Delft University of Technology
Master of Science Thesis in Computer and Embedded Systems Engineering

BLE Relay Attack Mitigation Using Multi-Antenna Bluetooth 6.0 Channel Sounding

Stijn van de Water

TU Delft Delft University of Technology

BLE Relay Attack Mitigation Using Multi-Antenna Bluetooth 6.0 Channel Sounding

Master of Science Thesis in Computer and Embedded Systems Engineering

Embedded Systems Group
Faculty of Electrical Engineering, Mathematics and Computer Science
Delft University of Technology
Van Mourik Broekmanweg 6, 2628 XE Delft, The Netherlands

Stijn van de Water
S

June 30th 2025

Author
Stijn van de Water (S.vandewater-1@student.tudelft.nl)
(vandewaterstijn@gmail.com)
Title
BLE Relay Attack Mitigation Using Multi-Antenna Bluetooth 6.0 Channel Sounding
MSc Presentation Date
July 7th 2025

Graduation Committee

Qing Wang	Delft University of Technology
Kaitai Liang	Delft University of Technology

Abstract

This thesis researches mitigations for BLE relay attacks. A design for a time-based distance bounding protocol using the Bluetooth channel sounding feature introduced in the new Bluetooth 6.0 core specification is presented. Bluetooth channel sounding is compromised of two distance measurement techniques: Phase-Based Ranging (PBR) and Round Trip Tim (RTT). The proposed protocol requires consistent channel sounding distance measurements in order to minimize the likelihood of succesfull relay attacks. Single-antenna channel sounding measurements have shown poor spatial and sequential consistency in a complex multipath office environment. In order to overcome inaccuracies that arise due to multipath propagation, this thesis investigates the optimal antenna configuration for Bluetooth channel sounding using multiple antennas. A comparison between the root-mean-square error and maximum error of the single-antenna baseline and the proposed multi-antenna solution for both spatial and sequential consistency in a complex multipath office environment shows that there is, on average, a 58% reduction in error metrics when the optimal multi-antenna setup is used. The performance of the optimal multi-antenna channel sounding setup in the complex environment approaches the single-antenna baseline performance in an ideal outdoor environment. This shows that the added antenna diversity successfully overcomes the negative effects due to multipath propagation.

Preface

The research presented in this thesis has been conducted in collaboration with an external company. While orientating for potential thesis topics, the company was in the process of assessing security threats to their BLE enabled access control system. This is periodically required, as part of their ISO27001 certification. The threats were ranked using the DREAD framework. From this, a BLE relay attack emerged as one of the highest ranked threats.

At the start of this thesis my aim was to realize this attack. For additional challenge (and fun), I decided to write all software for the relay attack using the Rust programming language. After the vulnerability was demonstrated, I continued my thesis by conducting research into mitigation techniques for BLE relay attacks. The recently introduced Bluetooth 6.0 core specification introduces channel sounding. This feature aims to provide Bluetooth devices decimeter level ranging accuracy, and, crucial for this research, the new specification also provides devices the ability to better detect and prevent BLE relay attacks.

I would like to thank the company where I performed my thesis. Not only for the freedom to analyze and demonstrate the vulnerability in their product, but also for the helpful insight and suggestions on how to mitigate this vulnerability. Another person I would like to thank is my supervisor Qing Wang. After our monthly meetings it was clear to me how to continue and confident that I was progressing at a good pace.

Stijn van de Water

Delft, The Netherlands
30th June 2025

Contents

Chapter 1

Introduction

Bluetooth Low Energy (BLE) is a common technology for short range wireless communication featured in nearly all available smartphones. A popular application using this technology is BLE proximity authentication using a Phone as a Key (PaaK). However, these applications have been proven to be vulnerable to relay attacks [20]. Conventionally relay attacks are prevented using (time-based) distance bounding protocols [1]. However, the current BLE V5.x specifications provides limited possibility for this [23], meaning that current mitigation techniques rely on signal analysis and fingerprinting [21].

In September 2024 Bluetooth 6.0 was introduced. This specification introduces new features that claim to prevent relay attacks. The most interesting feature introduced in this new specification is Bluetooth channel sounding, which allows two BLE devices, an initiator and a reflector, to estimate the distance between them using the Phase-Based Ranging (PBR) and Round-Trip Time (RTT) methods.

Goal & Research Questions

The research presented in this thesis aims to leverage these channel sounding techniques to develop a time-based distance bounding protocol to mitigate BLE relay attacks. This proposed protocol requires consistent channel sounding measurements, but initial measurements in a complex multipath environment not only showed poor consistency between measurements made at closely located locations, but sometimes even showed poor consistency between subsequent measurements at the same location. The performance of Bluetooth channel sounding can be improved using various methods, but due to the novelty of the Bluetooth 6.0 specification, the existing literature has primarily focussed on improving single antenna channel sounding performance [12] [27]. In [12] it is expected that multi-antenna channel sounding can significantly improve channel sounding performance in indoor environments.

Therefore, this research investigates the usage of multiple (up to 4) antennas during channel sounding. To this end this research aims to answer the following 3 questions related to the consistency of multi-antenna Bluetooth channel sounding:

(i) **What is the impact of antenna configuration on the consistency of channel sounding measurements?** [24] has already shown that there is some benefit in deploying multiple antennas during channel sounding.

The antenna orientation, antenna separation, and overall placement of the antennas can influence the channel sounding performance.

(ii) **What is the impact of antenna combining measurements on the consistency of channel sounding measurements?** Antennas can be combined using Individual Antenna Processing (IAP) or Summed Antenna Processing (SAP). In [14] it is shown that their IAP using minimal combining outperforms their SAP method. Therefore, this research will focus on antenna combining using IAP methods. Since these methods add additional processing to the channel sounding procedure the focus is on simple IAP combining methods that are able to run on the embedded hardware performing the channel sounding measurements.

(iii) **What is the optimal number of antennas to deploy for channel sounding?** It is expected that using more antennas improves the channel sounding performance. However, in addition to researching the peak attainable performance, it will also be researched how well the performance of the antenna configurations and antenna combining methods scale when more antennas are utilized.

Contributions

This paper demonstrates the performance and consistency of multi-antenna channel sounding in three distinct environments: an outdoor environment, a household environment, and an office environment. The PBR baseline (single-antenna) results showed that channel sounding in the office environment performed worst; the RMSE is 1.77 m and the maximum error is 7.00 m. The research into multi-antenna channel sounding showed that 4 antennas in a 'flip' configuration using the mean antenna combining method was optimal. When this setup is deployed in the office environment it allowed the RMSE to be reduced to 0.75 m and the maximum error to be reduced to 2.61 m. Crucially, deploying the proposed setup in the high multipath office environment approaches the performance of the baseline setup in the outdoor environment, showing that the improvements successfully overcome the effects of multipath propagation. Finally, while using more antennas significantly improves the consistency of channel sounding measurements, it is shown that the improvement achieved by adding more and more antennas is diminishing.

Structure

This thesis is structured as follows. First, chapter 2 provides the background for this work. In this background section, a BLE V5.x link-layer relay attack will be discussed and important features of the latest BLE 6.0 specification will be explained. In addition to this, related work in relay attack mitigation and Bluetooth localization will be discussed. Next, chapter 3 shows the design of a time-based distance bounding protocol along with the hardware and software design for a system to research the consistency of Bluetooth channel sounding. This chapter will also detail the researched antenna configurations and the environments in which the channel sounding performance will be evaluated. After that, the results are discussed in chapter 4. Finally, chapter 5 provides conclusions to this work and describes the limitations and options for future work.

Chapter 2

Background

This section provides the background for this research. First, the procedure of a BLE link-layer relay attack against a system using BLE proximity authentication will be discussed. Then, key concepts of the latest Bluetooth 6.0 standard, which includes promising technology to mitigate relay attacks, will be explained. Finally, related works in Bluetooth relay attack prevention and Bluetooth localization will be discussed.

2.1 BLE Link-Layer Relay Attack

2.1.1 BLE Proximity Authentication

BLE proximity authentication allows the user to conveniently open smart locks using their phone. The system contains two components, the peripheral (smart lock) and the central (phone), that communicate using BLE. The smart lock continuously advertises its presence to the surroundings, and the phone scans its surroundings for advertising devices. The phone tracks the Received Signal Strength Indicator (RSSI) from the smart lock and when the RSSI threshold is exceeded, it authenticates over BLE in order to open the smart lock. This authentication procedure can thus be triggered by increasing the RSSI, which is typically achieved by moving the phone closer to the smart lock.

During authentication the phone sends a 'token' which is verified by the smart lock. Each authentication procedure uses a nonce (number used only once), which is encrypted as part of the token and therefore prevents replay attacks.

2.1.2 BLE Link-Layer Relay Attack

The link-layer relay attack requires two attacking devices. The first device impersonates the smart lock and communicates with the phone, while the second device impersonates the phone and communicates with the smart lock. By relaying the received data between the two attacking devices both the smart lock and the phone are tricked into successfully completing the access procedure.

The attack scenario, as shown in Figure 2.1, shows that the mobile phone is vulnerable when within the RSSI threshold range of the attacking device. Since the attacker can freely adjust its transmit power, the RSSI threshold range can

thus be increased as required. Allowing the attacker a significant amount of flexibility when deploying the attacking device.

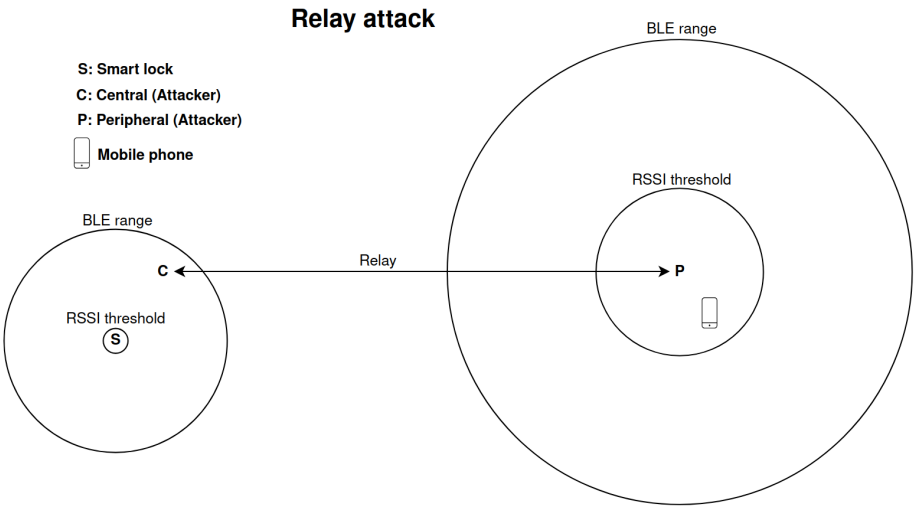


Figure 2.1: **Attack scenario for BLE relay attack.**

2.1.3 Attack Analysis

Comparing the relay attack to a normal access procedure shows that the relay attack requires additional steps. Not only must the Bluetooth signals be sent twice, the Bluetooth packets need to be encoded and decoded an additional time and the data needs to be relayed between the attacking devices. Each of these steps require additional processing meaning that the total duration of the access procedure is increased. This increased duration could therefore be used to detect and prevent relay attacks. However, as researched in [23], the latency of the BLE software stack of phones is unpredictable, meaning that this cannot be used to reliably prevent relay attacks.

2.2 Bluetooth 6.0 Channel Sounding

The latest Bluetooth specification published by the Bluetooth Special Interest Group (SIG) introduces channel sounding. Channel sounding is a combination of two techniques capable of estimating the distance between two Bluetooth devices. The channel sounding procedure is initiated by the initiator by sending a BLE signal to the reflector. The reflector processes the received signal and reflects it back towards the initiator. Measurements made during this procedure can be analyzed using two distinct methods; phase based ranging (PBR) and round trip timing (RTT). Both methods are described briefly below. For a more in depth explanation, it is highly recommended reading the technical overview published by the Bluetooth SIG[29].

2.2.1 Phase-Based Ranging (PBR)

Phase based ranging is a MultiCarrier Phase Difference (MCPD) technique. During phase based ranging the initiator sends an RF signal with a frequency of f_1 to the reflector. The RF signal arrives, with a phase offset, at the reflector. The reflector reflects the signal back to the initiator by sending an RF signal, which has the same frequency f_1 and starts at the same phase offset as the received signal. The initiator receives the reflected signal and measures the phase ϕ_1. The procedure is repeated with a different f_2 to obtain ϕ_2. The initiator can now, using the speed of light c, calculate the two-way distance d between itself and the reflector as shown in Equation 2.1.

$$d = \frac{c * (\phi_2 - \phi_1)}{2\pi * (f_2 - f_1)} \mod (\frac{c}{f_2 - f_1}) \tag{2.1}$$

The modular part of the above equation means that multiple distances d can be true for the used parameters. This is why the ranging procedure should be repeated using different f_1 and f_2 in order to disambiguate the calculated distances. Normally BLE utilizes 40 channels separated by $2MHz$, but when channel sounding is active this is extended to 72 channels separated by $1MHz$, meaning that, if all frequencies are used, distance ambiguity is only possible after 150 m. Another way to resolve the distance ambiguity is to cross-check the obtained result using an RTT measurement.

2.2.2 Round-Trip Time (RTT)

The procedure used for round-trip timing is similar to the procedure used for phase based ranging; the initiator sends an RF signal to the reflector, which reflects the signal back to the initiator. However, when using this technique the time of departure (T_{ToD}) and time of arrival (T_{ToA}) of the initiator are used in combination with the speed of light c to calculate the two-way distance d as in Equation 2.2.

$$d = c * (T_{ToA} - T_{ToD}) \tag{2.2}$$

In reality the procedure is slightly more complicated than described above. The reflector takes an unknown amount of time before the signal is reflected. This processing time needs to be subtracted from the total time, such that only the Time of Flight (ToF) of the signal is used in the calculations.

2.2.3 Challenges

In theory, phase based ranging and round trip timing allow for exact distance calculations, however in practice there are several limiting factors that need to be overcome. The most impactful factor is multipath propagation of RF signals, which is exaggerated during two-way ranging due to the squaring of multipath components [27]. This means that components of the same signal arrive at different times with differing phase offsets, impacting both the RTT and PBR methods.

Other challenges that may reduce the accuracy of channel sounding measurements are: the RF interference from nearby devices, and stability and accuracy of generated signals and internal clocks[29]. Finally, security considerations may

also reduce channel sounding performance. Additional processing can for example be required, which reduces the measurement frequency and increases the latency.

2.2.4 Security Implications

While PBR provides more accurate distance estimations, it is vulnerable to phase-slope rollover attacks, RF cycle slip attacks, and on-the-fly phase manipulation attacks[10]. [20] shows the implementation of a distance extending relay attack, while simultaneously manipulating the PBR measurements to a desired value. RTT distance measurements are more secure. An attacker would either have to relay the signal, which adds time, or the attacker would have to correctly guess bits in a randomly generated bit sequence.

Before two BLE devices can perform channel sounding measurements they need to set up an encrypted link by pairing both devices to each other. [28] showed that this pairing mechanism is not secure. They were able to let the user pair with an attacker, instead of a trusted device, in 92.5% of the cases. The attacker can now participate in the channel sounding procedure and reduce the estimated distance, even for RTT measurements, between the mobile phone and smart lock.

2.3 Related Work

2.3.1 Bluetooth Relay Attack Mitigation

The current state of the art in relay attack mitigation using BLE is based on channel reciprocity and RF fingerprinting [21]. Relay attack mitigation based on channel reciprocity leverages the fact that both parties observe the same random loss and multipath effects, since both communicate in a similar channel (e.g. frequency, environment, time). If an attacker performs a relay attack the communication with the smart lock occurs in environment A, while the communication with the mobile phone occurs in environment B. This can lead to uncorrelated measurements due to environmental differences, indicating a relay attack.

RF fingerprinting extracts features of the physical signal and compares these to stored fingerprints that were gathered previously in a non-adversarial setting. This allows the smart lock to detect if the signal comes from different hardware [11] or, in case of amplification, it is able to detect an increase in signal noise.

While the state of the art of Bluetooth relay attack mitigation relies on channel reciprocity and RF fingerprinting, relay attacks can best be prevented using distance bounding protocols [1]. These protocols allow the smart lock to establish an upper bound on the distance of the mobile phone. If the distance between the two devices is too large certain actions, such as unlocking a door, can be blocked by the smart lock. Distance bounding protocols can rely on various indicators to determine the distance between two devices. Of these indicators the time the RF signal has to travel from one device to another is the only value that cannot be reduced by an attacker, since RF signals already travel at the speed of light. This is why the recent addition of Bluetooth channel sounding,

and especially the round trip timing method, is a promising technology to build time based distance bounding protocols for relay attack mitigation.

2.3.2 Bluetooth Localization

Received Signal Strength (RSS)

Conventionally, RF distance estimations are performed using the received signal strength. These methods rely on the free-space path loss of radio signals; the further the receiver is from the transmitter, the lower the received signal strength. Unfortunately, the effects of multipath propagation heavily influence the RSS in undesired ways. These multipath effects are too complex to accurately model. Therefore, RSS fingerprinting is used to reduce the localization error [4]. A major limitation of RF fingerprinting is the reliance on the density of the beacon network for good performance. This is why RF fingerprinting techniques are often developed and researched for existing Wi-Fi systems [30] [13].

The cost and power advantages of BLE also make Bluetooth deployments utilizing these techniques interesting. [4] shows that Bluetooth RSS fingerprinting is able to achieve a 95% maximum error of 2.6 m in a high density BLE network (1 beacon per $30m^2$) and a 95% maximum error of 4.6 m in a low density BLE network (1 beacon per $100m^2$). This is shown to be an improvement over the 95% maximum error of 8.5 m using an existing Wi-Fi network in the same area.

Angle of Arrival (AoA)

A Bluetooth device can determine the angle of arrival of the signal coming from another BLE device. In order to determine this, the receiving BLE device is equipped with an antenna array. The wavefront of the incoming signal reaches each antenna in the array at a different time, which results in a different phase offset at each antenna. The fixed antenna separation of the receiver and the phase offsets can then be used to calculate the angle of arrival. This on its own is only able to provide a direction, but when three (or more) anchor BLE devices are used the location can be calculated using trilateration.

In [2] the localization performance of AoA is evaluated in a 7 m $\times$ 7 m square. It is shown that the error is less than 0.85 m in 95% of the tested positions. While this shows good accuracy for the AoA method, it needs to be kept in mind that this method might not as reliable as other methods at longer distances. The same inaccuracy in the calculated angle will lead to larger localization errors when the two BLE devices are separated by longer distances [31].

MultiCarrier Phase Difference (MCPD)

Multiple Signal Classification (MUSIC) is a popular method to perform distance estimations using MCPD (eg. [24], [27]). [14] proposes an enhanced super-resolution distance estimator that improves upon the MUSIC algorithm. The paper also briefly discusses the use of multiple antennas and shows that Individual Antenna Processing (IAP) using minimal combining outperforms Summed Antenna Processing (SAP). Their optimal solution allows the baseline single-antenna RMSE of 1.53 m to be reduced to 0.61 m.

In [6], first, the 1-dimensional distance measurement performance of different MCPD calculation methods is evaluated. The IFFT method outperforms the phase slope method, and both MCPD methods are shown to outperform the conventional RSSI distance estimation method. After this, the 2-dimensional localization performance is experimentally evaluated in an office environment of 100 m^2. This evaluation demonstrates that the MCPD using the IFFT method achieves similar localization performance as an AoA based method. Both methods are also shown to significantly outperform MCPD using the phase slope method and an RSSI based method.

One of the first papers to research MCPD using Bluetooth 6.0 is [12]. This paper presents a processing pipeline based on the minimum variance distortionless response (MVDR) algorithm. Part of the proposed pipeline implements scene identification in order to significantly improve the indoor channel sounding performance. Using these improvements, the average 90% peak error is reduced to 1.2 m and the average RMSE is reduced to 0.8 m. The authors suggest research into multi-antenna channel sounding, and expect significant performance benefits in indoor and dynamic environments.

Time of Flight (ToF)

In [5], the authors investigated the two-way round trip time of the advertisement of BLE beacons. The paper leverages the frequency diversity across the three main advertising channels in an attempt to overcome the effects of multipath propagation and improve measurement results. The paper demonstrates two methods; the first method simply averages the results across all channels, while the second method selects the measurement associated with the channel that has the highest received signal strength.

The authors of [22], providee a comparison between Bluetooth 6.0 channel sounding techniques. They show that measurements made using round trip timing have a larger deviation from the ground truth than measurements made using phase based ranging.

Chapter 3

Design

3.1 Time Based Distance Bounding Protocol

The addition of Bluetooth channel sounding, especially RTT, improves the capability of Bluetooth devices to mitigate relay attacks, as this allows for the establishment of a time based distance bounding protocol. This way physical-layer relay attacks can be prevented, since any relaying of the signal will take as much time, if not longer, to reach the other device.

Link-layer relay attacks, however, are still possible. Figure 3.1 shows that the attacking device can participate in the channel sounding procedure and still trick the mobile phone into sending its token. This 'early reflection' allows the attacker to reflect the channel sounding packets, effectively bypassing the distance bounding protocol, while still relaying the encrypted data between the true central and peripheral devices. Even tough relay attacks are still possible, the attack is already somewhat mitigated by using the RTT distance metric instead of the RSSI distance metric. Figure 3.2 shows that the attacker now has to be within a certain distance (d_{max}) of the smartphone, while previously, as described in chapter 2, they could simply increase their transmit power in order to appear closer.

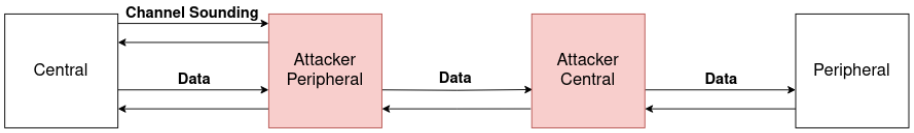


Figure 3.1: **Flowchart showing how the attacker can make the peripheral appear close to the central by participating in the channel sounding procedure.**

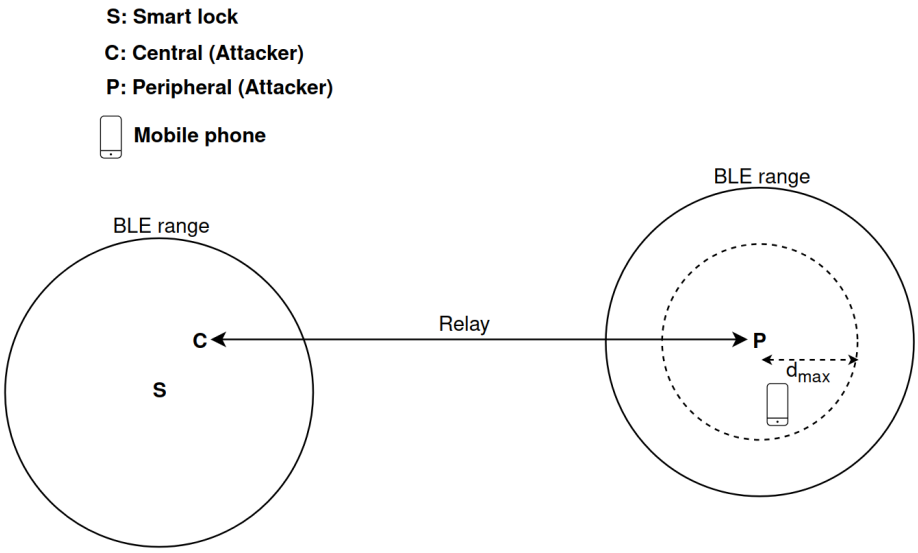


Figure 3.2: **Attack scenario when the protocol uses one way time based distance bounding. Note that the mobile phone must now be within d_{max} in order for the relay attack to succeed.**

To further mitigate the risk of BLE relay attacks the distance bounding protocol is extended by employing two-way ranging. Meaning that both the central and the peripheral will estimate the distance to each other, and since the channel is reciprocal both will obtain similar results. If an attacker is in the middle, the two measured channels are no longer the same. Not only can the actual distance of the measured channel be different, but also the propagation characteristics of the channel can be different. Measurements made in these dissimilar channels can therefore yield different results. Figure 3.3 shows that performing a relay attack is still possible, but this time the attacker does not only need to be close to the peripheral, the (measured) distance between the attacker and the central also needs to be the same as the (measured) distance between the attacker and the peripheral. Essentially the attacker is now restricted to pick a distance $d \leq d_{max}$ and place both attacking devices at this distance from the real devices. Figure 3.4 shows the attack scenario against this protocol. While this attack scenario is significantly mitigated, in practice performing the relay attack is still feasible. The attacker can, for example, deploy one of the devices in a hallway. When a victim walks through this hallway and passes the attacking device, the victim and the and device performing the relay attack are separated by d at two points. In addition to this the variance in channel sounding distance estimations gives the attacker some amount of flexibility when performing the relay attack.

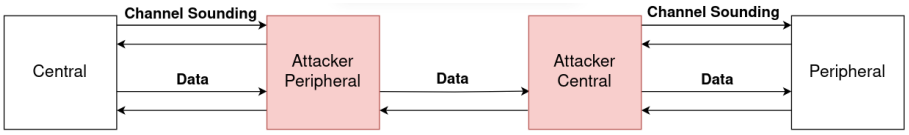


Figure 3.3: **Flowchart showing how the attacker can still participate in channel sounding during two-way ranging.**

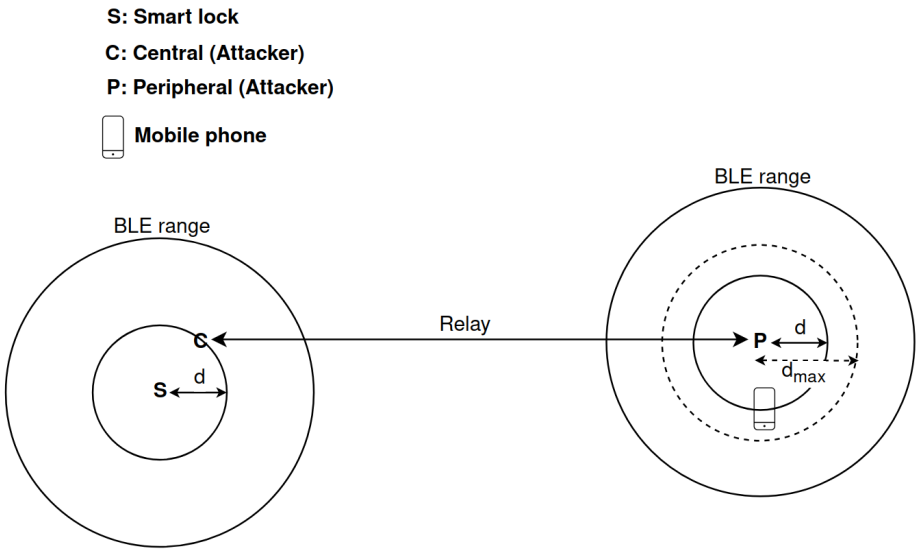


Figure 3.4: **Attack scenario when the protocol uses two-way time-based distance bounding. Not only does the mobile phone need to be within d_{max}, this time the distance from central to smart lock and from peripheral to mobile phone must now also be equal.**

To mitigate the risk of BLE relay attacks even further, additional nearby BLE devices are incorporated into the protocol. These devices can be other smart locks or beacons with the sole purpose to help mitigate relay attacks. From these new devices one is selected and both the smart lock and the mobile phone perform the two-way channel sounding procedure to this new device. This significantly constrains the attacker. Figure 3.5 shows that the attacker must now deploy an additional device acting as the second smart lock and place it at the correct distance from the mobile phone. The attack scenario shows that circles from the attacking devices intersect only at two locations, meaning that the mobile phone must be at one of those locations for the relay attack to succeed. By adding a third device the number of locations where the smartphone can be placed is reduced to 1. Adding even more devices requires the attacker to also deploy more devices at the correct distances, making it increasingly harder to successfully perform the relay attack.

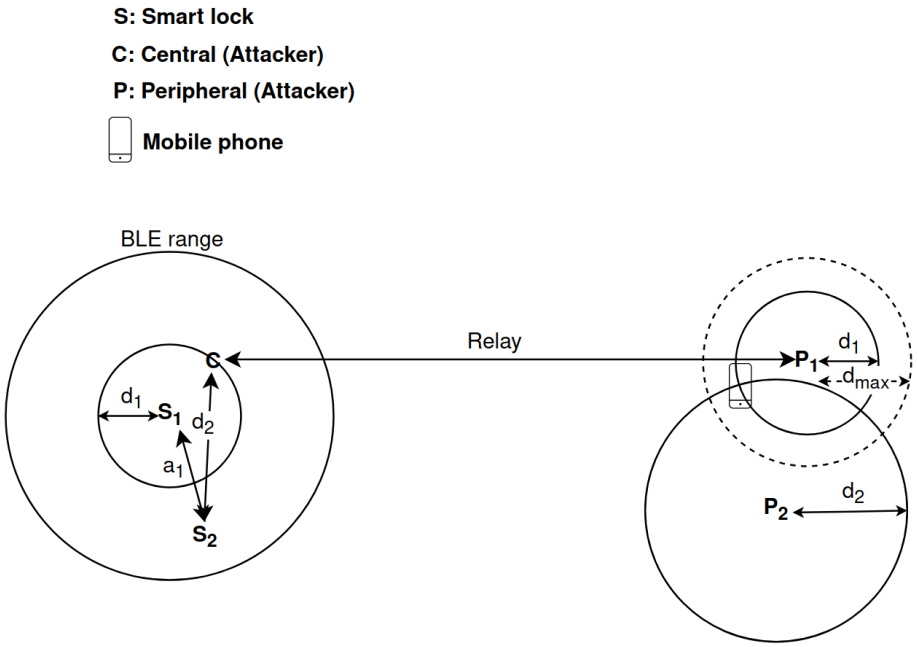


Figure 3.5: **Attack scenario when also performing channel sounding to a nearby smart lock S_2. The attacker must now also deploy P_2 and place it at the correct distance d_2 from the smartphone. The relay attack can now only succeed if the smartphone is located where the circles surrounding $P_{1,2}$ intersect.**

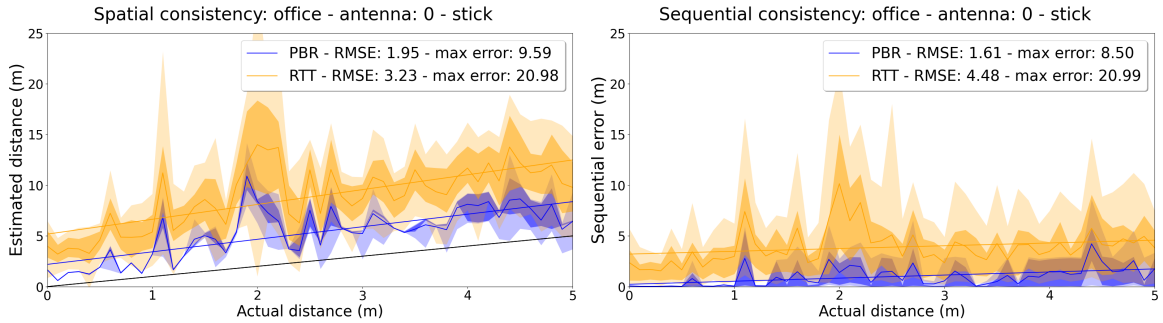
To summarize, the following changes or additions have been made to the RSSI based proximity authentication protocol to create the proposed time based distance bounding protocol. First, the RSSI distance estimator is replaced by the RTT distance estimator. Second, two-way ranging is used. Finally, multiple nearby BLE devices are incorporated into the procedure. Each improvement to the protocol aims to reduce the available attack surface to the attacker. This limits the flexibility of the attacker and reduces the likelihood of a successful relay attack.

3.1.1 Preliminary Results

Preliminary channel sounding results showed poor spatial and sequential consistency. Figure 3.6-a shows that, while the estimated distance increases with the actual distance as expected, there is regularly a large deviation between measurements made at closely located locations. Figure 3.6-b shows that there are even significant differences between subsequent measurements, this is especially true for RTT measurements.

In context of the proposed protocol described above, the inaccuracies in channel sounding measurements require the distance constraints to be relaxed. If these constraints are not relaxed, legitimate users will frequently be flagged for relay attacks (false positive). The relaxation of these constraints increases the attack surface available to the attacker. The distances d_1 and d_2, as shown in Figure 3.5, can now best be represented as $d_1 \pm \Delta$ and $d_2 \pm \Delta$, where Δ is a

parameter that depends on the spatial and sequential consistency of the channel sounding measurements. Figure 3.7 reflects this in the protocol. It can be seen that the circles are now replaced with rings, and that the intersection of the rings around P_1 and P_2 now forms an area instead of two points.



(a) Spatial consistency

(b) Sequential consistency

Figure 3.6: **Preliminary single antenna channel sounding results in a complex office environment.**

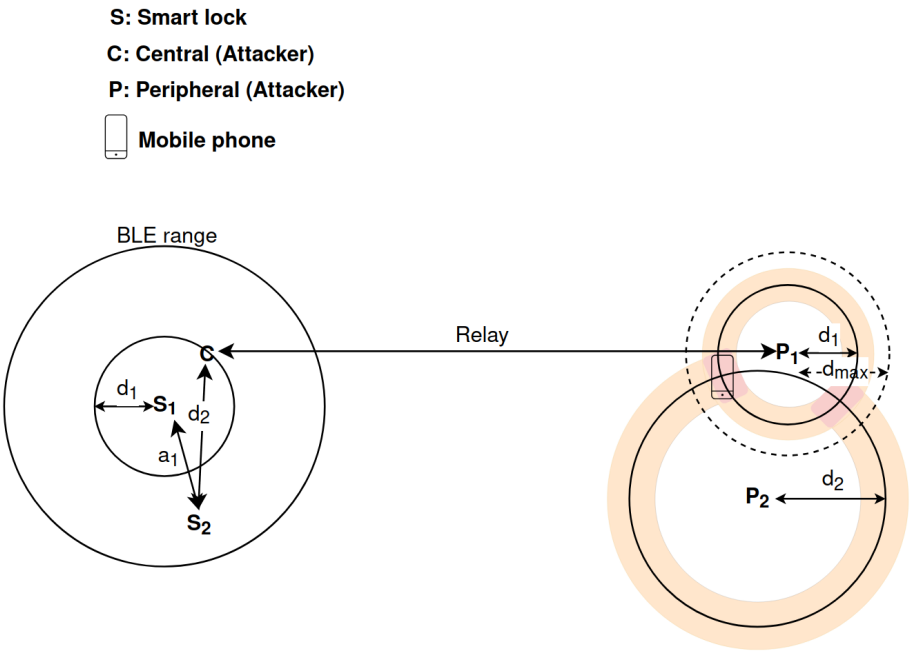


Figure 3.7: **Attack scenario of the proposed protocol accounting for variance in RTT measurements. The mobile phone is now vulnerable when inside the red area.**

3.1.2 Protocol evaluation

The goal of the proposed time-based distance bounding protocol is to reduce the likelihood of successful relay attacks. The proposed mitigation attempts to accomplish this by reducing the area where the mobile phone is vulnerable. Table 3.1 provides a comparison between the attack area for different versions of the proposed protocol discussed in section 3.1. This comparison was made using $d_1 = 3.0m$, $d_2 = 10m$, $d_{max} = 5.0m$, and Δ was selected as the largest root-mean-square-error present in the preliminary channel sounding results ($\Delta = 4.48m$). A realistic implementation of the protocol might select a different value for Δ in order to reduce false negative or positive detections of relay attacks, but since the RMSE represents the average magnitude of the errors, this metric was selected for the comparison. In addition to this smaller values for d_{max} (and thereby d_1) are expected. However, the value of Δ in the preliminary results is simply too large to provide an accurate performance evaluation of the proposed protocol, with a reduced d_{max}.

The comparison shows that each improvement to the distance bounding protocol reduces the expected attack area. Nevertheless, an attack area of roughly $80m^2$, achieved by the final version of the protocol, still gives an attacker a considerable amount of flexibility to perform the relay attack with high probability. While the protocol can be extended further to limit the available attack area, it will be more effective to improve the consistency of channel sounding measurements. This will decrease the value required for Δ, and will not only have a positive effect on the proposed version of the protocol, but will also improve potential extensions to the protocol, and could even bring less complex versions of the protocol back into consideration.

Table 3.1: **Protocol evaluation**

Protocol version	Attack area (m^2)
RSSI based distance bounding	907.92 [1]
RTT based distance bounding	282.34
Two-way RTT based distance bounding	175.77
Two-way RTT based distance bounding (1 beacon)	160.56 [2]
Two-way RTT based distance bounding (2+ beacons)	80.29 [2]

3.2 System Design

The final protocol described in the previous section imposes two requirements on the performance of channel sounding. Firstly, reciprocal channel sounding measurements should be consistent, and secondly channel sounding measurements made from co-located positions should be similar. The system design presented here is designed in order to research the effect of antenna diversity on the consistency and performance of Bluetooth channel sounding.

[1] BLE maximum range is calculated to be 17 m in an office using the NIST PAP02-Task 6 Model [15] [3]

[2] The area where the two rings intersect have been approximated as two squares with sides of length 2Δ.

3.2.1 Bluetooth 6.0 Development board

Options for development boards featuring support for Bluetooth 6.0 channel sounding are limited. During this thesis only three options were available: the nRF54L15 DK from Nordic Semiconductor, the xG24-RB4198A and xG24-DK2606A from Silicon Labs. While the current selection is limited, many manufacturers are actively working on Bluetooth 6.0 compatible microcontrollers. The authors of [12] are affiliated with Infineon Technologies, but the board used in their research is not (yet) available publicly, NXP has announced their MCX W72x family of MCUs, which are currently in preproduction [9] [8], and Texas Instruments' CC2755R10 is currently labeled as 'preview' [25] [26]. Table Table 3.2 provides a comparison of the capabilities of each available Bluetooth 6.0 compatible channel sounding board. The table shows that there are no significant differences between the three MCUs. All contain the same ARM Cortex-M33 core and operate at similar clock speeds and have similarly sized flash and RAM. One aspect that stands out is the dual antenna design present on the xG24-DK2606A, but since this thesis will research channel sounding with up to four antennas, this is not necessarily a benefit. Finally, none of the available MCUs provide additional processing units specifically designed to support channel sounding calculations. The upcoming products of NXP and Texas Instruments will feature a Localization Compute Engine (LCE) and an Algorithm Processing Unit (APU) respectively.

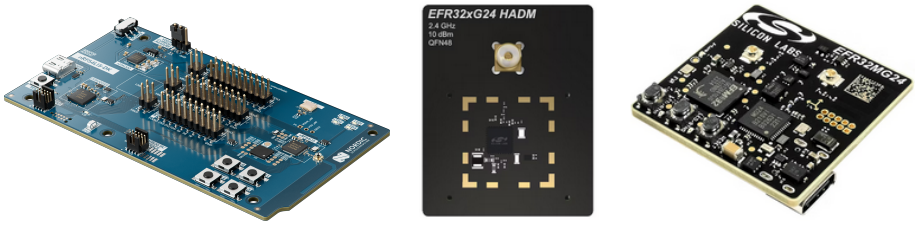


Figure 3.8: **Bluetooth 6.0 development board options. Nordic's nRF54L15 DK (left), Silicon Labs' xG24-RB4198A radio board (middle), and Silicon Labs' xG24-DK2606A dual antenna channel sounding devkit (right).**

Table 3.2: **Comparison of Bluetooth 6.0 development boards**

	Nordic nRF54L15 DK [7]	Silicon Labs xG24-RB4198A [18] [16]	Silicon Labs xG24-DK2606A [17] [16]
CPU core	ARM Cortex-M33	ARM Cortex-M33	ARM Cortex-M33
Clock speed	128 MHz	78 MHz	78 MHz
Flash size	0.5 - 1.0 - 1.5 MB	1.5 MB	1.5 MB
RAM	96 - 192 - 256 KB	256 KB	256 KB
Coprocessor	RISC-V (128 MHz)	Is itself a coprocessor to the Si-MB4002A mainboard	-
Antenna	1 PCB antenna	1 PCB antenna	2 PCB antennas
CS support	yes	yes	yes
Board cost	36.27	42.37	73.94
Chip cost	3.03	8,96	5.53

Ultimately, this research will use two nRF54L15 (preview) development kits from Nordic Semiconductor. This choice was made not only because of data provided in the table, but also due to the availability of channel sounding sample code in a familiar framework (Zephyr RTOS) and prior experience with microcontrollers from Nordic Semiconductor (nRF51822 and nRF52840). Finally, two samples of the nRF54L15 (preview) development kits were received for free from Rutronik.

3.2.2 RF switch selection

Selecting an RF switch was very different to selecting a Bluetooth 6.0 development board. Mouser lists over 1400 components in their RF switch category. In order to limit the options the following filters were applied.

- **Switch Configuration = SP4T.** The Bluetooth 6.0 core specification allows for up to 4 antennas on a BLE device during channel sounding. Even tough the antenna processing method, used in this research, can freely use more antennas, it was decided to adhere to the maximum number of antennas proposed in the specification. This allows for better comparisons with other research. The Single Pole 4 Throw (SP4T) configuration of the switch allows the RF output of the development board to be directly connected to one (and only one) of four external antennas.

- **Min. Frequency $\leq$ 2.4 GHz AND Max. Frequency $\geq$ 2.5 GHz.** Bluetooth (and channel sounding) operate in the 2.4 GHz ISM band. To be more specific, the 40 Bluetooth channels range from 2.402 GHz to 2.480 GHz and are 2 MHz wide. The operating range of the RF switch must completely cover this range in order to maintain optimal antenna performance.

- **Manufacturer = Skyworks.** With the other filter applied 107 options were remaining. To reduce the number of options even further inspiration was taken from the dual antenna design of Silicon Labs's xG24-DK2606A development board, discussed in the previous subsection. This design uses Skyworks' SKY13348-374LF RF switch. This SPDT switch is unfortunately not sufficient for this research, but selecting a SP4T switch with similar capabilities from the same manufacturer should lead to an RF switch capable of meeting the requirements set by this research.

The above filters reduced the available options to 7. From this Skyworks' SKY13575-639LF was selected. This SP4T RF switch operates from 0.1 GHz to 6 GHz, and features low insertion loss (0.6 dB) and high isolation (40 dB) at 2.5 GHz [19]. The switch can be controlled via a simple GPIO interface to switch the active antenna. Instead of designing a custom PCB around this component the evaluation board, shown in Figure 3.9, was used. This board features five SMA connectors, the RF switch with some external circuitry and two IO inputs, that can be used to select an antenna. This evaluation board limits the placement options of the antenna, but allows for easier and faster evaluation of whether the selected RF switch is suitable for this research.

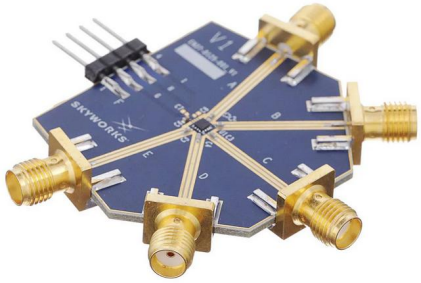


Figure 3.9: **Skyworks SKY13575-639 evaluation board**

3.2.3 Antenna selection

For this research three distinct antenna types were considered, shown in Figure 3.10. The first option is a PCB antenna. PCB antennas are compact and cost-effective solutions commonly used for radio communication. It is likely that, both smartphones and smart locks will contain PCB antennas. This means that researching channel sounding using these antennas would provide a system that is closer to a real world scenario, than a system using external antennas. However, a major downside to PCB antennas is that, once the PCB is manufactured, there is little that can be modified, limiting the experimental possibilities.

This is different for external antennas. Not only can the connected antennas be freely replaced by other types antennas, they can also be placed more freely in the environment. This can potentially help improve performance by increasing the spatial and polarization diversity. The difference between the stick dipole and puck antenna is not significant. Both antennas have a low gain (≤ 2 dBi) and are therefore omnidirectional. The main difference between the two antennas is the connector. The stick dipole antenna needs to be directly screwed onto the SMA connector, whereas the puck antenna is first connected to a 3 m cable. This provides more placement flexibility for the puck antenna, but also leads to overestimations of the distance during channel sounding. This is because the signal takes time to travel through the cable. For this reason it was chosen to research the performance of Bluetooth channel sounding using the stick dipole antenna.

Figure 3.10: **Different types of antennas considered for this research. From left to right: PCB antenna, stick dipole antenna, and puck antenna.**

3.2.4 Final system design

This research uses two nRF54L15 (preview) development kits from Nordic Semiconductor. These devices support BLE version 6.0, and in particular feature support for BLE channel sounding. During channel sounding one development kit acts as the initiator while the other acts as the reflector. The antenna output of the reflector is directly connected to an external 2.4GHz stick dipole antenna, while the initiator is connected to a Skyworks SKY13575-639 RF switch which uses GPIO inputs to switch between one of four external antennas. This corresponds to antenna configuration #3, as specified in the Bluetooth core specification. This configuration provides 4 distinct antenna paths between the initiator and reflector. In theory the antenna diversity allows the channel sounding procedure to yield more consistent results even when one or more antenna paths have unfavorable conditions.

Table 3.4 lists the hardware components used for multi-antenna channel sounding. Figure 3.11 and Figure 3.12 show how the hardware is connected. The initiator is powered by the PC via the USB connection, and the RF switch is powered by the initiator's VDDIO pin [3]. GPIO pins P2.07 and P1.14 select between RF1 to RF4 according to the table shown in Table 3.3. The used GPIO pins are shared with LED2 and LED3 of the development board, this gives a clear visual feedback of the currently selected antenna.

Table 3.3: **RF switch truth table**

P2.07 (VC_1)	P1.14 (VC_2)	RF_{out}
0	0	RF_1
0	1	RF_2
1	0	RF_3
1	1	RF_4

[3]Note that the default voltage of the VDD rail is 1.8V. This needs to be configured to 3.3V using the board configurator tool of nRF Connect

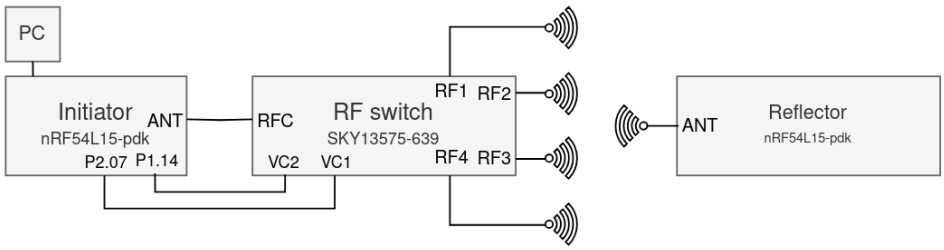


Figure 3.11: **System diagram for multi-antenna channel sounding.**

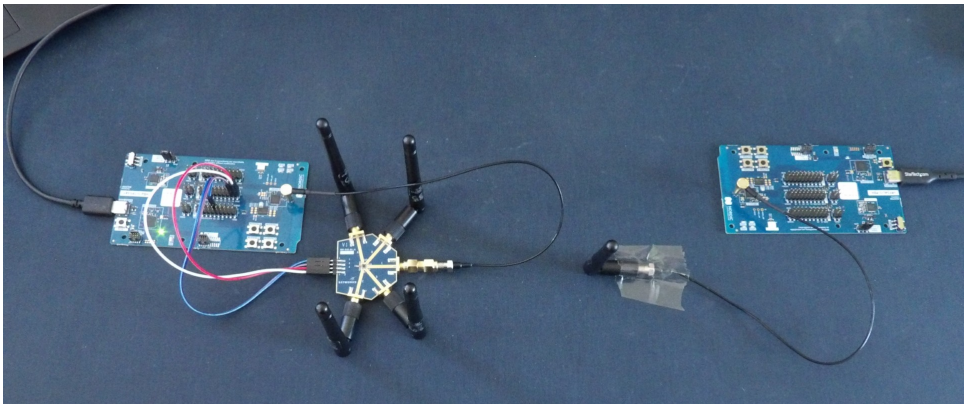


Figure 3.12: **System for multi-antenna channel sounding.**

Table 3.4: **List of hardware components required for the multi-antenna channel sounding system design.**

Item	Description	Amount
Nordic nRF54L15-dk	Channel sounding development kit	2
Murata MXHS83QE3000	Antenna adapter/connector	2
TE Connectivity ADP-SMAM-SMAM-G	Antenna adapter/connector	1
Skyworks SKY13575-639-EVB	RF switch evaluation board	1
Delock SMA antenna	SMA antenna	5

3.3 Software design

The software on the development kits is adapted from the initiator[4] and reflector[5] samples available in the nrfconnect sdk. These samples are built using the Zephyr RTOS. The reflector sample advertises the ranging responder service, and can connect to the initiator to reflect the received channel sounding packets. This sample is used without modification. The initiator sample scans

[4] `https://github.com/nrfconnect/sdk-nrf/tree/main/samples/bluetooth/channel_sounding_ras_initiator/src`

[5] `https://github.com/nrfconnect/sdk-nrf/tree/main/samples/bluetooth/channel_sounding_ras_reflector/src`

for the ranging responder service, and connects to the reflector. After the channel sounding parameters, further discussed in subsection 3.3.3, have been communicated between the initiator and reflector, the initiator, periodically, sends channel sounding packets to the reflector. IQ and timestamp measurements of the reflected packets are recorded for processing. From these measurements the distance between the initiator and reflector can be estimated. The PBR distance estimation uses the IQ samples and the phase-slope method to calculate the distance. And the RTT distance estimation is calculated using the timestamp information.

The initiator sample code is modified in order to perform multi-antenna channel sounding. The section below details how the existing initiator sample was modified. It will also explain how host code running on the PC is developed to capture data, process results, and create plots. After this, the antenna combining methods and the channel sounding parameters are discussed.

3.3.1 Software for multi-antenna channel sounding

Zephyr Configuration

First, the UART and GPIO pins 1.14 and 2.07 are enabled and configured using a new devicetree overlay file. The UART will be used to send channel sounding measurements to the PC and the GPIOs can be used to switch between antennas. Next the kconfig configuration file is updated to enable the async UART, and the GPIO drivers for the application. The options to obtain the RSSI of the connection, and to reboot board are also enabled.

Embedded Code

The source code of the initiator is updated to create a multi-antenna initiator. Not only is the used antenna incremented after every channel sounding procedure, the results are also processed and stored for each individual antenna. After the initiator has performed a measurement using each antenna, the results are combined using one of the antenna combining methods discussed in subsection 3.3.2. The combined results are then reported, along with the individual antenna results, over UART to the PC. The fact that the initiator has to wait until each antenna has made a measurement, increases the period between subsequent distance estimations from 0.4s to 1.6s.

Host Code

The PC host runs a python script to capture and store the multi-antenna channel sounding measurements reported by the development board. A separate python script processes the results. The processed data is transformed into plots, and various error metrics are calculated.

Since the individual antenna measurements are also stored on the PC, it is possible to replay this data. When doing this the PC sends the individual antenna measurements to the development board. The development board treats this data the same way as a new channel sounding measurement. This means that the data of the antennas is combined, and sent back to the PC. This allows for the recalculation of results when existing antenna combining methods are updated, or when new antenna combining methods are added, without the need

for the long and tedious process required to re-capture the channel sounding data.

3.3.2 Antenna Combining Methods

The key advantage of using multiple antennas is that it is possible to overcome difficult multipath scenarios. The method in which the information from each individual antenna is combined into a single distance estimation can greatly affect the overall channel sounding performance. Antenna combination methods can be divided into two categories; Individual Antenna Processing (IAP) and Summed Antenna Processing (SAP). Both processing methods combine the data gathered from multiple antennas into a single measurement, but the type of data used is different. Figure 3.13 shows how both methods combine and process the antenna data. In SAP the analog signals received by the antennas are first combined before being transformed to digital signals and processed. This is reversed for IAP methods. In this method, the signals are first digitally processed before the results are combined.

Both IAP and SAP antenna combining methods improve channel sounding measurements, but each method has their own strengths and weaknesses. SAP methods feature a lower computational complexity, while the IAP methods are able to more effectively exploit the spatial diversity offered by the antennas. This is due to the nature of how each method operates. SAP processes a single merged signal, whereas IAP is able to process each antenna individually.

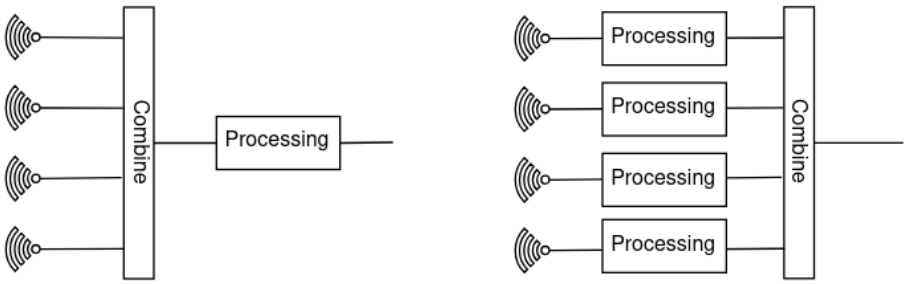


Figure 3.13: **Comparison between summed antenna processing (left) and individual antenna processing (right)**

This research focuses on IAP combining methods, this choice was not only made because IAP methods can theoretically exploit spatial diversity better, but also because [14] indeed demonstrated superior performance for IAP methods when compared to similar SAP methods. Below the IAP methods that will be used to combine the information of multiple antennas are described. For each combining method an equation is given, where N is the number of processed antennas, d_n is the processed distance estimation from antenna n, and d is the resulting distance estimation after applying the combination method.

- **Minimal** - Using the result of the antenna that reports the minimum estimation intuitively makes sense. We are interested in the line that directly connects the initiator and the reflector. If a different result is

used that is not the minimum then it must be from a multipath reflection. The minimal combining method is also proposed in [14] as a combining method for IAP.

$$d = \min_{n \in \{1,..,N\}} d_n$$

- **Maximum RSSI** - Select the antenna measurement that corresponds to the antenna with the highest RSSI. This method was used to select the optimal BLE channel for time of flight measurements in [5].

$$d = d_n,\ n = \operatorname*{argmax}_{n \in \{1,..,N\}} RSSI_n$$

- **Mean** - Calculate the mean of the results from all available antennas.

$$d = \frac{\sum_{n=1}^{N} d_n}{N}$$

- **Lowest standard deviation** - Select the antenna that has the lowest standard deviation in the previous x measurements.

$$d = d_n,\ n = \operatorname*{argmin}_{n \in \{1,..,N\}} \sqrt{\frac{\sum_{i=K-x}^{K} (d_{n,i} - \mu)^2}{x}}$$

- **Proportional RSSI** - Assign a weight to each antenna proportional to its received RSSI. The result is calculated as the weighted average over all antennas. The weights are linearly scaled such that the antenna with the lowest RSSI does not contribute to the final result.

$$d = \sum_{n=1}^{N} w_n * d_n, w_n = \frac{RSSI_n - \min_{n \in \{1,..,N\}} RSSI_n}{\sum_{n=1}^{N} (RSSI_n - \min_{n \in \{1,..,N\}} RSSI_n)}$$

3.3.3 Channel Sounding Parameters

The Bluetooth 6.0 core specification offers a significant degree of customizability of the channel sounding procedure. In theory, this means that the parameters of the channel sounding procedure can be tuned for specific requirements. Tradeoffs can be made in terms of accuracy, latency, measurement frequency, security, and robustness.

Unfortunately, the experimental status of channel sounding in the nRF Connect sdk meant that many configuration options were unavailable or not working properly. This severely limited the experimentation that could be done. To give an example, it was not possible to increase the ratio of RTT to PBR measurements by setting RTT as the main mode and PBR as the sub mode. Consequently, all data has been gathered using the same channel sounding configuration. The configuration and procedure parameters are shown in Table 3.5 and Table 3.6 below.

Table 3.5: **Channel sounding configuration parameters**

Parameter	**Value**
Main mode	PBR
Sub mode	RTT
Main mode steps	10 to 20
Main mode repetition	0
Mode 0 steps	3
RTT type	Access Address (AA)
Cs sync PHY	1M
Channel map repetition	5
Channel selection type	3B
Channel sequence shape	Hat shape
Channel sequence jump	2

Table 3.6: **Channel sounding procedure parameters**

Parameter	**Value**
Maximum procedure length	100 * 0.625 ms
Procedure interval	9
Maximum procedure count	No limit
Subevent length	10 ms
PHY	2M
SNR control	No SNR control

3.4 Evaluation setup

In each experiment, the initiator and reflector will be positioned facing each other. They start directly next to each other, and after 50 channel sounding measurements have been made for each antenna path, the initiator is moved away by 10 cm. This is repeated until the initiator and reflector are separated by 5 m, resulting in around 10,000 channel sounding measurements per experiment. Each experiment is performed using different antenna configuration, and in a different environment. Both, the configurations and environments, will be discussed in this section.

3.4.1 Antenna Configurations

The channel sounding experiments are repeated using 3 different antenna configurations. These configurations are named 'stick', 'flip', and 'star'. The 'stick' configuration has all 4 antennas sticking up in the same orientation, while for the 'flip' configuration two of the four antennas are flipped upside down. In the 'star' configuration the antennas are folded out, creating a pattern that resembles a star. In each of the configurations the antennas are directly attached to the RF switch evaluation board. Note that the tables in this subsection name the antennas A, B, D, and E, since connector C of the evaluation board is reserved for the RF input. The antenna configurations are described in more detail below.

‘stick’ configuration

The ‘stick’ antenna configuration, shown in Figure 3.14, features the minimal amount of antenna separation offered by the evaluation board of the RF switch. In addition to this, all antennas are oriented the same way, resulting in no polarization diversity. Table 3.7 shows that there is between 5.0 and 11.5 cm of separation between antenna pairs.

Figure 3.14: **‘stick’ antenna configuration.**

Table 3.7: **Separation (in cm) between antennas for the ‘stick’ configuration**

	A	B	D	E
A		5.0	11.0	11.5
B	5.0		8.5	11.0
D	11.0	8.5		5.0
E	11.5	11.0	5.0	

‘flip’ configuration

The ‘flip’ configuration, shown in Figure 3.15, is similar to the ‘stick’ configuration, but now, two of the four antennas are flipped upside down. While the orientation is no longer the same for all antennas, they still all have the same polarization. The benefit of the flipped antennas is that this increases the antenna separation considerably. Table 3.8 shows the ends of the antennas are now separated by at least 11.0 cm. Note that this entails that the maximum antenna separation featured in the ‘stick’ configuration is now similar to the minimal antenna separation of the ‘flip’ configuration.

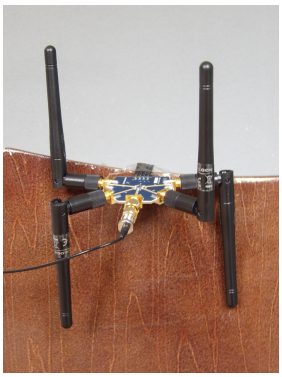


Figure 3.15: **'flip' antenna configuration.**

Table 3.8: **Separation (in cm) between antennas for the 'flip' configuration**

	A	B	D	E
A		17.5	11.0	20.0
B	17.5		19.0	11.0
D	11.0	19.0		17.5
E	20.0	11.0	17.5	

'star' configuration

The 'star configuration', shown in Figure 3.16, folds all antennas outward. This not only increases the antenna separation, but also introduces polarization diversity into the antenna setup. Table 3.9 provides the antenna separation between each antenna pair. This antenna configuration features the largest antenna separations and benefits from polarization diversity. It is therefore expected to perform well in complex multipath environments.

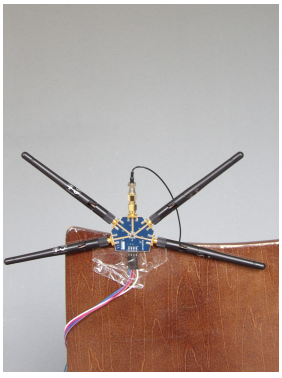


Figure 3.16: **'star' antenna configuration.**

Table 3.9: **Separation (in cm) between antennas for the 'star' configuration**

	A	B	D	E
A		12.0	27.0	26.5
B	12.0		22.0	26.5
D	27.0	22.0		12.0
E	26.5	26.5	12.0	

3.4.2 Antenna Permutations

While each configuration features all 4 available antennas, not every antenna is required to be used. Using fewer antennas could for example save costs, reduce implementation complexity, and increase measurement frequency. Therefore, the performance of each antenna configuration will be tested with 1, 2, or 4 active antennas, which results in the 11 possible permutations shown in Figure 3.17. The results for using a certain number of antennas are averaged. This is to compensate for (un)favorable conditions due to multipath propagation.

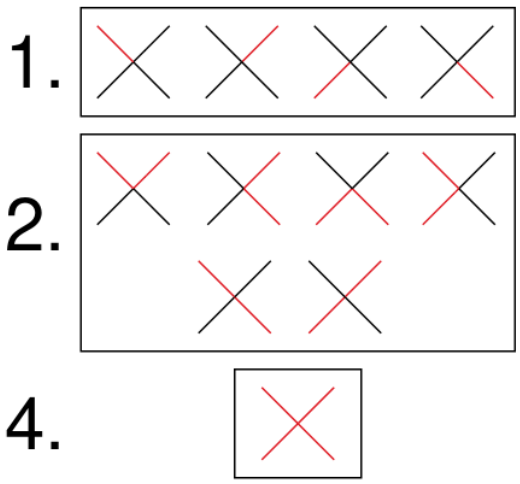


Figure 3.17: **Permutations of antennas using 1, 2, and 4 active antennas.**

3.4.3 Fair Antenna Combining

When four antennas are active the four individual channel sounding measurements are combined into a single measurement. This is unfair to the case when only a single antenna is active. In this case only a single channel sounding measurement is used to report a result. This means that the system is able to use four times as many resources to compute the result when four antennas are active.

To compensate for this unfairness the following is done: when a single antenna is active four channel sounding measurements are made using the available antenna. When two antennas are active two measurements are made on each antenna, and when four antennas are active each antenna performs a single

channel sounding measurement. This way each antenna permutation has access to four channel sounding measurements which can be combined using the combing methods described above. Any performance difference between the configurations must be due antenna diversity.

3.4.4 Environments

The channel sounding experiments have been performed in three distinct Line Of Sight (LOS) environments, which are shown in Figure 3.18. The first environment is an outdoor environment. This environment features minimal multipath and RF interference, and can therefore be used as a baseline of how the channel sounding algorithm performs under ideal conditions. The second environment is a home indoor environment that can be classified by low multipath and RF interference. The final environment is in an office containing metal cabinets and walls that reflect the RF signals leading to a high multipath environment. This environment also features a significant amount of interference in the 2.4GHz band. A BLE scan for advertising devices already reveals more than 100 nearby BLE devices.

Figure 3.18: **Environments: outdoor (left), home (middle), and office (right)**

Chapter 4

Results

This section shows and interprets the results of multi-antenna channel sounding. First, both the spatial and sequential consistency of single-antenna channel sounding are analyzed and will be used as a baseline. Then it is shown how adding a second antenna to the experiment in the office environment setup improves spatial consistency. After that averaged results of experiments using 1, 2, and 4 antennas are shown and discussed. Using these averaged results, the performance of the different antenna configurations and combining methods can be assessed. Finally, the channel sounding results using the optimal antenna configuration and combining method will be compared to the baseline.

This section will mostly present graphs containing averaged results. The complete set of results, from which the averages are calculated, is available in Appendix A.

4.1 Evaluation Metrics

The time-based relay attack mitigation protocol described in chapter 3 requires consistency of channel sounding measurements. In particular, it required consistency in reciprocal measurements and similarity between measurements made from similar distances. Both requirements will be evaluated using the root-mean-square-error and the maximum error. Before these metrics are calculated the outliers (highest and lowest 8% of the measurements) are removed from the data. The metrics are then calculated according to Equation 4.1 and Equation 4.2, where N is the number of measurements in the experiment p_i is the measured distance between initiator and reflector for measurement i, and $\hat{y_i}$ is the expected distance between initiator and reflector for measurement i.

$$\text{Root-mean-squared-error (RMSE)} = \sqrt{\frac{\sum_{i=1}^{N}(p_i - \hat{y_i})^2}{N}} \tag{4.1}$$

$$\text{Maximum error} = \max_{n \in \{1,..,N\}} \mid p_i - \hat{y_i} \mid \tag{4.2}$$

4.1.1 Spatial Consistency

The time between (reciprocal) measurements allow the mobile phone to travel a limited distance between two measurements. This means that it is unlikely that two subsequent measurement are made from the exact same distance. Multipath effects can cause large deviations between measurements. The measurements,

made at similar distances, should yield similar results. Spatial consistency is different from a perfect distance estimation. Therefore, the RMSE and the maximum error of the obtained measurements are not calculated to the line $y(x) = x$. Instead, a new line $\hat{y}(x) = ax + b$ is first fitted to the measurement results, and then the root-mean-square-error and maximum error to this line are used as metric. This means that any offset is compensated for when calculating the metric, allowing for better comparison of consistency between experiments.

4.1.2 Reciprocal Consistency

In order to evaluate the reciprocal consistency of the experiments, two channel sounding measurements are made. Ideally, in one measurement device A is the initiator and in the other measurement device B is the initiator. Unfortunately the software development kit used to program the embedded devices, does not allow for hybrid initiator/reflector roles. Therefore, device A is the initiator in both measurements, and the sequential consistency of two subsequent measurements is used instead.

The two subsequent measurements are compared to each other. In a perfectly consistent scenario, there is no difference in the two distance estimations. Therefore, the root-mean-square error and the maximum error to 0 m ($\hat{y}(x) = 0$) are used as evaluation metrics.

4.2 Baseline Results

Before the multi-antenna channel sounding results can be analyzed, it is important to first analyze the baseline performance. Figure 4.1, shows the single antenna spatial consistency in the three environments. The graphs show that the PBR method performs better than the RTT method. Not only are the PBR distance estimations closer to the reference, they are also more consistent. Both channel sounding methods perform best in the outside environment, followed by the home environment, and perform worst in the office environment. The high error metrics in the office environment can be attributed to multipath propagation. In the graph this can best be seen by the large increase in distance estimation around 2 m.

Figure 4.2 shows the baseline sequential consistency of single antenna channel sounding. The baseline results show good PBR consistency across all three environments. Even in the office environment, the PBR consistency is better than the RTT consistency in the outside environment. The RTT consistency is similar between the outdoor and the home environment, but in the office environment there is a large decrease in sequential consistency of the RTT channel sounding measurements. As can also be seen in the spatial consistency plot, the error in the office environment is again the largest around 2 m. From the graphs it also becomes evident that the sequential error is not dependent on the distance between the initiator and the reflector.

The baseline results show the worst performance in the office environment. This environment thus necessitates the most improvement. Therefore, the following subsection will focus on improvements in the office environment.

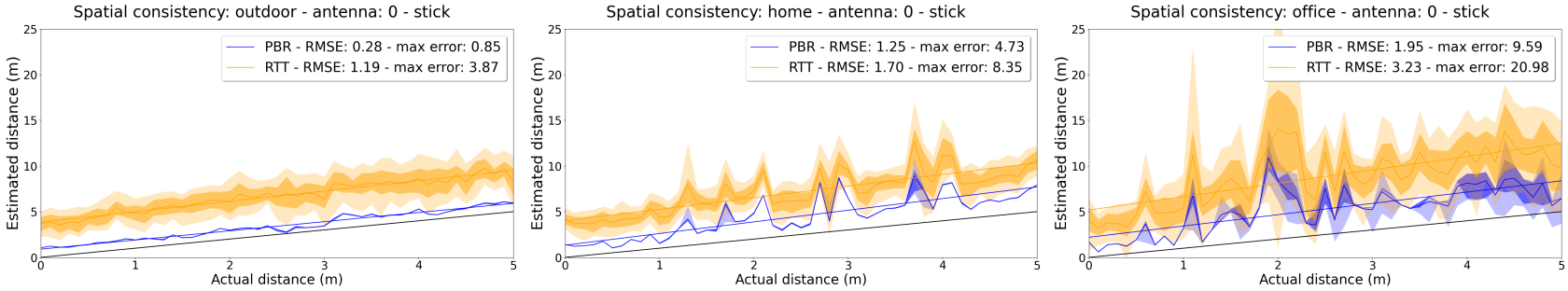


Figure 4.1: **Single antenna channel sounding results for spatial consistency in the outdoor, home, and office environment.**

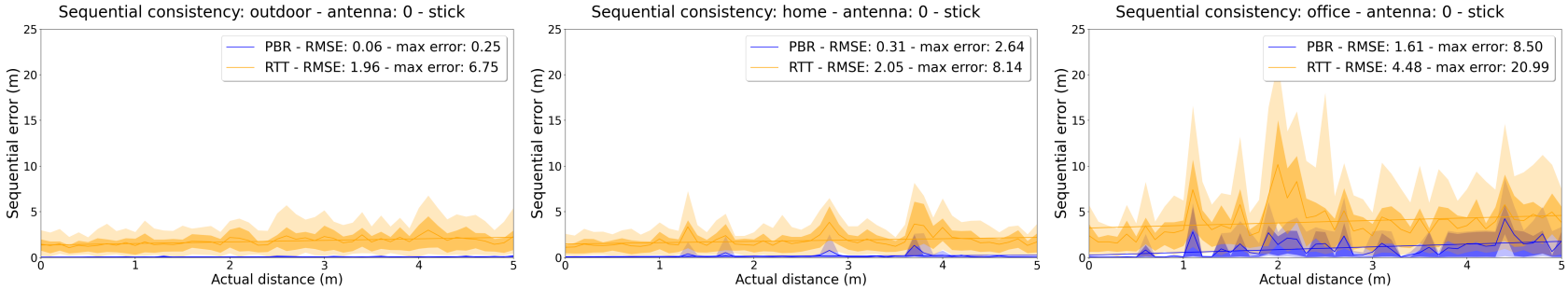


Figure 4.2: **Single antenna channel sounding results for sequential consistency of measurements in the outdoor, home, and office environment.**

4.3 Multi-Antenna Results

In order to overcome the problems associated with multipath propagation, multiple antennas are deployed. Figure 4.3 and Figure 4.4 show the channel sounding measurements from two different antennas during the same experiment in the office environment. Comparing the antennas shows that both experience the effects of multipath propagation, however each antenna is impacted differently and reductions in performance occur at different locations. Figure 4.5 and Table 4.1, show how the measurements from the two antennas can be combined in order to yield more consistent results. By combining the two antennas using the minimal antenna combining method the root-mean-square error (RMSE) compared to the single antenna results of antenna 0 decreased by 0.73 m and 0.50 m, for PBR and RTT respectively. Even antenna 1, which significantly outperforms antenna 0 in both metrics, benefits from the additional antenna; the RMSE for this antenna reduces by 0.06 m for PBR and by 0.24 m for RTT. Unfortunately, the maximum error is increased slightly when compared to the maximum error of antenna 1. This shows that, the antenna combining method is not perfect and that the performance trade-offs must be considered critically.

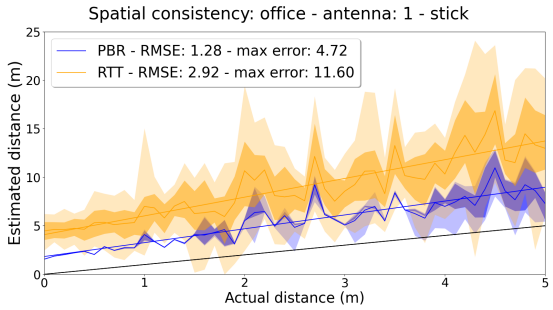


Figure 4.3: **Channel sounding measurement of antenna 1 in the stick configuration and office environment.**

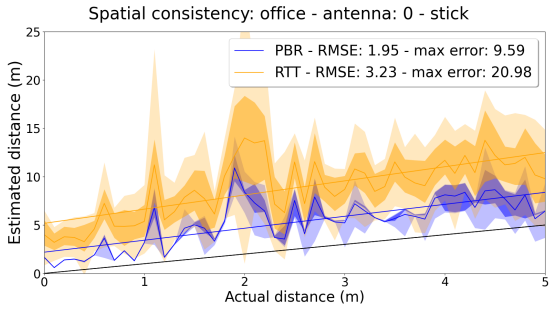


Figure 4.4: **Channel sounding measurement of antenna 0 in the stick configuration and office environment.**

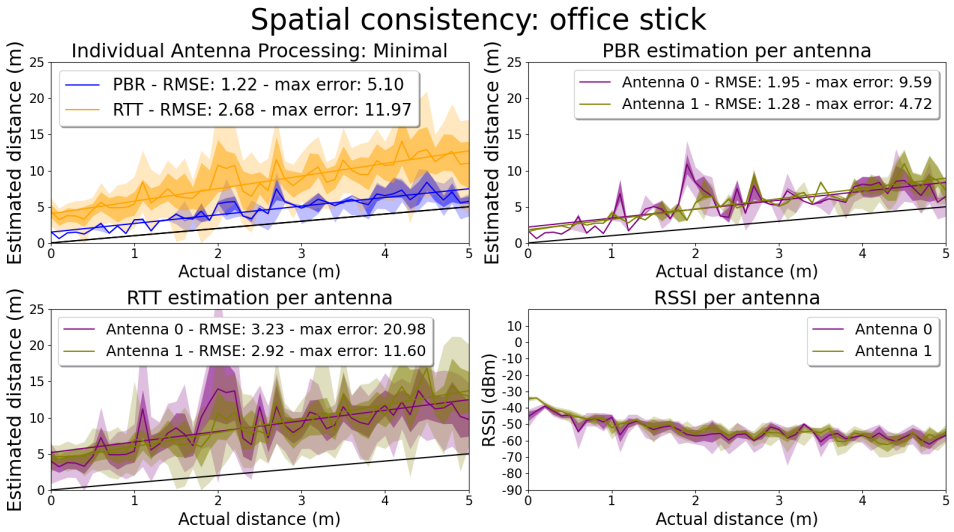


Figure 4.5: **Plots showing the measurements of PBR (top-right), RTT (bottom-left), and RSSI (bottom-right) for the individual antennas. The combined results (top-left) combines the individual antenna measurements from the other graphs using the minimal method to create improved distance estimations.**

Table 4.1: **RMSE results of antenna 0 and 1 individually and after combining using the minimal combining method.**

	PBR	RTT
Antenna 0	1.95	3.23
Antenna 1	1.28	2.92
Combined	1.22	2.68

4.3.1 Spatial Consistency

Figure 4.6 shows that, on average, the single antenna RMSE for PBR and RTT are 1.5 m and 2.5 m. By increasing the number of antennas the RMSE in the office environment is reduced by 0.5 m for both PBR and RTT. These improvements are achieved using the flip antenna configuration and the Mean or proportional RSSI combining method. The Minimal combining method performs equally for PBR, but it performs the worst out of all options for RTT. It can be seen from the plot that the RMSE can be reduced to 1.0m for PBR and 1.9m for RTT when using this setup.

The maximum error metric improves similarly. From Figure 4.7 it can be seen that again the flip method performs best and that the minimal and mean, and proportional RSSI methods perform well for PBR while only the mean and proportional RSSI methods perform well for RTT. The maximum error when using all four antennas is reduced from 6.1 m to 3.8 m for PBR and from 11.6 m to 8.6 m for RTT compared to the average single antenna metric.

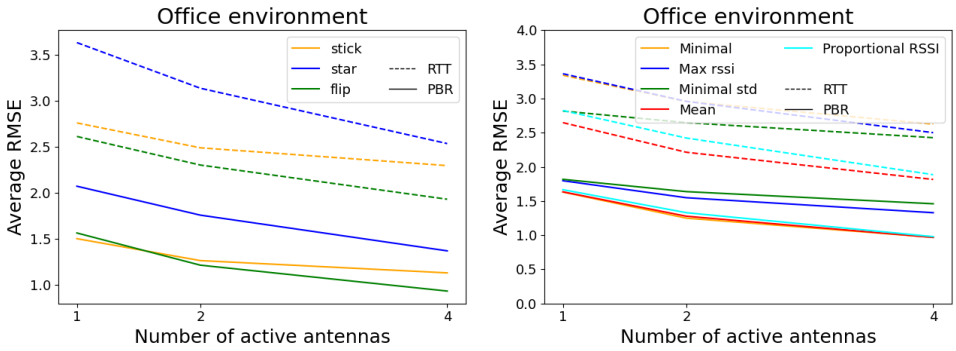


Figure 4.6: **Average RMSE results for antenna configurations (left) and antenna combining methods (right) in the office environment.**

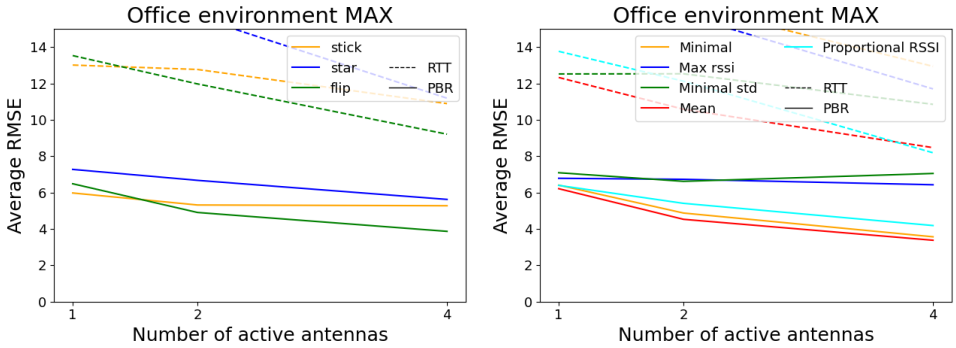


Figure 4.7: **Average maximum error results for antenna configurations (left) and antenna combining methods (right) in the office environment.**

4.3.2 Reciprocal Consistency

Figure 4.8 shows that in the office environment there is little improvement to the reciprocal consistency after adding multiple antennas to the channel sounding procedure. The mean combining method significantly outperforms the other methods. The improvement in RMSE when using four instead of one antenna is only 0.1 m and 0.2 m for PBR and RTT respectively. The same observation is also true for the outdoor and home environment.

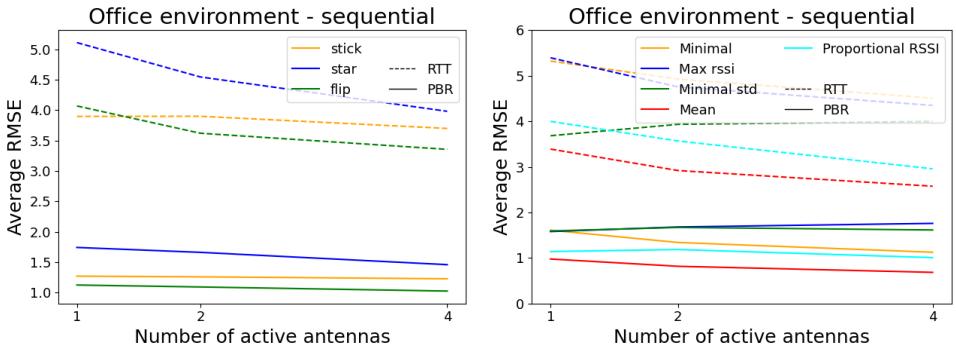


Figure 4.8: **Average RMSE results for antenna configurations (left) and antenna combining methods (right) in the office environment.**

Even tough there is no significant benefit in utilizing multiple antennas, there is a significant improvement over the baseline channel sounding consistency. This means that nearly all performance gain over the baseline is due to the fact that more measurements are used to compute the result. By comparing Figure 4.8 to Figure 4.9 using one antenna it becomes evident that by using more measurements the mean combining method is able to reduce the RMSE by 0.59 m (PBR) and 1.96 m (RTT).

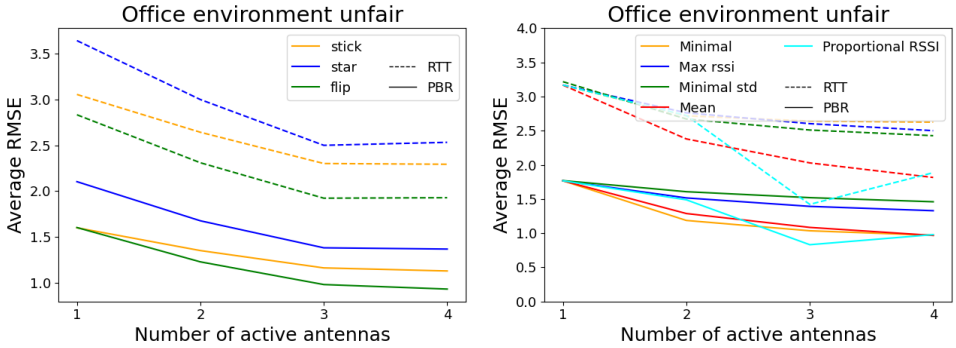


Figure 4.9: **Average RMSE results for antenna configurations (left) and antenna combining methods (right) in the office environment. Note that these graphs show 'unfair' values.**

While the multi-antenna channel sounding results show no improvement for the RMSE of sequential consistency, Figure 4.10 shows that there is a reduction in the maximum error metric. The maximum error using the mean combining method is reduced by 0.71 m (PBR) and 4.09 m (RTT) in the office environment. The other environments also show improvements, but the gains are slightly reduced. The maximum sequential error in the home environment is reduced by 0.39 m (PBR) and 2.15 m (RTT) and the outdoor environment sees reductions of 0.39 m (PBR) and 0.39 m (RTT). Nevertheless, this shows that, especially in the office environment, there still is a performance benefit in deploying multiple

antennas for the sequential consistency of channel sounding measurements.

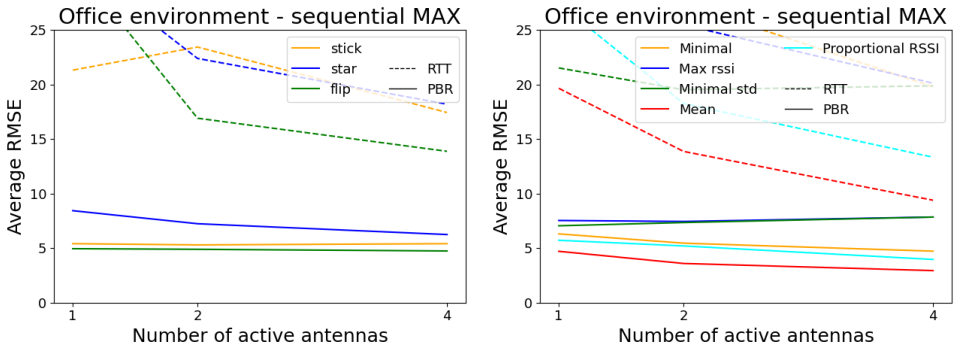


Figure 4.10: **Average maximum error results for antenna configurations (left) and antenna combining methods (right) in the office environment.**

4.4 Optimal Configuration Results

In all environments and for both spatial and sequential consistency it is optimal to use all four antennas. The 'stick' and 'flip' antenna configurations perform similar, but in almost each scenario the 'flip' configuration performs slightly better. The results also showed that the 'star' configuration consistently performed worst. This is despite the fact that this antenna configuration featured the largest antenna separation in addition to polarization diversity. It is possible that the polarization diversity actually had a negative impact. This could be because the antenna at the reflector side no longer had the same polarization.

The optimal combining method depends not only on the environment, but also on used channel sounding method and the evaluation metric. For RTT the mean combining method significantly outperforms the other methods, but for PBR there are sometimes other methods that perform better. The max RSSI method performs well in the outdoor environment, while the minimal method performs well in both indoor environments. The proportional RSSI method generally performs similar as the mean method. Between these two the mean method performs better for sequential consistency, and it also performs better in the office environment, but the proportional RSSI method overtakes it in both the home and outdoor environment.

This section compares the performance of the optimal channel sounding configuration to the baseline. The baseline results are calculated in two ways. The first baseline is calculated from the average single antenna results, and the second baseline is calculated using the fair single antenna results, where the antenna makes four measurements and combines this into the final measurement. This analysis will therefore highlight both the impact of additional data points and antenna diversity on the channel sounding performance.

4.4.1 Spatial Consistency

Figure 4.11 shows the spatial consistency while using the optimal channel sounding configuration in each of the three environments. Visually comparing these graphs to the graphs shown in section 4.2 already shows noticeable improvements to the baseline. This observation is also reflected in Table 4.2. Compared to the baseline this table shows a total reduction in RMSE of 0.35 m (PBR) and 0.81 m (RTT) in the outdoor environment, 0.81 m (PBR) and 0.94 m (RTT) in the home environment, and 1.02 m (PBR) and 1.60 m (RTT) in the office environment. Similar improvements can also be seen for maximum error for both PBR and RTT in all three environments. Table 4.2 shows that most of these gains are between 'Baseline fair' and 'Optimal', meaning that these improvements come from the additional antenna diversity. Finally, the table shows that the performance of the optimal configuration in the office environment approaches the baseline performance in the outdoor environment, showing that the addition of antenna diversity successfully overcomes the problems associated with multipath propagation.

Table 4.2: **Comparison of spatial consistency error metrics. The baseline configuration uses one antenna with one measurement. The baseline fair configuration uses one antenna that makes four measurements. And the optimal configuration uses four antennas that make one measurement each.**

	RMSE (m)		Maximum error (m)	
	PBR	RTT	PBR	RTT
Outdoor				
Baseline	0.44	1.52	2.39	6.20
Baseline fair	0.38	0.94	1.81	4.34
Optimal	0.09	0.71	0.24	2.28
Home				
Baseline	1.20	1.74	5.11	10.15
Baseline fair	1.10	1.37	4.29	6.34
Optimal	0.39	0.80	1.32	2.60
Office				
Baseline	1.77	3.17	7.00	16.01
Baseline fair	1.53	2.46	5.74	11.42
Optimal	0.75	1.57	2.61	6.86

4.4.2 Sequential Consistency

Table 4.3 and Figure 4.12 show that the improvement in sequential consistency of the optimal configuration over the baseline is similar to the improvement in spatial consistency. However, the table reveals that for sequential consistency most of the improvement is between the 'Baseline' and the 'Baseline fair', meaning that the antenna diversity due to additional antennas has no significant impact on the sequential consistency. Nevertheless, there is a performance gain when using the optimal configuration. Especially the maximum error is reduced significantly, meaning that it is still beneficial to deploy multiple antennas in order to improve sequential consistency.

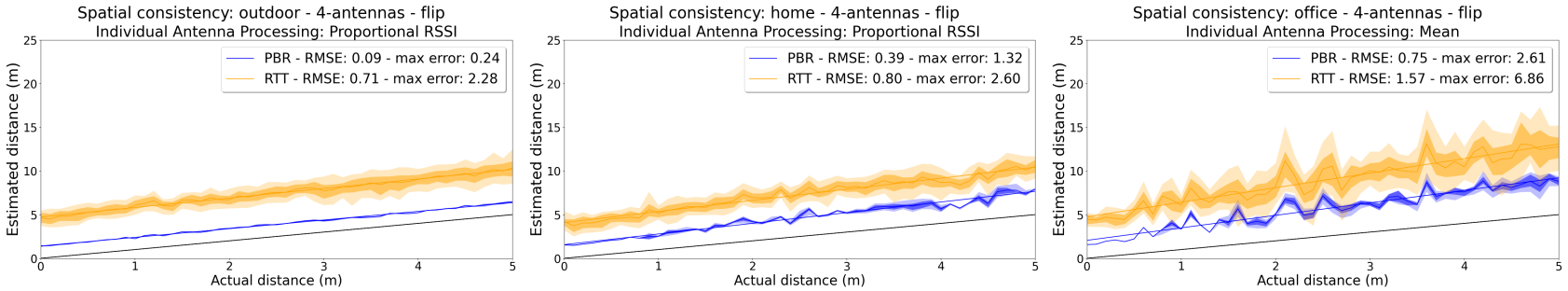


Figure 4.11: **Optimal 4-antenna channel sounding results in the outside, home, and office environment.**

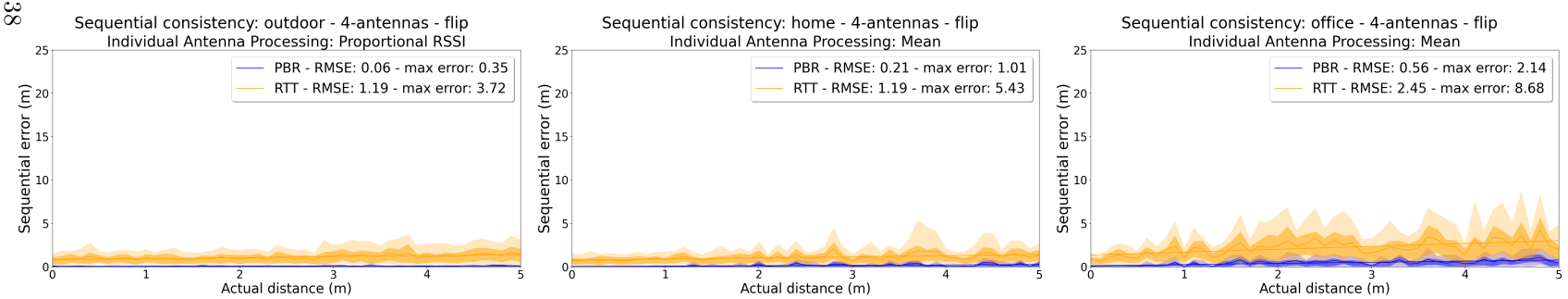


Figure 4.12: **Optimal 4-antenna channel sounding results in the outside, home, and office environment.**

Table 4.3: **Comparison of sequential consistency error metrics. The baseline configuration uses one antenna with one measurement. The baseline fair configuration uses one antenna that makes four measurements. And the optimal configuration uses four antennas that make one measurement each.**

	RMSE (m)		Maximum error (m)	
	PBR	RTT	PBR	RTT
Outdoor				
Baseline	0.24	2.50	1.50	10.86
Baseline fair	0.17	1.39	1.27	6.41
Optimal	0.09	1.19	0.35	3.72
Home				
Baseline	0.43	2.45	3.08	13.85
Baseline fair	0.24	1.35	1.57	7.28
Optimal	0.21	1.19	1.01	5.43
Office				
Baseline	1.40	4.82	6.85	22.23
Baseline fair	0.77	2.75	3.69	13.63
Optimal	0.56	2.45	2.14	8.68

4.5 Protocol Re-evaluation

Again, as in chapter 3, Δ has been selected as the largest RMSE from the office environment ($\Delta = 2.45$ m). The new evaluation of the proposed protocol, shown in Table 4.4, shows a significant reduction in the available attack surface for the attacker. Both version 3 and 4 now outperform version 4 using the baseline channel sounding. Even version 3 of the protocol now has a similar attack surface as version 4 had with the baseline performance. When the attacker now deploys its relay attack, there is only an area of 24 m^2 where the mobile phone is vulnerable.

While a relay attack is still possible, the likelihood of succeeding in such an attack is severely mitigated. The attacker must now purposefully position their attacking devices in the correct area.

Table 4.4: **Protocol evaluation using optimal channel sounding configuration.**

Version	Description	Attack area (m^2)
0	RSSI based distance bounding	907.92 [1]
1	RTT based distance bounding	174.37
2	Two-way RTT based distance bounding	92.36
3	Two-way RTT based distance bounding (1 beacon)	48.02 [2]
4	Two-way RTT based distance bounding (2+ beacons)	24.01 [2]

[1] BLE maximum range is calculated to be 17 m in an office using the NIST PAP02-Task 6 Model [15] [3].

[2] The area where the two rings intersect have been approximated as two squares with sides of length Δ.

Chapter 5

Conclusions

This thesis investigated BLE relay attacks. To mitigate the risks of these attacks a design for a time based distance bounding protocol was proposed. This protocol relies heavily on Bluetooth 6.0 channel sounding distance measurements. In order for this protocol to effectively mitigate relay attacks the channel sounding measurements must be consistent. Unfortunately, single-antenna channel sounding measurements showed poor spatial and sequential consistency in a complex multipath environment. To improve the consistency of these measurements, it was researched which antenna configuration (using up to 4 antennas) and antenna combining method provided the best spatial and sequential consistency in channel sounding measurements.

The best antenna configuration using four antennas across all experiments is the 'flip' configuration. The best antenna combining method depends on the channel sounding method and the environment. PBR measurements can best be combined using the proportional RSSI method in the outside environment and using the proportional, minimal or mean method in indoor environments. RTT measurements are almost always best combined using the mean combining method. Using this optimal channel sounding configuration allowed the RMSE of spatial consistency to be reduced from 1.77 m (PBR) and 3.17 m (RTT) to 0.75 m and 1.57 m respectively. The RMSE for sequential consistency showed similar improvements; this metric could be reduced from 1.40 m (PBR) and 4.82 m (RTT) to 0.56 m and 2.45 m respectively. Crucially, these improvements allow the channel sounding performance using the optimal configuration in the high multipath office environment to approach the baseline performance in a low multipath outdoor environment. Showing that the added antenna diversity effectively reduces the impact of multipath propagation on the channel sounding measurements.

The channel sounding improvements reduce the attack surface for the attacker during a relay attack. This decreases the likelihood of such an attack succeeding, effectively mitigating BLE relay attacks.

5.1 Future Work

While Bluetooth 6.0 channel sounding is a promising technology for indoor localization and relay attack mitigation, the technique requires a considerable

amount of further research before it can effectively be deployed in the real world. The three main avenues for future work described below focus on the evaluation of relay attack mitigation, further multi-antenna channel sounding improvements, and real world implementation and evaluation.

Relay attack mitigation

It needs to be researched to what extent the proposed protocol in combination with the multi-antenna channel sounding setup mitigates the risk of a BLE relay attacks. From this evaluation, it can be determined if the current channel sounding performance sufficiently mitigates relay attacks or if further improvements are required. By performing this evaluation it will also be possible to highlight the specific metrics that need to be improved. This will allow for more focussed research into relay attack mitigation using Bluetooth channel sounding.

Multi-antenna channel sounding improvements

The research presented in this paper can be extended. Future research can focus on different antenna configurations, new and more advanced combining methods, and more data can be gathered in different environments. In addition to purely continuing the research presented in this paper, it is also possible to research other methods to improve channel sounding performance. For example, single antenna channel sounding improvements, as discussed in the background, can be combined with the multi-antenna approach presented in this thesis. Another improvement that can be researched is the use of Summed Antenna Processing instead of Individual Antenna Processing. Finally, channel sounding measurements can be fused with existing Bluetooth localization techniques, such as RSSI and angle of arrival localization. The combination of these localization methods can yield better and/or more consistent localization performance.

Real world implementation and evaluation

Hardware costs need to be reduced, and real world performance needs to be evaluated. In order to reduce the cost of hardware it is likely required to use PCB antennas instead of external antennas. Therefore, the optimal layout of PCB antennas for channel sounding needs to be researched. This new configuration must then be evaluated in real world scenarios. Real world evaluation requires smartphones that are capable of channel sounding and move freely throughout a space.

Other real world considerations are the frequency of channel sounding measurements, and the energy consumption. This research proposes to leverage channel reciprocity by using two-way ranging in order to mitigate relay attacks. Using the current 6.0 specification, the signal needs to travel four times between the initiator and reflector. This could be reduced to three times, and will not only increase the measurement frequency and reduce energy consumption, but could also improve the measured result.

5.2 Limitations

The Bluetooth 6.0 core specification was only introduced in September 2024, meaning that it is still a new technology. This severely limited the research performed in this work in the following areas.

First, while nearly every available smartphone features Bluetooth, there is no smartphone available that features support for Bluetooth 6.0. Therefore, it was not possible to effectively evaluate the real world performance of channel sounding in the context of access control and Phone as a Key.

In addition to this the development boards used for this research are also brand new (this research used 'preview' development kits, which were not publicly available). This meant that while the hardware was complete and functioning, it most likely will not have the same performance as the finished product. The same was also true for the experimental software support of channel sounding; the provided samples worked, but are still updated with new commits monthly. Unfortunately this also meant that many configuration options were not yet supported. It was for example not possible to make RTT the main channel sounding mode, or to dynamically switch between initiator/reflector role. Another notable limitation was the absence of the IFFT calculation method for PBR. Support for the IFFT method was only added after all data for this thesis was gathered. According to [6] the IFFT method is able to achieve better performance than the phase slope method used in this thesis.

Finally, the novelty of Bluetooth 6.0 also meant that there was limited prior work. The available previous works were mostly concerned with improving the performance of single antenna channel sounding, and not with improving measurements using antenna diversity or the implications of channel sounding on the security against relay attacks. Therefore, it is unknown if the method and approach used in this research is optimal.

Bibliography

[1] Stefan Brands and David Chaum. Distance-bounding protocols. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 344–359. Springer, 1993.

[2] Marco Cominelli, Paul Patras, and Francesco Gringoli. Dead on arrival: An empirical study of the bluetooth 5.1 positioning system. In *Proceedings of the 13th international workshop on wireless network testbeds, experimental evaluation & characterization*, pages 13–20, 2019.

[3] David E Cypher and Nada T Golmie. Nist priority action plan 2, guidelines for assessing wireless standards for smart grid applications rev. 1. Technical report, NIST Interagency/Internal Report (NISTIR) 7761, 2011.

[4] Ramsey Faragher and Robert Harle. Location fingerprinting with bluetooth low energy beacons. *IEEE journal on Selected Areas in Communications*, 33(11):2418–2428, 2015.

[5] Supatana Hengyotmark, Teerayut Horanont, Kamol Kaemarungsi, and Kazuhiko Fukawa. Pseudo-ranging based on round-trip time of bluetooth low energy beacons. In *Recent Advances in Information and Communication Technology 2017: Proceedings of the 13th International Conference on Computing and Information Technology (IC2IT)*, pages 202–211. Springer, 2018.

[6] Maciej Nikodem, Grzegorz Trajnowicz, Gabriele Salvatore De Blasio, and Francisco Alexis Quesada-Arencibia. Experimental evaluation of multi-carrier phase difference localization in bluetooth low energy. *IEEE Sensors Journal*, 2024.

[7] Nordic Semiconductor. nRF54L15 — nRF54L10 — nRF54L05 Preliminary Datasheet. `docs.nordicsemi.com/bundle/ps_nrf54L15/page/keyfeatures_html5.html`, 2025. Last Updated Jun 03, 2025.

[8] NXP Semiconductors. *Fact Sheet - MCX W71x and W72x connected microcontrollers.*

[9] NXP Semiconductors. MCX W72x Secure and Ultra-Low-Power MCUs for Matter, Thread, Zigbee and Bluetooth LE. `https://www.nxp.com/products/MCX-W72X`, 2025. Last acessed: Jun. 20, 2025.

[10] Hildur Ólafsdóttir, Aanjhan Ranganathan, and Srdjan Capkun. On the security of carrier phase-based ranging. In *International Conference on*

Cryptographic Hardware and Embedded Systems, pages 490–509. Springer, 2017.

[11] Kasper Bonne Rasmussen and Srdjan Capkun. Implications of radio fingerprinting on the security of sensor networks. In *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops-SecureComm 2007*, pages 331–340. IEEE, 2007.

[12] Avik Santra, Igor Kravets, Nazarii Kotliar, and Ashutosh Pandey. Enhancing bluetooth channel sounding performance in complex indoor environments. *IEEE Sensors Letters*, 2024.

[13] Shuang Shang and Lixing Wang. Overview of wifi fingerprinting-based indoor positioning. *Iet Communications*, 16(7):725–733, 2022.

[14] Shamman Noor Shoudha, Jayson P Van Marter, Sherief Helwa, Anand G Dabak, Murat Torlak, and Naofal Al-Dhahir. Reduced-complexity decimeter-level bluetooth ranging in multipath environments. *IEEE Access*, 10:38335–38350, 2022.

[15] Bluetooth SIG. Understanding bluetooth® range. `https://www.bluetooth.com/learn-about-bluetooth/key-attributes/range/`.

[16] Silicon Labs. *EFR32MG24 Wireless SoC Family Data Sheet*, October 2024. Rev. 1.2.

[17] Silicon Labs. EFR32xG24 Channel Sounding Dev Kit. `https://www.silabs.com/development-tools/wireless/efr32xg24-channel-sounding-dev-kit?tab=overview`, 2024.

[18] Silicon Labs. xG24-RB4198A - EFR32xG24 Wireless Channel Sounding Radio Board. `https://www.silabs.com/development-tools/wireless/xg24-rb4198a-efr32xg24-channel-sounding-radio-board?tab=overview`, 2024.

[19] Skyworks Solutions, Inc. *SKY13575-639LF: Dual-Band Matched SP4T Wi-Fi Switch*, July 2018.

[20] Paul Staat, Kai Jansen, Christian Zenger, Harald Elders-Boll, and Christof Paar. Analog physical-layer relay attacks with application to bluetooth and phase-based ranging. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 60–72, 2022.

[21] Paul Staat, Kai Jansen, Christian Zenger, and Christof Paar. Securing phone as a key against relay attacks. *18th escar Europe*, pages 48–58, 2020.

[22] D Suresh, Prashant V Joshi, Parag Parandkar, Ameya Gambhir, and KM Sudharshan. Ble channel sounding: novel method for enhanced ranging accuracy in vehicle access. *IEEE Access*, 2025.

[23] Jeremy Symon. *Detecting relay attacks against Bluetooth communications on Android*. PhD thesis, The University of Waikato, 2018.

[24] Zaid Bin Tariq, Jayson P Van Marter, Anand G Dabak, Naofal Al-Dhahir, and Murat Torlak. A data-driven signal subspace approach for indoor bluetooth ranging. *IEEE Journal of Indoor and Seamless Positioning and Navigation*, 2024.

[25] Texas Instruments. CC2755R10 - SimpleLink™ 32-bit Arm® Cortex®-M33 Bluetooth® Low Energy wireless MCU with 1MB flash. `https://www.ti.com/product/CC2755R10`, 2024. Last acessed: Jun. 20, 2025.

[26] Texas Instruments. *CC2755x10 SimpleLink Family of 2.4GHz High Performance Wireless MCUs*, October 2024. Rev. B.

[27] Jayson P Van Marter, Anand G Dabak, Naofal Al-Dhahir, and Murat Torlak. Support vector regression for bluetooth ranging in multipath environments. *IEEE Internet of Things Journal*, 10(13):11533–11546, 2023.

[28] Maximilian Von Tschirschnitz, Ludwig Peuckert, Fabian Franzen, and Jens Grossklags. Method confusion attack on bluetooth pairing. In *2021 IEEE symposium on security and privacy (SP)*, pages 1332–1347. IEEE, 2021.

[29] Martin Wooley. Bluetooth® channel sounding: A technical overview. `https://www.bluetooth.com/channel-sounding-tech-overview/`, Jul 2024.

[30] Wondimu K Zegeye, Seifemichael B Amsalu, Yacob Astatke, and Farzad Moazzami. Wifi rss fingerprinting indoor localization for mobile devices. In *2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pages 1–6. IEEE, 2016.

[31] Yuan Zhuang, Chongyang Zhang, Jianzhu Huai, You Li, Liang Chen, and Ruizhi Chen. Bluetooth localization technology: Principles, applications, and future trends. *IEEE Internet of Things Journal*, 9(23):23506–23524, 2022.

Appendix A

Channel Sounding Plots

A.1 Single-Antenna Channel Sounding Plots - Spatial Consistency

Outdoor Environment

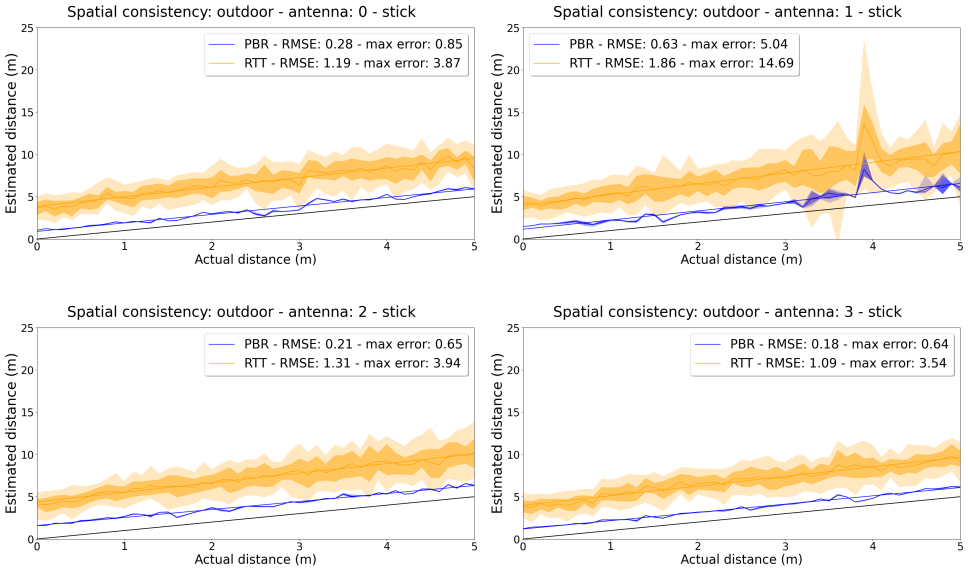


Figure A.1: **Plots of the 4 individual antennas in the outdoor environment using the stick configuration.**

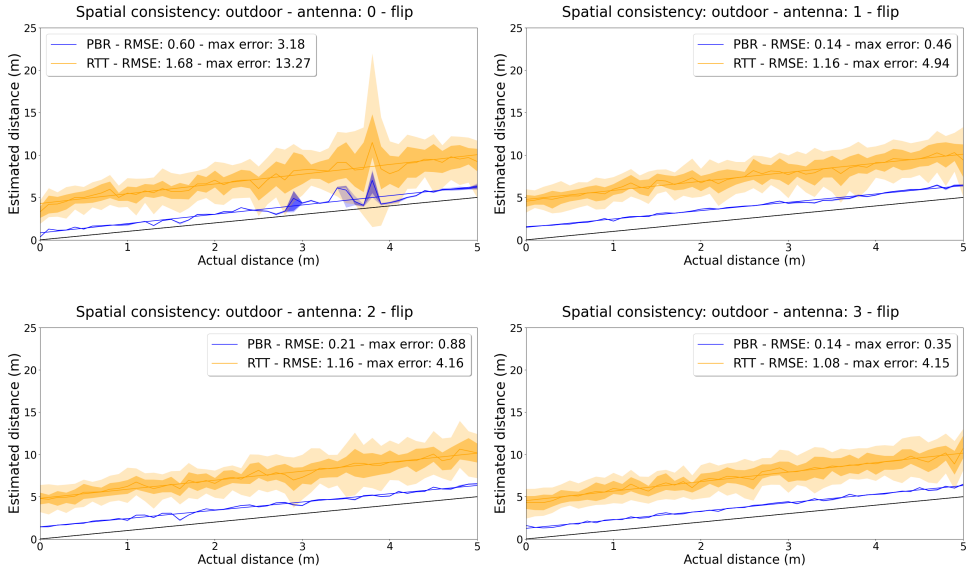


Figure A.2: **Plots of the 4 individual antennas in the outdoor environment using the flip configuration.**

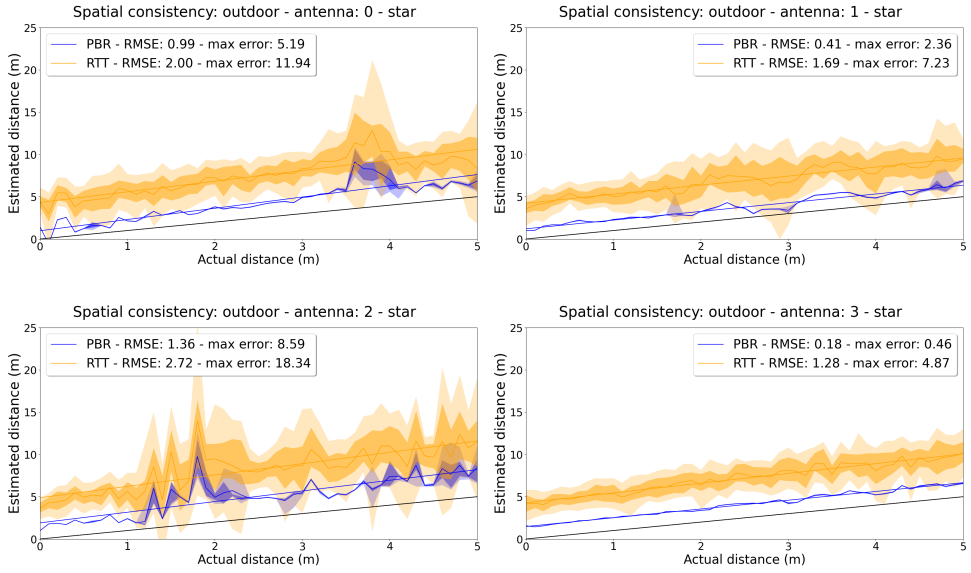


Figure A.3: **Plots of the 4 individual antennas in the outdoor environment using the star configuration.**

Home Environment

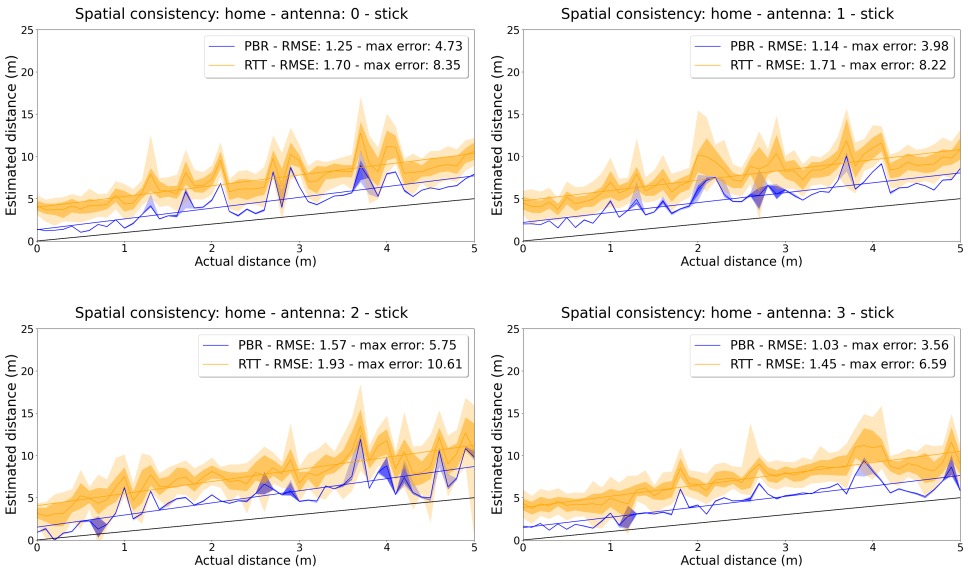


Figure A.4: **Plots of the 4 individual antennas in the home environment using the stick configuration.**

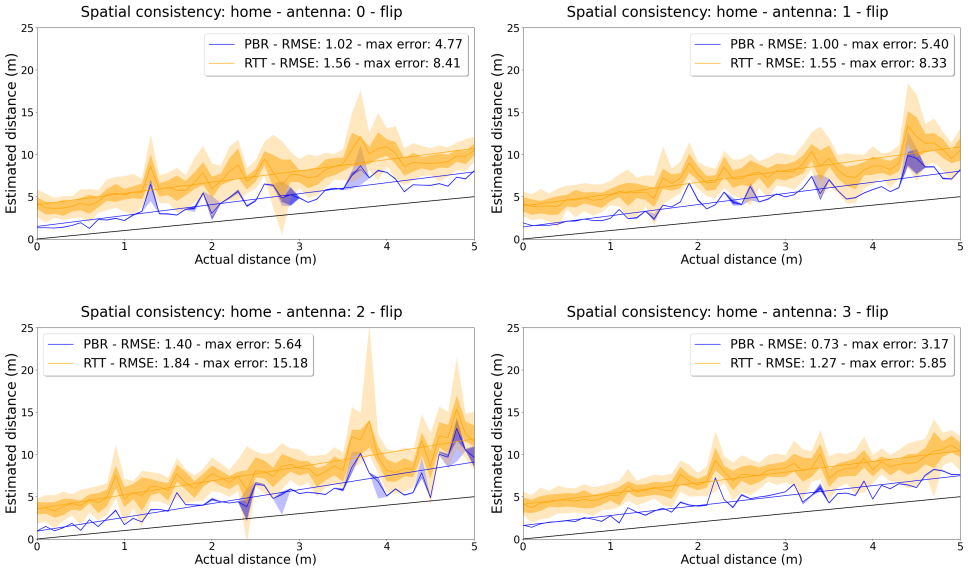


Figure A.5: **Plots of the 4 individual antennas in the home environment using the flip configuration.**

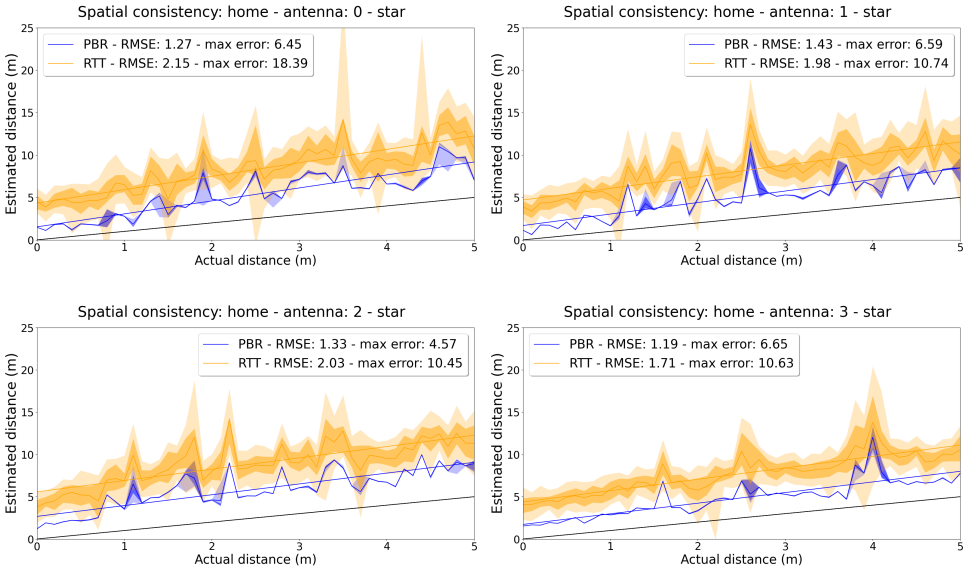


Figure A.6: **Plots of the 4 individual antennas in the home environment using the star configuration.**

Office Environment

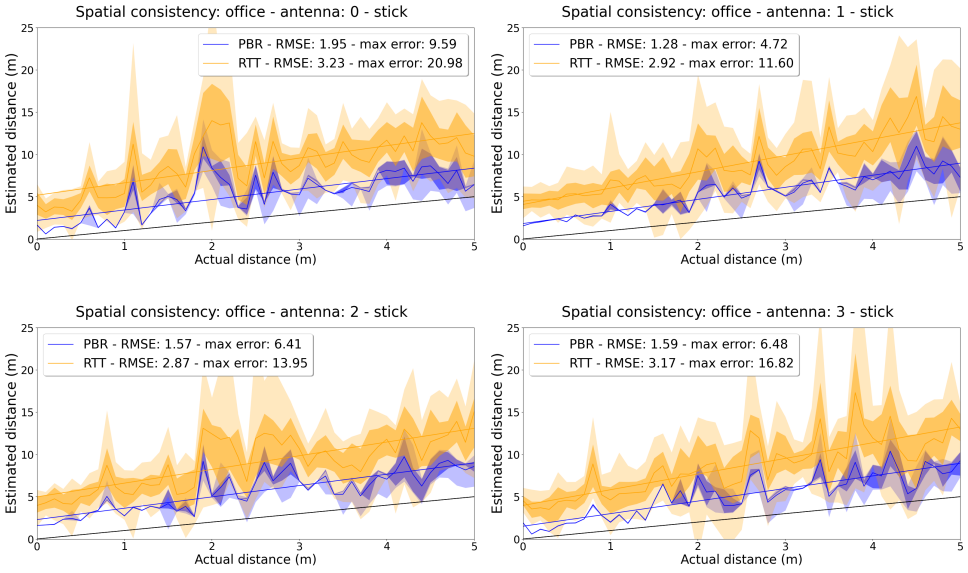


Figure A.7: **Plots of the 4 individual antennas in the office environment using the stick configuration.**

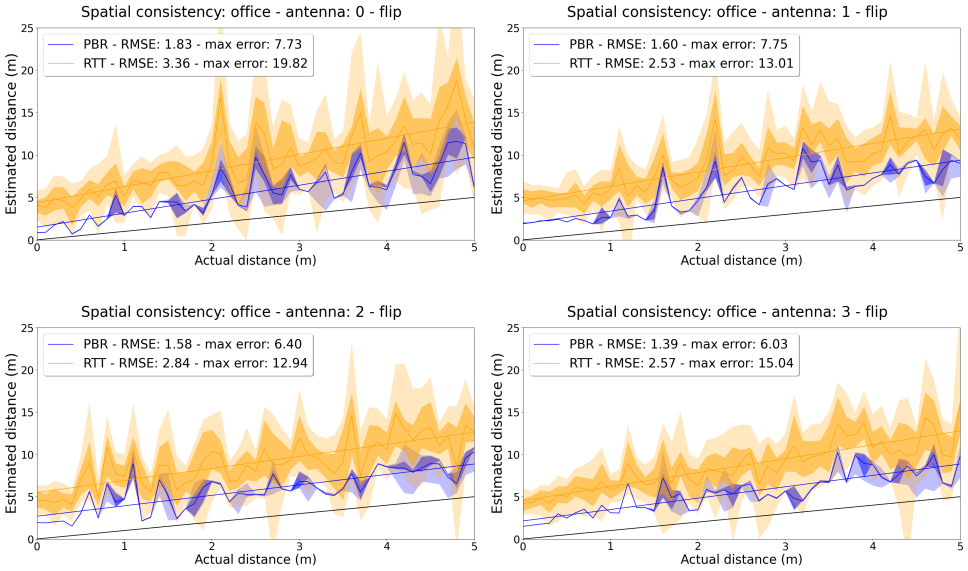


Figure A.8: **Plots of the 4 individual antennas in the office environment using the flip configuration.**

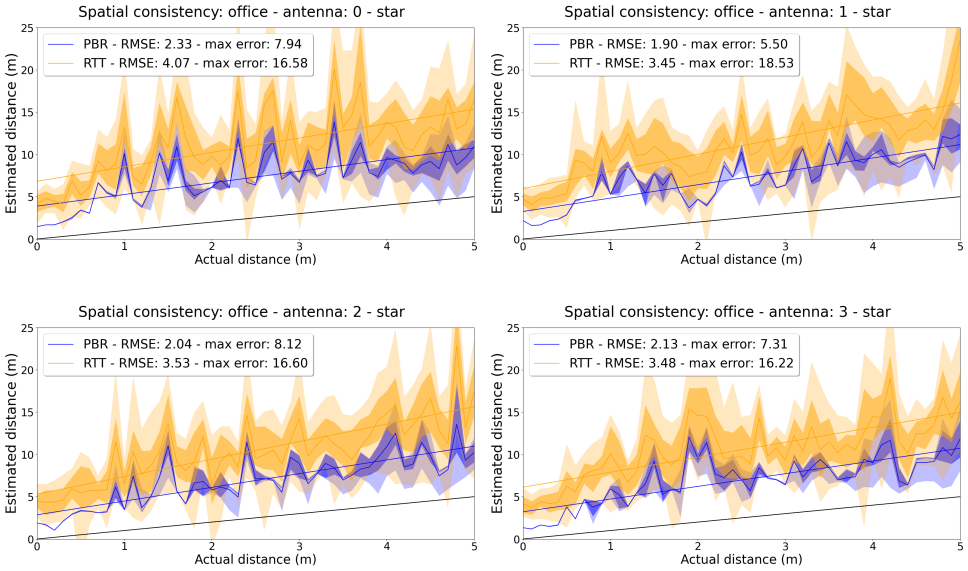


Figure A.9: **Plots of the 4 individual antennas in the office environment using the star configuration.**

A.2 Multi-Antenna Channel Sounding Plots - Spatial Consistency

Outdoor Environment

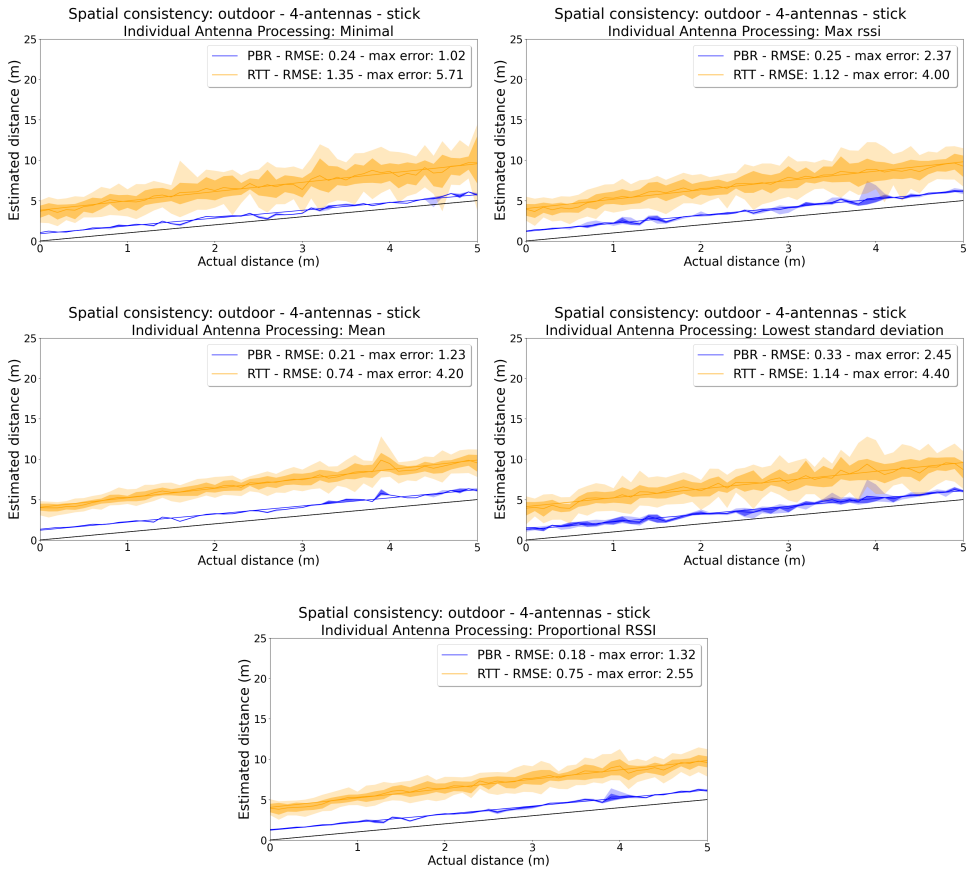


Figure A.10: **Plots of the 5 antenna combining methods in the outdoor environment using the stick configuration.**

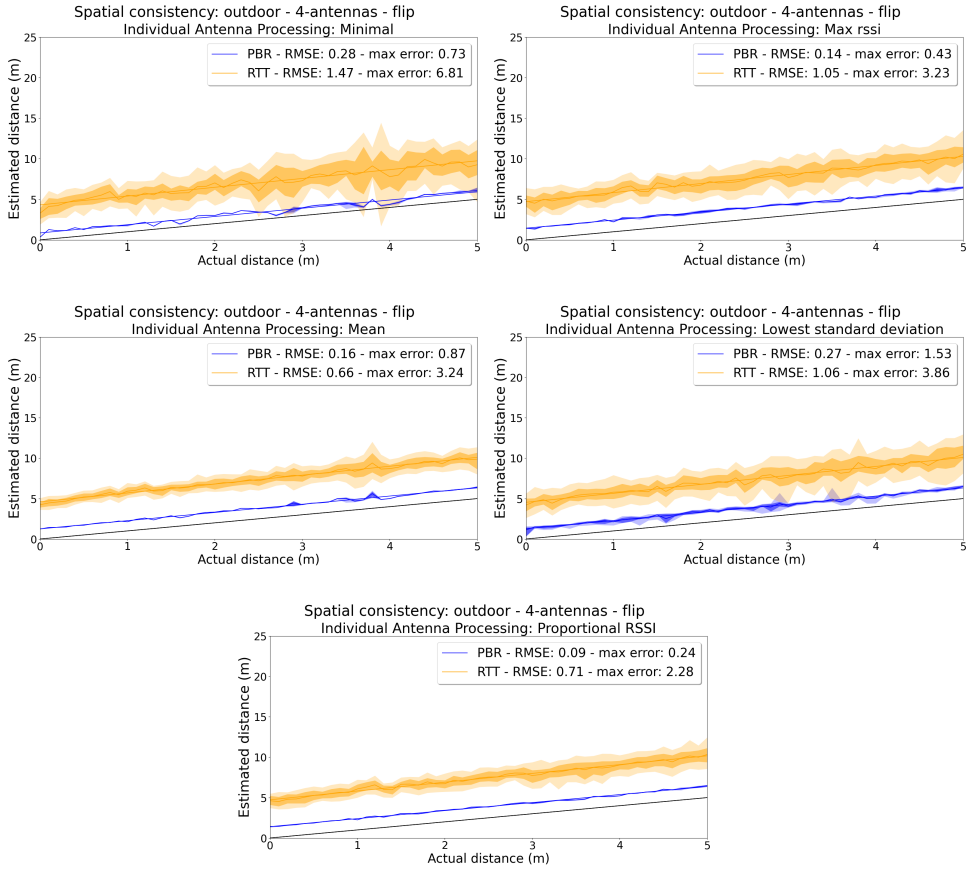


Figure A.11: **Plots of the 5 antenna combining methods in the outdoor environment using the flip configuration.**

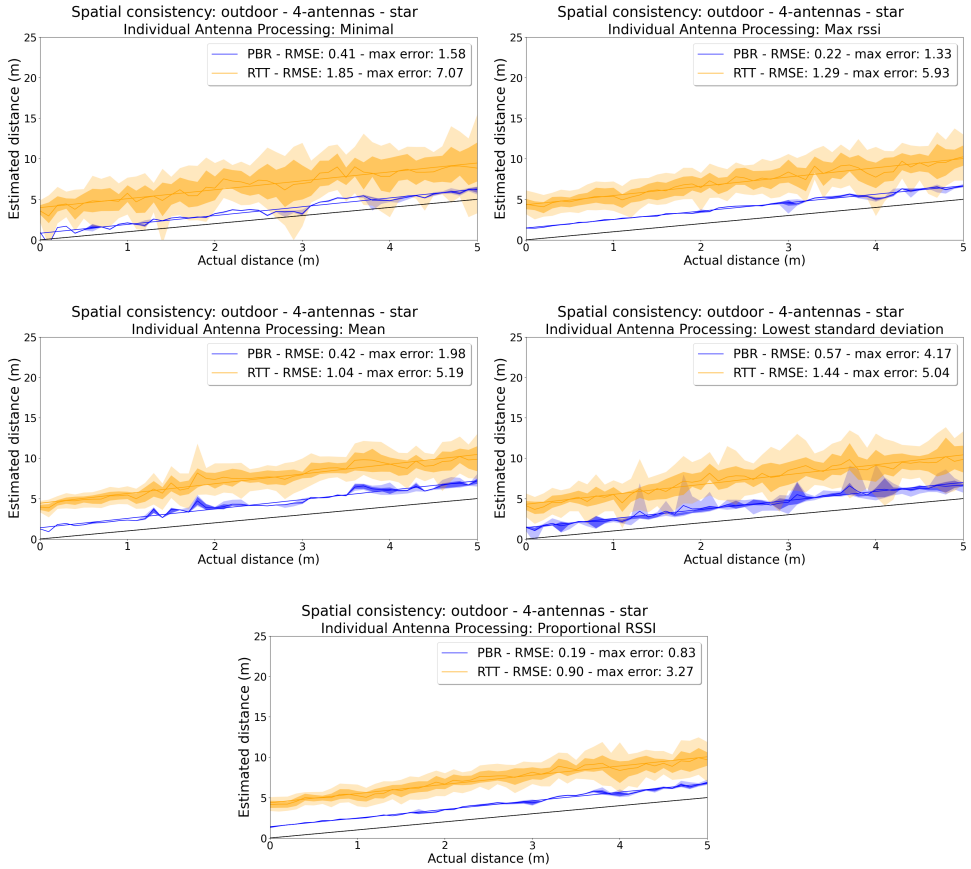


Figure A.12: **Plots of the 5 antenna combining methods in the outdoor environment using the star configuration.**

Home Environment

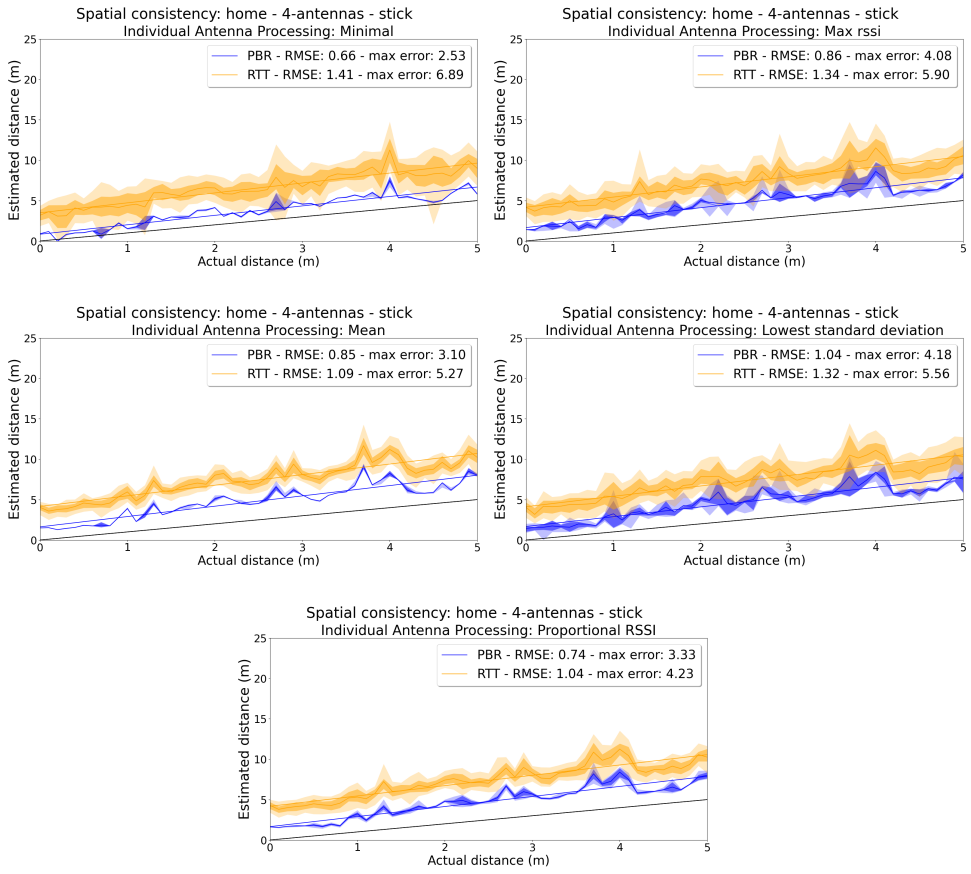


Figure A.13: **Plots of the 5 antenna combining methods in the home environment using the stick configuration.**

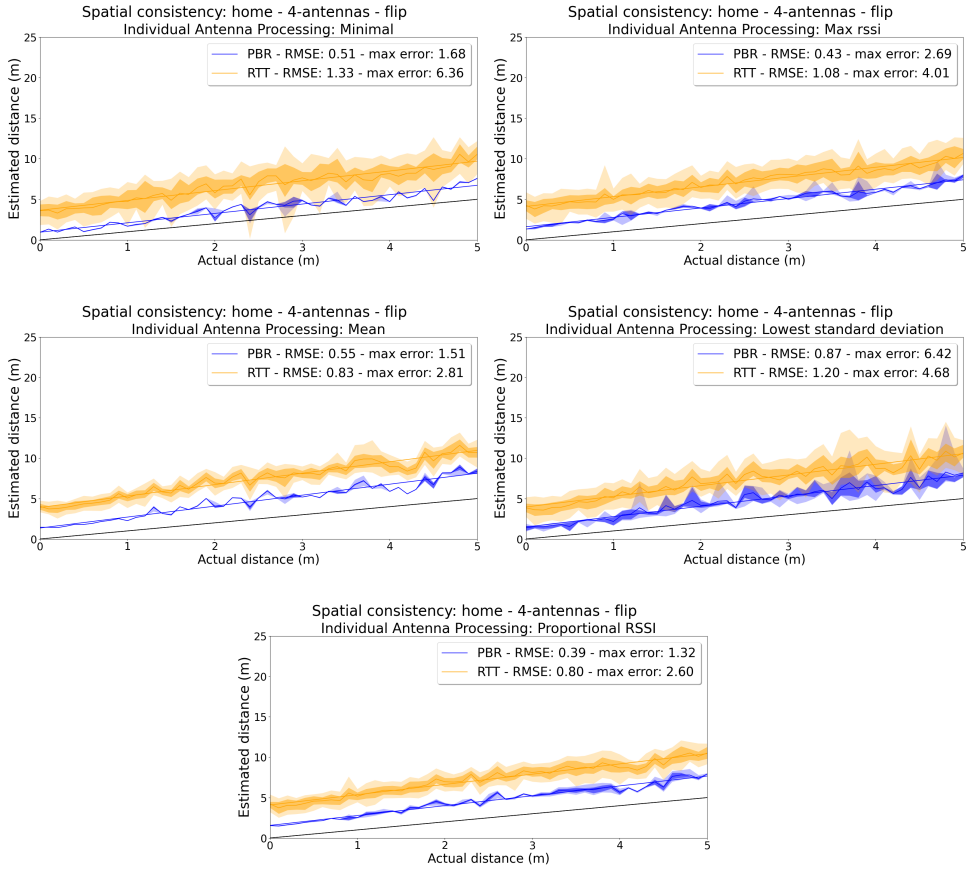


Figure A.14: **Plots of the 5 antenna combining methods in the home environment using the flip configuration.**

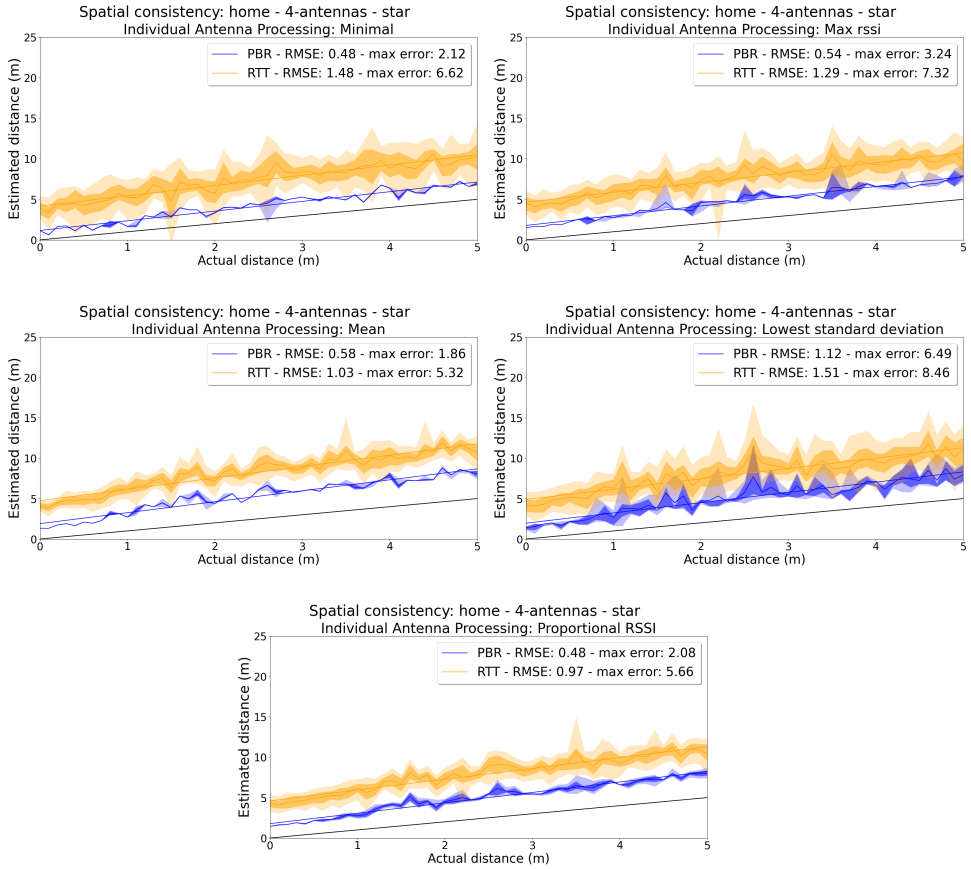


Figure A.15: **Plots of the 5 antenna combining methods in the home environment using the star configuration.**

Office Environment

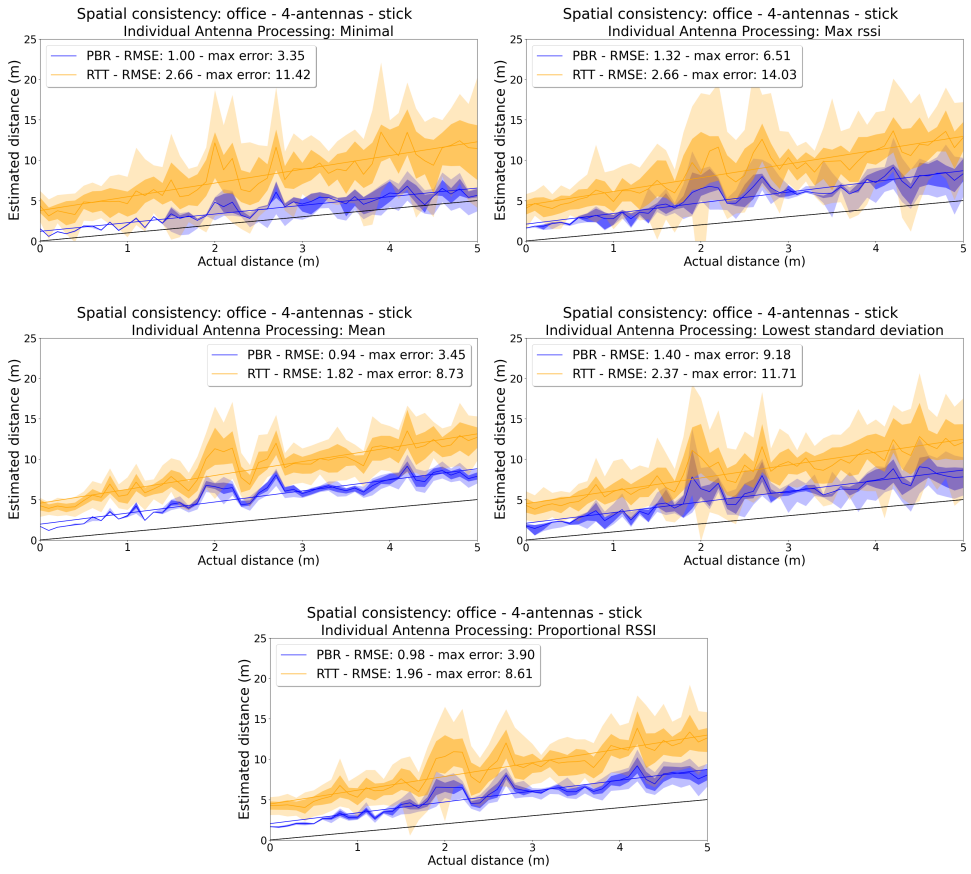


Figure A.16: **Plots of the 5 antenna combining methods in the office environment using the stick configuration.**

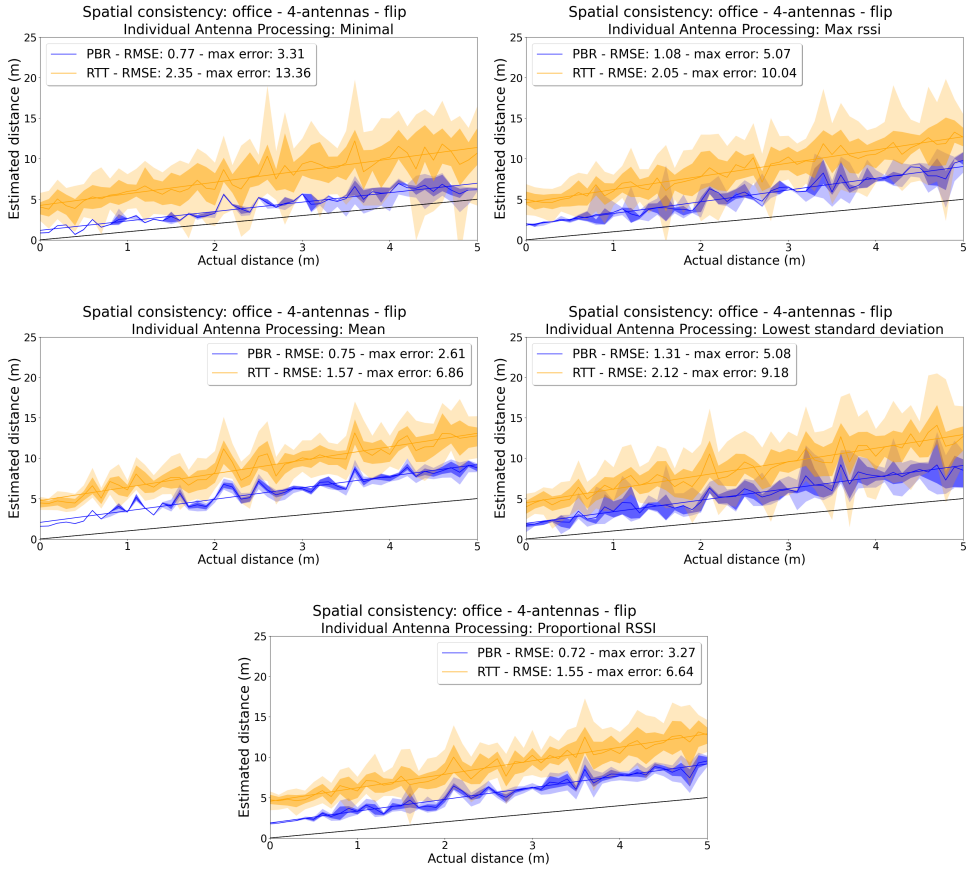


Figure A.17: **Plots of the 5 antenna combining methods in the office environment using the flip configuration.**

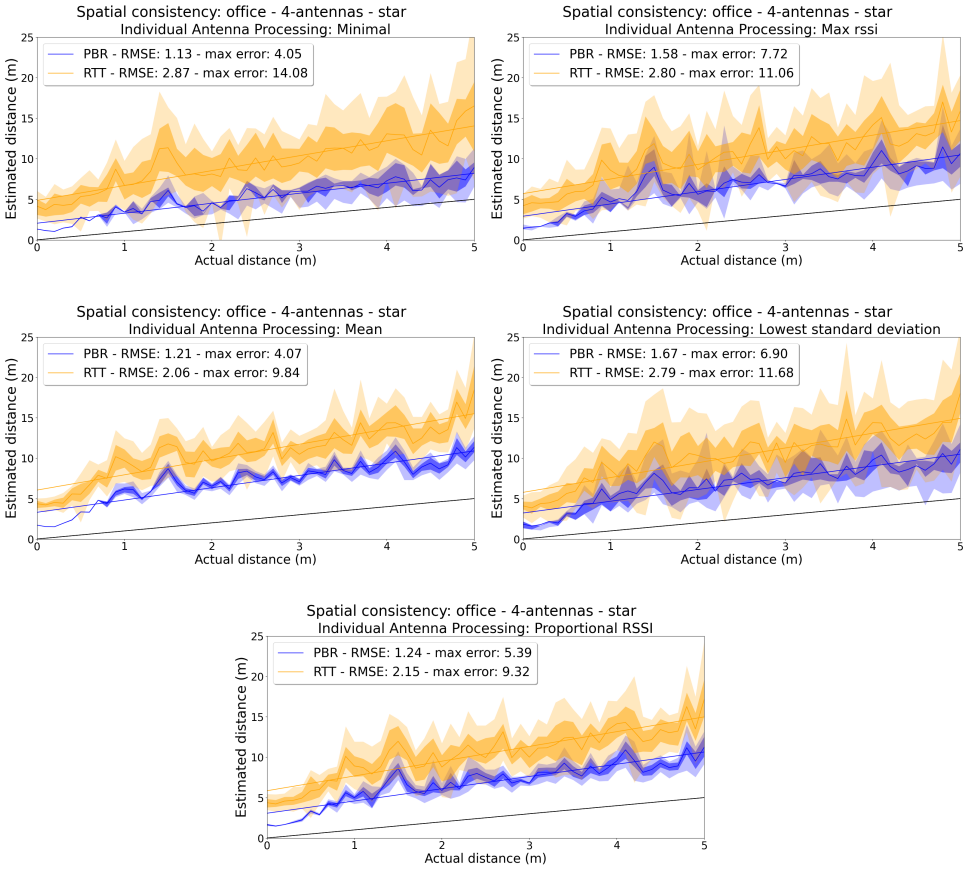


Figure A.18: **Plots of the 5 antenna combining methods in the office environment using the star configuration.**

A.3 Single-Antenna Channel Sounding Plots - Sequential Consistency

Outdoor Environment

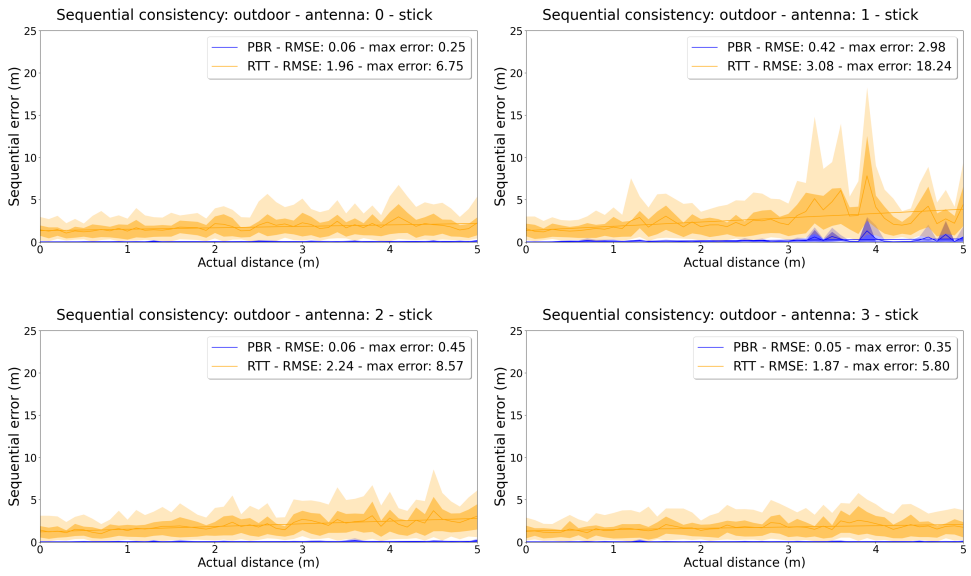


Figure A.19: **Plots of the 4 individual antennas in the outdoor environment using the stick configuration.**

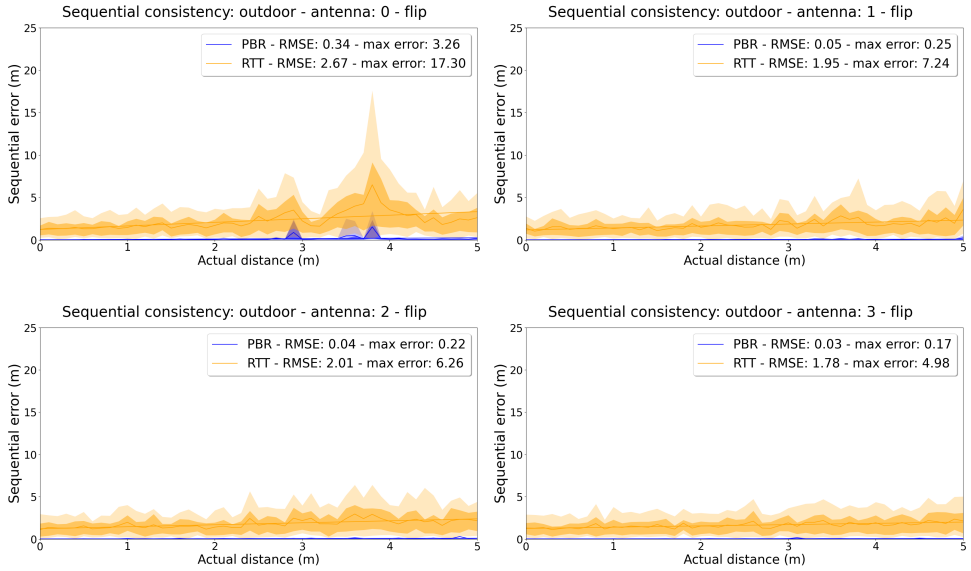


Figure A.20: **Plots of the 4 individual antennas in the outdoor environment using the flip configuration.**

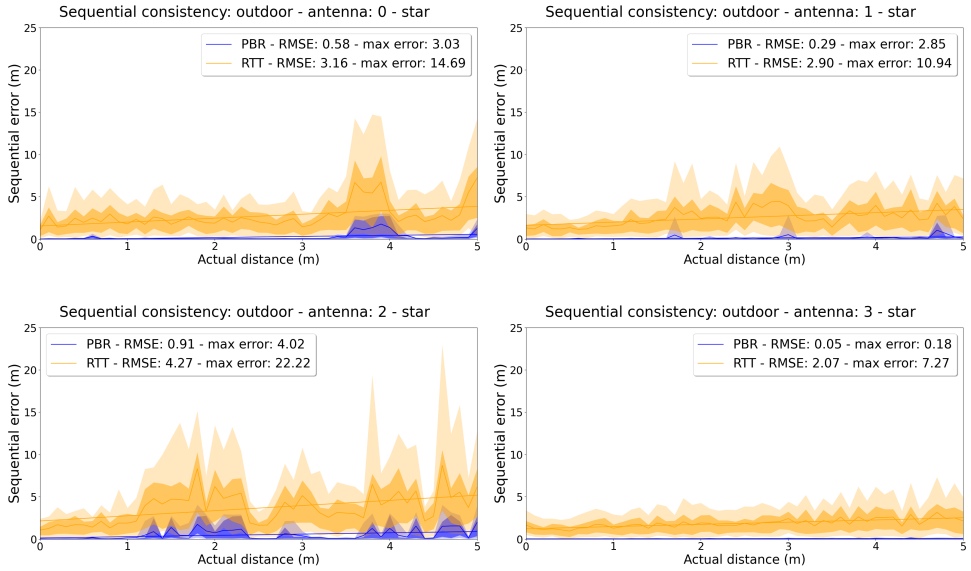


Figure A.21: **Plots of the 4 individual antennas in the outdoor environment using the star configuration.**

Home Environment

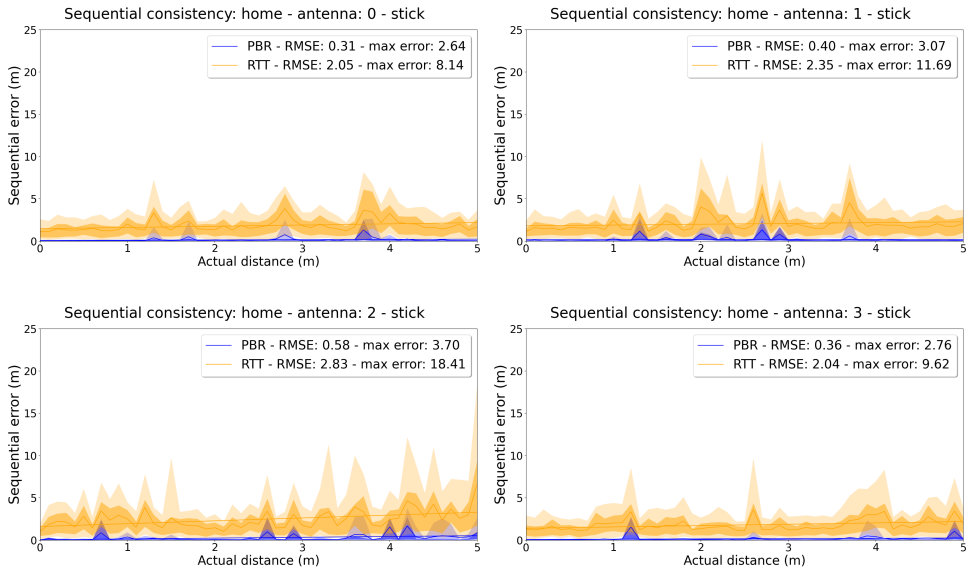


Figure A.22: **Plots of the 4 individual antennas in the home environment using the stick configuration.**

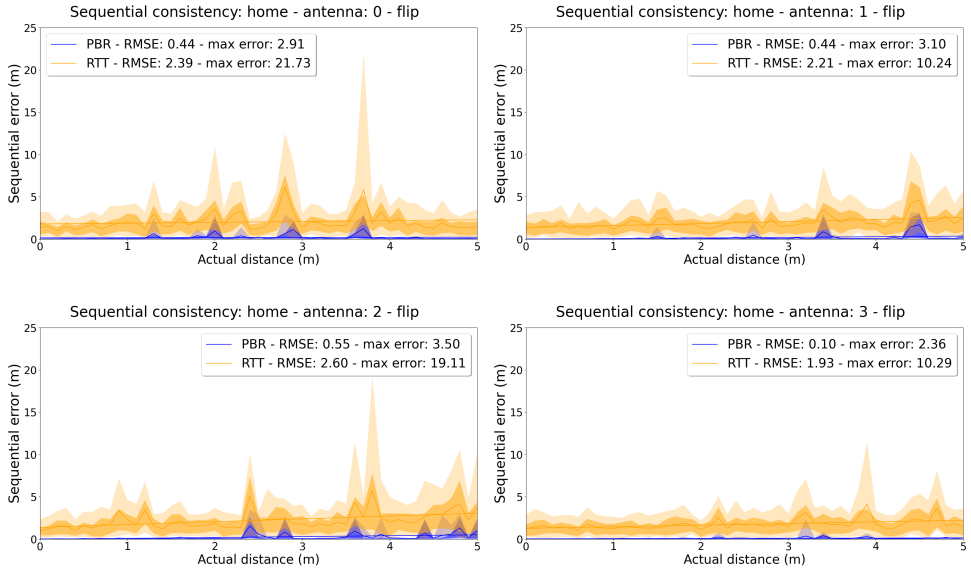


Figure A.23: **Plots of the 4 individual antennas in the home environment using the flip configuration.**

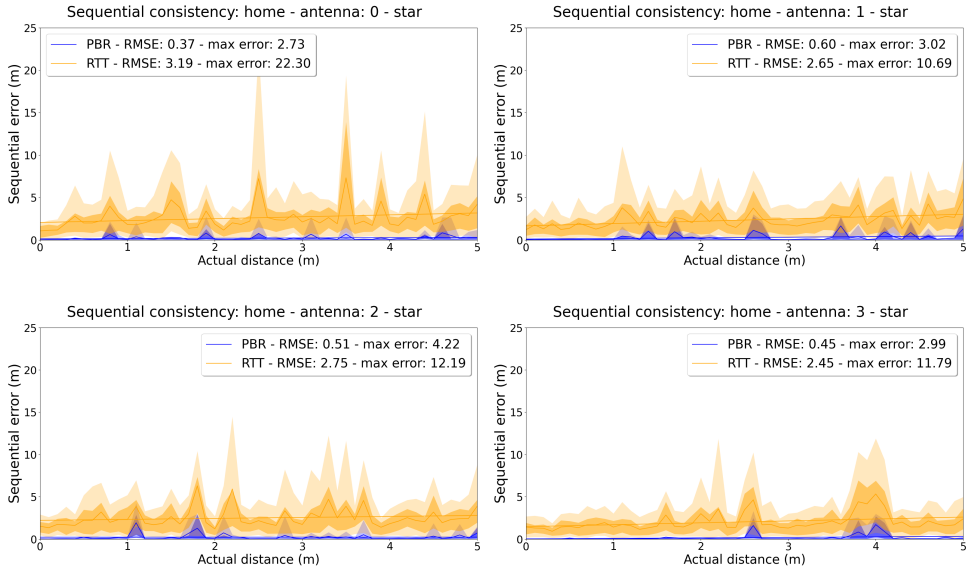


Figure A.24: **Plots of the 4 individual antennas in the home environment using the star configuration.**

Office Environment

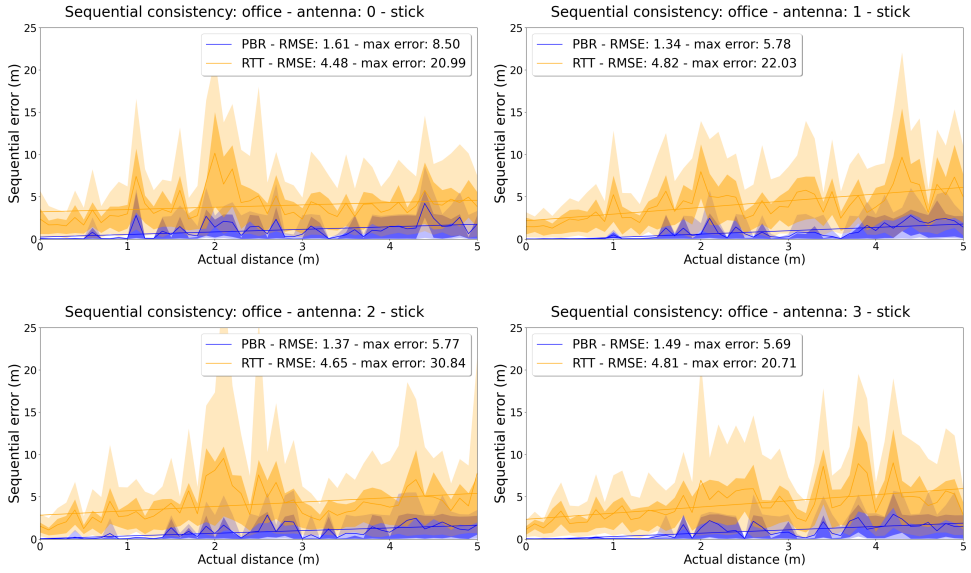


Figure A.25: **Plots of the 4 individual antennas in the office environment using the stick configuration.**

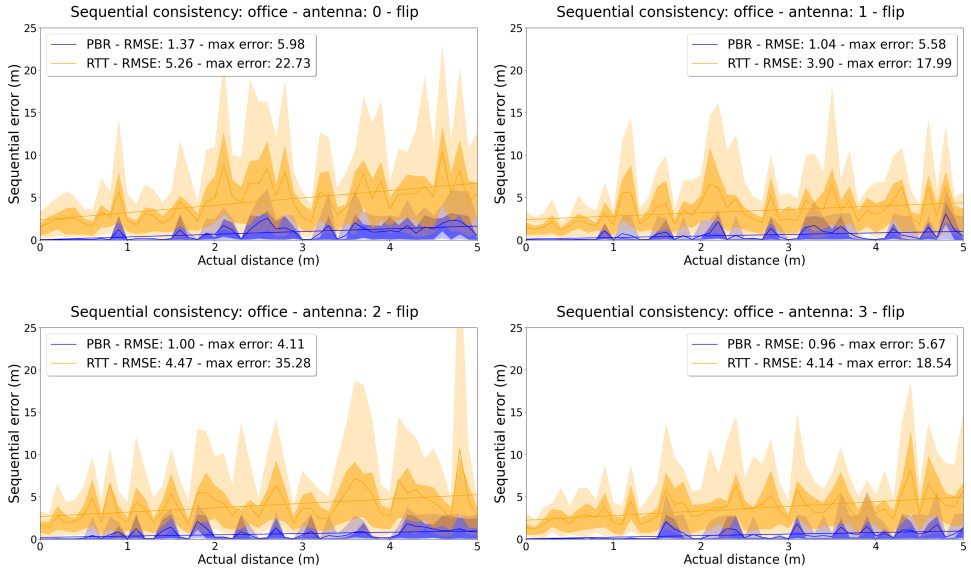


Figure A.26: **Plots of the 4 individual antennas in the office environment using the flip configuration.**

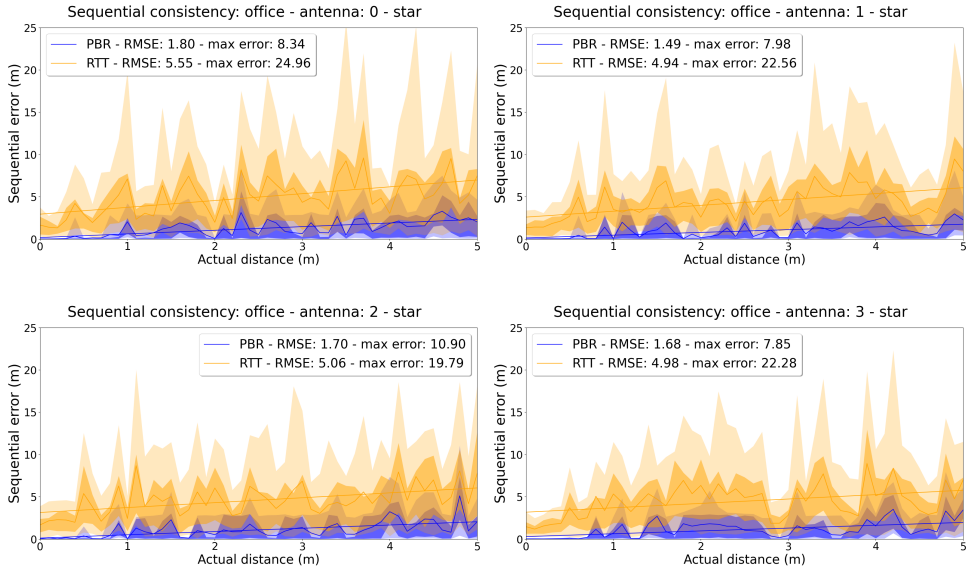


Figure A.27: **Plots of the 4 individual antennas in the office environment using the star configuration.**

A.4 Multi-Antenna Channel Sounding Plots - Sequential Consistency

Outdoor Environment

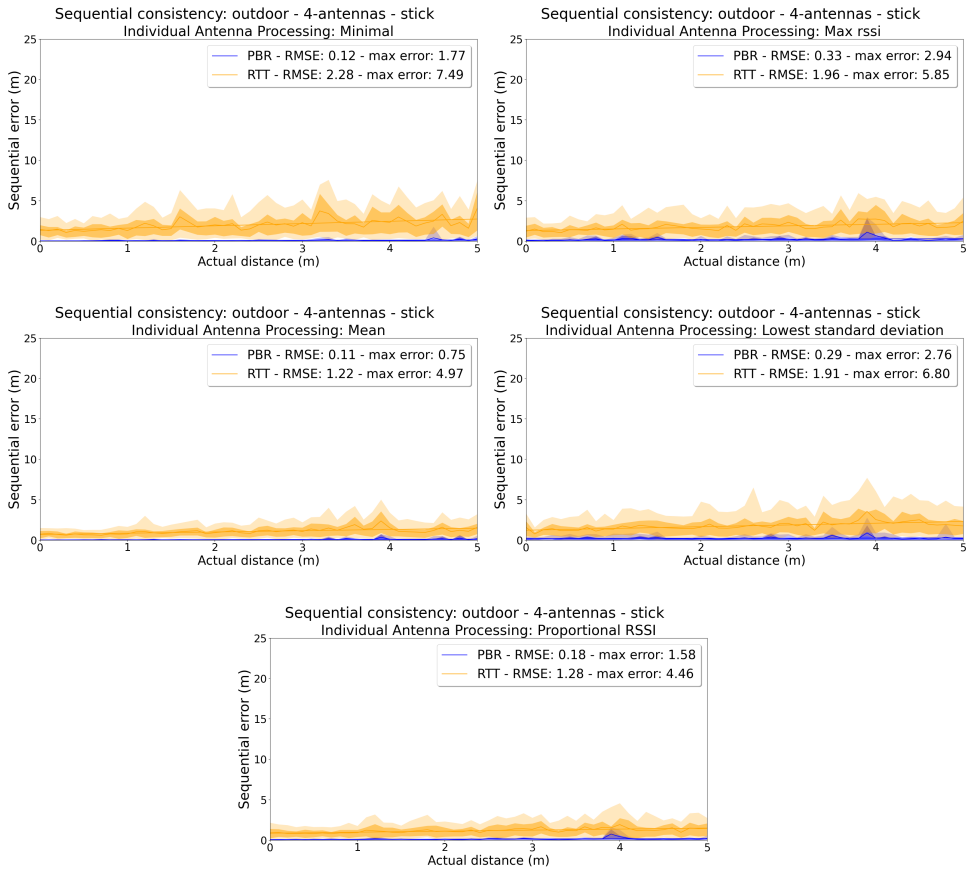


Figure A.28: **Plots of the 5 antenna combining methods in the outdoor environment using the stick configuration.**

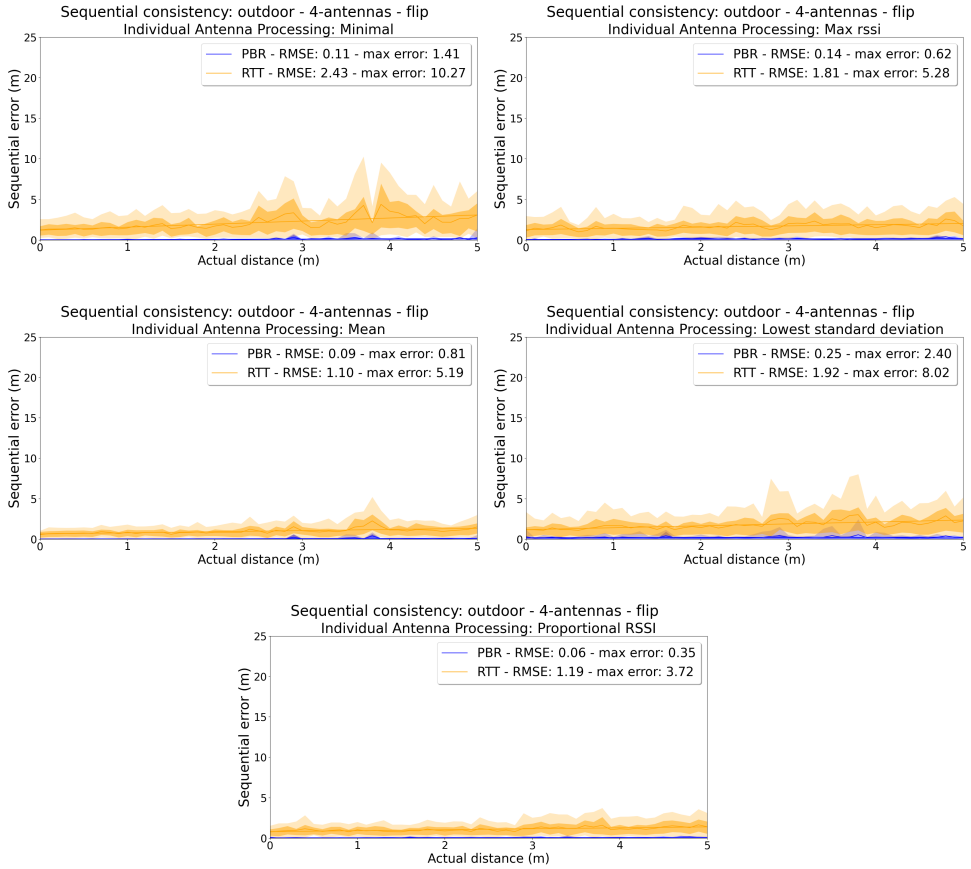


Figure A.29: **Plots of the 5 antenna combining methods in the outdoor environment using the flip configuration.**

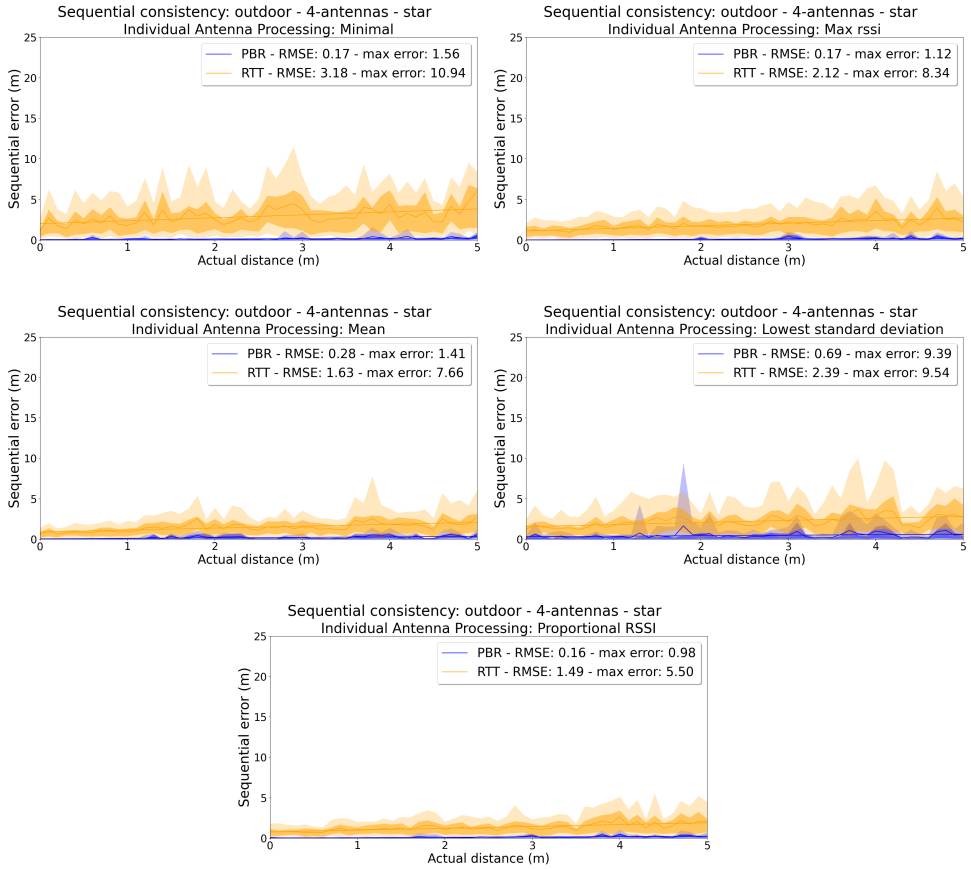


Figure A.30: **Plots of the 5 antenna combining methods in the outdoor environment using the star configuration.**

Home Environment

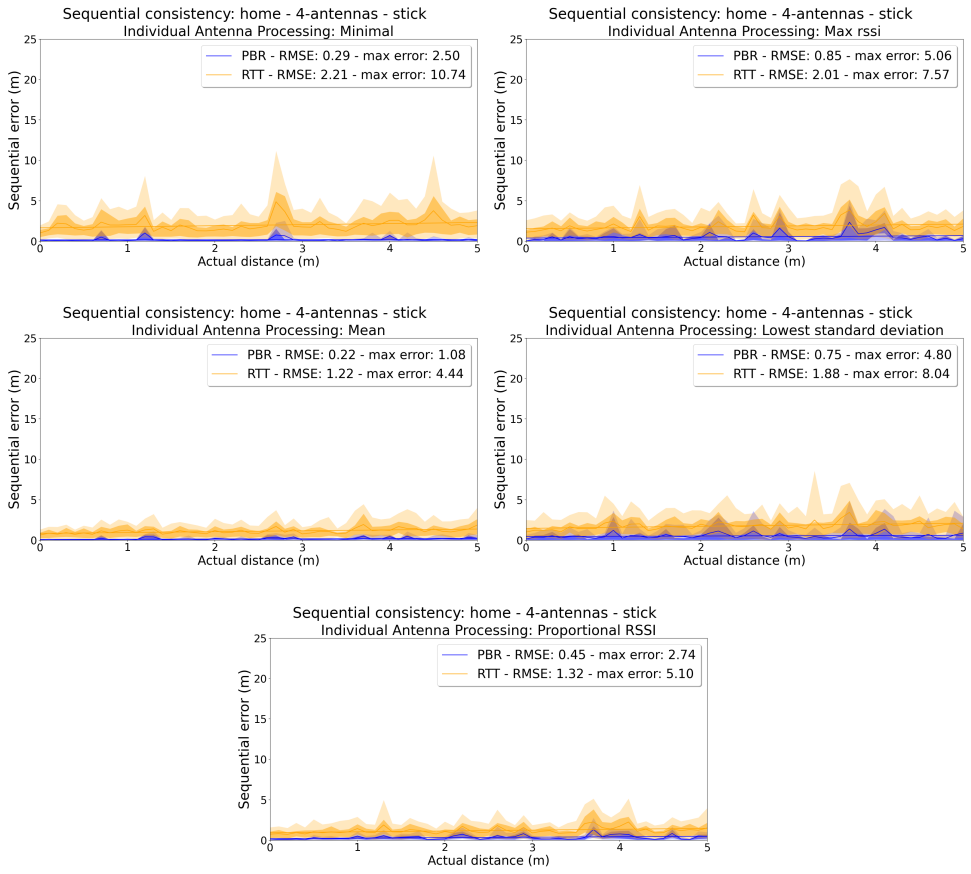


Figure A.31: **Plots of the 5 antenna combining methods in the home environment using the stick configuration.**

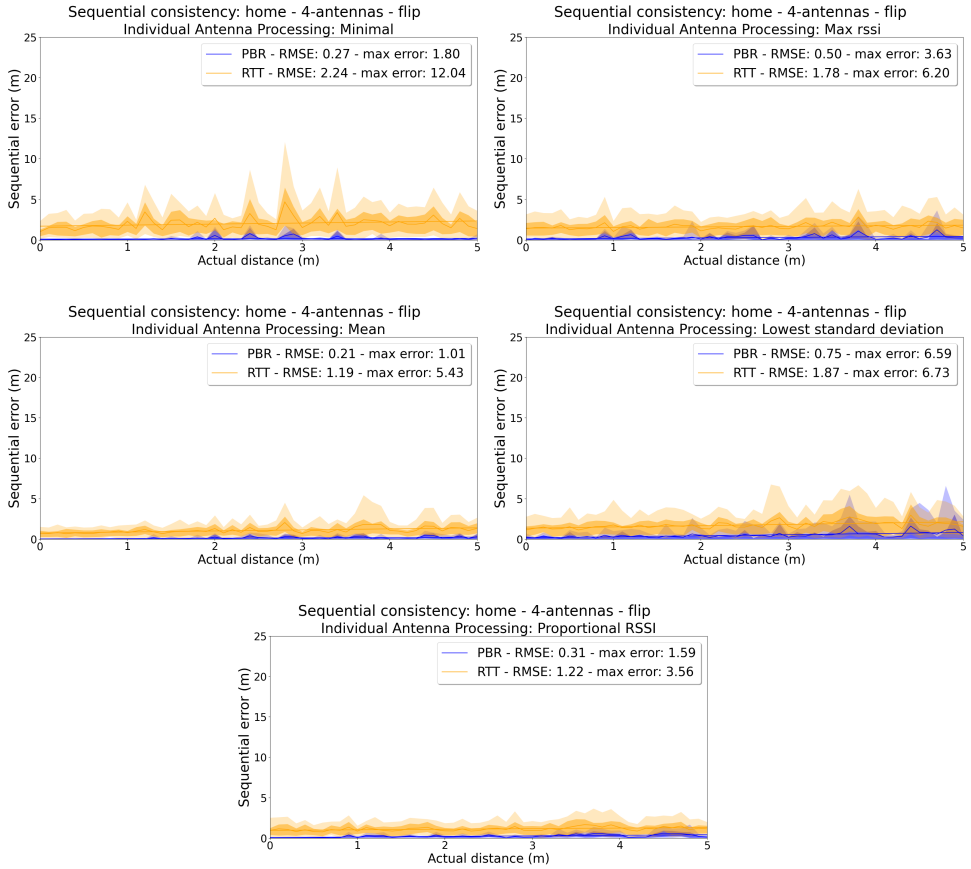


Figure A.32: **Plots of the 5 antenna combining methods in the home environment using the flip configuration.**

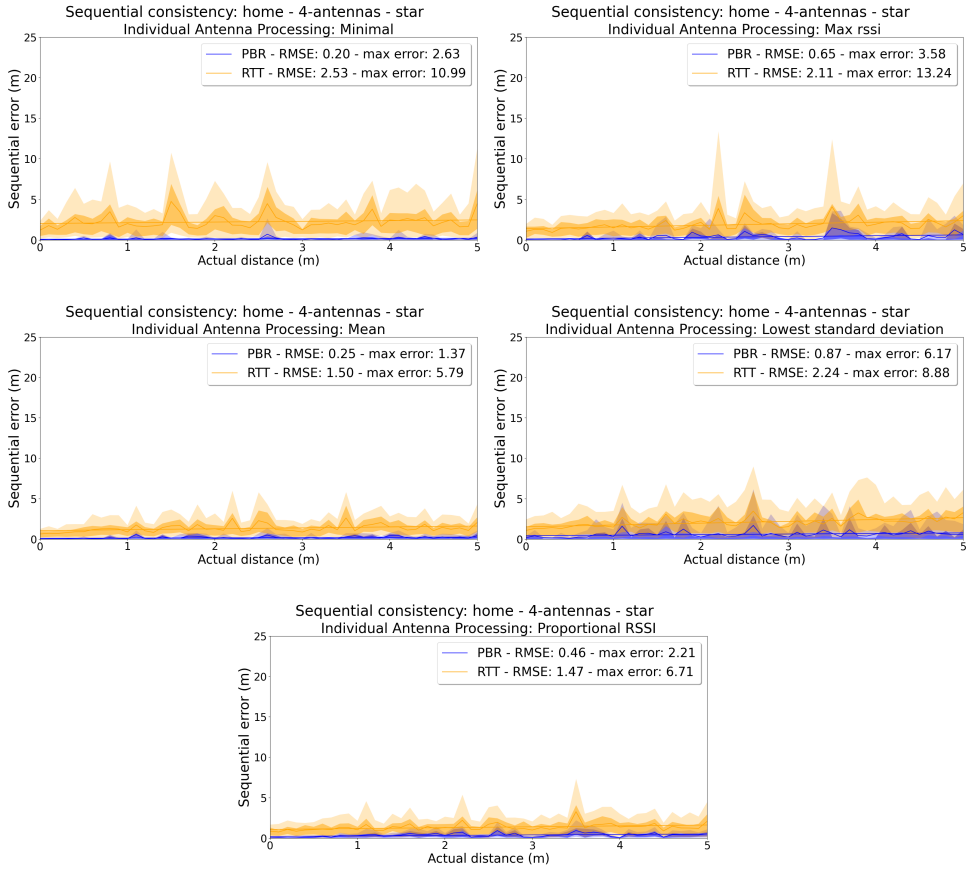


Figure A.33: **Plots of the 5 antenna combining methods in the home environment using the star configuration.**

Office Environment

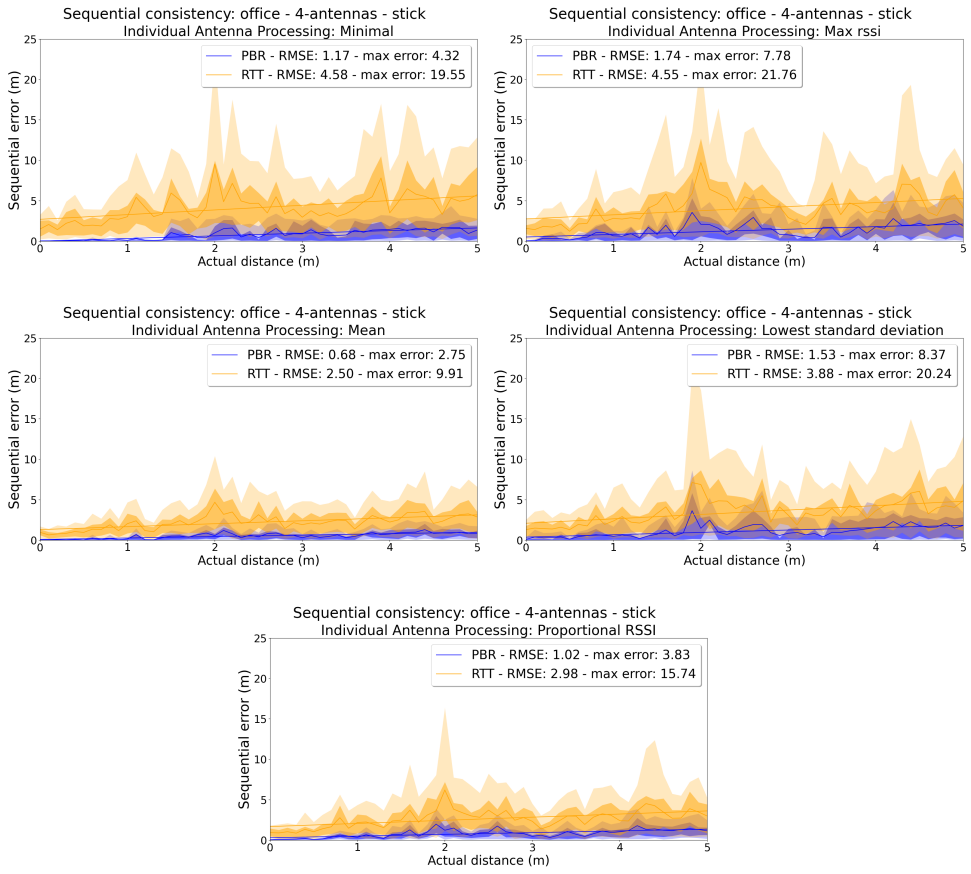


Figure A.34: **Plots of the 5 antenna combining methods in the office environment using the stick configuration.**

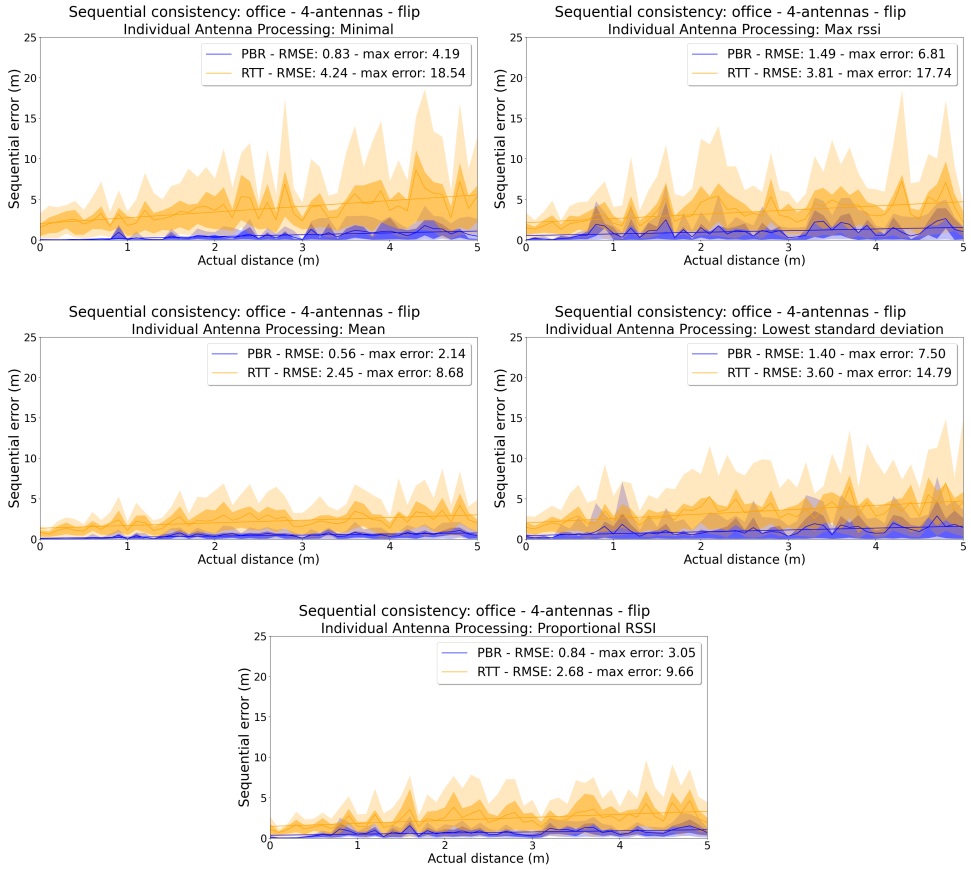


Figure A.35: **Plots of the 5 antenna combining methods in the office environment using the flip configuration.**

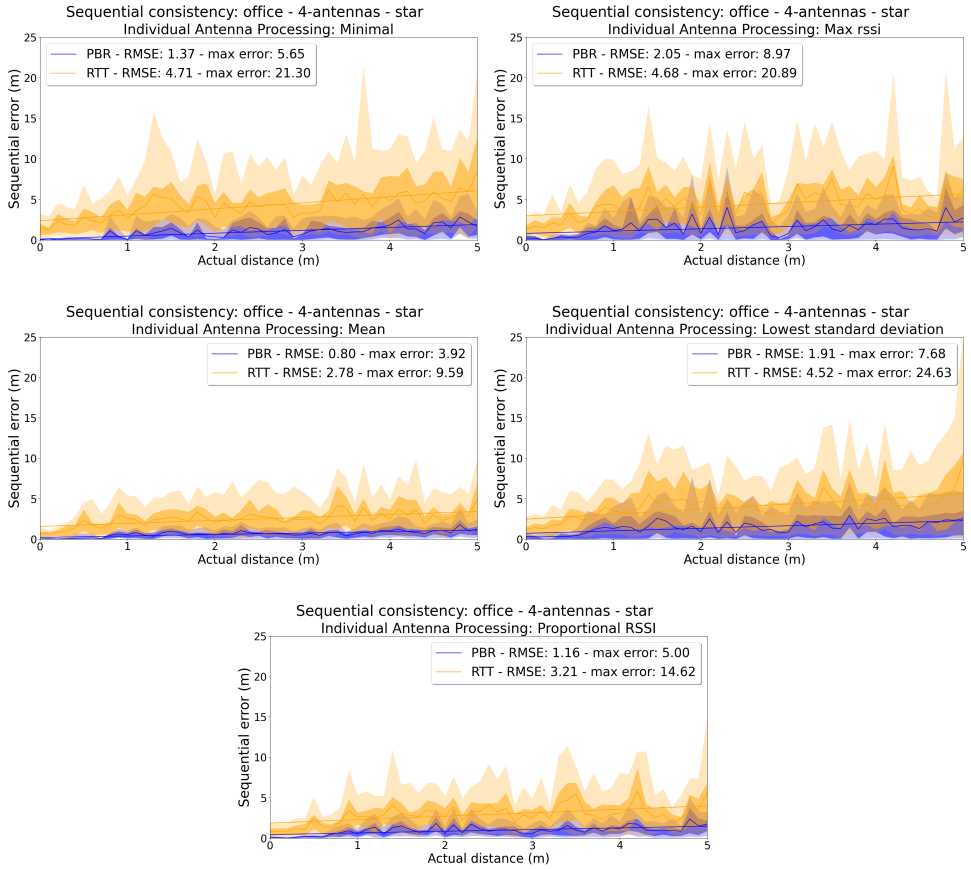


Figure A.36: **Plots of the 5 antenna combining methods in the office environment using the star configuration.**

A.5 Average metric Plots - Spatial Consistency

Outside Environment

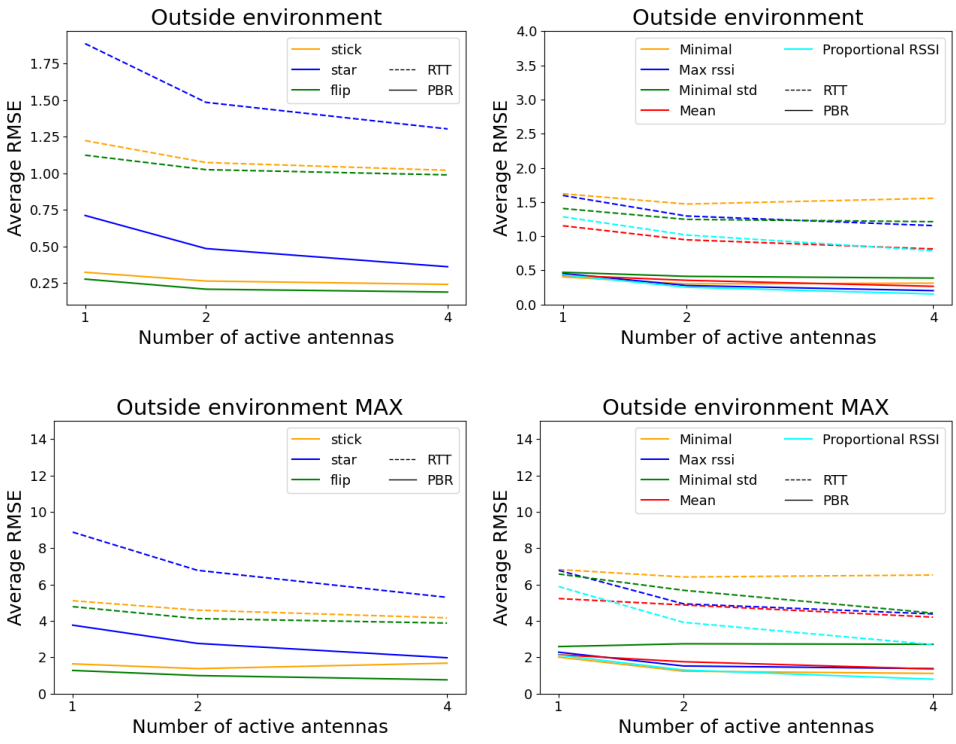


Figure A.37: **Fair averaged RMSE (top) and maximum error (bottom) for spatial consistency in the outside environment for 1, 2, and 4 active antennas.**

Home Environment

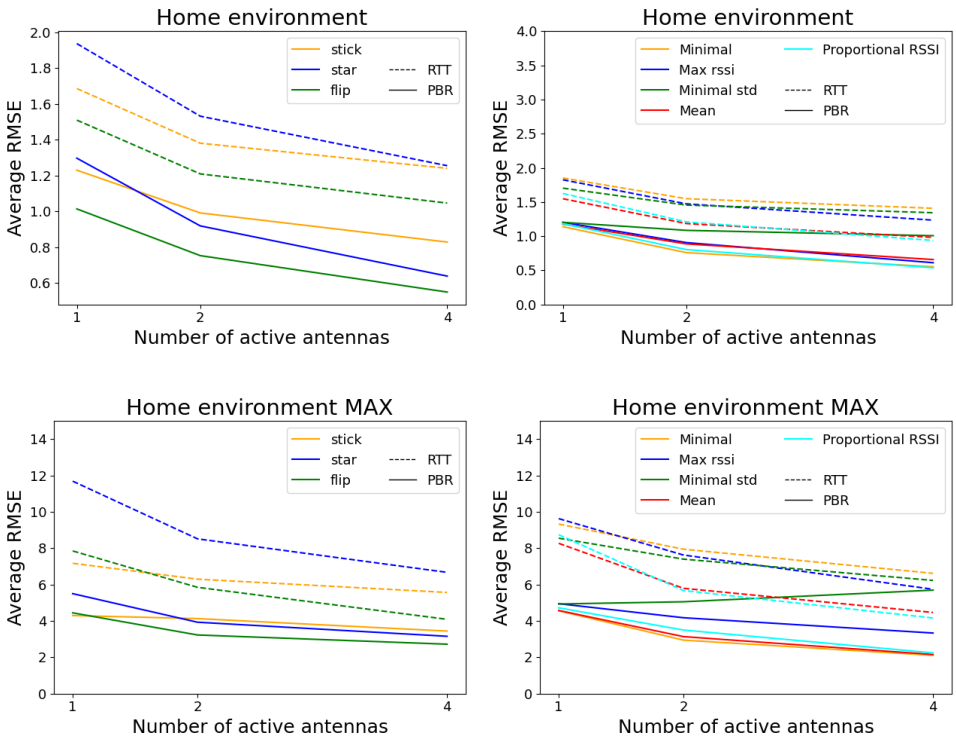


Figure A.38: **Fair averaged RMSE (top) and maximum error (bottom) for spatial consistency in the home environment for 1, 2, and 4 active antennas.**

Office Environment

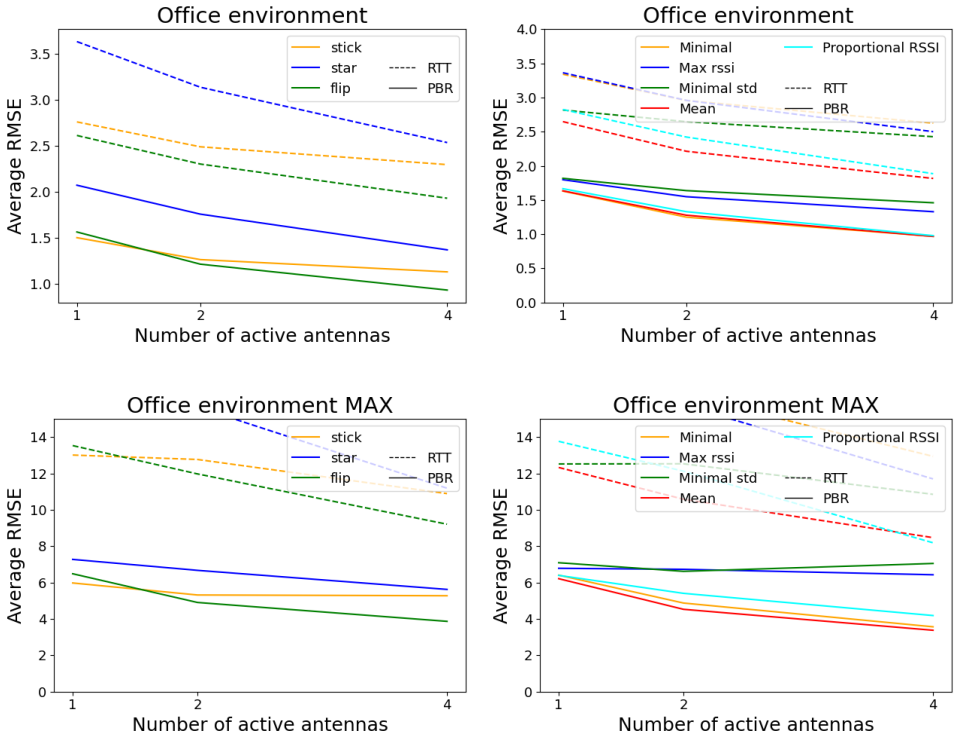


Figure A.39: **Fair averaged RMSE (top) and maximum error (bottom) for spatial consistency in the office environment for 1, 2, and 4 active antennas.**

A.6 Average metric Plots - Sequential Consistency

Outside Environment

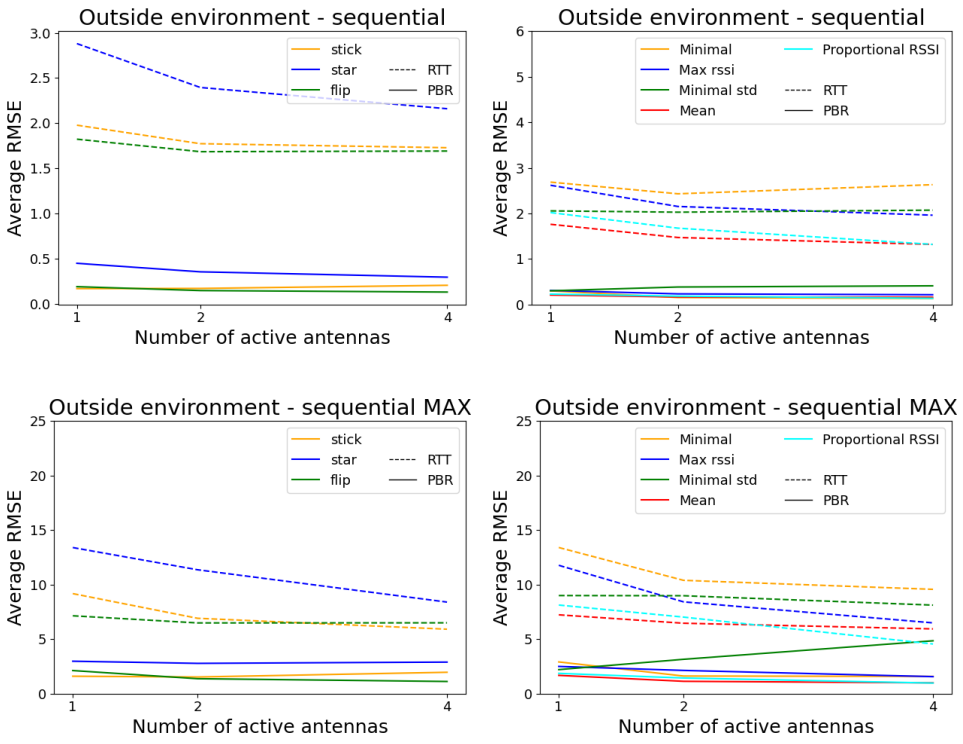


Figure A.40: **Fair averaged RMSE (top) and maximum error (bottom) for sequential consistency in the outside environment for 1, 2, and 4 active antennas.**

Home Environment

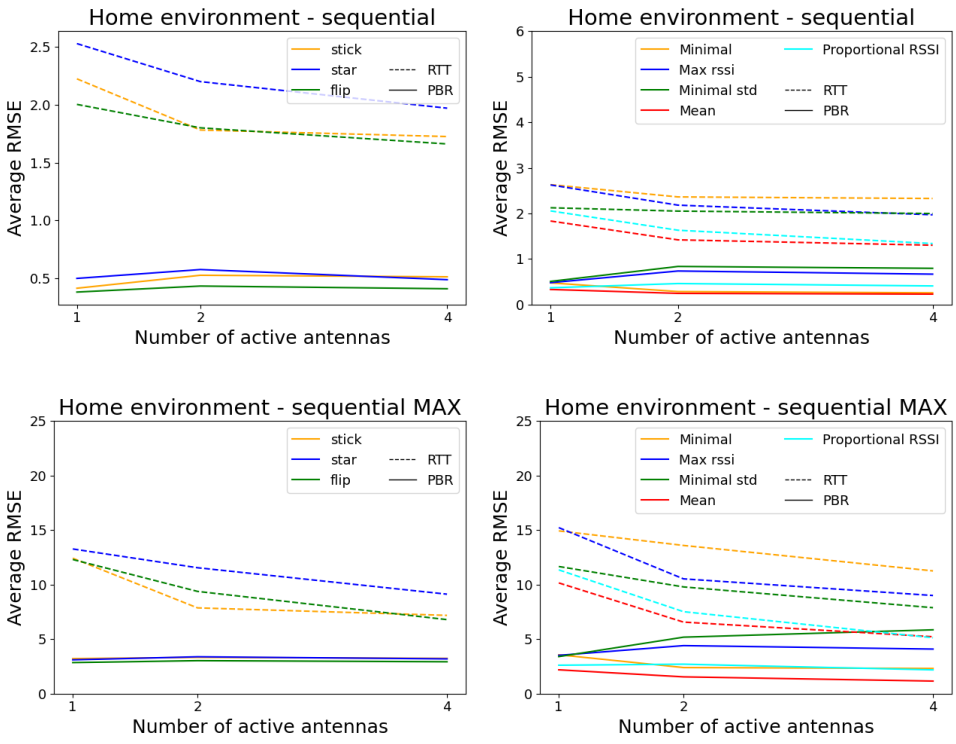


Figure A.41: **Fair averaged RMSE (top) and maximum error (bottom) for sequential consistency in the home environment for 1, 2, and 4 active antennas.**

Office Environment

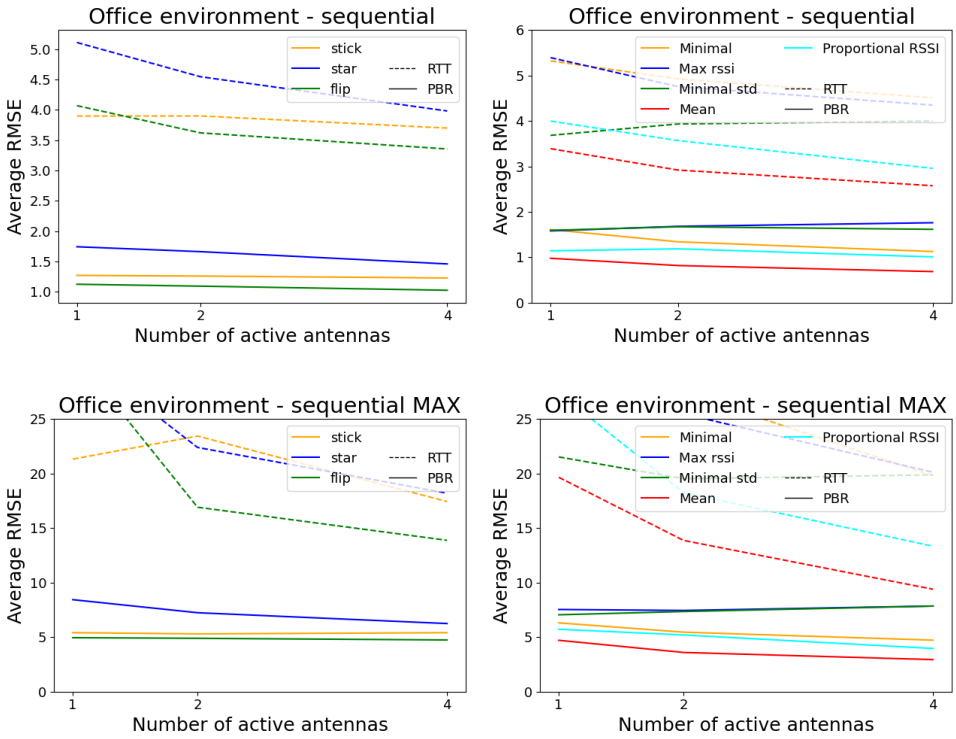


Figure A.42: **Fair averaged RMSE (top) and maximum error (bottom) for sequential consistency in the office environment for 1, 2, and 4 active antennas.**