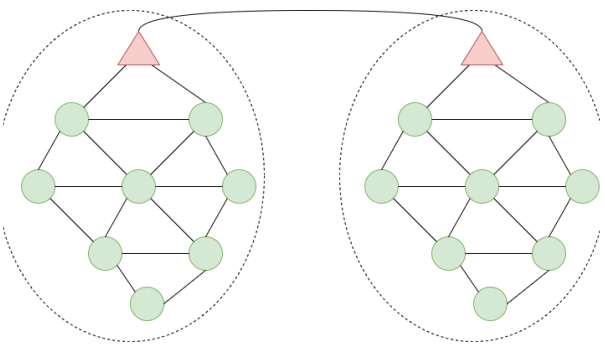

Figure 3: Bluetooth and LoRa Mesh Network.

With two LoRa nodes, we can combine two separate Bluetooth mesh networks, allowing for communication between any two users of either network.

DISCUSSION

Why Bluetooth

Bluetooth is the de facto standard for close-proximity communication, included in every smartphone and most smart devices today. For the mesh network to be resilient, scalable, efficient, and most of all accessible for everyone, Bluetooth is a very good protocol to rely on. Normal phones can not use LoRa, so our solution has them using Bluetooth to communicate with each other and the LoRa microcontrollers.

A study from 2014 by Aislelabs found that a phone that is sending data to 10 beacons at the same time, will use 1.79 % of the phone's battery in an hour. That is just about 1% more than it would use when Bluetooth is not active at all (Aislelabs, 2014). Bluetooth is therefore a very low-power solution to internet-less communication.

Why LoRa

We chose to use LoRa for long-range communication for several reasons. Firstly, it is cheap. LoRa modules can cost downwards of 2$. LoRa is also a very common radio communication protocol, with 166 networks already operational all over the world (Lora, u.d). Secondly, LoRa allows for extremely long-range communication. LoRa is known to be able to communicate with other LoRa devices around 6,5 kilometers apart in urban areas (Sanchez-Iborra, Sanchez-Gomez, Ballesta-Viñas, Cano, & Skarmeta, 2018), and 22 kilometers apart in open landscapes (Taste the code, 2022). It is worth noting that LoRa additionally has a world-record transmission distance of 832 kilometers, however, this is unlikely to be reproducible and applicable to our project.

LoRa has, however, some limitations, as outlined in Ferran Adelantado's paper *Understanding the limits of LoRaWAN* (Adelantado, Vilajosana, Tuset-Peiro, Martinez, Melia, & Watteyne, 2017). One of those limitations is transmission speed, which limits the network's overall speed. With that in mind, we need to limit the amount of data sent over the network. This means that larger files like videos and images will not be supported. We have also set an arbitrary number of 200 characters per message, but you are free to send as many messages as you want.

These modules would have to be made, as there are not many consumer smart devices that use LoRa natively. To make a microcontroller like this you need three things: a computing unit (Arduino/esp32 etc.), a LoRa module, and a Bluetooth module. The microcontroller also needs power, which can be power banks, solar, etc. In total, a microcontroller with this setup can cost downwards of 6$ to buy, and even less to manufacture.

These modules are also very small and can easily be hidden, which can make them difficult to take down. Additionally, they can be placed anywhere and still relay messages to the network. This is because the entire network is ad-hoc.

LoRa also uses very little power (Giovino, 2019). A small microcontroller with a battery can be created and hidden somewhere no one has access to it (e.g. buried in dirt, on a roof) and be left alone for months, fully operational. With a tiny solar panel, they will work indefinitely.

Privacy

The privacy on the network is very good as everyone receives and sends all the messages on the network, which means that it is impossible to track down the message's original sender and whom the message was meant for. This is known as *shadow messaging* or *managed flooding*. Furthermore, there is no compromising data connected to the message, nor the connection between the devices. Bluetooth uses an address system, similar to IP addresses, that can not be natively tracked down. In dense areas, there will be a lot of Bluetooth-enabled devices so finding one specific device based on the ID is very difficult.

The messages are also encrypted upon sending. This will further add to the size of the message but is still integral to providing privacy and security to make the network usable.

Prototype

As mentioned, we have created a prototype for both the microcontrollers and *The Freedom Forum* application. With our three microcontrollers and the app running on our phones, we achieved flawless communication between the three red points on the map in figure 4 below. We tested with three nodes. All the nodes had microcontrollers close by, and we used the app which

communicated with the microcontroller over Bluetooth. Then the microcontrollers communicated with each other and to the phones connected to them. This all happened completely seamlessly for us, the users.

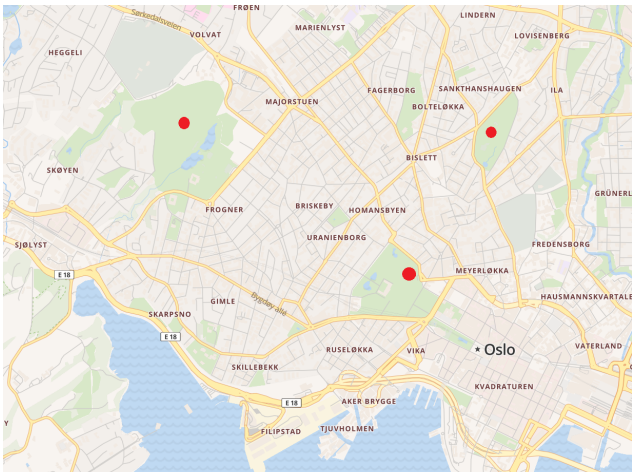

Figure 4: Our Results

We achieved flawless communication in the Oslo city center between the three red dots on this map.

The microcontrollers

The microcontrollers we used vary in size and shape (this is due to us having limited resources and using what we had on hand), but they all have the same abilities and are all very small. Two of the microcontrollers we used are depicted below in figure 5. As you can see, they are about the same size as an AirPods case.

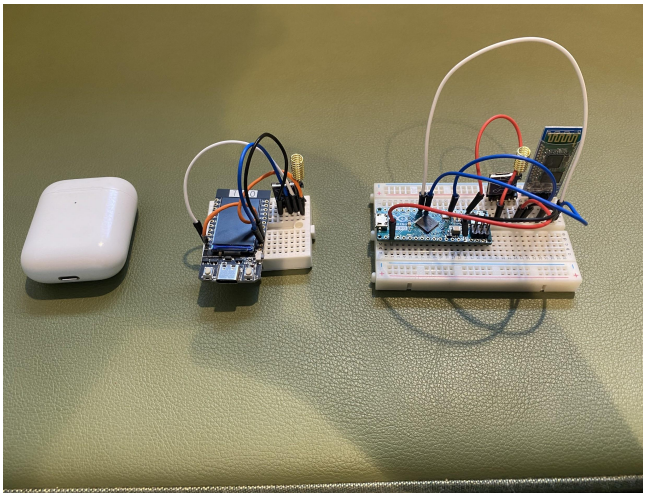

Figure 5: Microcontrollers

Two of our microcontrollers. They have slightly different parts but communicate flawlessly.

The App - The Freedom Forum

We designed the app to be intuitive and easy to use for anyone, no matter their skillset. The app features a single chatroom that everyone connected to is a part of. The app also features a "Connected"-indicator, to make sure it is obvious if a person is connected to a network or not. The app has two additional pages, one for changing settings (such as name), and one for a simple FAQ and explanation of the app and the protocol used.

When a person is using the app, their phone is used as a node in the mesh network, resulting in everyone close to them being able to participate in the chatroom as well. This all happens completely seamlessly. The app is depicted below in figure 6.

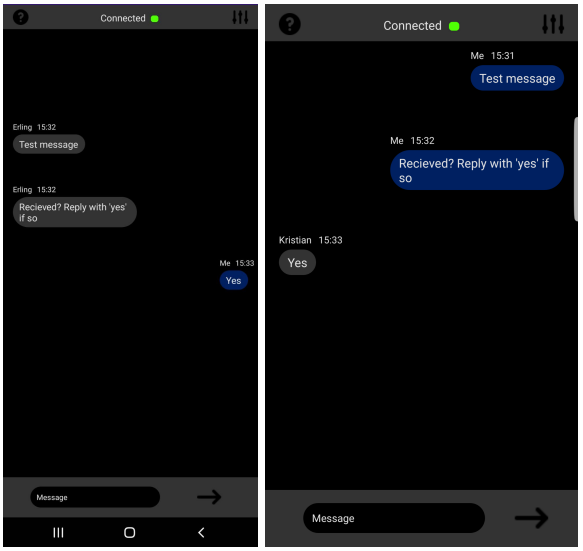

Figure 6: The Freedom Forum

Our chat app - The Freedom Forum. It has a simple interface and allows for communication without access to the internet, even without LoRa microcontrollers nearby.

Installation

One issue that is yet to be resolved is installation. In a situation where the internet is shut down, it might be difficult to install the app. One possibility is to host the app on the network and be able to transfer the app from one device to another using LoRa and Bluetooth, although this could put a huge strain on an already limited network.

Sideloading, downloading an app from outside the official store, is another feasible option. However,

doing so on iOS devices might pose an issue. Apple has been clear that they do not want the possibility to sideload applications (Apple, 2021). Still, there are some projects out there that show that it is possible to do so, like Altserver (Testut, 2022).

Sideloading on Android is substantially easier. As long as we can provide a .apk file, which can easily be installed outside of the google play store.

Future work

While we have a completed and functional prototype, we did not have the time or resources to fully test it to its limit. One potential issue is bandwidth issues over LoRa, which has a low rate of transfer. However, this could potentially be fixed with a message queue system on the microcontrollers, but it is not something we had time to implement. We did create a testing script that sent messages very rapidly after each other over the network (~100ms between each message), but we did not perceive any issues with messages dropping or similar bugs. Additionally, as mentioned earlier, we do compress messages up to 50% which takes some of the stress off the network.

The prototype of the app is as of writing also only available on Android, because neither of us has access to a Mac, which is required to write native iOS applications.

We also wish to engineer a simple method of obtaining the app and microcontroller code during an internet shutdown for both Android and iOS, as described in the “Installation”-section.

Conclusion

Our solution combats complete internet shutdowns by providing a long-range, accessible communication platform that works without the need for internet access. Our solution is accessible to everyone with a smartphone, as well as easy and cheap to extend for those with some technical knowledge. The solution is also feasible and effective as we have proven with our prototype. It additionally provides a simple and understandable user experience. Our project undoubtedly improves upon currently available solutions, all while still having clear areas of possible improvements, such as engineering a method of downloading the app without internet access.

References

Adelantado, F., Vilajosana, X., Tuset-Peiro, P., Martinez, B., Melia, J. & Watteyne, T. (2017). *Understanding the limits of LoRaWAN.* https://arxiv.org/abs/1607.08011

Aislelabs. (2014). *iBeacon and Battery Drain on Phones: A Technical Report.* Retrieved from https://www.aislelabs.com

Albrecht, M., Blasco, J., Jensen, R., & Marekova, L. (2021). Mesh Messaging in Large-Scale Protests: Breaking Bridgefy. *CT-RSA 2021*, 375-398. https://link.springer.com/chapter/10.1007/978-3-030-75539-3_16

Albrecht, M., Eikenberg, R. & Paterson, K., (2022). *Breaking Bridgefy, again: Adoption libsignal is not enough.* https://doi.org/10.3929/ethz-b-000535118

Apple. (2021, October). *Building a Trusted Ecosystem for Millions of Apps.* Retrieved from https://apple.com

Giovino, B. (2019, 13 February). *How to Implement LoRa Firmware Over the Air (FOTA) with Minimal Power Consumption.* Retrieved from https://www.digikey.com/en/articles/how-to-implement-lora-fota-minimal-power-consumption

Lora. (u.d) *LoRa by the numbers*. Retrieved 2 May 2022 from https://www.semtech.com/lora

Ratcliffe, R. (2021, 2 April). *Myanmar coup: military expands internet shutdown.* Retrieved from https://www.theguardian.com

Repucci, S. & Slipowitz, A. (2021, March), *Democracy is under Siege*. Retrieved from https://freedomhouse.org/report/freedom-world/2021/democracy-under-siege

Repucci, S. & Slipowitz, A. (2022, February). *The global expansion of authoritarian rule.* Retrieved from https://freedomhouse.org

Samsung. (2020, 22 September). *What is the maximum range of a Bluetooth connection?*. Retrieved from https://www.samsung.com

Sanchez-Iborra, R., Sanchez-Gomez, J., Ballesta-Viñas, J., Cano, M. D., & Skarmeta, A. F. (2018). Performance Evaluation of LoRa Considering Scenario Conditions. Sensors (Basel, Switzerland), 18(3), 772. https://doi.org/10.3390/s18030772

Shahbaz, A. (2018). *The Rise of Digital Authoritarianism.* Retrieved from https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

Taste The Code. (2022, 4 March). *LoRa Distance Testing with RYLR998 in open field – Amazing Results!* [Video]. YouTube. https://youtu.be/d9u6QIyR8a8

Testut. R. (2022). *Altstore* [Computer software]. Retrieved 2 May 2022 from https://github.com/rileytestut/AltStore

van den Broek, F. (2011). *Eavesdropping on GSM: state-of-affairs.* https://arxiv.org/abs/1101.0552