

# Private Data Exfiltration from Cyber-Physical Systems using Channel State Information

Anonymous Author(s)

## ABSTRACT

Data exfiltration methods aim to extract data without authorization from a network or device without detection. In this paper, we present a novel data exfiltration method making use of Channel State Information (CSI) from ambient WiFi signals. Modulation is performed by modifying the environment by moving a physically actuated machine resulting in a change to the channel response that is measurable by a distant receiver that is capable of collecting CSI samples. This can be used to exfiltrate data when transmission using conventional methods is not possible but the attacker has control of a moving mechanism. We discuss the design of the covert channel in detail and produce a proof of concept implementation to evaluate the performance in terms of communication quality. We find that even a very simple implementation provides robust communication in an office environment. Additionally, we present several countermeasures against an attack of this type.

## KEYWORDS

Data Exfiltration, Channel State Information, Covert Communication

### ACM Reference Format:

Anonymous Author(s). 2021. Private Data Exfiltration from Cyber-Physical Systems using Channel State Information. In *WPES 2021: 20th Workshop on Privacy in the Electronic Society*, November 15, 2021, Seoul, South Korea. ACM, New York, NY, USA, 13 pages. <https://doi.org/10.1145/xxxxxxx.xxxxxxx>

## 1 INTRODUCTION

Air-gapped systems are common in critical infrastructure, military and intelligence networks, and industrial control systems. The purpose of air-gapping a system by physically isolating it from the Internet and other non-essential networks is two-fold: to prevent malware from getting in and to prevent confidential data from getting out. It is a critical tool in the arsenal of security engineers, and when combined with other appropriate physical security controls and protocols, it can drastically reduce the risks posed by malware, although it is not impenetrable. In other settings where air-gapped systems are impractical or impossible to deploy, because of the need to communicate with other networks, other techniques are employed to achieve these two goals including firewalls, subnets, network monitoring, and endpoint malware detection, to name just a few.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](mailto:permissions@acm.org).

WPES 2021, November 15, 2021, Seoul, South Korea

© 2021 Association for Computing Machinery.

ACM ISBN 978-1-4503-XXXX-X/21/06...\$15.00

<https://doi.org/10.1145/xxxxxxx.xxxxxxx>

Covert communication schemes aim to send data between devices without detection by bypassing security control mechanisms put in place and without interfering with legitimate communications if they are piggybacking off existing messages. On a terminology note, depending on the exact application, the idea of covert communication may sometimes be referred to using other names: *data exfiltration* is most commonly used when malware or an unauthorized user transfers data off a device; and *side-channel attack* is conventionally used when data is extracted at a distance using signals emanating from a target device without direct access or interference with it. Existing covert communication schemes [45] make use of a range of methods from exploiting redundant or modifiable fields of data packets [14], changing the timing of packet transmission [6, 38], making modifications to a device's wireless chip firmware to change the modulation scheme [26], using the audible or the ultrasonic audio range [10, 23], to using device vibrations and accelerometers [18], and using various hardware components of a device to emit electromagnetic (EM) signals [19–21]. These various methods have different limitations, but the main drawbacks are that they either require access to conventional radio hardware, which is not available for wired network devices on air-gapped networks or on systems with strict access control, or their power output is very low which limits the operationally effective distance.

It is known from extensive research in the field of human activity recognition [32] and health monitoring [46], that small changes in the environment can have a significant change on Channel State Information (CSI), which is a measure of an environment's effects on a wireless signal. When combining this with cyber physical systems (CPS) that allow interaction with the physical environment, we believe it is possible to achieve data exfiltration in a diverse set of environments from industrial and factory to office and domestic spaces, and could be used to bypass existing network security controls including physical and logical air-gapping.

We propose a data exfiltration technique that makes use of CSI from ambient wireless signals in an environment. This is applicable whenever an attacker can modify the state of physical mechanisms, but does not have the ability to transmit using conventional communication channels or other side-channels. The advantages of our proposed method include: it can be used to exfiltrate data from an air-gapped system; can be used to exfiltrate data wirelessly (i.e., the attacker does not need to transfer the data using physical storage device or transfer medium); the maximum range is only limited by the ability of a receiver to reliably detect WiFi packets transmitted by a conventional and legitimate wireless cards or access points; communication can be conducted through walls, partitions, and other furniture items; the covert communication frequency can be selected to be resilient to normal noise in the environment; and as we will explain in more detail, using periodic motion removes the need for a training phase which is commonly required in CSI applications.

We make the following key contributions:

- (1) We identify the challenges with conducting a data exfiltration attack of this type and limitations of existing methods.
- (2) We propose a novel covert communication and data exfiltration attack method using Channel State Information (CSI).
- (3) We produce a proof of concept implementation to show and discuss the relationship of various factors that effect communication quality of the channel.
- (4) Finally, we discuss potential countermeasures against this type of attack.

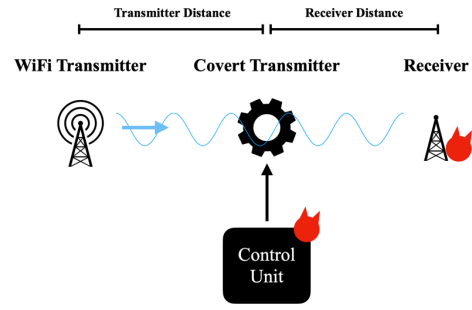
The remainder of the paper is laid out as follows: in Section 2 we provide the background knowledge for CSI necessary to understand our proposed method; in Section 3 we present the scenario and adversarial model that we design our attack around; in Section 4 we present the challenges for using CSI for data exfiltration; Sections 5 and 6 provide a detailed description the design of the covert transmitter and receiver respectively; Section 7 is a discussion of the system as a whole; in Section 8 we describe our proof of concept implementation and evaluate its success by exploring the relationship between several factors and channel quality; Section 9 presents and discusses potential countermeasures to this type of attack; in Section 10 we present related work; and finally we conclude in Section 11.

## 2 TECHNICAL BACKGROUND

Channel State Information (CSI) describes the effect of the environment on a wireless signal as it travels from a transmitter to a receiver [15, 27, 43]. Orthogonal Frequency Division Multiplexing (OFDM) uses many subcarriers to transmit data and CSI describes the effects on each of these individual subcarriers which are each a different frequency. Therefore, CSI differs from the more commonly discussed Received Signal Strength (RSS or RSSI), which is the superposition of multiple subcarriers. As RSS is the combination of many subcarriers, this gives a fairly poor resolution when examining the environments effect on the channel state. CSI is conventionally used to improve the reliability of communication, but being able to view subcarrier level effects caused by the environment has led to improvements in the fields of localization [41, 43, 47], device-free activity recognition [13, 28, 48], fall detection and health monitoring [46], smartphone gesture recognition [30], and cross-technology communication [16].

To calculate CSI we must first calculate the channel matrix  $H$  and this is calculated using the equation  $Y = HX + N$  where  $X$  and  $Y$  are the transmitted and received signal vectors, respectively, and  $N$  is the channel noise. The channel matrix  $H$  is called the Channel Frequency Response (CFR) and the CSI measurements are then extracted by sampling the CFR at the frequencies of the different subcarriers. The CSI measurements are given in the form  $a_n \cdot \exp(j\theta_n)$ , where  $a_n$  is the signal attenuation and  $\theta_n$  is the phase shift for each subcarrier  $n$ . For our purposes, the data of interest is the signal attenuation, which is commonly referred to as the *CSI amplitude* [15, 27], and this is normally output from CSI extraction tools in arbitrary units.

The production of tools [1, 4, 5, 15, 25, 36] to easily extract CSI data from commercial-off-the-shelf (COTS) WiFi cards has made it cheaper and simpler than ever to access this data. These tools normally provide firmware updates for a specific wireless chipset



**Figure 1: System model.** The ambient signals from the Wifi transmitter are affected by the physical position of the covert transmitter which creates a measurable impact on the CSI when the signals are analysed by the receiver.

and the associated software to process the data that it outputs. The CSI from these tools is provided on a per packet basis, as they use the known packet preamble as a reference to compare the received signal too during the calculations. CSI extraction does not require the receiver to be connected to the same wireless network as the device that CSI is being collected from as it is a passive process.

## 3 SYSTEM AND ATTACKER MODEL

In this section, we present the system and adversarial model that our attack is designed around.

The system is composed of several entities. Their relationships are shown in Figure 1 and they have the following roles:

- The *WiFi Transmitter* is a device that is broadcasting wireless signals that provides a source of WiFi packets to piggyback communication off. This device creates a steady stream of wireless network traffic throughout the environment.
- The *Covert Transmitter* is a mechanical device, that when operated, creates an impact on the CSI of the wireless packets sent by the WiFi transmitter. Examples of possible covert transmitters include: pumps, mixers, centrifuges, automatic doors, printers, air conditioning units, or other IoT devices with moving components, etc.
- The *Control Unit* is a computing device that controls and monitors the mechanical state of the covert transmitter.
- The *Receiver* is an attacker's receiver device which is capturing CSI from WiFi Transmitter packets.
- In addition, there may be other WiFi transmitting entities in the environment that the receiver is in range of, but whose signals are not influenced a detectable amount by the covert transmitter. We refer to these as *Additional Transmitters*.

From the covert transmitter, there are two distances of interest: 1) the *transmitter distance*, which is the distance to the WiFi transmitter; and 2) the *receiver distance*, which is the distance to the receiver.

The attacker's goal is to exfiltrate data from the control unit to the receiver using the covert transmitter. The attacker has gained access to the control unit, so is able to modify the mechanical state of the covert transmitter causing it to move and these movements have an impact on CSI. The attacker is able to search the data stored

on the control unit, with the aim of finding data of interest that should be confidential (e.g., encryption keys, passwords, customer data, or trade secrets). The receiver is positioned some distance away from the covert transmitter. However, it is free to move to optimize the reception. The receiver captures CSI from any wireless devices in range and the CSI is processed to search for any covert communications in the form expected using the method we propose.

The attacker does not have the ability to transmit from the control unit using conventional wireless networking or use any other means to exfiltrate the data, other than using the technique we propose. The covert transmitter and control unit also have no way to receive communications from any other entities in the system. The attacker does not control the location of the WiFi transmitter or covert transmitter. The attacker does not know the identity of the WiFi transmitter, so if there are additional transmitters then part of the receiver's task is to identify the WiFi source that is being impacted by the movement of the covert transmitter.

## 4 CHALLENGES

Using the impact of a moving object on CSI for communication has a number of challenges:

*Dynamic Environments.* Environments are rarely completely static, whether it is a domestic, office, commercial, or an industrial environment. Movement of people and objects other than the covert transmitter will have some impact on CSI. Therefore, the receiver must be capable of filtering out the other noise.

*One Way Communication.* Like other data exfiltration methods [18, 23], the fact that communications are one way introduces a number of difficulties for the attacker as the covert transmitter is transmitting in the blind and has no way to monitor the wireless channel. Firstly, there is no way for the receiver to send an acknowledgement or request a retransmission, so the covert transmitter cannot know if a message is received, not received, or is only partially received. Secondly, there is no way to detect the packet transmission rate of the WiFi transmitter, so if it falls below a usable rate for sustained period of time the covert transmitter will be unable to piggyback off the messages, but at the same time the covert transmitter will not know that the receiver will be unable to reconstruct the affected parts of the message.

*Risk of Detection.* Finally, as the attack involves manipulating physical mechanisms to behave in an incorrect and unexpected manner, it is possible that the user or operator may notice a change in behaviour. Whether or not they realise it is a data exfiltration attack, they may take action to resolve the incorrect behaviour of the device.

## 5 COVERT TRANSMITTER DESIGN

We now present the details of the covert data exfiltration scheme. In this section we present the design of the covert transmitter, followed by the receiver design in Section 6, and a more in depth discussion and reasoning behind some of the design decisions that affect the entire system in Section 7.

## 5.1 CSI Impact and Attacker Setup

When a wireless signal propagates through an environment it interacts with objects causing reflection, diffraction, refraction, and absorption. What the receiver actually receives is a sum of signals that have travelled along different paths, which have been attenuated by varying amounts, and are at different phases relative to each other. Our communication method fundamentally relies on the principle that signal paths will vary if the environment changes, and this is measurable using channel state information (CSI). CSI amplitude data for each subcarrier is very stable when the environment is static, much more so than RSS [? ], effectively giving the receiver a CSI fingerprint of a particular environment. If the environment changes to a new state we get a new CSI fingerprint. As stated in the attacker model, the attacker controls a mechanical device, called the *covert transmitter* using the *control unit*. When the covert transmitter moves under the instructions of the control unit, it modifies the environment and this impacts the CSI in a measurable way.

At this point a number of approaches could be taken to identify changes in CSI to transfer information. Machine learning is common for CSI applications [28, 32, 44] as it allows the system to classify changes to the CSI measurements. However, without extensive prior facilities access, a training phase is difficult to perform. Instead, we propose taking a different approach by using periodic motion of the covert transmitter. Using periodic motion will create a repeating pattern in the CSI measurements, an example of which is shown in Figure 2. The figure shows a clear and distinct repeating pattern as time progresses on the horizontal axis which can be picked up by the receiver. The advantage of this approach is that we do not need to compare the CSI data to any data collected or CSI fingerprints measured prior to data exfiltration, so there is no need for training, and if other parts of the environment change communication can still continue.

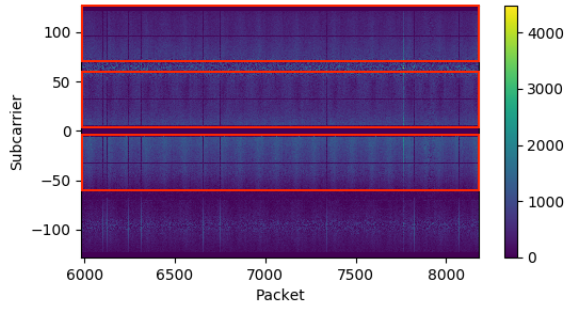
The essence of the concept is that it is now possible to use the frequency of this periodic motion as a carrier signal to send a message. It can be as simple as on-off keying where binary data can be encoded using an OFF and ON state. With the OFF state meaning the covert transmitter is not moving and the ON state meaning the covert transmitter is producing periodic motion at a set frequency. Note that the periodic motion is not limited to rotating objects, it can also be applied to non-rotational motion (e.g., an automatic door opening and closing). The only requirement is that there is repetition of the motion and the influence on CSI of the repeating motion is consistent.

## 5.2 Parameters

To communicate effectively, there are essentially three important parameters that the attacker must carefully consider in order to communicate effectively, depending on the scenario.

**Packet transmission frequency  $F_p$**  from the WiFi Transmitter. This is the average number of packets per second sent by the WiFi transmitter. The attacker does not control this value but it determines the optimal choice of the next two parameters, so if the adversary has an opportunity to measure it, it will be helpful. If not, a small value should be assumed.





**Figure 2: Plot of CSI amplitude data measured with the covert transmitter performing periodic motion. The regions marked by the red boxes show a clear, distinct repeating pattern.**

**The frequency of the mechanical movement  $F_c$**  is in effect the covert transmitter frequency. It will need to be controlled with precision in order to achieve more advanced modulation schemes, but for on-off keying a relatively coarse control is sufficient.

**The length of a covert transmission symbol  $L_s$**  in seconds. This is decided by the attacker but is strongly related to the  $F_p$  and  $F_c$  values. A high value of  $F_p$  and a high level of control over  $F_c$  will allow the attacker to select a short symbol length, thereby increasing the bandwidth of the resulting channel. Conversely, if  $F_p$  is low (or unknown) a longer symbol length is used that fits the modulation scheme.

### 5.3 Modulation

Choosing an appropriate modulation scheme is a decision that will drastically impact the resulting channel. The choice is dictated by the available covert transmitter, and the value of  $F_c$ . For example, if a ceiling fan is being used as the covert transmitter and the attacker is stuck with two states ON and OFF for the fan, then the attacker is somewhat limited in the choice of schemes, e.g., on-off keying or other binary schemes. If the rotational speed can be varied continuously, or in small enough increments, more sophisticated modulation schemes that incorporate multiple frequencies are possible, e.g., phase- and frequency shift keying, or even chirp spread spectrum.

Although the attacker may be limited to binary modulation schemes, he can still make good use of this. For example, binary phase-shift keying (BPSK), specifically a bi-phase Manchester encoding as defined in the IEEE 802.3 standard Section 7.3.1.1 [2] brings with it several advantages which are very important given the drawbacks of blind transmission. Bi-phase Manchester can be modulated with the covert transmitter ON for HI and OFF for LO. Thus a 0 symbol is transmitted with the covert transmitter ON for the first half of the symbol and OFF for the second half, and a 1 symbol with the covert transmitter OFF for the first half and ON for the second half. Importantly, using a bi-phase Manchester encoding provides the advantage that single bit-errors per symbol will result in either HI/HI or LO/LO both of which are identifiably corrupt bits.

Multiple symbol single bit-errors for a byte will corrupt the entire byte so even if the original cannot be reconstructed, the receiver will know that byte is corrupt. Manchester encoding also assists in maintaining time synchronisation, as the modulation will switch between HI and LO at least once every full symbol length. We discuss the potential benefits of more advanced modulation schemes in Section 7.

### 5.4 Message Structure

The data to be exfiltrated can be split into messages with a recognisable structure and length in order to facilitate error correction and recovery. A message starts with a known preamble that the receiver will search for. This is followed by a small header that contain the length of the message and a message sequence number to identify retransmissions or missing messages. This is followed by the body of the message, i.e., the actual data to be exfiltrated. Finally, the message should have some form of integrity check, which can be anything from a proper MAC if a key is shared between the control unit and the receiver, to some form of checksum or even a parity-check scheme.

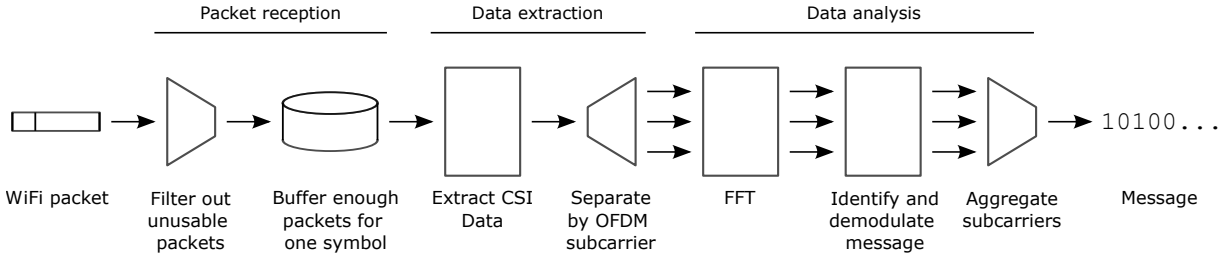
## 6 RECEIVER DESIGN

We now present the design of the receiver and the process it performs to reconstruct the transmitted message from the CSI data. An overview of the receiving process is shown in Figure 3.

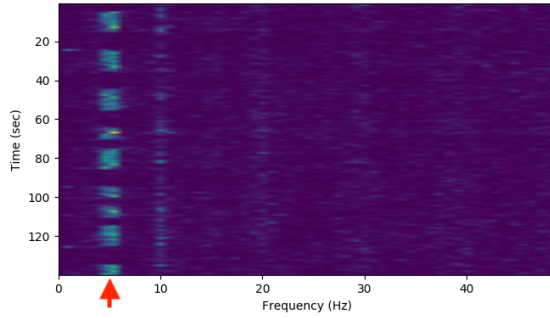
The receiver will extract the CSI from any WiFi source which includes useful information about the message. Our system model assumes that there is at least one such source, namely the WiFi transmitter, however the scheme can use as many WiFi sources as might be available. Each WiFi source is uniquely identified by its MAC address and the receiver will start by filtering out packets that do not contribute based on the MAC address. The receiver does not know the identity of the WiFi transmitter or how much it might contribute to the message—at least for the first message it receives—so the following process needs to be performed at least once for each WiFi source.

The receiver first buffers enough packets to make the subsequent analysis possible, i.e., at least one symbols length worth of packets. It then extracts the CSI amplitude data and performs a frequency analysis on each subcarrier. For each subcarrier, the attacker now has time and amplitude data at each frequency. An example of the output from one subcarrier for multiple symbols is shown in Figure 4. The receiver tries to match the frequency information to the modulation scheme used. At this point the receiver can check many different modulation schemes in case the transmitter has been configured to choose different options. In the case of a bi-phase Manchester encoding, this is done by using an amplitude threshold above which the symbol is HI and below which the symbol is LO. The receiver searches the data at the different frequencies looking for a peak in cross correlation between the expected message preamble and the measured and processed digital signal. If the preamble is identified in enough subcarriers, the receiver moves onto the message decoding step using the identified frequency and message start time.





**Figure 3: The process performed by the receiver to identify and extract the message sent by the covert transmitter. Wifi packets from any number of access points are received on the left and the resulting message comes out on the right.**



**Figure 4: An example frequency analysis (FFT) on a single subcarrier showing a covert transmitter sending a bi-phase Manchester encoded message at approximately 5Hz.**

After the preamble, the header fields of the message and the data field are decoded. It is very likely, regardless of the type of modulation, that some subcarriers will produce different values as each subcarrier is differently affected by the covert transmitter’s movement. To resolve this a subcarrier aggregation stage is needed. For subcarrier aggregation, the most common 0 or 1 symbol across all signal carrying subcarriers—as defined in IEEE Std 802.11-2020 [3] Section 21.3.7.2—is selected to be the decoded value for each bit. Invalid bits (e.g., full symbols that are made of 1/1 and 0/0 in the case of bi-phase Manchester) are ignored. The output of the carrier aggregation phase gives the receiver the transmitted message with any completely corrupt bits marked.

### 6.1 Dynamic Sampling Frequency

As we have already mentioned, the scheme relies on the WiFi transmissions that the attacker does not control, so it is possible that the packet transmission rate  $F_p$  may be dynamic. Therefore, when processing the output of the frequency analysis, care needs to be taken to account for changes in sample rate over time. To deal with this, rather than adjusting the FFT sampling rate, the sample rate is fixed at the mean packet rate and the symbol lengths during demodulation should be shifted by the receiver to account for the changing packet rate. In our evaluation, it is possible to see this change in packet rate on the normalised amplitude graphs. This is most noticeable on Figure 16, where it is possible to see that the vertical green and red dashed lines delineating the half and full

symbols are not equally spaced. Despite this our scheme can reliably receive data even though the background WiFi transmissions rate varies significantly.

## 7 DATA EXFILTRATION SCHEME

Now that we know the basic operation of the transmitter and receiver we look at a few problems in more detail and present our reasoning behind some of the design decisions, and particular methods used.

### 7.1 Creating an Impact on CSI

For the scheme to be usable in practice, the covert transmitter must have an impact on the CSI that is large enough to be detected and distinguishable from background noise. Given that even small changes in the environment can have a significant impact on CSI [8, 32, 43], impacting CSI in a way that is distinguishable from background noise is the major challenge. Background noise in this case does not come from RF sources, but rather from things like other moving machines or humans, normal variations of CSI measurements, artefacts caused by transmitter or receiver imperfections, and potentially duplicates of the same device or machinery used for data exfiltration. The impact of these noisy objects are influenced by their size, material, the wavelength of the WiFi signal, distance to the WiFi transmitter, the relative position of all the key components of the system, and the frequency of movement. We investigate the specific contribution of these factors in Section 8.

Using periodic motion provides a key advantage over simply making one off changes to the environment, it allows a repeated CSI change to be made and then picked out from the background noise using a frequency analysis. Non-periodic movement (e.g., a person moving randomly around an environment) will cause random changes throughout the frequency domain, meanwhile controlled periodic motion will be consistent and distinguishable from the random fluctuations at other frequencies.

The period of the motion is not particularly important for identification, as to find lower frequency messages the frequency analysis window simply needs to be extended. This gives our scheme great flexibility in terms of the type of devices that can be used as the covert transmitter, but it also has implications for the duration of each transmission symbol. For example, if the covert transmitter is a large mechanical mixing machine that has a period of 10 seconds, then the window length of the frequency analysis, and thus

the symbol length, needs to be much longer than for a desk fan spinning at 50Hz.

## 7.2 Frequency Analysis Constraints

As previously mentioned, the receiver performs a frequency analysis on the CSI amplitude data using a Fast Fourier transform (FFT) to calculate a spectrogram for each subcarrier. The FFT sampling frequency is set by the mean WiFi transmitter packet rate  $F_p$  and this value is what determines the upper limit on the frequencies that can be used for covert communication.

If the covert transmitter is in an active state at time  $t$  this will be visible as a higher amplitude on the output of the spectrogram at  $t$  for frequency  $F_c$ . If the covert transmitter is physically symmetrical the frequency may appear as a multiple of  $F_c$ . There may also be harmonics of  $F_c$  which will have an amplitude that is lower than the actual frequency.

The upper and lower bound of  $F_c$  (i.e., the FFT range) is determined by a combination of the sample rate (i.e., the WiFi transmitter packet rate) and the length of the FFT window  $W$ .

$$\frac{1}{L_s} < \frac{1}{W} \leq F_c \leq \frac{F_p}{2} \quad (1)$$

When a lower sample rate (i.e., a smaller  $F_p$ ) forces a smaller  $F_c$ , the window length  $W$  and symbol length  $L_s$  can be increased to compensate. To ensure accurate measurement of each symbol, it must be that case that  $L_s > W$ . Increasing the symbol length comes at a cost to the maximum bitrate. If the packet rate is not consistent or is non-uniform then it is required that  $F_p \gg F_c$  to ensure that (1) still holds when instantaneous packet rate drops below  $F_p$  for a short duration.

The acceleration and deceleration of the covert transmitter needs to be accounted for in the symbol length, as it can take time for covert transmitter to reach the peak frequency during the acceleration phase and it may take some time for the covert transmitter to fall below the  $F_c$  during the deceleration phase depending on the mechanical mechanism.

Although we talk about the sample rate being  $F_p$ , in practice, the actual received packet rate is influenced by two factors: the packet transmission rate by the WiFi transmitter ( $F_p$ ); and the ability of the receiver to detect packets which may be affected by range and obstructions. The packet rate of the WiFi transmitter can vary considerably depending on the type of device and its purpose. Any device that transmits WiFi packets can be used, but there are advantages if the WiFi transmitter is a network access point (AP). If the wireless network has little to no traffic, our scheme must rely on beacon frames, usually sent at intervals of around 100ms, i.e., ten packets per second. If traffic load is high the total number of packets sent by the AP can be in the hundreds of packets per second as it handles all the network traffic for nearby devices. Although all these parameters can be configured, in most cases the beacon frames essentially guarantees a lower bound of packet rate at approximately 10 packets per second.

## 7.3 Multiple Receivers

To supplement moving the receiver, multiple receivers can also be used. Multiple receivers can be used to increase the chance of initial message detection and to improve communication quality.

From different receiving locations the influence on CSI of the environment is unique and random bit-errors are likely to manifest differently.

After receiving the messages, the message outputs from the various receivers can be compared and aggregated in the same manner as for the subcarrier aggregation step. This does not need to be done at runtime so there is no requirement that multiple receivers need to be able to communicate.

## 7.4 Length, Integrity and Error Correction

As with many conventional communication systems, verifying message integrity is important. However, given that the receiver cannot ask for a retransmission of the message if the integrity verification fails, forward error correction is potentially more important. Error correction however does come at a cost of bit rate so the attacker must consider this trade-off carefully.

One parameter the attacker can tune before deploying the attack is the message length. A shorter message, with appropriate integrity checks, will have a higher overhead in terms of additional data needed for headers and checks, but if an unrecoverable error does occur the amount of corrupted data that has to be discarded is less. In general, the better the communication channel is expected to be, the larger the message size should be used.

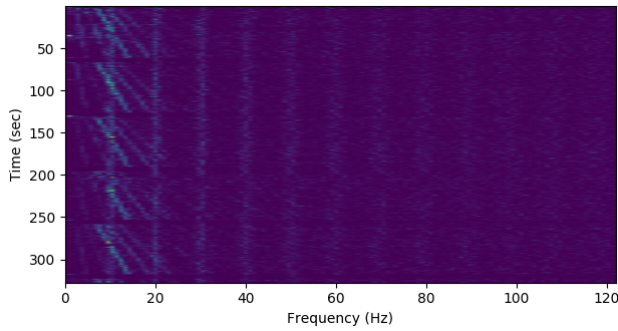
The choice also depends on the nature of the data. In some scenarios receiving a few corrupt bits may not be too much of a problem. For example, stealing a partial encryption key will still be an improvement over having no key as it would reduce the number of brute force attempts required to decrypt some data. This assumes that the corrupted parts of the message are marked, which they are in our scheme as described in Section 6.

Since the covert transmitter cannot verify if the message has been correctly received, the best strategy is usually to keep transmitting the data over and over. That way, if some messages were corrupted when they were first transmitted, the receiver can just wait and hopefully get an uncorrupted version next time. We use the sequence number in the message header to facilitate this kind of retransmission.

## 7.5 Risk of Detection

In our attacker model there is no time limit for the attacker to complete his objective so he may be active for days, weeks, or maybe even years. However, in practice, each time the covert transmitter transmits there is a chance of detection as the machine being manipulated will behave in an unexpected way from the perspective of the user, operator, or nearby people. For this reason, we briefly discuss detection here, even though we do not attempt to provide a solution to the issue of detection in this paper.

The chance of physical detection varies significantly depending on the scenario and machine being manipulated (e.g., a hydraulic press on a factory floor behaving incorrectly during the middle of working hours would be more noticeable than a shrouded air conditioning fan inside a vent outside of office hours). In practice, the consequences of detection when exfiltrating data will also vary depending on the objective of the attacker. In some scenarios, detection may lead to the changing of cryptographic keys or other critical data, which if that was the attacker's target as part of a



**Figure 5: Spectrogram of a chirp spread spectrum transmission by the covert transmitter.**

larger overall attack, then the overall attack may not be successful if they are detected, even if they do exfiltrate the data. On the other hand, if the attacker is targeting permanent data (e.g., customer data or trade secrets), then once the data has been exfiltrated being detected is of little consequence.

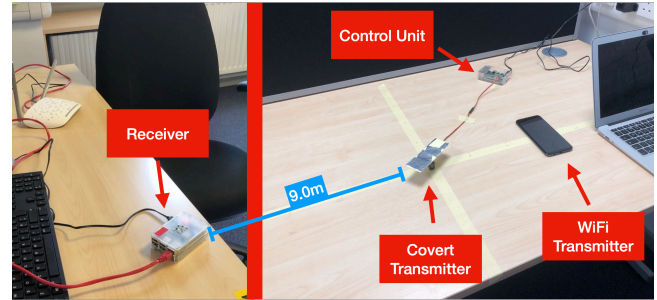
## 7.6 Modulation and Multiplexing Schemes

In our covert transmitter and receiver design sections (Section 5 and 6), we discuss the use of more sophisticated modulation schemes if the covert transmitter is able to modify its frequency with some degree of precision. However, similar techniques can be used if the attacker is able to compromise multiple pieces of machinery, i.e., has multiple covert transmitters operating at different frequencies, connected to the same control unit. The attacker can make use of frequency division multiplexing to increase data throughput or have multiple streams of independent data. Spatial multiplexing is also very promising as different WiFi transmitter sources are impacted differently by different covert transmitters even on the same covert frequency.

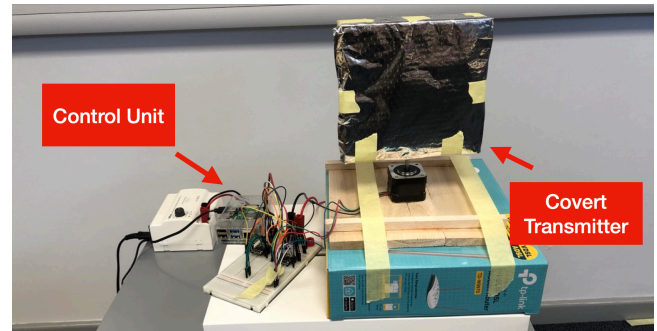
Given the importance of avoiding noise, using spread-spectrum techniques may present a way to reduce the impact of background noise. Frequency-hopping spread spectrum (FHSS) is a technique where the frequency is rapidly changed in a predefined sequence to reduce the impact of noise at any particular narrowband frequency, chirp spread spectrum (CSS) uses signals with an increasing or decreasing frequency to encode data as such chirps are very easy to detect even in noisy environments. These techniques are useful given that one-way communication means that the transmitter is unaware of changing noise levels at different frequencies. To take full advantage of this diversity the parameters would need to be defined ahead of attack deployment but it remains a very interesting option for boosting both range and throughput. In Figure 5, we show the spectrogram produced when using a chirp spread spectrum-like change in frequency. The graph clearly shows the change in rotation speed as chirps at an increasing frequency along with multiple harmonics.

## 8 IMPLEMENTATION AND EVALUATION

We create a proof of concept implementation and evaluate our method by exploring the relationships between communication



**Figure 6: The experimental setup used for the transmitter-transmitter distance experiment, consisting of the WiFi transmitter, covert transmitter, control unit, and receiver.**



**Figure 7: The experimental setup used for covert transmitter experiments with various sized and frequencies. The Receiver and WiFi transmitter are not shown.**

quality and various factors including distance, covert transmitter, size, WiFi frequency band, materials, and other movement in the environment.

For all the experiments, for our implementation we use a Samsung Galaxy A50 smartphone as the WiFi transmitter as this has the flexibility to be moved without having to deal with power cables and it had a constant transmission power. The smartphone is connected to a 5GHz or 2.4GHz band WiFi channel and forced to transmit at configurable intervals using a web socket connection to an external server. For the receiver, we use a Raspberry Pi Model 4 that is configured using the Nexmon CSI tool [15, 36] to record CSI samples. The recorded CSI samples are transferred to another computer for analysis after collection. For the covert transmitter, we use a range of objects of different materials including lengths of aluminium foil folded multiple times, cardboard with a sheet of foil laid over one side, wood, and plastic. To move the covert transmitter, we use either a MG90S continuous rotation micro servo (setup shown in Figure 6) or a permanent magnet stepper motor which allows for larger covert transmitters and variable frequency control (shown in Figure 7). Another Raspberry Pi Model 4 is used as the control unit.



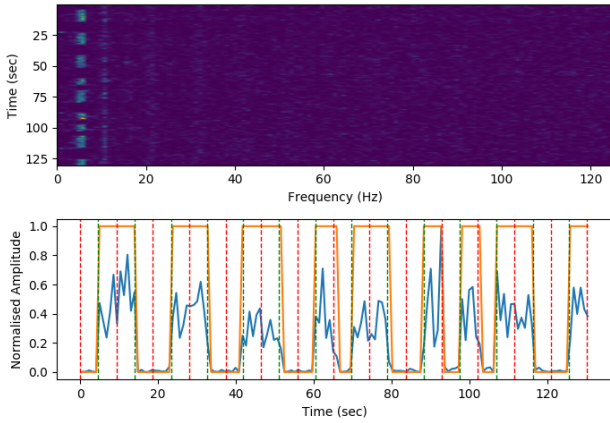


Figure 8: Example decoding of message 10101011011101 in bi-phase Manchester encoding. The top plot shows a spectrogram representation of the frequency analysis of a single subcarrier. The bottom plot shows the normalised amplitude plot at 6Hz from the spectrogram. The orange line shows the recovered digital signal. The red and green dashed vertical lines show the start and midpoint of each symbol. This example shows the message being correctly decoded in its entirety.

### 8.1 Proof of Concept Decoding

We first demonstrate our proof of concept implementation by decoding a bi-phase Manchester encoded test message transmitted at a rate of 0.1 bits/second. Figure 8 shows the decoding of subcarrier index -121 and Figure 9 shows the result of the subcarrier aggregation stage where the number of successfully decoded 0 and 1 symbols by each subcarrier are counted, and the results show that this message was correctly decoded. An average signal-to-noise ratio (SNR) of 9.56dB was achieved across all the subcarriers with the maximum SNR from any subcarrier being 24.96dB. From now on we refer just to the maximum SNR.

### 8.2 Transmitter Size

We next evaluate the effect the size of the covert transmitter and the WiFi frequency band has on the ability to measure the periodic movement. We touch on the impact of distance between the various system components but we focus on that in more detail later in Section 8.3.

*Lower Bound of Covert Transmitter Size.* To test the absolute lower bound of object size, we use a range of different sized aluminium folded foil sheets as our covert transmitter. The WiFi transmitter and covert transmitter were placed as close together as possible with the receiver about 3m away. The five different folded foil sheets used measure: (1) 1cm × 1cm; (2) 6cm × 3cm; (3) 12cm × 4cm; (4) 21cm × 4cm; and (5) 41cm × 4cm.

Our experiments show that the signal wavelength gives the approximate lower bound for what is detectable. In the 2.4GHz band (wavelengths between 12.1cm and 12.4cm), we find the three smallest covert transmitters do not create a detectable impact on

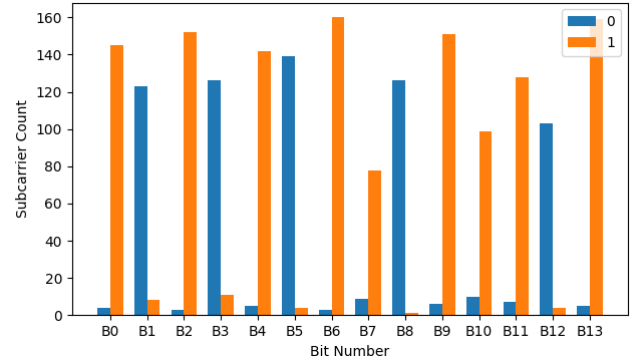


Figure 9: Example of the subcarrier aggregation step of message 10101011011101. The bars show the number of subcarriers that successfully return 0 or 1 for each bit for the message. We see that a simple majority vote is sufficient to get the right bit with high probability. The total number of signal-carrying subcarriers is 242.

the output of the frequency analysis for any subcarrier. However, the two larger sheets, above the size of wavelength do. In the 5GHz band (with wavelengths of 5.1cm to 5.6cm), the effect is easily detectable on all sizes above and including the 6cm size, but cannot be seen on the smallest size. In summary, we find that the lower bound of the object size that can produce detectable movement is around the wavelength size.

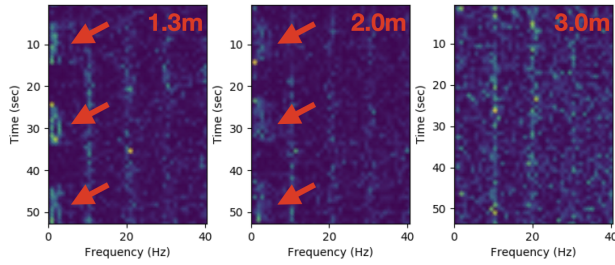
*Covert Transmitter Size and Maximum Detectable Distance.* We explore the relationship between the size of the covert transmitter and the impact on CSI through a comparison of the frequency analysis outputs. We demonstrate that larger covert transmitters have a detectable impact on CSI out to a much larger distance. This is shown in Figures 10 and 11, where a smaller 17cm × 15cm foil sheet and a larger 27cm × 23cm foil sheet are used to transmit the same message. Both sheets are rotated at the same speed but at a distance of 3m, the smaller covert transmitter no longer has a visible effect. However, the effect from the larger covert transmitter continues to be visible past 5m and beyond.

For this demonstration, to account for longer acceleration and deceleration time of the larger covert transmitter it was necessary to increase the ON length from 10 seconds to 20 seconds.

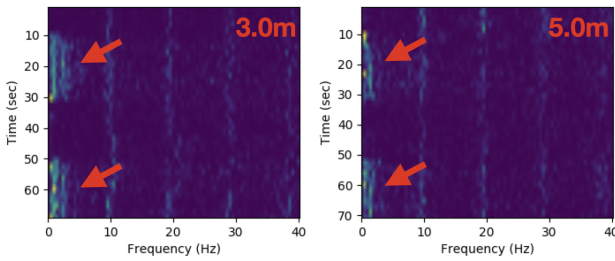
### 8.3 Distance

Next, we evaluate the relationship of distance between the various components in more detail. We first focus on the distance between the covert transmitter and receiver (the *receiver distance* as defined in the system model), and then the distance between the two transmitters (the *transmitter distance*).

*Receiver Distance.* The WiFi and covert transmitter pair are placed with a fixed distance of 10cm between the them. Data is then collected using the receiver at different distances from the covert transmitter. The bit error ratio (BER) prior to any error correction and maximum SNR are calculated for 5 messages at each of the



**Figure 10: Frequency analysis output at different distances with a  $17\text{cm} \times 15\text{cm}$  covert transmitter. Red arrows point to the areas on the spectrogram where the movement of the covert transmitter is visible at around 1Hz.**

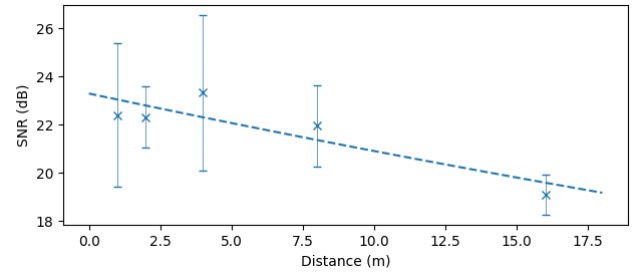


**Figure 11: Frequency analysis output at different distances with a  $27\text{cm} \times 23\text{cm}$  covert transmitter. Red arrows point to the areas on the spectrogram where the movement of the covert transmitter is visible at around 1Hz.**

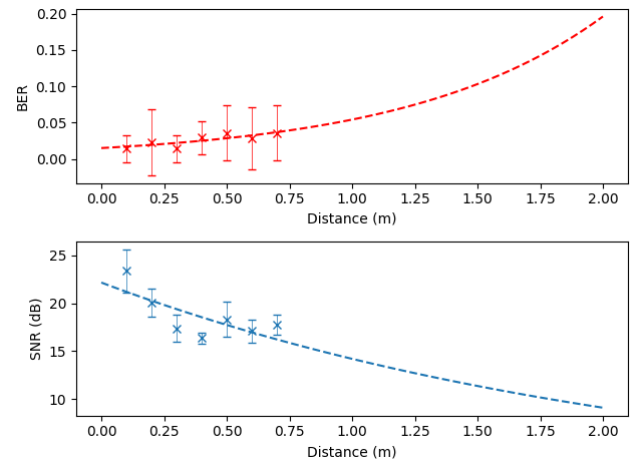
distances. To get as close as possible to realistic conditions, the experiment is conducted in an office environment, so there are some furniture items, objects, and walls in the vicinity. In an attempt to exacerbate the effect of distance, we deliberately use a small covert transmitter, a  $12\text{cm} \times 4\text{cm}$  folded sheet of aluminium foil. This experiment is done on channel 100 (80MHz bandwidth) in the 5GHz band.

At all five distances, the messages are correctly decoded without any bit errors. Although we do not exceed the range of the receiver's ability to detect packets, the max SNR does decrease slightly as the distance increases. The results of this are shown in Figure 12. This is clearly not an exhaustive test of the distance capabilities of our system, but it shows that data can be exfiltrated out of a normal room without any issues, even using normal omnidirectional antennas. If the distance is increased to the point where errors do start to occur, a high-gain antenna can be used on the receiver to detect packets at much longer range.

**Transmitter Distance.** Next, we evaluate the effect of the distance between the covert transmitter and WiFi transmitter on the communication quality. For this experiment the covert transmitter and receiver are placed at fixed locations 9 meters apart, and the WiFi transmitter is then moved away in 10cm increments. Line of sight between the two transmitters is maintained throughout the experiment. Once again, to maximise the impact of the change in distance, we deliberately use a small covert transmitter, the  $12\text{cm} \times 4\text{cm}$  foil



**Figure 12: The SNR of the subcarrier with the highest SNR value, as a function of distance between the covert transmitter and the receiver. The error bars indicate the 95% confidence intervals for 5 experimental runs. The dashed line shows a fitted exponential curve.**

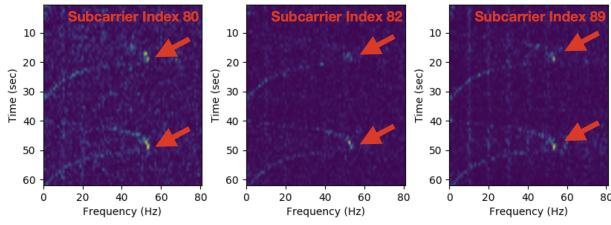


**Figure 13: The BER and SNR of the subcarrier with the highest value, as a function of distance between the covert and WiFi transmitters. The error bars indicate the 95% confidence intervals for the 10 experimental runs. The dashed lines show fitted exponential curves.**

strip. The experiment is done on channel 100 (with 80MHz bandwidth) in the 5GHz band, and data is collected by cycling through all the measurements points 10 times.

As the distance between the WiFi transmitter and covert transmitter is increased, the communication quality degrades, as shown in Figure 13, both in terms of BER and SNR. We also plot a fitted exponential curve to show the expected performance of our setup beyond the measured distance.

We see that as the covert transmitter gets further away from the WiFi transmitter the amount of energy reaching the covert transmitter—and therefore influenced by its rotation—decreases by the inverse-square of the distance. This behaviour is expected and helps to validate our experimental setup.



**Figure 14: Frequency analysis output of multiple subcarriers when using a 14" desk fan spinning at approximately 54Hz. We see that the same pattern is clearly visible in all three subcarriers, allowing aggregation to yield a more robust result.**

#### 8.4 Material of the Covert Transmitter

Most of our experiments are done using a mixture of cardboard and aluminium foil for the covert transmitter, however any material that has an influence on signal propagation is usable. For example, we found that even low-density balsa wood has a significant measurable effect. With a 21cm  $\times$  2cm  $\times$  2cm length of balsa wood, a max SNR of 15.50dB was achieved at a transmitter distance of 20cm, with no bit-errors in the final message output.

We also demonstrate the effect using a standard 14" plastic desk fan with the transmitters at a distance of 20cm. The desk fan's impact on CSI can be seen in Figure 14. The red arrows mark the peak frequency of the fan once it was up to speed. The curved lines caused by the slow acceleration and deceleration of the fan blades are also clearly visible.

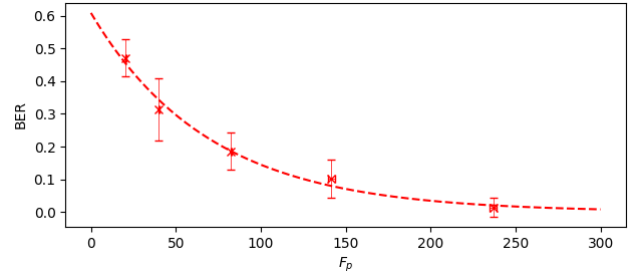
#### 8.5 WiFi Transmitter Packet Rate

Since the packet rate  $F_p$  is outside of the attacker's control, we need to test how the system performs at different rates. In general, with a lower packet rate we would expect the bit error ratio to be higher if the symbol length is kept constant, as there are less samples per symbol available for the receiver. The scheme can be adjusted to compensate for lower packet rates by increasing the symbol length. The numbers presented here reflect the performance of our prototype setup with a very simple modulation scheme and an omnidirectional antenna on the receiver.

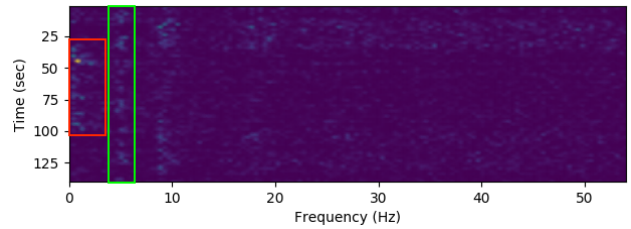
To explore the impact of packet rate using our implementation, we place the transmitters and receiver in positions with a known bit-error ratio around 50%. Using a covert transmitter with a rotation speed of  $F_c = 5\text{Hz}$  and a fixed symbol length, we slowly increase the packet rate  $F_p$ . As shown in Figure 15, the bit-error ratio does in fact decrease as  $F_p$  is increased.

#### 8.6 Susceptibility to Noise

Because the attacker cannot control the exact impact a covert transmitter has on the WiFi signal, we test the effect of noise in nearby frequencies and show that while the noise does have an impact on the quality of communication, it is still possible to correctly decode the final message as each subcarrier is influenced differently. The probability that any specific environment causes corruption for all subcarriers is low, which means that our scheme works even if there are significant disturbances in the environment.



**Figure 15: BER as a function of packet rate  $F_p$  for our setup. The vertical error bars indicate the 95% confidence intervals for the bit-error ratio across 5 runs. The horizontal error bars indicate the 95% confidence interval for  $F_p$  as the mean packet rate is varied by a small amount for each experimental run. The dashed line shows a fitted exponential curve.**



**Figure 16: The spectrogram plot for a single subcarrier, with noise created by human movement. The covert channel frequency is highlighted by the green box and the noise produced by the human movement is indicated by the red box.**

To show this, we position the transmitters 9m from the receiver and transmit a series of known packets. During the transmission, for the bits between the 4th bit (B3) and the 10th bit (B9), both included, a human walked back and forth across the path between transmitters and receiver.

As is shown by Figure 16, in this case, the effect of noise mostly appears below the covert transmitter frequency. Although, there are more corrupt bits for each subcarrier than for the experiments with no human movement, once all the subcarriers are aggregated the message is correctly decoded with no bit-errors.

Of course, there is a limit at which point the receiver can no longer reconstruct the message. However, this experiment shows that even with an extremely simple modulation scheme and no error correction code, the message is robust to normal activity. Better modulation and error correction can be used to increase robustness as in all other wireless transmissions.

## 9 COUNTER-MEASURES

There are a number of countermeasures that can be employed to counter this type of threat.

The first logical approach is malware checking software deployed on devices with control of mechanical devices. The software would need to check for unauthorized modifications to the software running on the control unit, specifically targeting instructions that tell



the mechanical components what to do, or mismatches between what the controller is instructing the mechanism to do and what data it intends to send back to any monitoring units, if the attacker is using sophisticated methods to hide the effects of the attack. The limitation of this approach is that it requires the control units to be capable of running extra software which may not be possible for low computational power controllers and the attacker could also modify this malware checking software at the same time.

While deliberately creating noise in various frequencies of the covert channel, to make the environment too noisy for the attacker to be communicated, may seem like a possible idea, in practice the operator would need to identify every WiFi source and put in place devices to create noise in as large a frequency range as possible. However, communication may still be possible with certain combinations of receiver and covert transmitter positions, using multiple receivers, particular frequencies, more advanced modulations schemes, or some extra signal processing.

The next approach is to ensure significant physical separation between WiFi transmission sources and mechanical devices. As we have shown, the larger this distance the lower the SNR and the worse this becomes as a communication method. This would reduce the attacker's ability to use it as a communication method.

The final possible approach, is to use this method as a way to monitor the behaviour of systems. If the device operator sets up receivers and performs the same frequency analysis process, they should be able to monitor the state of various mechanisms through a second channel that cannot be influenced by attacker through isolated control of the control unit. We are not suggesting that the device operators attempt to search for and decode messages, as the attacker is free to use whatever modulation and encoding scheme he wishes. However, the operator can compare the expected behaviour of the system components, the live monitoring data, and the CSI to look for inconsistencies which would indicate some system misbehaviour. Additionally, the operator has the advantage of being able to measure baseline CSI from normal operations.

## 10 RELATED WORK

Existing work on data exfiltration, covert communication, and side channel attacks can be placed into two categories: air-gapped and RF covert channels. In the air-gapped case, computers do not have the capability to communicate using conventional wireless radios. Within the air-gapped type Guri [18] recognised the following categories of communication channel: electromagnetic, magnetic, acoustic, thermal, optical, and seismic. RF channels make use of transmission properties of conventional wireless radios to communicate while remaining hidden to particular types of monitoring.

### 10.1 Air-Gapped Covert Channels

Air-gapped covert channels come in the following forms:

*Acoustic.* There are a range of existing acoustic data exfiltration schemes making use of both ultrasound and sound within a human's audible range [7, 10]. Guri et al. [23] presented Fansmitter that uses CPU and chassis fans to communicate. The authors were able to demonstrate communication at distance of up to 8 meters with a rate of up to 0.25 bits/second.

*Thermal.* Although having a much lower bit rate than other methods, thermal emissions can be used for covert communication. Masti et al. [33] showed that the temperature in multicore processors could be used to transfer information between processes on the same computer even with strict process isolation. Guri et al. [22] went a step further and demonstrated a data rate of 8 bits/hour could be achieved for bi-directional communication at a distance of up to 40cm between different computers using thermal emissions.

*Vibration.* Guri [18] showed that it is possible to use the vibrations generated by a computer's fans to communicate by using smartphone accelerometers as a receiver. It was limited to a short range desk environment.

*Magnetic.* Matyunin et al. [34] have demonstrated that smartphone magnetic field sensors can be used to detect various I/O operations from close range laptop hardware components.

*Electromagnetic.* A number of pieces of existing work have demonstrated that components of a device can be used to produce an RF signal in a way that it was not intended to. Guri et al. [20] demonstrate the ability of a video display adapter to generate a FM signal that can be detected by a smartphone with an inbuilt FM receiver. Guri [19] also separately shows that memory access operations can be used to transmit in the GSM frequency range for distances up to 5.5 metres using a standard mobile phone as a receiver with a rate of 1-2 bit/s, and further ranges of up to 30 metres using dedicated receiver hardware with a rate of 100-1000 bit/s. More recently Guri [17] has demonstrated that various hardware components can be used to transmit several metres in the WiFi frequency band. A usable software package for RF data transmission using a Raspberry Pi is available [11]. This is capable of transmitting from 5 KHz up to 1500 MHz over very short distances using just a GPIO pin from a Raspberry Pi board and over longer distances with a wire attached to the pin or with a purpose made antenna. It has also been demonstrated that communication using electrical power infrastructure within a building to communicate is possible [39].

All of the above methods (i.e., acoustic, thermal, vibration, magnetic, and electromagnetic) have varying levels of robustness, but commonly have a limited effective range as the power with which the signal is transmitted is very low. In the case of acoustic, to avoid detection, the frequency must be above the audible spectrum or the volume level needs to be low and in some cases the volume it is fundamentally limited by the mechanism creating the sound. In addition, audio waves are absorbed by walls and furniture normally limiting the applicability of this method to room level communication. Methods using vibrations are also limited by the seismic power that can be produced and the vibrations attenuate very quickly as they travel through the communication medium. The magnetic field produced by smartphone hardware is very weak so using magnetic field sensors is only possible over a short range and creating EM signals with non-conventional hardware components also produces a signal with very low power.

Recently the effective range of EM side-channel communication has been extended using LoRa like modulation for CPU-memory operations. Shen et al. [40] have demonstrated EMRLoRA which uses chirp spread spectrum to increase the effective range to approximately 250m and is capable of penetrating shielding. However,

this is demonstrated on hardware that is not necessarily available on embedded systems and other low powered devices.

*Optical.* It has been shown that an attacker can modify the state of a status indicator or LED to leak information visually [24, 31]. This method requires direct line of sight.

*Physical Storage Medium.* Attacks using physical storage mediums (e.g., USBferry [9]) to collect and transfer information have been demonstrated in the wild. Attacks of this nature are appropriate for office like settings where USB sticks are being used to constantly bring information in and out. However, this is not necessarily the case in an industrial environment. Additionally, once the attack is deployed it is now outside the control of the attacker and it is not up to the attacker when or if they will finally receive the data they are aiming to exfiltrate.

## 10.2 RF Covert Channels

In non-air-gapped covert channels it is assumed that the attacker's device or software has the capacity to control transmission or modify antenna parameters. These methods include using the timing of transmissions [6], modifying the modulation scheme at a very low level to add additional information [26, 37, 49], and modifying the impedance of a device's wireless network card to make use of the backscatter effect [42].

For these methods of attack, the device infected by the data-exfiltration malware requires wireless networking hardware and the malware requires permission to transmit or access particular firmware files on the system. These types of attack can be prevented through careful permission controls, using hardware without radio chips, and potentially by using network-based intrusion detection systems (IDS) [12, 29, 35].

## 11 CONCLUSION

In this paper, we have introduced a novel data exfiltration attack using the impact of physically actuated devices on a wireless channel, measurable using Channel State Information (CSI). This is useable in scenarios where the attacker cannot communicate using conventional communication hardware, has the ability to physically interact with the environment, and there is ambient WiFi traffic. A message to send is encoded, then modulated using the change in state of periodic motion of the actuated device. The receiver collects CSI data from ambient WiFi traffic in the environment and then performs a frequency analysis on the CSI amplitude to decode and recover the original message. We discussed in detail the design of the covert transmitter and receiver, and discussed how periodic motion of the covert transmitter allows the attacker to perform communication without having the train the system to recognise specific changes to the environment. We also discussed further enhancements for scenarios where the attacker has precise and flexible control of the covert transmitter movement. We produced a proof of concept implementation which was used to demonstrate robust communication and evaluate the key relationships between channel quality and several variables. These variables were the distance between system components, transmitter size, transmitter material, WiFi frequency band, other movement in the environment, and the WiFi transmitter packet rate. Finally, we presented and discussed several countermeasures to such an attack.

## REFERENCES

- [1] [n.d.]. Atheros CSI tool. <https://wands.sg/research/wifi/AtherosCSI/>
- [2] 2018. IEEE Standard for Ethernet. *IEEE Std 802.3-2018 (Revision of IEEE Std 802.3-2015)* (Aug. 2018), 1–5600. <https://doi.org/10.1109/IEEESTD.2018.8457469> Conference Name: IEEE Std 802.3-2018 (Revision of IEEE Std 802.3-2015).
- [3] 2021. IEEE Standard for Information Technology–Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks–Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016)* (Feb. 2021), 1–4379. <https://doi.org/10.1109/IEEESTD.2021.9363693> Conference Name: IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016).
- [4] 2021. seemoo-lab/nexmon. <https://github.com/seemoo-lab/nexmon> original-date: 2016-10-27T09:31:28Z.
- [5] 2021. seemoo-lab/nexmon\_csi. [https://github.com/seemoo-lab/nexmon\\_csi](https://github.com/seemoo-lab/nexmon_csi) original-date: 2019-08-15T18:00:52Z.
- [6] Serdar Cabuk, Carla E. Brodley, and Clay Shields. 2004. IP covert timing channels: design and detection. In *Proceedings of the 11th ACM conference on Computer and communications security (CCS '04)*. Association for Computing Machinery, New York, NY, USA, 178–187. <https://doi.org/10.1145/1030083.1030108>
- [7] Brent Carrara and Carlisle Adams. 2015. On Acoustic Covert Channels Between Air-Gapped Systems. In *Foundations and Practice of Security (Lecture Notes in Computer Science)*, Frédéric Cuppens, Joaquin Garcia-Alfaro, Nur Zincir Heywood, and Philip W. L. Fong (Eds.). Springer International Publishing, Cham, 3–16. [https://doi.org/10.1007/978-3-319-17040-4\\_1](https://doi.org/10.1007/978-3-319-17040-4_1)
- [8] M. Chen, K. Liu, J. Ma, Y. Gu, Z. Dong, and C. Liu. 2021. SWIM: Speed-Aware WiFi-Based Passive Indoor Localization for Mobile Ship Environment. *IEEE Transactions on Mobile Computing* 20, 2 (Feb. 2021), 765–779. <https://doi.org/10.1109/TMC.2019.2947667> Conference Name: IEEE Transactions on Mobile Computing.
- [9] Catalin Cimpanu. 2020. Hackers target the air-gapped networks of the Taiwanese and Philippine military. <https://www.zdnet.com/article/hackers-target-the-air-gapped-networks-of-the-taiwanese-and-philippine-military/>
- [10] Luke Deshotels. 2014. Inaudible sound as a covert channel in mobile devices. In *Proceedings of the 8th USENIX conference on Offensive Technologies (WOOT'14)*. USENIX Association, USA, 16.
- [11] F5OEO. 2021. F5OEO/rpitx. <https://github.com/F5OEO/rpitx> original-date: 2015-10-21T16:06:52Z.
- [12] Alexey G. Finogeev and Anton A. Finogeev. 2017. Information attacks and security in wireless sensor networks of industrial SCADA systems. *Journal of Industrial Information Integration* 5 (March 2017), 6–16. <https://doi.org/10.1016/j.jii.2017.02.002>
- [13] G. Forbes, S. Massie, and S. Craw. 2020. WiFi-based Human Activity Recognition using Raspberry Pi. In *2020 IEEE 32nd International Conference on Tools with Artificial Intelligence (ICTAI)*. 722–730. <https://doi.org/10.1109/ICTAI50040.2020.00115> ISSN: 2375-0197.
- [14] S. Z. Goher, B. Javed, and N. A. Saqib. 2012. Covert channel detection: A survey based analysis. In *High Capacity Optical Networks and Emerging/Enabling Technologies*. 057–065. <https://doi.org/10.1109/HONET.2012.6421435> ISSN: 1949-4106.
- [15] Francesco Gringoli, Matthias Schulz, Jakob Link, and Matthias Hollick. 2019. Free Your CSI: A Channel State Information Extraction Platform For Modern Wi-Fi Chipsets. In *Proceedings of the 13th International Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization (WiNTECH '19)*. Association for Computing Machinery, Los Cabos, Mexico, 21–28. <https://doi.org/10.1145/3349623.3355477>
- [16] Xiuzhen Guo, Yuan He, Xiaolong Zheng, Liangcheng Yu, and Omprakash Grawali. 2018. ZIGFI: Harnessing Channel State Information for Cross-Technology Communication. In *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*. 360–368. <https://doi.org/10.1109/INFOCOM.2018.8486364>
- [17] Mordechai Guri. 2020. AIR-Fi: Generating Covert Wi-Fi Signals from Air-Gapped Computers. *arXiv:2012.06884 [cs]* (Dec. 2020). <http://arxiv.org/abs/2012.06884> arXiv: 2012.06884.
- [18] Mordechai Guri. 2020. AIR-ViBeR: Exfiltrating Data from Air-Gapped Computers via Covert Surface ViBeRAtIoNs. *arXiv:2004.06195 [cs]* (April 2020). <http://arxiv.org/abs/2004.06195> arXiv: 2004.06195.
- [19] Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici. 2015. GSMem: data exfiltration from air-gapped computers over GSM frequencies. In *Proceedings of the 24th USENIX Conference on Security Symposium (SEC'15)*. USENIX Association, USA, 849–864.
- [20] M. Guri, G. Kedma, A. Kachlon, and Y. Elovici. 2014. AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies. In *2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE)*. 58–67. <https://doi.org/10.1109/MALWARE.2014.6999418>
- [21] Mordechai Guri, Matan Monitz, and Yuval Elovici. 2016. USBee: Air-gap covert-channel via electromagnetic emission from USB. In *2016 14th Annual Conference*

- on Privacy, Security and Trust (PST). 264–268. <https://doi.org/10.1109/PST.2016.7906972>
- [22] M. Guri, M. Monitz, Y. Mirski, and Y. Elovici. 2015. BitWhisper: Covert Signaling Channel between Air-Gapped Computers Using Thermal Manipulations. In *2015 IEEE 28th Computer Security Foundations Symposium*. 276–289. <https://doi.org/10.1109/CSF.2015.26> ISSN: 2377-5459.
- [23] Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, and Yuval Elovici. 2016. Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-Gapped Computers. *arXiv:1606.05915 [cs]* (June 2016). <http://arxiv.org/abs/1606.05915> arXiv: 1606.05915.
- [24] Mordechai Guri, Boris Zadov, Andrey Daidakulov, and Yuval Elovici. 2018. xLED: Covert Data Exfiltration from Air-Gapped Networks via Switch and Router LEDs. In *2018 16th Annual Conference on Privacy, Security and Trust (PST)*. 1–12. <https://doi.org/10.1109/PST.2018.8514196>
- [25] Dan Halperin. 2021. dhalperi/linux-80211n-csitool. <https://github.com/dhalperi/linux-80211n-csitool> original-date: 2010-12-17T03:26:58Z.
- [26] N. Hou and Y. Zheng. 2020. CloakLoRa: A Covert Channel over LoRa PHY. In *2020 IEEE 28th International Conference on Network Protocols (ICNP)*. 1–11. <https://doi.org/10.1109/ICNP49622.2020.9259364> ISSN: 2643-3303.
- [27] J. Hua, H. Sun, Z. Shen, Z. Qian, and S. Zhong. 2018. Accurate and Efficient Wireless Device Fingerprinting Using Channel State Information. In *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*. 1700–1708. <https://doi.org/10.1109/INFOCOM.2018.8485917>
- [28] Hoonyong Lee, Changbum R. Ahn, and Nakjung Choi. 2020. Fine-grained occupant activity monitoring with Wi-Fi channel state information: Practical implementation of multiple receiver settings. *Advanced Engineering Informatics* 46 (Oct. 2020), 101147. <https://doi.org/10.1016/j.aei.2020.101147>
- [29] Sung-Won Lee, Ji-Hun Kim, and Jonghee Youn. 2021. Simulation and Analysis of RF Attacks on Wireless SCADA System. In *Advances in Computer Science and Ubiquitous Computing (Lecture Notes in Electrical Engineering)*, James J. Park, Simon James Fong, Yi Pan, and Yunsick Sung (Eds.). Springer, Singapore, 281–287. [https://doi.org/10.1007/978-981-15-9343-7\\_38](https://doi.org/10.1007/978-981-15-9343-7_38)
- [30] Tao Li, Chenqi Shi, Peihao Li, and Pengpeng Chen. 2021. A Novel Gesture Recognition System Based on CSI Extracted from a Smartphone with Nexmon Firmware. *Sensors* 21, 1 (Jan. 2021), 222. <https://doi.org/10.3390/s21010222> Number: 1 Publisher: Multidisciplinary Digital Publishing Institute.
- [31] Joe Loughry and David A. Umphress. 2002. Information leakage from optical emanations. *ACM Transactions on Information and System Security* 5, 3 (Aug. 2002), 262–289. <https://doi.org/10.1145/545186.545189>
- [32] Yongsan Ma, Gang Zhou, and Shuangquan Wang. 2019. WiFi Sensing with Channel State Information: A Survey. *ACM Comput. Surv.* 52, 3 (2019), 36.
- [33] Ramya Jayaram Masti, Devendra Rai, Aanjan Ranganathan, Christian Müller, Lothar Thiele, and Srdjan Capkun. 2015. Thermal covert channels on multi-core platforms. In *Proceedings of the 24th USENIX Conference on Security Symposium (SEC'15)*. USENIX Association, USA, 865–880.
- [34] Nikolay Matyunin, Jakub Zefer, Sebastian Biedermann, and Stefan Katzenbeisser. 2016. Covert channels using mobile device's magnetic field sensors. In *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE Press, Macao, Macao, 525–532. <https://doi.org/10.1109/ASP-DAC.2016.7428065>
- [35] Sajid Nazir, Shushma Patel, and Dilip Patel. 2017. Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security* 70 (Sept. 2017), 436–454. <https://doi.org/10.1016/j.cose.2017.06.010>
- [36] Matthias Schulz, Wegemer Daniel, and Matthias Hollick. 2017. Nexmon: The C-based Firmware Patching Framework. <https://nexmon.org>
- [37] Matthias Schulz, Jakob Link, Francesco Gringoli, and Matthias Hollick. 2018. Shadow Wi-Fi: Teaching Smartphones to Transmit Raw Signals and to Extract Channel State Information to Implement Practical Covert Channels over Wi-Fi. In *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services - MobiSys '18*. ACM Press, Munich, Germany, 256–268. <https://doi.org/10.1145/3210240.3210333>
- [38] Gaurav Shah, Andres Molina, and Matt Blaze. 2006. Keyboards and covert channels. In *Proceedings of the 2006 USENIX Security Symposium (July–August. 59–75)*.
- [39] Zhihui Shao, Mohammad A. Islam, and Shaolei Ren. 2020. Your Noise, My Signal: Exploiting Switching Noise for Stealthy Data Exfiltration from Desktop Computers. *Proceedings of the ACM on Measurement and Analysis of Computing Systems* 4, 1 (May 2020), 07:1–07:39. <https://doi.org/10.1145/3379473>
- [40] Cheng Shen, Tian Liu, Jun Huang, and Rui Tan. 2021. When LoRa Meets EMR: Electromagnetic Covert Channels Can Be Super Resilient. *IEEE Computer Society*, 529–542. <https://doi.org/10.1109/SP40001.2021.00031> ISSN: 2375-1207.
- [41] C. Studer, S. Medjkouh, E. Gonultas, T. Goldstein, and O. Tirkkonen. 2018. Channel Charting: Locating Users Within the Radio Environment Using Channel State Information. *IEEE Access* 6 (2018), 47682–47698. <https://doi.org/10.1109/ACCESS.2018.2866979> Conference Name: IEEE Access.
- [42] Zhice Yang, Qianyi Huang, and Qian Zhang. 2017. NICScatter: Backscatter as a Covert Channel in Mobile Devices. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking (MobiCom '17)*. Association for Computing Machinery, New York, NY, USA, 356–367. <https://doi.org/10.1145/3117811.3117814>
- [43] Zheng Yang, Zimu Zhou, and Yunhao Liu. 2013. From RSSI to CSI: Indoor localization via channel response. *ACM Computing Surveys (CSUR)* 46, 2 (Dec. 2013), 25:1–25:32. <https://doi.org/10.1145/2543581.2543592>
- [44] S. Yousefi, H. Narui, S. Dayal, S. Ermon, and S. Valaee. 2017. A Survey on Behavior Recognition Using WiFi Channel State Information. *IEEE Communications Magazine* 55, 10 (Oct. 2017), 98–104. <https://doi.org/10.1109/MCOM.2017.1700082> Conference Name: IEEE Communications Magazine.
- [45] Sebastian Zander, Grenville Armitage, and Philip Branch. 2007. A survey of covert channels and countermeasures in computer network protocols. *IEEE Communications Surveys Tutorials* 9, 3 (2007), 44–57. <https://doi.org/10.1109/COMST.2007.4317620> Conference Name: IEEE Communications Surveys Tutorials.
- [46] Daqing Zhang, Hao Wang, Yasha Wang, and Junyi Ma. 2015. Anti-fall: A Non-intrusive and Real-Time Fall Detector Leveraging CSI from Commodity WiFi Devices. In *Inclusive Smart Cities and e-Health (Lecture Notes in Computer Science)*, Antoine Geissbühler, Jacques Demongeot, Mounir Mokhtari, Bessam Abdulrazak, and Hamdi Aloulou (Eds.). Springer International Publishing, Cham, 181–193. [https://doi.org/10.1007/978-3-319-19312-0\\_15](https://doi.org/10.1007/978-3-319-19312-0_15)
- [47] Lei Zhang, Enjie Ding, Yanjun Hu, and Yafeng Liu. 2019. A novel CSI-based fingerprinting for localization with a single AP. *EURASIP Journal on Wireless Communications and Networking* 2019, 1 (Feb. 2019), 51. <https://doi.org/10.1186/s13638-019-1371-y>
- [48] Yanzi Zhu, Zhujun Xiao, Yuxin Chen, Zhijing Li, Max Liu, Ben Y. Zhao, and Haitao Zheng. 2020. Et Tu Alexa? When Commodity WiFi Devices Turn into Adversarial Motion Sensors. *Proceedings 2020 Network and Distributed System Security Symposium* (2020). <https://doi.org/10.14722/ndss.2020.23053> arXiv: 1810.10109.
- [49] Hassan ZivariFard, Matthieu R. Bloch, and Aria Nosratinia. 2020. Keyless Covert Communication via Channel State Information. *arXiv:2003.03308 [cs, math]* (March 2020). <http://arxiv.org/abs/2003.03308> arXiv: 2003.03308.