NSN: 140469120 Name: William Martin

HOWICK COLLEGE

2024

Digital Technologies and Hangarau Matihiko
3.1 (AS91900)

Conduct a critical inquiry to propose a digital technologies outcome

Level 3, Version 1, Credits 6
Due:23/08/24

Conduct a critical inquiry to propose an Electronics outcome

Achievement	Achievement with Merit		Achievement with Excellence	
Conduct a critical inquiry to propose a digital technologies outcome.	Conduct an in-depth critical inquiry to propose a digital technologies outcome		Conduct a comprehensive critical inquiry to propose a digital technologies outcome.	
Final Grade	**N**	**A**	**M**	**E**

Authenticity Statement

I declare that all work presented for this assessment is my own and I have acknowledged all sources that I have used.

Signed William Martin **Date** 01/09/2024

Problem:

Many people are conscious of their personal privacy online and in the real world and spend much of their time worrying about their security against outsiders accessing their personal information or the ever present opportunities for nefarious activity in their everyday lives used to harvest data. These people may feel like they have very little opportunity to stop strangers or even their own devices from nonconsensually harvesting their personal data. There are currently few easily accessible solutions for consumers to buy or build themselves.

Potential Arduino solution:

A possible way to give consumers a way to minimise the amount of information outsiders have access to, in order to improve personal privacy, is to build and design a system that prevents the ability for devices to record you and others' conversations and actions without their consent. The system explored in this inquiry sets out to give open access to an audio privacy device design that would be assemblable with minimal cost and easily accessible equipment; able to emit silent white noise, inaudible to the human ear, causing no environmental disturbance to users whilst giving them confidence in privacy of their conversations.

Potential Inquiry Questions:

What concerns are there around personal privacy regarding audio recording and listening devices?

- What concerns exist around personal privacy and the freedom to have a closed conversation and why is it important for people to be able to do so?
- What challenges can be faced when attempting to build privacy while having conversations with peers/family/friends/co-workers?
- Why do we experience these challenges and who are the causes of these privacy concerns/challenges?

Is there a plausible way to find a universal solution for all types of audio recording devices?

- What frequencies can different types of microphones pick up?
- Do frequencies out of these ranges affect the audio being captured within this range?
- How do ultrasonic sound waves affect audio recordings across all recording hardware?
- What ethical/health and safety concerns must be considered for the use of ultrasonic sound waves to improve privacy?

How can an arduino be utilised to solve this problem?

- How can ultrasonic sensors be utilised to distort and obscure the recording capabilities of listening devices?
- How best can this outcome be achieved and optimised for discrete and easy deployment by the user?

What concerns are there around personal privacy regarding audio recording and listening devices?

What concerns exist around personal privacy and the freedom to have a closed conversation and why is it important for people to be able to do so?

There are many areas in which privacy is important to everyone in the world, however, there is an ever growing list of concerns people have about the security of their personal privacy in a world of always developing technology.

“Smart devices with the capability to record audio can create a trade-off for users between convenience and privacy”[1]

These technological advancements have allowed for people to operate in their daily lives with much more ease than they would otherwise be able to but this has come at a cost; this cost being their privacy.

We live in a world of data harvesting and targeted advertising where our own privacy has shifted from being an important right to something of a second thought. It has become the standard to expect even your own devices to be tuned to spy on you. This, along with threats of nefarious activities by unknown eavesdroppers makes navigating the world of privacy difficult for consumers.

“The proliferation of rogue bugs and audio listening devices poses a significant threat to individuals’ privacy and security. Whether deployed for corporate espionage, personal vendettas or surveillance, these devices can compromise sensitive information and undermine trust in personal and professional relationships.”[2]

This problem of personal privacy is an everlasting battle as the compactness of audio listening devices is constantly improving and making it harder for people to manage their privacy from unwanted ears.

Many people may feel as though this is not a concern in their lives as they have no reason to suspect anyone would spy on them in their own life but it is important to remember that our own devices aren’t always our friends and can often be used against us to non-consensually gather out data and personal information.

“Alexa is an always-on device, so it's constantly listening for the wake word and will record anything that comes after it. However, just because Alexa is always listening doesn't mean it's always recording.”[4]

“Companies offer "always-on" devices that listen for our voice commands, and marketers follow us around the web to create personalised user profiles so they can (maybe) show us ads we'll actually click. Now marketers have been experimenting with combining those web-based and audio approaches to track consumers in another disturbingly science fictional way: with audio signals your phone can hear, but you can't. And though you probably have no idea that dog whistle marketing is going on, researchers are already offering ways to protect yourself.”[5]

Like many fields it is important to get informed consent from any technology user before accessing or gathering their personal information but we find more and more that this virtue is disregarded and revenue and profit come first for many technology producers or can be all too easily compromised by malicious external access to these devices.

“Our analysis suggests that institutional concerns, particularly about contractors and third party developers, are most pronounced. At the same time, privacy protection behaviour is largely absent, with few users engaging regularly in technical, data-related, or social forms of privacy protection. Nevertheless, certain privacy concerns are significantly and positively associated with privacy protection behaviour, partly refuting the notion of the privacy paradox.”[3]

What challenges can be faced when attempting to build privacy while having conversations with peers/family/friends/co-workers?

As we have already established, privacy is a very important aspect of technological design, but, unfortunately it is apparent that the current privacy measures in place for users are inadequate. This is due to a wide array of problems with the way the devices we all carry on our persons or have in our homes operate. Many household objects and personal devices can double as a spying device.

“Rogue bugs and audio listening devices operate by capturing sound waves in their vicinity and converting them into electrical signals that can be recorded or transmitted to a remote location. These devices can be concealed in a wide range of objects, including household items such as clocks, lamps, or even electrical outlets.”[2]

As previously mentioned, an eavesdropper doesn’t even need to plant one of these devices in your home, car or work place, many times it is as easy for them as getting access to your phone, laptop, Amazon Alexa or even your smart fridge.

“That’s to name just a few of the things it can do. Yet with all these connected conveniences, can smart homes get hacked? The short answer is, unfortunately, yes.”[6]

All of this makes it very hard for consumers to “get ahead” and keep even their own homes a safe haven from spying.

“Moreover, the surreptitious nature of rogue bugs makes them difficult to detect, allowing eavesdroppers to covertly monitor conversations without arousing suspicion.”[2]

This also means that it is hard to fight the problem at its roots as it can really be so widespread, so in the meantime it can be helpful for consumers to have access to some universal solutions to work against all of these possible breaches of privacy.

Why do we experience these challenges and who are the causes of these privacy concerns/challenges?

There are many reasons we might find our privacy is being compromised, some of which are collateral damage of having consumer aides like personalised content/advertising and other services related to big data, like route memory on maps services, or data collection for developers and product designers to review their products’ abilities (like windows diagnostic data[7].

Alongside these optimistic forms of “helpful” spying the door for more malicious forms of spying is opened. This would be due to intruders accessing these sets of data.[8] This shows that even when developers have good intentions with their data collection they themselves are still at risk of privacy breaches, meaning that these useful features could come at the price of your privacy.

These breaches of your personal data can be used by sinister actors to steal your identity, access your banking information or even affect your credit.

“If your information is exposed because of a data leak, you may become a victim of identity theft. This can have long-term financial consequences and a negative impact on your credit.”[9]

Is there a plausible way to find a universal solution for all types of audio recording devices?

What frequencies can different types of microphones pick up?

Most microphones you will find in the average person's home can be affected by ultrasonic sound waves. This however does not mean that the devices are designed for this frequency, many microphones, like the ones in most mobile phones, are limited to a frequency range of the audible spectrum of sound.

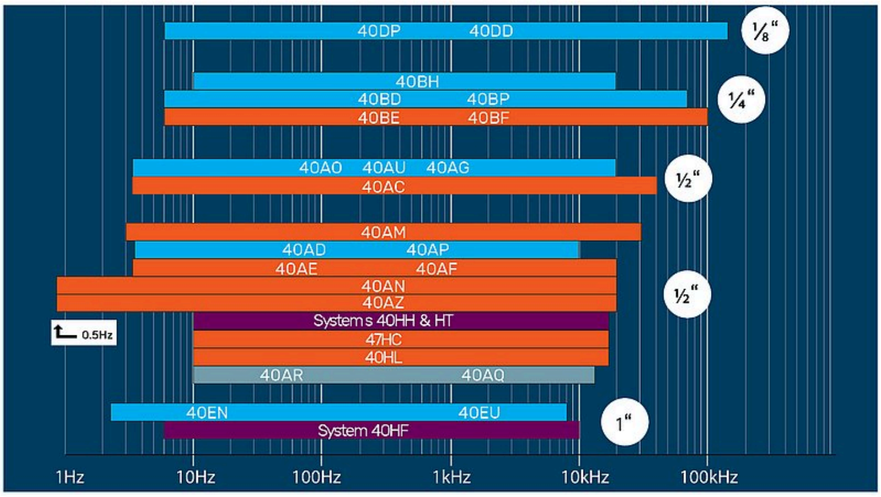
“A frequency region refers to a specific range of frequencies within the audible range of human hearing (typically 20 Hz to 20,000 Hz).”[10]

“Microphones generally have a bias towards the audible range (20Hz-20kHz) simply because that's what we generally want them for”[11]

This is certainly true for the microphones that would be found in the average person’s home and thus will be used as the range for this inquiry.

It is possible to record sound above this frequency range and in theory it could be reduced using physical filters or an equaliser to lower the volume of the ultrasonic frequency band, so the effectiveness against ultrasonic microphones is questionable.

- Higher end equipment and skilled technicians seem to be an effective counter to the idea of ultrasonic jamming.[12]
- We can see, generally most microphones do not capture past 20khz[13]



The microphones are grouped according to size of external diameter, i.e. 1”, 1/2”, 1/4” and 1/8”. The Part or Model number of each microphone is also shown.

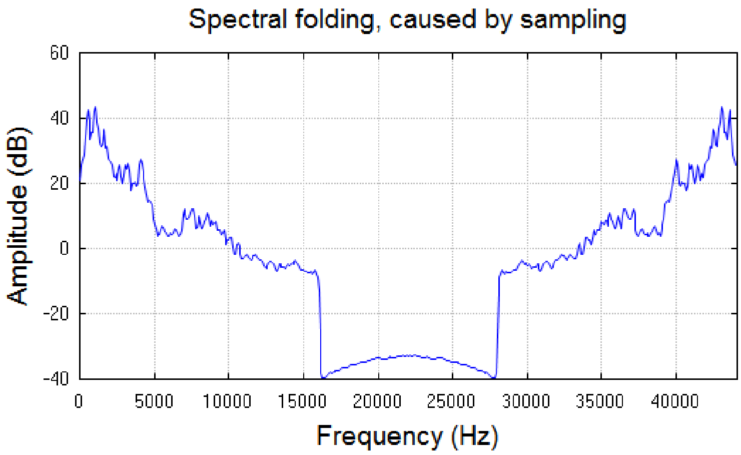
Do frequencies out of these ranges affect the audio being captured within this range?

Ordinarily this limited frequency range would seem like a bad thing but it is actually invaluably useful and that is because of an audio phenomenon called anti-aliasing.

“Aliasing is a phenomenon inherent to Doppler modalities which utilize intermittent sampling in which an insufficient sampling rate results in an inability to record direction and velocity accurately”[14]

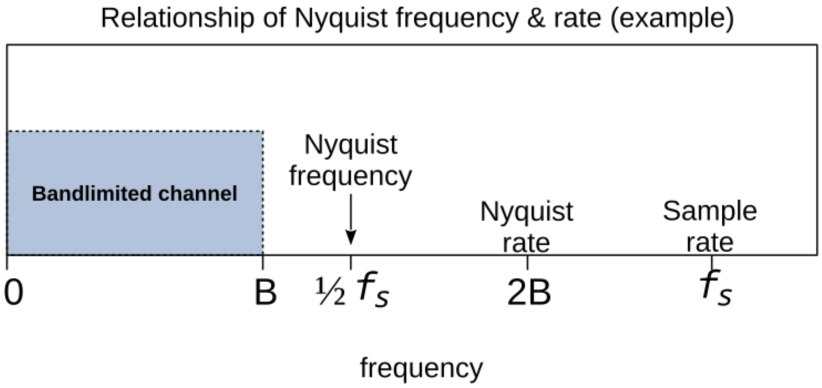
“Audio aliasing is a type of distortion that can occur when a signal is sampled at a rate that is too low to accurately represent its high-frequency content. When this happens, the high-frequency signals can "fold over" into lower frequencies, creating unwanted artifacts and distortion in the audio signal.”[15]

This phenomenon can be utilised in this project as we have already determined that most consumer microphones will be limited to the 20Hz-20kHz range; so we will see that using frequencies slightly above this range will cause them to “fold back” into the audible sound range in a recording, allowing any conversation to now be overlaid with white noise.



[15]

We can also use Nyquist frequency principal to determine this “folding point” and figure out the exact ultrasonic frequencies (or range of frequencies) to use to maximally interrupt the recording of dialogue.[16]



[17]

How do ultrasonic sound waves affect audio recordings across all recording hardware?

The aforementioned research suggests that the proposed solution, whilst not bulletproof, is a commendable start in attempting to give users better control of their privacy. Not all microphones will be affected by ultrasonic interference and others that will be can be processed to remove this interference; but for the purpose of this inquiry it is true that this could in theory be a practical solution, when applied in the average person's home against consumer grade microphones like their mobile phones, computers, smart speakers.

What ethical/health and safety concerns must be considered for the use of ultrasonic sound waves to improve privacy?

An immediate ethical concern is the legality of such a device, as many jurisdictions around the world would be prone to disallowing the personal use of any jamming device. Ultrasonic jammers are prohibited in many countries and states and it is best to check local laws around ultrasonic interference.

“Despite being commercially available, the legality of using such devices varies by region. These jammers respond to growing concerns about privacy amid a proliferation of ever-listening smart devices.”[18]

New Zealand is one of the countries where this kind of interference is prohibited.

“In New Zealand, the use of signal jammers is prohibited by law. Intentional interference with wireless signals is illegal and can result in a fine of up to NZD 10,000 (approximately €5,800) or a two-year prison sentence. The Radiocommunications Act 1989 and the Radio Spectrum Management Act 2014 are the main laws governing the use of signal jammers in New Zealand. These laws define the conditions for the use of radio spectrum, including transmitters and receivers.”[19]

Alongside legal concerns there is a present concern for the physical effect on the health of humans and household pets.

“Humans can hear sound at frequencies up to about 23,000 Hz (Hertz). Louisiana State University researchers report that mice and rats are sensitive to sound up to 60,000 and to about 76,000 Hz, respectively. However, common house pets such as cats and dogs can also hear ultrasonic frequencies. Cats can perceive sound up to about 64,000 Hz, and dogs perceive sounds up to 45,000 Hz. You should consider not using noise as a repellent for mice if you have pets.”[20]

However it has been shown that although pets can hear this range of frequency they will not be harmed by it and are not disturbed by it.

“Thankfully, there’s no evidence to support the claim that ultrasonic pest repellers are not safe for dogs (or will cause long-term neurological damage).”[21]

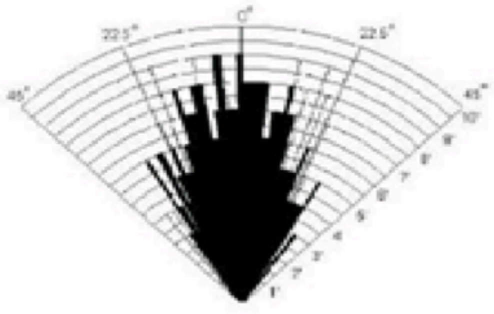
How can an arduino be utilised to solve this problem?

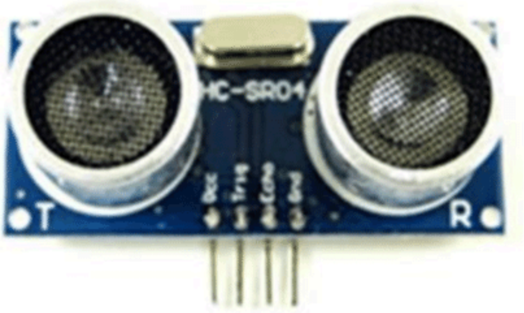
How can ultrasonic sensors be utilised to distort and obscure the recording capabilities of listening devices?

To utilise ultrasonic sound waves, using the principles and ideas discussed in previous sections I intend to use a (or multiple) HC-SR04 to produce these ultrasonic frequencies as it is a simple and cost effective arduino component that I have personal experience using and is widely available.

This ultrasonic sensor is used for measuring rough distances and has an emitter and a collector for ultrasonic waves. The component has a 30 degree operating range but as we are not using it for measuring distance and do not need to receive ultrasonic signals back the actual ultrasonic emission cone is 60 degrees.

“Typical ultrasonic sensor radiation pattern and external view of HC-SR04. The viewing angle is 50-60 degrees, but effective viewing angle is less, about 30-40 degrees.”[22]

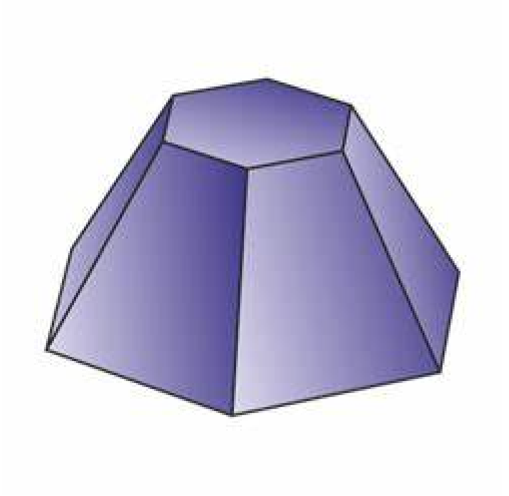


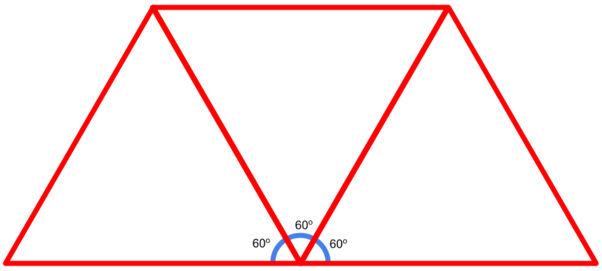


[22]

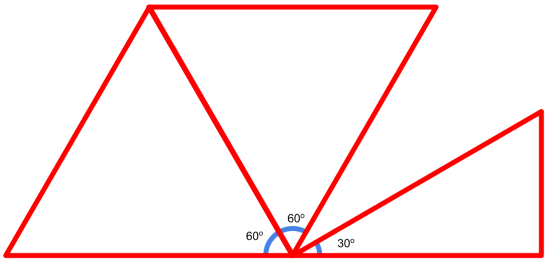
I had hypothesised that both the emitter and collector are the same component but are utilised by the HC-SR04 board differently and conferred with my electronics teacher; he confirmed my hypothesis so I plan to disassemble multiple of the HC-SR04 boards so that I can use them independently from the board and will only need a single HC-SR04 controller board in my project.

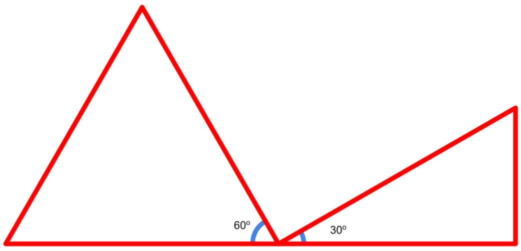
I intend to implement these boards in a 3D printed housing allowing for exact placement, leading to better coverage of an area. This device is intended to be placed on top of a surface such as a table or bench so the device only needs to cover 180 degrees above the plane it is placed on. This means that a truncated hexagonal pyramid (with the sloped sides having a 60 degree slope) would allow for a full coverage if all faces (excluding the bottom) have an emitter mounted to it.





This would allow for the sensors (on a perpendicular plane to the table) to cover 180 degrees



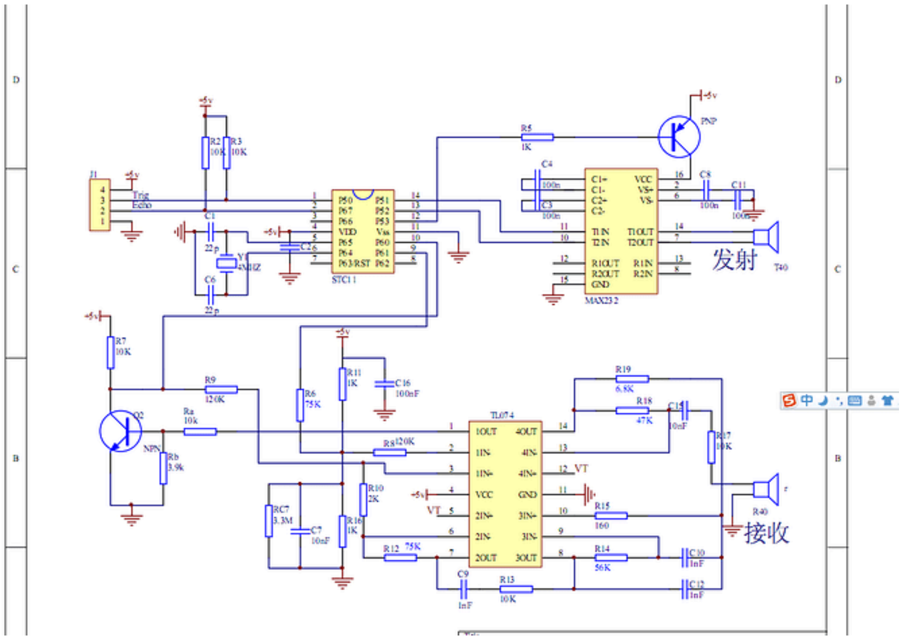


Having the slope be 60 degrees allows for the sensor's effective cone of 60 degrees to be in line with the plane it is placed upon.

How best can this outcome be achieved and optimised for discrete and easy deployment by the user?

The outcome could be further optimised by fluctuating the frequency emitted by the HC-SR04 to maximise distortion. This is not something that the HC-SR04 allows for in its typical configuration but with another small tweak to its controller board we can “hijack” one of its microprocessors and gain direct access to its input pins with the arduino board.

This is a diagram of the HC-SR04 circuit board (provided by John Wasser, long term user of the arduino forum):

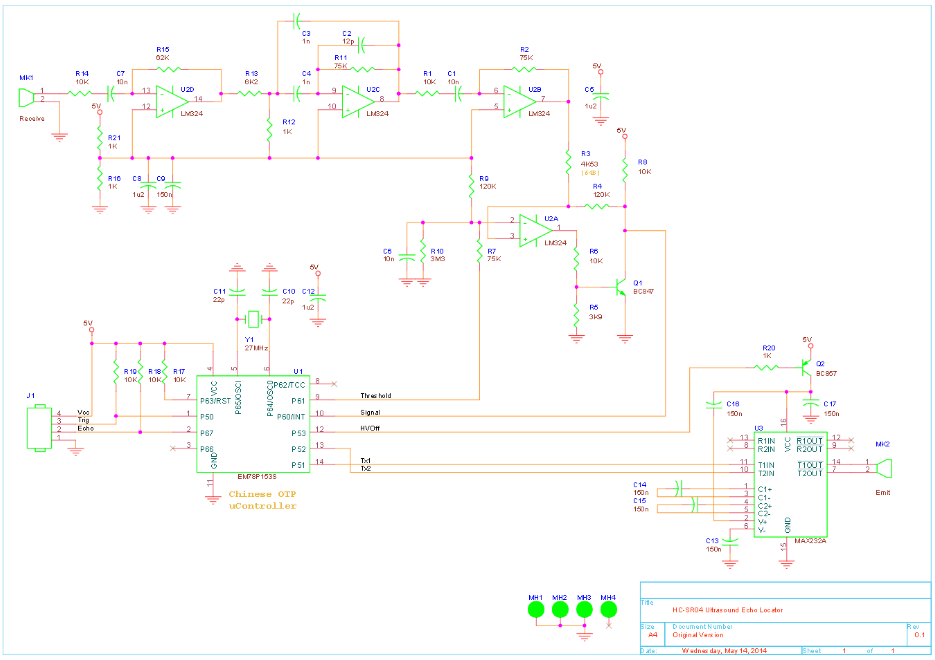


[22]

“The HC-SR04 uses a MAX232 chip to boost the voltage going to the ultrasonic sender. It uses two pins of the little processor chip to send constant 40 kHz square waves that are 180° out of phase (one is HIGH while the other is LOW). There is also an 'enable' pin to turn the pinger on and off. See the upper-right part of the attached schematic.

Un-solder the processor and connect the Arduino in place of those three pins. Use the Output Compare Register pins of one timer (probably Timer1) and you should be able to easily cover the desired frequency range.” - John Wasser[22]

This is a diagram (from Emil's Projects and Reviews) where he is achieving a similar outcome and is able to "hijack" the HC-SR04 microprocessor:

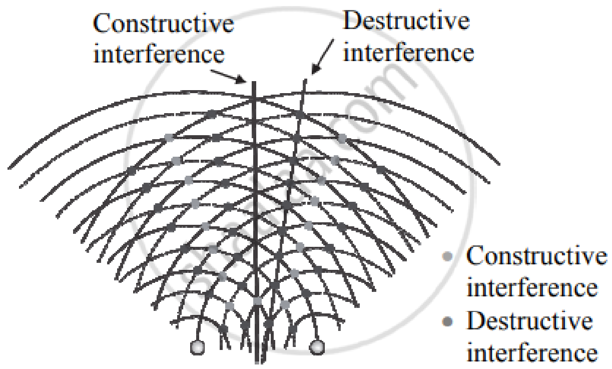


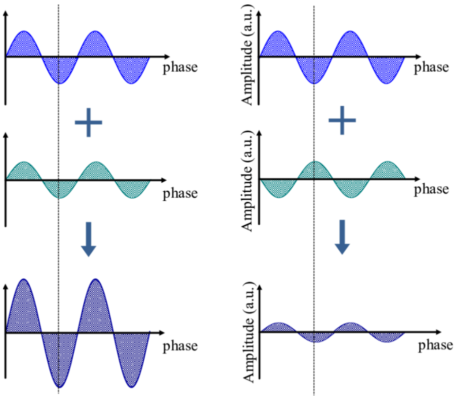
[23]

This helps confirm that the frequency emitted by the HC-SR04 can be manipulated by "hijacking" its T1in, T2in and power supply and connecting them to the arduino.

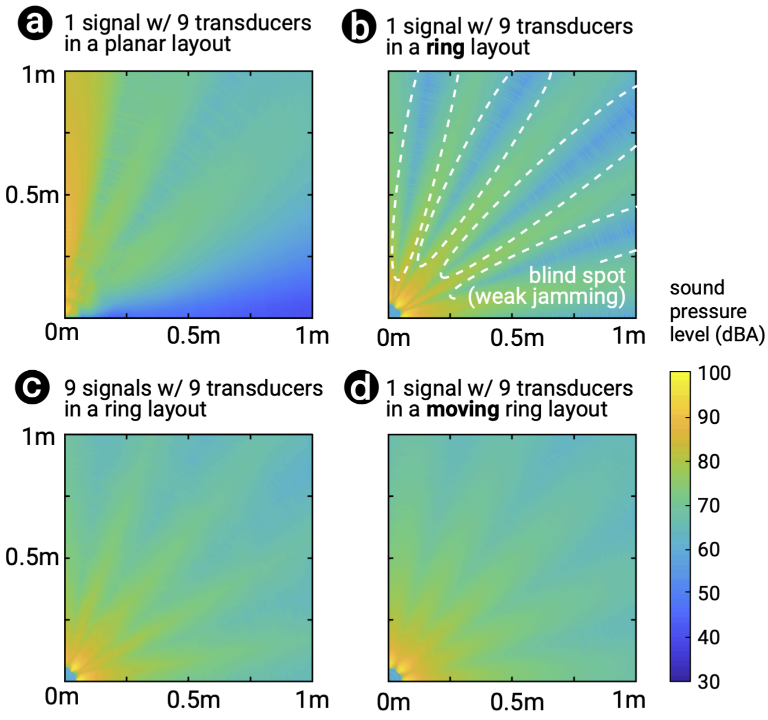
I aim to better optimise ultrasonic coverage, as the strength of the ultrasonic waves will be weaker near the edges of their cone and there will already be minimal gaps between the cones at certain points in space; either due to the emitters being slightly offset and not directly against each other as shown in my diagrams displaying the angles and coverage and also as we are working in 3D space and even though there will be full coverage of the x,y, and z plane there will be gaps in coverage as we rotate between these planes.

In order to do this I could make the housing a more complex shape allowing for the placement of more ultrasonic emitters, thus allowing for an overlap of the ultrasonic coverage; however, as all of the emitters are going to be controlled by the same HC-SR04 board (see previous section) they will all be in phase and this will cause both destructive and constructive interference in these overlaps. This new problem was not encountered before when there was no overlap.





A study conducted by the University of Chicago[24] testing the effectiveness of a similar device found the same issue in their overlaps.



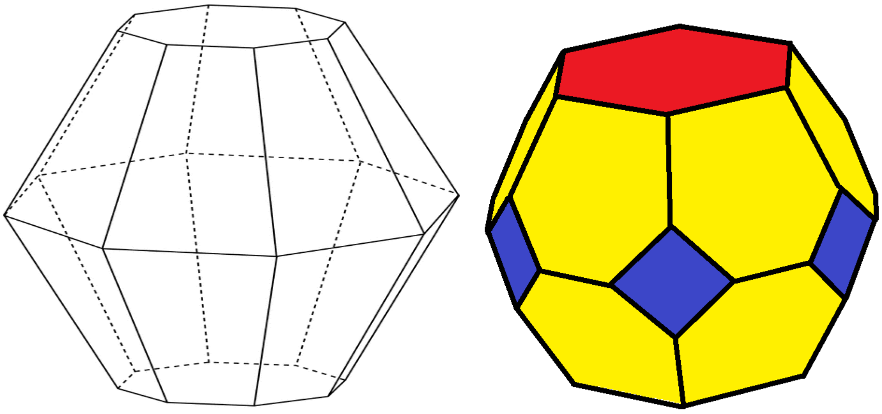
[24]

The way they planned to overcome this issue was by making a device that was wearable. This ensured that the user of the device was always in close proximity and was protected, whilst also giving the emission better consistency, due to inherent movement of the device (and user's arm) during conversation.

"our device exploits a synergy between ultrasonic jamming and the naturally occurring movements that users induce on their wearable devices (e.g., bracelets) as they gesture or walk."[24]

For similar results I intend to construct the housing for my project on a rotating base, I could either have it flat on the active surface, or raised on a tripod, with a new truncated hexagonal bipyramid shape to give space for circuit housing underneath (the bottom half of the bipyramid would stay stationary while the top half would rotate using a motor). The former may give better coverage but the latter would give a better aesthetic for the product and would make it look much more professional and could possibly cause it to be more compact.

Truncated hexagonal bipyramid:

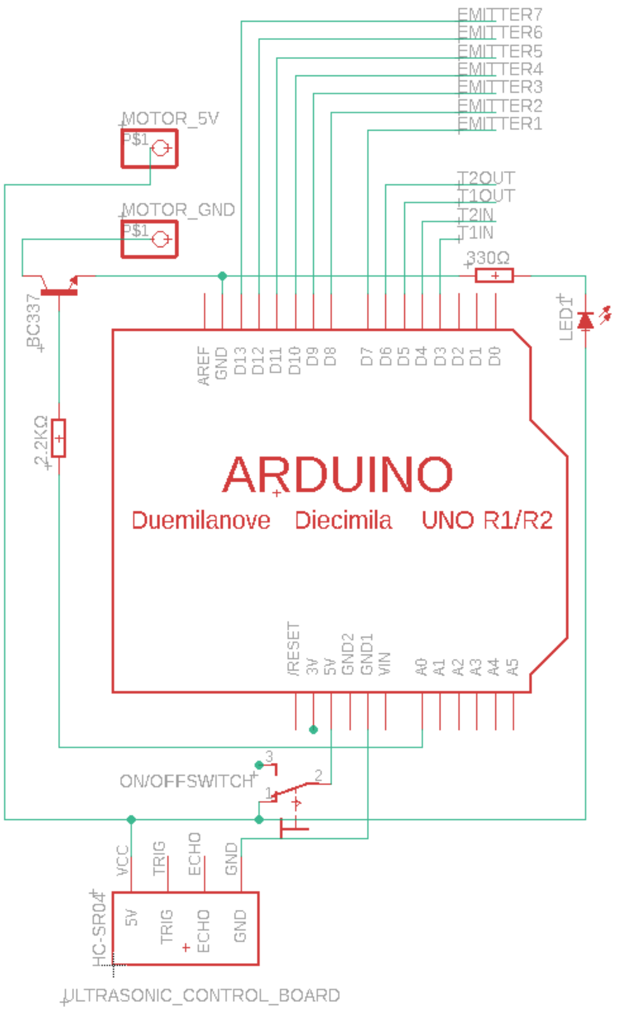


Project Timeline:

02/09/2024 - 04/09/2024	Disassemble HC-SR04 components and repurpose their parts.
06/09/2024	Evaluate the outcome of disassembly and test HC-SR04 components in new configuring and decide if a custom circuit board should be made or the original HC-SR04 board should be used.
09/09/2024 - 11/09/2024	Learn to use new Fusion CAD software and make a proposed design for the outcome. Finalise if the original HC-SR04 board is used or a custom one will be.
14/09/2024 conditional	Design a custom board for the repurposed HC-SR04 components and arduino uno.
14/09/2024 - 18/09/2024	Construct the final circuit and take measurements of components to use for modelling the project's housing.
20/09/2024 - 22/09/2024	Design CAD model in class and in personal time.
23/09/2024 - 24/09/2024	Construct CAD model and begin assembling the product.
14/09/2024 - 27/09/2024	Program and test the board between other processes and during down time to make sure the outcome is successful.

Proposed electronics outcome

System diagram



This diagram is a simple representation of how the product will work. It is difficult to display how it will work as I am deconstructing components of the HC-SR04 whilst still utilising the board itself. Because of this I have notated where wires will go to their respective components as it is unrealistic to have them all in the schematic. The emitters 1 - 7 will be all of the independent emitters connecting directly to the arduino board, this is due to them being two pin so in order to power them with the right signal I have linked T1OUT and T2OUT from the earlier diagrams of the HC-SR04 layout to the arduino's pin 5 and 6, one or both of these should give an output to arduino, I currently do not know enough about how this works so will have to test this myself. The arduino will take this as an input and then output it back to all of the emitters individually.

The T1IN and T2IN pins will be used to send input to the HC-SR04 microprocessor for it to set the frequency of the emitters correctly.

I will have to extensively test how this will actually work as it is hard to simply theorise such a radical idea and it seems to me at the moment like I might be able to remove the HC-SR04 microprocessor from the board entirely and design my own as I may only need that singular microprocessor for purely the emissions. Alternatively the other microprocessors may still play an important role so I will only know when I have physically carried out extensive testing.

The rotating platform will function by being rotated at a constant speed by a dc motor controlled by the arduino using a transistor.

Component list

- 330Ω resistor
- 2.2kΩ resistor
- 5 x HC-SR04
- LED
- Arduino uno
- Toggle switch
- Motor
- BC337 NPN transistor

Evaluating the proposed electronics outcome

Effectiveness

The proposed outcome is relatively effective for its intended purpose and user base. Unfortunately it is not a universal solution to the proposed problem, however it does seem like a large step in the right direction as there really seems to be no alternative solution. The proposed design should be very effective where applicable (with the ideal microphone types present and not higher grade industry recording equipment). It seems as though there is no lack of effectiveness when deployed against the correct type of microphone and in theory the outcome should be capable of preventing most audio recordings the average user could expect to experience in their own home.

This leads me to believe that if the proposed design is followed the outcome would be extremely successful at providing the privacy protection this inquiry set out to find. When deployed within the correct contexts the product should be able to keep the user’s conversation private and there seems to be no way to counter this jamming device without the use of very expensive audio equipment that would need to be physically present, which, when having the device deployed in the appropriate location, would never be possible. Thus I believe the proposed outcome is extremely effective at solving the problem.

Potential limitations

As stated before, the only limitations that could be expected are with using the product outside of its intended environment where professional grade equipment could be used to record the audio. This is an inherent limitation of the use of ultrasonic waves to prevent recording and could only be fixed by using an alternative approach that does not use ultrasonic sound. However, This equipment is bulkier, larger, more expensive and would not be viable in any kind of secret spying device, so in my opinion this is not a particularly relevant limitation with the design.

The only other limitation could arise from the fact that the proposed device may either be elevated by its own design, or, if the flat design is chosen, by the placement of the device by the user. This could possibly cause the device to have no effect on listening devices below the ultrasonic privacy device. This limitation is not very thought out as I am unable to simulate the travel of ultrasonic waves so cannot test if this would be a genuine problem. Even though this cannot be tested, this limitation seems, to me, as if it would be an inherent flaw in any large open space with no surfaces for the emitted ultrasonic waves from the device to bounce off. This flaw could be mitigated by using the proposed truncated hexagonal bipyramid design and adding additional emitters to the slopes and possibly base of the underside but this in itself has limitations as having the top side and bottom side both rotate would require a very complex design and even more complex wiring in order to maintain connections to both. Additionally, with the current proposed circuit diagram and my understanding of the two pin emitters suggests that no more emitters could be connected to the arduino board and multiple communicating microcontrollers would have to be used which would cause the complexity of this project to be far too steep for the projects intended goal of being replicable by anyone with access to the design and the correct basic equipment.

In the current proposed configuration this possible limitation, if true, would mean that the device would need to be used in a relatively small space. I do not believe this limitation is detrimental to the success of the outcome of the device as this project is to protect private conversations, which would likely happen in an enclosed space.

Another previously mentioned limitation is the gaps in ultrasonic coverage, this is mostly solved by the rotating design but as I am unable to test how the emitters function and have utilised all of them individually, connecting to the arduino board. I could not use the previously mentioned solution of adding additional emitters and altering the housing design to give them overlapping cones of emission as the current circuit design is theoretically limited to 7 emitters (from my understanding of how the emitters function, as they are two pin and do not have an input pin independent of the power and ground pin).

Ethical implications

This project brings up many ethical implications. One that has not previously been mentioned is the possibility of this device to be used for illicit activities. This device, in theory, could potentially be used to prevent law enforcement from being able to record or monitor criminals. However, I do not believe this would be effective against equipment available to any policing agency who use listening devices and due to the nature of it possibly being ineffective in larger open spaces I do not feel as though it would interfere with the general practices policing agencies take with surveillance.

A related ethical implication is the legality of this product. Radio Jamming equipment is illegal when used intentionally in New Zealand but it is difficult to know if that is on a large scale or not as this device would only be intended for use in the home and likely would only be effective for use in the home, where devices such as ultrasonic pest repellers are legal and work by emitting the exact same kind of ultrasonic frequencies. I believe it is best to consult with a legal professional, lawyer or local law enforcement before operating one of these devices.

The final ethical implication is the possibility for physical harm to humans and animals, and as previously stated this should not cause harm to either. This product works using the same kinds of ultrasonic emissions as ultrasonic pest repellents and distance sensors and should not cause any physical or psychological harm to humans or animals. However it may be a good idea to monitor your pets when such a device is in use as these frequencies are within their hearing range and it may upset them.

Bibliography

[1] Is Someone Listening?: Audio-Related Privacy Perceptions and Design Recommendations from Guardians, Pragmatists, and Cynics
[2] Understanding Rogue Bugs and Audio Listening Devices - IconGD Security Consulting
[3] Full article: Privacy and smart speakers: A multi-dimensional approach (tandfonline.com)
[4] Can Alexa Record Conversations in a Room? (lifewire.com)
[5] How to Block the Ultrasonic Signals You Didn't Know Were Tracking You | WIRED

[6] Is Your Smart Home Vulnerable to a Hack Attack? | McAfee Blog
[7] Configure Windows diagnostic data in your organization (Windows 10 and Windows 11) - Windows Privacy | Microsoft Learn
[8] Microsoft data breach exposes customers' contact info, emails (bleepingcomputer.com)
[9] What To Know About Data Breaches, ID Theft And Your Credit | Money
[10] Audio Frequency Range: Seven Crucial Zones You Need to Know (soundgym.co)
[11] microphone - Is there equipment capable of recording the entire audio spectrum (audible through ultrasonic)? - Sound Design Stack Exchange
[12] How does ultrasonic noise affect the sound quality? | Audio Science Review (ASR) Forum
[13] Frequency range of a microphone: GRAS Sound and Vibration (grasacoustics.com)
[14] Aliasing phenomenon (ultrasound) | Radiology Reference Article | Radiopaedia.org
[15] What Is Aliasing In Audio? The Science, Sound, And How To Avoid It (audiosorcerer.com)
[16] Nyquist frequency - Wikipedia
[17] File:Nyquist frequency & rate.svg - Wikipedia
[18] Microphone Jammers Promise Better Privacy, But How Do They Work? (howtogeek.com)
[19] jammermaster.com - regulations - Signal Jammers in New Zealand: Current Laws and Regulations
[20] mice - Are ultrasonic repeller devices painful for dogs? - Pets Stack Exchange
[21] Are Ultrasonic Pest Repellers Safe For Dogs? (Solved) (bcpestcontrol.com)
[22] Ultrasonic Khz - Using Arduino / Project Guidance - Arduino Forum
[23] Emil's Projects & Reviews: Making a better HC-SR04 Echo Locator (vajn.icu)
[24] Wearable Microphone Jamming (uchicago.edu)

Uncited Relevant Sources:
acoustics - How can ultrasound hurt human ears if it is above audible range? - Physics Stack Exchange

Source Analysis and Critiquing

Source 1:

The full paper featured in this source is only available behind a paywall, but we can see from the brief that there is a serious concern for people's privacy regarding audio recording devices. This source has many authors listed and over 80 sources cited whilst having a very professional layout. This is not a very useful source of information although it does seem very reliable and accurate, helping us to build an idea of the gravity of this problem.

Source 2:

This website cites no sources but is published by a security consultancy company as an educational piece. This makes the source very reliable as the publisher(s) are professional security analysts and will have the expertise and knowledge to provide accurate information on the topic of listening devices.

Source 3:

This source also seems very reliable as it is written and presented in a very professional format and has two authors, both listed with their qualifications and positions; both being employed at the Department of Communication and Culture at Nordic Centre for Internet and Society, BI Norwegian Business School, Oslo, Norway. This makes me very confident that the source is extremely reliable and has very accurate data and information.

Source 4:

This source is published by LifeWire, a technology news website; boasting an impressive 200 million annual readers, 10000 product reviews, 15000 how-to guides and 80 tech industry experts. The author of this source is Shannon Flynn, a "Business technology & entertainment journalist with 5 years of experience writing in the industry"[external] who's expertise specialises in "Internet Technology, Networks & Security, Android, Consumer IoT and Video Games, Consumer Technology."[external] This gives me extreme confidence in the source and leads me to believe the information given here is very accurate and reliable as it is from an expert of the industry with years of experience.

Source 5:

This article is authored by a "senior writer at WIRED focused on information security, digital privacy, and hacking. She previously worked as a technology reporter at Slate, and was the staff writer for Future Tense, a publication and partnership between Slate, the New America Foundation, and Arizona State University."[external] who boasts an impressive career in cyber security journalism. This leads me to believe that this source is credible, accurate and reliable.

Source 6:

This is another extremely reliable source as it is published by McAFee, a world renowned cyber security company. The author of the piece is Jasdev Dhaliwal who is a Director of Marketing at McAFee and a self described "Security Evangelist." This makes me very confident in the reliability of the information in this source as it is from a distinguished cyber security expert with "over 10 years of security industry experience, he is a regular writer on the current security landscape and likes to educate others on how to keep themselves, their families, and their homes safe online."[external]

Source 7:

This is a direct guide published from microsoft about windows' data collection and is a direct reference to what was being discussed when the source was cited. This is an indisputable fact and hence the reliability and accuracy of the source is without question.

Source 8:

This is an article published on the tech news site BleepingComputer, "Bleeping Computer® is an information security and technology news publication created in 2004 by Lawrence Abrams. Millions of visitors come to BleepingComputer.com every month to learn about the latest security threats, technology news, ways to stay protected online, and how to use their computers more efficiently."[external] and was authored by Sergiu Gatlan who is a "news reporter who has covered the latest cybersecurity and technology developments for over a decade"[external]

Source 9:

This source is an article posted by what seems to be a clickbait news site by the name of Money. This puts the credibility of the article under heavy scrutiny. However the author is Amarilis Yera, a "lead writer at Money, specializing in consumer credit and credit cards."[external] who has worked at money since 2019 and "graduated from the University of Puerto Rico with a Bachelor's in Linguistics and a minor in Writing and Communication. Her work has been featured in MSN, Yahoo! Money, Nasdaq and more."[external] and has been edited by Taína Cuevas, a "managing editor for Money's consumer credit team."[external] who "has worked as a writer, researcher and editor in an array of industries for close to 20 years."[external] and "graduated from Franklin University Switzerland, where she earned a Bachelor of Arts degree in Visual and Communication Arts and Italian with honors. She also pursued post-graduate training in print journalism from Boston University."[external]

This makes me trust the source more as they are well educated and experienced writers/editors and have sources cited throughout the source

Source 10:

This source is somewhat questionable as no author/editor is listed and the site has no sources cited. This would lead me to believe that this source is unreliable and not trustworthy; however, as the information found and used from this source is concurrent with the information obtained in source 11 I believe that, despite the source itself being questionable, the data provided is accurate and reliable.

Source 11:

This source would immediately be questionable as it was posted to a public forum, accessible for anyone to post to, however, the information gathered here is concurrent with the information found in source 10 which would lead me to believe that the data used is accurate. Additionally, the user who posted this information is run by 7Hz Research, a creative audio company, who are self proclaimed "experts in sound design, composition, music production and sound effects. We have the knowledge and skills to create emotive musical scores for every one of our clients. From some of the world's greatest brands and advertising agencies to indie filmmakers and game developers, we create engaging sounds for all!"[external] This would suggest to me that the information provided has been supplied by people who work in the audio field who can and have provided reliable and accurate information.

Source 12:

This source is relatively unreliable as it has been posted on an open access forum where anybody can post. I have still cited this source as it reinforces the information provided by source 13. This leads me to believe that although the source itself may not be reliable, the information provided and extracted should be as it is concurrent with previously established data.

Source 13:

This source has been published by GRAS, a "worldwide leader in the sound and vibration industry. We develop and manufacture state-of-the-art measurement microphones and related equipment to industries where acoustic measuring accuracy and repeatability is of utmost importance."[external] This is an incredibly reliable source as the data used here is directly from the company and is a publication of data relating to their own audio recording equipment and should be incredibly accurate and reliable.

Source 14:

This source has been published by Radiopedia, their public mission is stated as "to create the best radiology reference the world has ever seen and to make it available for free, for ever, for all."[external] They are a "Rapidly growing peer-reviewed open-edit educational radiology resource"[external] This would cause concern on the reliability as it is open edit but due to the nature of it being peer review it can be, to some degree, assumed that publications should be reviewed and controlled by many experts to prevent incorrect data from being spread. Additionally this source cites many sources. The author, Amir Mahmud, is a MBChB, Radiology Resident with a claim of being a radiology specialty trainee of three years, however this has not been verified. This builds a case for trusting this source but as it is not actually verified by the site there is still reason to be sceptical. Despite this the data extracted from this source is concurrent with source 15, hence why it has been trusted as accurate in this inquiry.

Source 15:

The publisher of this source does not seem professional or reliable, however, the data and information extracted from this source is concurrent with the information extracted from source 14 and is further backed up by data from source 16/17. As this information is concurrent between three distinct sources I believe it is sensible to treat this source and the information extracted from it as being accurate.

Source 16:

This source is cited from Wikipedia, a site that usually cannot be deemed reliable as it is an open-edit source of information, however, this is a fundamental principle of physics and thus is actually indisputable fact. Additionally the information from this source is concurrent with the information in source 14 and 15.

Source 17:

N/A - this source is purely of an image provided in the previous source

Source 18:

This source is published by How-To-Geek, “We’re the team of experts you turn to when your computer isn’t working right, you need to do something technical, or you want to understand the latest gadgets”[external]

They have been recommended as experts by many major publications and respected resources “How-To Geek has been used as a resource for everything from university textbooks to late-night TV.”[external]

(see specific examples)

The author of the article in this source is Sydney Butler, an “Editor, Hardware and Cutting Edge Technology”[external] who has expertise in “pc building, video games, hardware”[external] This suggests that the information provided will be very reliable and accurate. This is further enforced by the fact it refers directly to source 24, having concurrent data.

Source 19:

The credibility of this source is without question as it is directly referring to new zealand law.

“The Radiocommunications Act 1989 and the Radio Spectrum Management Act 2014 are the main laws governing the use of signal jammers in New Zealand. These laws define the conditions for the use of radio spectrum, including transmitters and receivers.”[19]

Source 20:

This source is a public forum where anybody can post so this would suggest it is unreliable; however, the data extracted from this forum was provided by a user who cited the source of this data, giving much more confidence in the credibility of this source. Additionally this source’s data is concurrent with source 21.

Source 21:

This source is authored by Nathan Pavy who “has been in the pest control industry for over 16 years. These days he splits his time between writing for this site, and continuing to work in the field.”[external]

The article itself was posted on the site, BC Pest Control. They state that “We focus on providing information and advice that’s effective and actionable. Nothing more. And with over 16 years of experience, we’ve seen it all.”[external]

Nathan is the primary manager of this site which gives me much confidence in the credibility and reliability of the source and hence the accuracy of the information provided.

Source 22:

This source is another public forum where anybody can post which immediately raises concerns about the credibility of the information provided here, however, the information and schematic extracted from this source was provided by a poster by the name of John Wasser who has an astonishing resume on the site. He is listed as having read over 150 thousand posts, has over 80 days of read time, has visited the site on over 3.6 thousand days and has made over 31 thousand posts. This gives me great confidence in his expertise and given that the circuit diagram and advice given is concurrent with the information extracted from source 23 I am confident that this source is credible and trustworthy.

Source 23:

This is a blog post by the owner of a site called Emil's Projects & Reviews. This post has an incredible amount of data and evidence of data that I would immediately be inclined to believe that the source is credible but as it is also concurrent with the changes suggested in source 22 and achieves the exact outcome proposed I believe that this source is undoubtedly reliable.

Source 24:

This source is a publication from the University of Chicago which received multiple awards and was featured in many publications, has an incredible amount of data recorded and has many sources listed (in the actual paper, the source linked in this inquiry just links to their web page that summarises their findings).