On the Feasibility of Detecting Non-Cooperative Wi-Fi Devices via a Single Wi-Fi-Router

Daniel Vogel[1,*], Markus Krämer[1], Ben Swierzy[1], Daniel Meyer[1] and Michael Meier[1,2]

[1] *University of Bonn, Regina-Pacis-Weg 3, 53113 Bonn, Germany*

[2] *The Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE, Fraunhoferstr. 20, 53343 Wachtberg, Germany*

Abstract

Detecting intruding devices using Wi-Fi based indoor positioning systems running on commodity Access Points (APs) makes demands on both compatibility with available hardware as well as not depending on the intruding device to cooperate with the system. In this paper, we examine the feasibility of detecting non-cooperative Wi-Fi devices with a single AP reliably and whether available hardware in affected homes is sufficient in carrying out the task. Commonly, indoor positioning systems require non-trivial setups with specifically tailored hard- and software, as the aspiration is to maximize precision for which the devices to be located will actively assist, which we cannot rely upon. First, criteria are derived that help identify indoor positioning systems suitable in our use case, specifically Channel State Information (CSI)-based approaches. These systems are then evaluated on both compatibility with commodity hardware and accuracy by conducting experiments on available devices. We show that despite promising premises the commodity hardware landscape is insufficiently supporting such a system for widespread use and that the one compatible router we found can not detect an intruding Wi-Fi device accurately enough even in favourable conditions.

Keywords

Wi-Fi positioning, CSI, COTS, Commodity, Router

1. Introduction

Nowadays criminals use modern equipment like smartphones in order to commit or support crimes. This may be by calling their victims and pressurizing them to hand out valuable objects. Other criminals use those equipment to plan crimes accurately and communicate with their accomplices, which in turn suggests that Wi-Fi devices are sometimes being used during the committal of a crime. Wi-Fi devices such as smartphones constantly probe their surrounding environment for available networks, and thus, may be detected. We think there is yet untapped potential in persecution of crime particularly for cases, where Wi-Fi devices are brought to crime scenes.

While thefts by burglary of a dwelling suffer from constantly low crime clearance rates until today, the idea of the german federally founded project WACHMANN is to use their modern

Proceedings of the Work-in-Progress Papers at the 13th International Conference on Indoor Positioning and Indoor Navigation (IPIN-WiP 2023), September 25 - 28, 2023, Nuremberg, Germany

[*] Corresponding author.

vogel@cs.uni-bonn.de (D. Vogel); kraemerm@cs.uni-bonn.de (M. Krämer); swierzy@cs.uni-bonn.de (B. Swierzy); meyer@cs.uni-bonn.de (D. Meyer); mm@cs.uni-bonn.de (M. Meier)

CEUR Workshop Proceedings (CEUR-WS.org)

equipment against culprits: A home Wi-Fi router scans its environment for Wi-Fi packets. Intruders not bringing a Wi-Fi device cannot be detected using this approach, which seems to be an easy workaround from a burglar's point of view. However, police intelligence shows that organized groups of criminals are technologically well equipped to plan and conduct their action meticulously, which in turn would need to change their modus operandi. A less technologically equipped criminal is a less powerful one after all. If any home that has a router installed could therefor house a security system, burglars might be less inclined to commit to their crime in general. Also, culprits by opportunity may not be aware of either the deployed system or their own device they bring. [1]

Based on the Wi-Fi device's packets' information and a preconfigured perimeter, this approach as depicted in Fig. 1 decides whether the smartphone (and thus, the person using it) is either outside the perimeter (green), inside the perimeter (red) or somewhere in between (orange) which means more monitoring is necessary. For privacy reasons, only publicly readable information like headers are evaluated and in case of localizing a device outside the perimeter, all its respecting information is dropped.

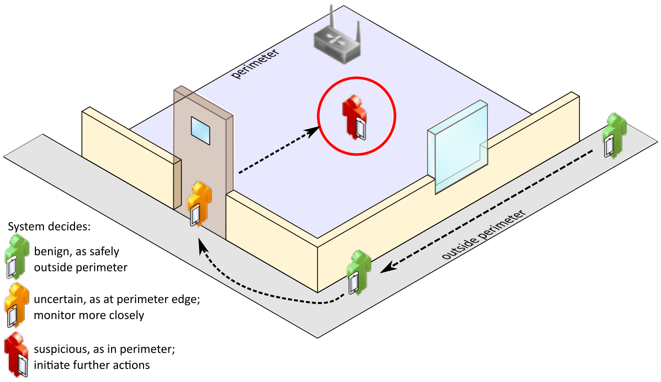
perimeter
outside perimeter
System decides:
benign, as safely outside perimeter
uncertain, as at perimeter edge; monitor more closely
suspicious, as in perimeter; initiate further actions

Figure 1: Use case: Detecting and differentiating an intruding device inside the protected perimeter (red) from devices outside the perimeter (green) using a single AP. Devices located within the error margin of the positioning system (yellow) may require further monitoring for a reliable assessment.

In case of detecting an unauthorized device inside the perimeter, the home owner is alarmed. Furthermore, Device Identifying Data (DID) like MAC-addresses or IMSI numbers are collected. Collection processes and further DID are described by Vogel and Krämer [2]. Subsequently, using the collected DID, a sensor-net-based device tracking as described by Swierzy et al. [3] can be enforced. In order to track a fleeing culprit as long as possible and support police pursuit, DID could be multicast to selected neighbour routers which try to recognize the culprits device. For completeness, authorized devices may be saved by their DID and will not be considered in the detection process any more. Though identifying and pursuing identified devices is of research interest, it is out of scope for this paper.

As for the collection of DID and device-tracking approaches exist, the scope of this paper comprises the initial problem of detecting unauthorized persons in a perimeter by detecting their Wi-Fi devices. As there exist many different approaches for Wi-Fi positioning in the literature, in this paper, there is a focus on systems using only a single Wi-Fi router as this limitation is given in many homes. The overall research question is:

- Are state-of-the art Single-AP-CSI-Localization approaches suited for scanning a perimeter for unauthorized intruders?

As this is an rather extensive research question, it will be answered by two more fine-grained sub-questions:

- Can CSI be extracted out of commodity Wi-Fi devices to use for intruder detection?
- Is a localization fulfilling our accuracy constraints feasible, using the extracted information?

First, in order to use CSI, it must be extractable from off-the-shelf hardware. Second, there exist accuracy constraints as mislocalization inside the perimeter causes costs for unnecessary police operations, ties police forces and causes accusation and privacy loss for mislocalized devices. Thus, apart from demanding high accuracy from localization systems, depending on the expected localization error, the owner will only be alarmed if a localization inside the perimeter is without a doubt.

The rest of this paper is organized as follows: Section 2 covers related work from the field of Wi-Fi localization. Section 4 gives an overview on existing different approaches on Wi-Fi localization. Furthermore, based on our criteria, some are selected for testing them with our use-case. The results for our use-case are presented in section 5. A conclusion and needs on further research are given in section 6.

2. Related Work

We selected some Wi-Fi-based positioning systems to show that current research is interested in their effectiveness in solving problems or assisting in tasks where a physical access may be restricted in some way or features of Wi-Fi are uniquely helpful.

In 2019 Mutiawani et al. proposed a WLAN based Indoor Localization System for Assisting Victim's Evacuation Process. Their idea is to utilize indoor positioning to locate devices in damaged building. Knowing the location of these devices can assist rescuers in planning the rescue of victims having their smartphone with them. A coordinate and Received Signal Strength (RSS) fingerprinting approach lets an app display the estimated locations of victims. Wi-Fi is selected as the WLAN technology for their proposed RSS-based system, which uses a computer, smartphone and three APs as hardware. [4] From their paper we cannot derive any practical evaluation of the system, as the system was claimed to be in development. [**?**]

In 2020 Dmitrienko et al. proposed a Wi-Fi colocation approach that has a Wi-Fi device scan and store nearby AP information and perform proximity inference. For sparse rural scenarios without many APs nearby, the device can run in a hotspot mode, if it is an android device. They propose a deterministic classifier using the Pearson correlation of RSS from overlapping APs between two devices, Jaccard similarity between the lists of APs and a proximity feature called Das proximity. This classifier is evaluated and reaches an F-score of 0.65 at a 10ft distance threshold, which given the recommended social distancing guidelines was a range for which they aimed for a high accuracy. [5]

For scenarios with a larger scale in both size and observed devices, Wi-Fi is a promising technology due to its flexibility and affordable infrastructure. To assist indoor localization, Li et al. proposed a Wi-Fi-based fast indoor localization system for exhibition venues. They show that their RSS to distance model can yield localization errors of less than 3 m for 80 % CDF even in large scale, multi-AP scenarios for many observed devices. [6]

3. Criteria & selection of positioning systems for our use case

From our use case we deduce the following criteria that a deployed system needs to fulfill:

- the system must be able to act on signals and packets sent by the intruder's Wi-Fi device, which in most cases should act as a **non-cooperative device** as described below
- the system must be able to run on a **single AP**
- the system must be **compatible with commodity Wi-Fi routers**, where
  - the router must be able to collect required input data for the positioning approaches
  - the router must be able to make the required input data available to the positioning approaches
  - the router must possess sufficient processing power and memory
- the system must have sufficient localization precision

For our given use case we expect the brought Wi-Fi device to be set up in a way that it is not readily communicating or connecting to any Wi-Fi network present in the victims home. That said, Wi-Fi devices are following the protocols as defined by the Wi-Fi standard. In this work, we define a Wi-Fi device as *non-cooperative*, if it behaves like a regular Wi-Fi device without: a) connecting to the home Wi-Fi network of the victim and b) actively assisting the deployed positioning system i.e. through specific client-side installed software. The device should still act Wi-Fi standard compliant with regards to protocol definitions and thus respond to certain packets, which is important for data collection as explained below.

A specifically modified AP may trick a non-cooperative device to try to connect to a Wi-Fi network that it advertises i.e. using association attacks [7]. In case of a successful attack, the system may have access to additional data and/or more measurements when compared to the collectable data from a non-associated device. For this work we omit any discussion that would stem i.e. from successful association attacks and their impact on our selected positioning approaches as we did not test them. Still, there is a potential for collecting additional data from non-cooperative devices, when employing attacks on its Wi-Fi communication.

For such a system to be easy to deploy and thus likely achieve a high acceptance within the population, we investigate only systems that can run on a single AP. While upgrading available hardware by attaching dedicated hardware should be possible most of the time and thus would likely assist in achieving better localization results, this process would increase cost and setup complexity. Instead, we aim for systems that should be deployable through simple AP firmware upgrades. We assume homes to commonly only have a single AP deployed for their Wi-Fi needs, particularly in dense urban environments, where homes are spacially limited and a single AP is sufficient.

To evaluate the capabilities of these home-deployed APs, we checked commodity routers used and sold by common service providers in Germany, such as Asus, Cisco, TP-Link and more. For characteristics of routers that are most important for the compatibility with positioning systems we looked at the amount and position of antennas, the Network Interface Card (NIC) as well as their processors and memory.

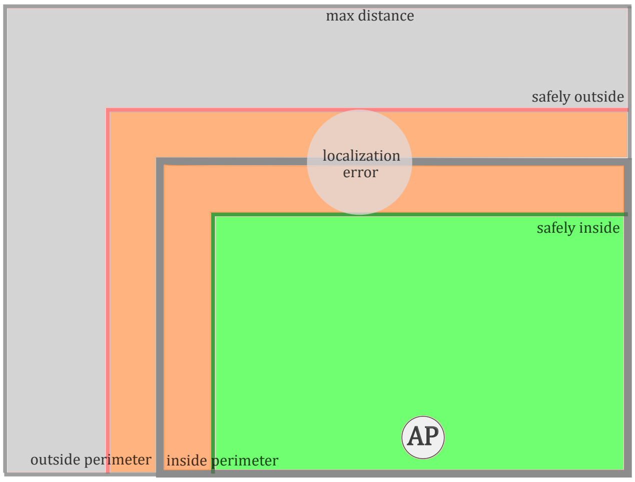

Figure 2: The localization error paints a region around the edge of the perimeter, where a localization of the device within that region does not safely determine whether the device is inside the perimeter or not.

Fig. 2 shows the perimeter that is being monitored by the AP. Given the expected maximum localization error of the chosen positioning system and assuming that this error is constant regardless of where the device is located, we can define three regions: The green region is the collection of all locations that if the device is located there lets the system safely deduce that the device is within the perimeter, as even the worst possible localization error is not sufficient to mislocalize an outdoor device as inside. The gray region is the collection of all locations of outside devices that will never be falsely mislocalized inside the perimeter. The region around the edge of the perimeter is where mislocalizations may happen with regards to the systems precision. The size of this error region should be minimized. A mislocalization may lead to legal consequences if false accusations are being made based on a faulty conclusion leading to a critical importance for the applicability of the detection approach.

In our use case we are mainly interested in whether a device is inside the perimeter or not and thus we can formulate a classification problem. Though this does omit the necessity of deriving precise location coordinates for practical use, we are still interested in quantifying the localization precision, which may assist in system calibration.

4. Wi-Fi Positioning Systems

We identified two main families of positioning approaches that appear promising when working with non-cooperative devices: RSS-based and CSI-based approaches. We consider approaches as RSS-based, if they use RSS and do not rely on CSI for their positioning. These RSS-based approaches commonly share the quality of requiring multiple APs or additional sensors i.e. in form of Wi-Fi enabled ESPs as shown by Abedi et al. [8]. CSI-based approaches rely on collecting CSI and deriving metrics like the Angle of Arrival (AoA) from them to aid in their positioning [9]. Oftentimes these approaches also measure RSS to improve their precision in some form. These CSI based approaches commonly share the quality of requiring multiple antennas in a certain configuration, which for some approaches a single AP can support.

There are a number of Wi-Fi-based device-free positioning systems, that may be able to detect intruders who do not bring a Wi-Fi device and thus could act as a Wi-Fi based burglar alarm. These systems would not be able to collect any DID from intruding devices however, which is the main premise of assisting in the pursuit of the burglar. Therefore we focused on approaches that utilize packets sent by intruding devices.

Given our requirement of having the system run on only a single AP and thus minimizing necessary hardware upgrades, we chose to focus on CSI-based positioning approaches, as they seem more likely to fit our requirements than RSS-based approaches.

How to collect CSI? CSI can be measured from packets sent in Orthogonal Frequency Domain Multiplexing (OFDM). Wi-Fi defines different rates and modulation schemes that can be used and some, that must be supported by all devices. Since we are restricted to packets sent by non-cooperative devices, we are limited in the amount and variety of packets we can expect to receive from these devices. As we cannot directly control the data rate that a brought device is sending its packets with, we investigated ways to enforce the usage of OFDM packets by the targeted device.

Generally, sending and modulating signals follows packet rates that are defined per packet as by the Wi-Fi standard. For control response frames, specifically Clear-To-Send (CTS) and ACK frames, the data rate and thus their modulation scheme is depending on the packet it is sent in response to. We found that we can force a non-cooperative device to send OFDM frames, when initiating communication with an OFDM stimulus packet which is to be responded to with an OFDM frame by the stimulated device. No established connection is required to force responses, as it is possible to just forge stimulus packets as shown by Abedi et al. [10] They suspect that the required response time as defined by the Wi-Fi standard is not sufficient to check the validity of said packets.

Even though CTS and ACK frames do not carry enough DID for a robust device identification, their underlying OFDM signals still provide CSI for positioning purposes. Once correctly detected inside the perimeter, DID can be gathered from other packets sent by the intruding device. These methods of gathering more CSI can be implemented on any router with a simple firmware upgrade.

4.1. Selected Positioning Systems

We will now briefly describe the CSI-based positioning approaches that we selected for implementation and why we chose these. We surveyed scientific papers for Wi-Fi compatible positioning systems, which we first filtered for single AP compatible systems first. The resulting roughly 80 papers were further checked for general compatibility with non-cooperative devices and hardware requirements, which resulted in only nine papers, of which we chose six for implementation. The positioning systems in these papers were the most promising when considering implementation details given and proposed performance in indoor environments.

Multiple Signal Classification (MUSIC) [11] is a signal processing algorithm presented first in 1986 by R. Schmidt and is used a foundation for many indoor positioning approaches using antenna arrays and still holds considerable importance today. While not a positioning approach as is, estimating AoA at multiple positions allows multi-angulation to be used as a positioning approach. A requirement are measurements from an equidistant antenna array with the distance d being no more than half the wavelength of the signal, meaning $d \leq 6\,\mathrm{cm}$ in the $2.4\,\mathrm{GHz}$ band. For these signals the AoA can be derived from a pseudo spectrum indicating incoming energy. Additionally MUSIC allows to derive further useful signal properties like the power delay profile, which is used by some other approaches like Cupid [12]. While MUSIC itself can be utilized for indoor positioning purposes using multi-angulation approaches, many researchers found ways to improve on it over the years to make it more robust and/or applicable in more scenarios.

An Indoor AoA Estimation Algorithm (AIAEA) [13] has been presented by Wen et al. that acknowledges problems with MUSIC as it assumes that multi-path signals are uncorrelated and/or when limited in bandwidth. Their approach improves the quality of the pseudospectrum generated by MUSIC, resulting in more prominent peaks and as well as less divergence to the true AoA. Though the authors used seven equidistant antennas, we expect that their approach will yield improvements over native MUSIC even when used with the typical three antennas for Wi-Fi routers.

FUSIC [14] as presented by Jiokeng et al. combines Fine Timing Measurement (FTM) with MUSIC to measure accurate distances between two Wi-Fi devices. FTM is a method, where two Wi-Fi devices measure Round Trip Times of exchanged packets to derive the Time of Flight (ToF), which in turn is used to calculate the distance between the devices [15]. MUSIC also allows ToF estimation by using CSI measurements of multiple subcarriers in Wi-Fi and their predictable phase differences for specific positions of the sending device. FTM allows only for a meter level distance estimation in direct LoS scenarios but struggles in non-LoS scenarios. FUSIC leverages the ToF estimations that MUSIC provides for multi-path components to correct positioning inaccuracies in these non-LoS scenarios. FUSIC achieves a median error of $1.27m$ in all scenarios and an error of less than $3.41m$ in 90% of measurements. FTM requires support by both the AP and the target device, we consider FUSIC only as a viable candidate once FTM support is wide spread for both device classes.

LaSa [16] is a location-based access control scheme presented by Lu et al., leveraging crowd sourced data combining RSS with coarse AoA information to train a One-Class Support Vector Machine (OSVM) model. While LaSa aims to restrict the Wi-Fi access of devices to those which are located within a protected perimeter, we expect the fundamental principle to be conceptually compatible with our use case. For data preprocessing RSS, CSI and AoA data are collected using an Atheros AR9580 NIC and the Atheros CSI tool [17]. The "visual angle" approach acknowledges the fact, that precise AoA estimation is a difficult task on commodity hardware using algorithms like ArrayTrack [18] or SpotFi [19]. Instead of relying on a precise angular estimation, coarse AoA estimation suffices as a "visual angle" to identify a region as a candidate. Using an OSVM model, LaSa can make an accurate decision, realizing a In-Region Verification, with 97% accuracy identifying devices inside or outside the perimeter.The system allows calibration via a "Cold Start" to skip a lengthy crowd sourcing process (and therefore *step 2: Enter and Exit Pattern Discovery and Recognition*) and deply the system quickly in a new environment, which is a convenient feature for installing this system in homes to protect. Also only data measured from inside the perimeter is required to train the model, which allows its application in dense urban environments and thus makes it particularly well suited for our use case.

CUPID [12] was presented by Sen et al. and describes a method to distinguish the direct signal from any reflected signal in a multi-path environment. It leverages AoA and the distance between sender and receiver for positioning, both available from CSI. For determining the distance the power delay profile is used, which can be derived using MUSIC. Combined with the RSS it allows to minimize the impact of secondary, reflected signals. CUPID extends MUSIC by an additional method to enhance its reliability in multi-path scenarios, where the movement of the targeted device is leveraged to correct AoA estimation. Even with a low received packet rate CUPID achieves a precision of around $7m$ for 80% of the measurements according to the authors. Since CUPID is designed to work with non-cooperative devices and tested for low packet rates, we consider it.

ACAI [20] is a system based on creating and comparing location specific fingerprints and was presented by Chen et al. As a fingerprint based approach, it uses two phases. During the training-phase fingerprints are created for known locations, which comprise of RSS and CSI data of all individual antenna connections to enhance the available bandwidth. During the localization phase so called Time-Reversal Resonating Strength values are leveraged to find the correct position within the fingerprint database. If that value breaks a threshold, the measurement is considered to not lie within the known locations. The approach is being evaluated with an AP and a target device with 3 antennas each. They show a promising robustness against noise or changing channel conditions as with people or furniture being moved. ACAI finds the correct fingerprint location for 99.91% of the measurements the system considers within its threshold. Since for our use case a fingerprinting database for the perimeter can be created, we consider ACAI to be a viable candidate.

A CSI-based Fingerprinting Approach (ACbFA) [21] by Zhang et al. leverages CSI data of an AP equipped with three antennas to create a fingerprinting database on an even grid of cells and uses two phases, similar to ACAI. The system focuses on detecting multi-paths from reflections on walls, furniture and other objects within the perimeter. The collected CSI data is being adjusted to separate signals from different paths and improve the positioning precision using machine learning. Different machine learning approaches are then used in various configurations and their precision is being evaluated. According to the authors, the system achieves a mean error of around 1.2 m on only one AP, though only one wall is blocking the direct path between the AP and the target device. As ACbFA was evaluated on a single AP for indoor environments, we consider it as similarly viable as the other fingerprinting approach ACAI for our use case.

When examining the approaches it appears that certain of these could be used alongside each other to unlock synergies or increase confidence in the resulting classification, as most use the same data as input. For example, AIAEA could be used for the coarse AoA estimation in LaSa. A system combining multiple of these approaches could be considered for future work.

How to deploy these positioning systems? The deployment of any of these selected systems on commodity routers could be done through so much as firmware upgrades, as long as the router is compatible with with the approach as discussed in the next section. Calibration and training for some of the approaches would be necessary to be done prior to productive operation but can be enhanced through some methods of crowd sourcing as described by the authors. The simplicity of deployment stems directly from the selection criteria established in section 3 and is the main appeal on why we chose to avoid complicated setups and additional special hardware.

5. Feasibility of selected localization systems on commodity devices

When evaluating the compatibility of the chosen positioning approaches with commodity hardware, we identified three aspects to be critical, as introduced in section 3: data collection, processing power and memory. Taking a look at the required input data for the indoor positioning approaches, which must be collectable and provided by the hardware, we identify a major problem. To our knowledge there is no commodity router available that allows collecting and providing CSI when in its factory delivery condition. For some Wi-Fi chip sets there are alternative firmware available which add that functionality. These chips comprise the Linux 802.11n CSI tool [9], the Atheros CSI tool [17] and Nexmon CSI [22].

The Linux 802.11n CSI tool [9] only works on the IWL5300-network chips, published in 2012, which are based only on mini-PCI-express cards. Secondly its operation mode as an AP is running very unstable and when in monitor mode, only those packets are used, which use a specific source and destination MAC-address. In our use case the target device will never send such packets. Finally, since the source code of this firmware is based on internal documents maintained by Intel and is not publicly available, these problems cannot be resolved.

The Atheros CSI tool [17] functions on various chips of the Atheros family, though chips newer than 2018 are no longer supported. Using this firmware allows to force sounding PPDUs, which allow the measurement of CSI at the receivers side. As the CSI measurement is only done at the receiver's side, the sender must send these sounding PPDUs, which implies that the sender - in our case the intruder's device - must also use this firmware or send sounding PPDUs triggered through any other mechanism. Since we consider the intruder's device to act non-cooperative, using the Atheros method is not applicable in our use case.

Nexmon [23] is a firmware patching framework for Broadcom Wi-Fi chips. Building upon it is Nexmon CSI [22], which allows measuring CSI on various current Broadcom chips. In practice, these chips are only rarely used in routers, which is why Asus RT-AC68U is the only officially compatible router we found. Since this router does not include a modem we expect it to not be widely distributed in many german homes. Therefore it is unlikely to result in a widespread coverage by upgrading these to fit our use case.

When considering processing power and memory, commodity routers should suffice. While neural nets require considerable processing power for their training process, the training process might be obsolete during operation. The training process may only be required once for calibration during the initial setup. We expect that setup to be realistically feasible on commodity hardware. The same is true for the OSVM used in LaSa, which also only requires low processing power. Additionally, we expect memory to be uncritical for all components. It must be stressed, that these are estimations based on our implementations on more capable hardware.

5.1. Practical results

We used a measurement setup to collect CSI in two different scenarios. The first scenario (S1) comprises measurements in two adjacent office rooms, where we labeled one room as the perimeter and the other room as well as the connecting corridor as outside the perimeter. The second scenario (S2) was a lab room on the ground floor, where we could get measurements from outside the building as well as inside. We implemented the CSI collector on an Asus RT-AC86U, with Asuswrt-Merlin as an alternative operating system and Nexmon-CSI. This Asus router was one of the only commodity Wi-Fi routers that was compatible and we were able to acquire. The Nexmon firmware was extended to also provide RSS measurements via a small patch. The actual data processing for the positioning systems was implemented on other computers to retain flexibility with software development.

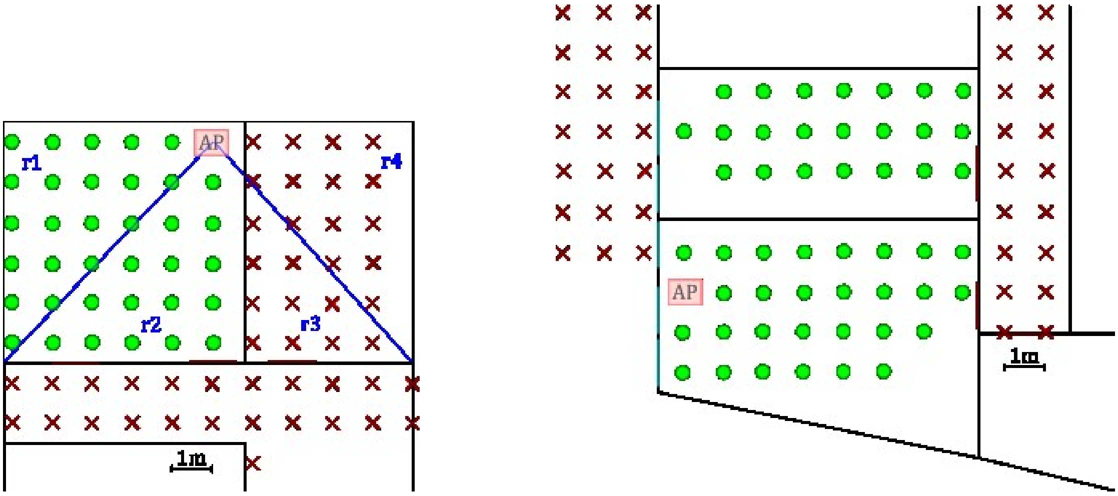

Figure 3: Measurement scenarios S1 (left) and S2 (right) in rooms at different floors of the University of Bonn. A 1 m × 1 m grid was used as far as furnishing allowed. Scenario S1 features regions r1-r4 which were used as verification regions for LaSa. Green circles denote measurement points inside the perimeter, red crosses outside.

We implemented a simple app that allowed the smartphone, a Samsung Galaxy A51, to send

Wi-Fi packets to the measurement router on demand for consistency and planning purposes. For our measurement, we decided to use a high packet sending rate to evaluate the positioning precision of the system in luxurious conditions. If the system showed promising results, the next step would be to use unaltered smartphones and test the system a real environment.

Across both measurement scenarios CSI measurements were collected by positioning the smartphone along a grid. In scenario S1 the grid comprised 82 measurement points over 11 m by 9 m for measurement points in both rooms and the corridor. In scenario S2 the grid comprised 85 measurement points over 13 m by 10 m for measurement points both inside the building and outside. For each measurement point roughly 80 CSI measurements were collected, amounting to 13612 CSI measurements total. The chosen grid layout allows the CSI data to be used as input data for the fingerprinting approaches as well as input data for LaSa in scenario S1.

We implemented MUSIC, AIAEA, LaSa, CUPID, ACAI and ACbFA. Since we did not have access to FTM compatible devices, we did not implement FUSIC.

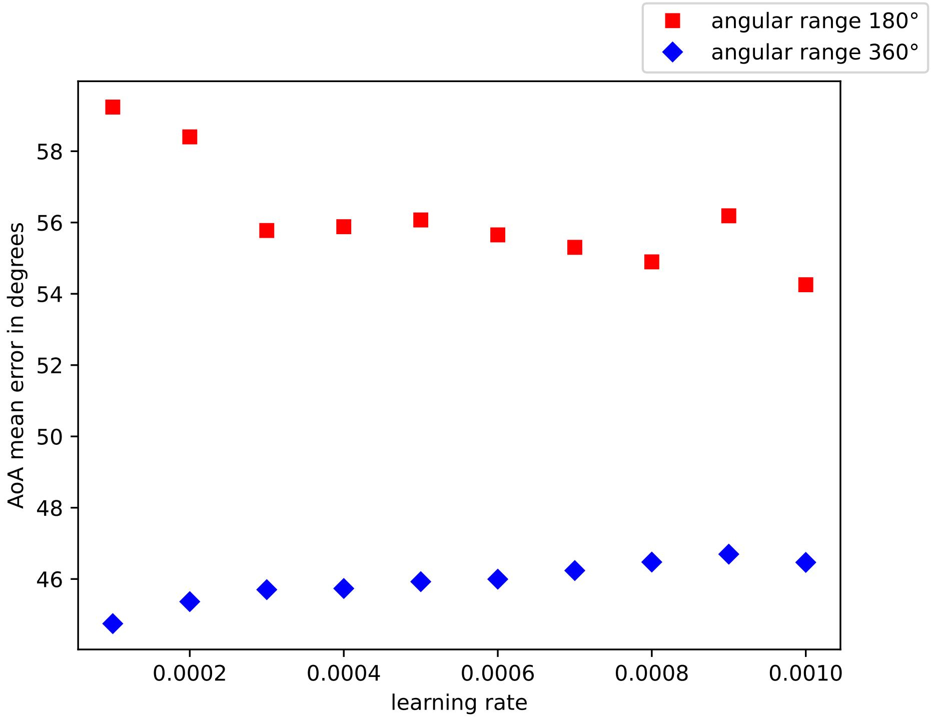

Figure 4: Mean error of estimated AoA for AIAEA in scenario S2.

The approaches that derive AoA (MUSIC, AIAEA, CUPID) did yield poor results compared to the results presented in their respective papers. For AIAEA we used Leave-one-out cross validation for varying configurations of the parameters for angular range (180°, 360°), learning rate (between 0.0001 and 0.001) and topology nodes for the different layers of the neural network. Figure 4 depicts the mean errors for estimated AoA for different learning rates and angular ranges for measurements for scenario S2. The best performing configuration we found reaches a mean error of around 43° with a learning rate of 0.0004 at an angular range of 360° in S2, and around 26° with a learning rate of 0.0004 at an angular range of 180° in S1.

When using CSI collected with our Asus router with three antennas for both scenarios S1 and S2, the estimated AoA show a mean error of 20 degrees to 40 degrees in the 180 degree spectrum for all implementations we tested. Given these results we concluded that any multi-angulation approach would not yield a sufficient precision for our use case.

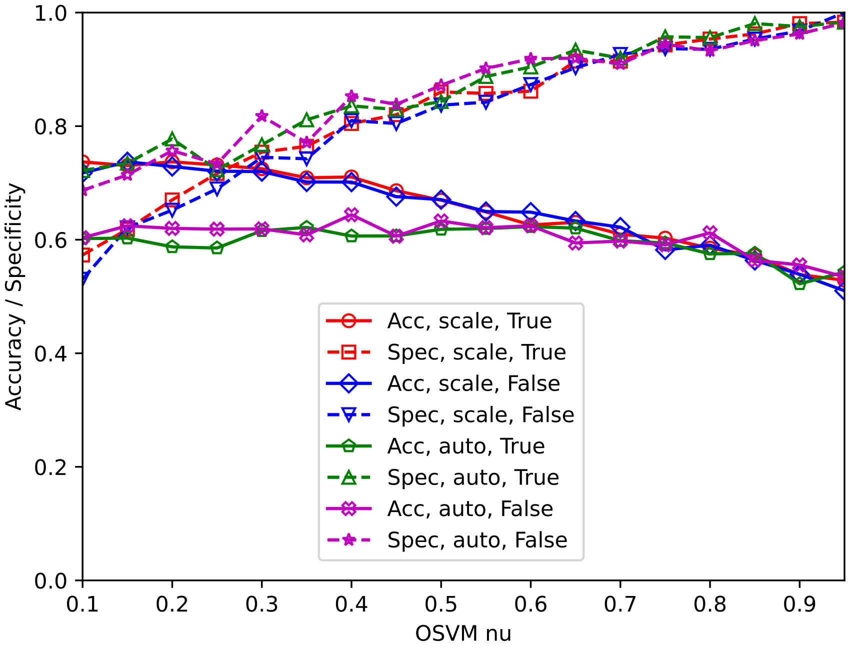

Figure 5: Accuracy and specificity results for LaSa OSVM on CSI collected with the Asus router for different settings for gamma, shrinking and nu.

As LaSa uses coarse AoA estimation, mean errors of this magnitude may proof problematic for the "visual angle" approach used by LaSa. Since the authors of LaSa did not specify, how exactly to split the perimeter in regions for the in-region-verification to work, we split the adjacent rooms into four regions as seen in Fig. 3: region 1: $[0-40)$, region 2: $[40-90)$, region 3: $[90-140)$, region 4: $[140-180]$ degrees. Regions r2 and r3 were differentiated by a wall next to the AP, where we didn't capture any measurements. Fig. 5 shows the classification accuracy and specificity of the LaSa OSVM when trained on the captured CSI data and assisted by in-region-verification. Though different OSVM settings for *gamma*, *shrinking* and *nu* allow for slight tuning whether to optimize for correct classification inside or outside, the overall $accuracy = (TP + TN)/(TP + TN + FP + FN)$ and $specificity = TN$ rate are below what we consider acceptable for our use case, with the highest accuracy not exceeding 0.73. While we evaluated LaSa on trained data only, it is reasonable to assume that on untrained data it would perform worse, not better.

The results for the fingerprinting approach ACAI are shown in Table 1. We split the measured

Table 1: Accuracy and mean error for ACAI for different thresholds. Only results for values within the threshold are shown.

threshold	S1 accuracy	S1 mean error	S2 accuracy	S2 mean error
-	0.61	4.18 m	0.68	4.19 m
0.7	0.61	3.90 m	0.74	3.03 m
0.8	0.61	2.73 m	0.65	2.67 m
0.9	0.86	0.37 m	0.78	1.42 m

data for each scenario and landmark. For each landmark we randomized the measurements and selected 80% as training data and the remainder as testing data. For both scenarios the accuracy and the mean localization error are heavily dependent on the threshold and only for very strict settings the results look promising. However, for thresholds of 0.9 and above the algorithm considers many measurements to not lie within known locations for which it then does not report a classification. For scenario S1 only 35 out of 370 testing samples reported a classification, for scenario S2 only 169 out of 378 testing samples reported a classification. Due to this, the resulting accuracy might be inflated.

The results for ACbFA are not finished yet as of writing.

In summary, all approaches that we implemented and were able to examine show an insufficient precision when using CSI collected by the commodity router Asus RT-AC68U. Since we were unable to find and thus test other commodity routers due to a lacking widespread compatibility with CSI collection, our practical results can only hold for this one device.

6. Conclusion

In this paper we analyze the feasibility of detecting non-cooperative Wi-Fi devices via a single Wi-Fi AP. For utilizing commodity routers installed in homes for detecting and enabling pursuit of burglars by their brought Wi-Fi devices, we defined requirements for indoor positioning systems to be able to assist in reaching that goal. Indoor positioning systems able to run on a single AP were investigated on whether they work with non-cooperative devices and on their hardware requirements. Five selected CSI-based positioning systems were implemented and both their compatibility with commodity hardware as well as their performance evaluated. Some of the evaluation is still in need to be finished and as we only were able to evaluate on a single compatible router, the validity of our findings can be increased using other devices.

We found current commodity routers to be ill-equipped for running these systems for the required CSI input data cannot be provided by the routers without having very specific chip sets installed. When evaluating our implementations of the selected systems, we measured mean errors between 20-40 degrees for AoA and accuracy values generally not exceeding 0.75. These results show that proposed indoor positioning systems cannot run on widespread commodity routers yet to a positioning precision required to fulfill our use case.

We conclude that current research on indoor positioning is not transferred easily for usage in realistic on-use-case scenarios. Hardware advances on commodity routers are expected to alleviate that transfer as both FTM compatibility and more sensitive hardware is likely to help. We advocate for more research transfer to realistic on-use-case scenarios and hardware to facilitate widespread usage and encourage targeted commodity hardware development.

7. Acknowledgments

The work on this paper has been funded by the German Federal Ministry of Education and Research (BMBF) for the project WACHMANN (WLAN-based recording of mobile device characteristics for alarming and fighting property crime) under grant number 13N15357.

References

[1] Bundeskriminalamt, Polizeiliche Kriminalstatistik, 2022. URL: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2022/pks2022_node.html.

[2] D. Vogel, M. Krämer, Collecting identifying data for re-identification of mobile devices carried at a crime scene using wi-fi routers, INFORMATIK 2022 (2022).

[3] B. Swierzy, M. Krämer, D. Vogel, D. Meyer, M. Meier, Analyzing the feasibility of privacy-respecting automated tracking of devices fleeing a burglary, in: 2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2023, pp. 452–459.

[4] V. Mutiawani, C. T. Nazila, K. Saputra, A. Mabrina, Design of an indoor localization system based on wlan for assisting victim's evacuation process, in: 2019 2nd International Conference on Applied Information Technology and Innovation (ICAITI), IEEE, 2019, pp. 6–10.

[5] M. Dmitrienko, A. Singh, P. Erichsen, R. Raskar, Proximity inference with wifi-colocation during the covid-19 pandemic, arXiv preprint arXiv:2009.12699 (2020).

[6] H. Li, J. K. Ng, V. C. Cheng, W. K. Cheung, Fast indoor localization for exhibition venues with calibrating heterogeneous mobile devices, Internet of Things 3 (2018) 175–186.

[7] G. Chatzisofroniou, P. Kotzanikolaou, Association attacks in ieee 802.11: Exploiting wifi usability features, in: Socio-Technical Aspects in Security and Trust: 9th International Workshop, STAST 2019, Luxembourg City, Luxembourg, September 26, 2019, Revised Selected Papers 9, Springer, 2021, pp. 107–123.

[8] A. Abedi, D. Vasisht, Non-cooperative wi-fi localization & its privacy implications, in: Proceedings of the 28th Annual International Conference On Mobile Computing And Networking, 2022, pp. 570–582.

[9] D. Halperin, W. Hu, A. Sheth, D. Wetherall, Tool release: Gathering 802.11 n traces with channel state information, ACM SIGCOMM computer communication review 41 (2011) 53–53.

[10] A. Abedi, O. Abari, Wifi says" hi!" back to strangers!, in: Proceedings of the 19th ACM Workshop on Hot Topics in Networks, 2020, pp. 132–138.

[11] R. Schmidt, Multiple emitter location and signal parameter estimation, IEEE transactions on antennas and propagation 34 (1986) 276–280.

[12] S. Sen, J. Lee, K.-H. Kim, P. Congdon, Avoiding multipath to revive inbuilding wifi localization, in: Proceeding of the 11th annual international conference on Mobile systems, applications, and services, 2013, pp. 249–262.

[13] F. Wen, C. Liang, An indoor aoa estimation algorithm for ieee 802.11 ac wi-fi signal using single access point, IEEE Communications Letters 18 (2014) 2197–2200.

[14] K. Jiokeng, G. Jakllari, A. Tchana, A.-L. Beylot, When ftm discovered music: Accurate wifi-based ranging in the presence of multipath, in: IEEE INFOCOM 2020-IEEE Conference on Computer Communications, IEEE, 2020, pp. 1857–1866.

[15] I. C. S. L. S. Committee, et al., Ieee standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications, IEEE Std 802.11ˆ (2007).

[16] B. Lu, L. Wang, J. Liu, W. Zhou, L. Guo, M.-H. Jeong, S. Wang, G. Han, Lasa: location aware wireless security access control for iot systems, Mobile Networks and Applications 24 (2019) 748–760.

[17] Y. Xie, Z. Li, M. Li, Precise power delay profiling with commodity wifi, in: Proceedings of the 21st Annual international conference on Mobile Computing and Networking, 2015, pp. 53–64.

[18] J. Xiong, K. Jamieson, {ArrayTrack}: A {Fine-Grained} indoor location system, in: 10th USENIX Symposium on Networked Systems Design and Implementation (NSDI 13), 2013, pp. 71–84.

[19] M. Kotaru, K. Joshi, D. Bharadia, S. Katti, Spotfi: Decimeter level localization using wifi, in: Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication, 2015, pp. 269–282.

[20] C. Chen, Y. Chen, Y. Han, H.-Q. Lai, K. R. Liu, Achieving centimeter-accuracy indoor localization on wifi platforms: A frequency hopping approach, IEEE Internet of Things Journal 4 (2016) 111–121.

[21] L. Zhang, E. Ding, Y. Hu, Y. Liu, A novel csi-based fingerprinting for localization with a single ap, EURASIP Journal on Wireless Communications and Networking 2019 (2019) 1–14.

[22] F. Gringoli, M. Schulz, J. Link, M. Hollick, Free your csi: A channel state information extraction platform for modern wi-fi chipsets, in: Proceedings of the 13th International Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization, 2019, pp. 21–28.

[23] M. Schulz, D. Wegemer, M. Hollick, Using nexmon, the c-based wifi firmware modification framework, in: Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, 2016, pp. 213–215.