tions, our adversary may want to be classified as colocated from a non-colocated position, or she may want other devices to be classified wrongly. To achieve these goals, she can use the same resources, i.e., hardware and software, as legitimate devices. We further assume that the adversary knows which software and hardware are currently used in a scenario she wants to attack. Finally, our adversary has extensive sensing capabilities, empowering her to gain fundamental findings of the communication, like channel, frame type, and transmission power.

3.3 STUDY DESIGN

In our experiments, we utilize up to 12 Nexus 5 smartphones to gather labeled CSI. More precisely, we configure one device to listen for incoming frames and extract CSI from them. In addition, it labels the data thus obtained as either co-present (label '1') or not co-present (label '0'). This specific Nexus 5 is referred to as *Collector*, while the remaining devices are called *Transmitters* in the following. Depending on the scenario, we place some or all of the *Transmitters* around the *Collector* in spots, representing potential IoT functionality. For instance, a device placed near a screen may simulate a smart workstation, a device on a window sill may represent a smart blinder. Their purpose is to periodically transmit frames as broadcasts which are then processed by the *Collector* as we defined above. In any case, the *Collector* resides at a prominent location within the room (or car). A *Transmitter* counts as co-present if it is in the same room (or car). Devices which are located outside the room (or car) are considered non-colocated. As the content of the frames does not matter in our experiments, we limit ourselves to sending smaller IEEE 802.11 QoS frames (approximately 100 Bytes) in order to allow higher transmission rates. Previous results show that our application, in combination with the current version of our firmware, can extract CSI of up to 20 frames per second using this frame size. Therefore, we limit the transmission rate of a single *Transmitter* to 3 frames per second at a maximum. This is a tradeoff between a good utilization of the maximum collection rate on the one hand and the loss of as few frames as possible on the other hand. However, frames may still get lost due to random overlaps of arrival times at the *Collector*.

In order to keep the labeling process as effortless as possible, we define which of the *Transmitters* are considered co-present (e.g., inside the same room as the *Collector*) at the start of every collection round. If the *Collector* receives a message from a device which has not been identified as co-present beforehand, it will automatically assign the label '0' (non-colocated) to the CSI extracted from that message. The list of colocated devices must be reviewed (and if necessary updated) as the role of the *Collector* is assigned to a new device (i.e., in the phase between two collection rounds).

Our experiments consider carrier frequencies from both 2.4 GHz and 5 GHz bands. Hereby we have to keep in mind that, when using a frequency from the 5 GHz band, the distance between *Collector* and *Transmitter* may not exceed certain limits. Otherwise, the *Collector* cannot receive any frames. For 2.4 GHz, we test different channels (e.g., channel 1, 5, 7, and 13). We observe that the collection runs most stable on channel 1. Hence, we decide to use this channel in our 2.4 GHz experiments.
In order to evaluate which area can be covered by our 5 GHz experiments, we test various channels from the 5 GHz band in matters of the maximum distance between *Collector* and *Transmitter* that still allows us to collect CSI. For channel 116, we observe the following: in the case of a clear line-of-sight between sender and receiver, the distance may be seven meters at most. If there is only a small barrier between them (like a wooden door), the maximum distance reduces to five meters and it decreases further, the thicker the obstacle is: if we place two devices with a 30 cm wall in between, we can only receive a signal at a distance of about three meters. As this was a limiting factor for the scenario design of our study, we test further channels. Fortunately, it turns out that channel 157 allows longer distances between sender and receiver. Thus, we can define similar scenarios for our experiments in both bands:

1. **Urban office:** We collect CSI in an office of our university. As we expect the highest rate of motion and environmental change in general here, we consider this scenario the most challenging.

2. **Urban flat:** This scenario is representative of a domicile in Darmstadt. It is less busy than the office, but still subject to certain changes in environmental conditions due to higher population density in the urban environment.

3. **Rural flat:** We also collect CSI in a non-urban environment. In particular, this is a medium-sized two-room apartment which is inhabited by only a single person. We expect only minor changes to the environment and little movement here compared to office and urban flat scenarios.

4. **Parking cars:** Our third scenario consists of two cars which are parked close to each other. The phones are placed at distinctive spots inside the cars to simulate smart equipment with communication interfaces (e.g., smart dashboard).

5. **Cars in motion:** Finally, we also accumulate CSI for the case that the cars are not static but driving close to each other.

In each of the scenarios described above, we place a number of Nexus 5 smartphones at prominent spots. These spots are at predefined locations which do not change during the experimental run.

Mobile devices are not considered in our study design. To perform a complete experiment within a certain scenario, we conduct several *CSI aggregation rounds*. The number of *CSI aggregation rounds* to be carried out corresponds to the number of smartphones used in the experiment. A single *CSI aggregation round* includes the following steps:

1. Define one device as *Collector*, the remaining devices send broadcast messages and are hence *Transmitters*.
2. Configure the *Collector* to label CSI which is received from copresent devices with '1' and any other CSI with '0'.
3. Start the collection procedure.
4. Interrupt the collection procedure after a predefined time t which is equal for all *CSI aggregation round* of an experiment.

In order to reduce the effort for the composition of a single *CSI aggregation round*, devices which are *Transmitters* in two consecutive runs do not have to be restarted but can keep on sending while the *Collector* is prepared. However, in order to avoid unpredictable behavior, we agree to restart a *Transmitter* at the latest after one hour of sending. An experiment is complete once all devices of the scenario have participated in a *CSI aggregation round* as *Collector*.
The environment may change while CSI is gathered: People may walk around, sit down, get up or move items. Varying environmental conditions may result in different degrees of difficulty regarding the classification task. Taking this assumption into consideration, we define various experimental setups, depending on the requirements we identify for a scenario. We discuss the requirements and the resulting experimental setups in the following.

3.3.1 *Urban office scenario*

Our first scenario incorporates three offices located nearby (Figure 3.2). Its neighborhood of this building is characterized by a high fluctuation of human beings and vehicles, or, to sum it up, the environmental conditions are constantly changing. The same applies to the office rooms of our scenario. In particular, we consider three office rooms which are spatially close to each other and which are separated only by a hallway or a wall. Although we merely observe three rooms with our CSI measurements, these are surrounded by other offices. It is the aim of our experiment to aggregate CSI that is recorded during all the characteristic actions of a working day, hoping that subsequently, every action will be uniquely identifiable by its corresponding CSI. Of course, as this is a very dynamic setting, the characteristic actions which we can observe are dependent on the time of the day: in the early morning, many offices will probably be unoccupied. We can assume that at this

time fewer people will be in the monitored rooms, and fewer people walking along the hallway between the offices. Consequently, there will be fewer obstacles between *Transmitters* and *Collector*. During the remaining day, we expect typical office activities: employees who are walking towards the offices of their colleagues, temporarily increased numbers of persons due to meetings in certain offices, the slowdown at lunchtime and speed-up thereafter, office doors and windows which are opened and closed, and so on. Finally, most employees leave in the afternoon so that we observe a setup similar to the morning hours.
Thus, it becomes clear that our chosen scenario is subject to a constant change in terms of its composition. In addition to the difficulties described above, which are caused by the movement of people, the setup of the offices is constantly changing, for example, due to experiments conducted by the employees. We can hence assume that the classification task will be more challenging in this scenario than in the other ones. We highlight the complexity with an example: two phones reside in different offices, they are not co-present consequently. The offices are located exactly opposite, separated only by the hallway. We further assume that the phones are in the line of sight to each other, if the doors of both offices are open. In addition, there is at least one more phone in both offices so that we can also collect CSI from a co-present device. We start the collection of CSI for a certain period of time. By chance, at least one door is closed during the entire collection phase. This may occur, for example, if the employee of one office is sick on the day of the experiment. After finishing the collection, we use the CSI thus obtained as the training set for a classifier. Finally, we try to use this classifier in the same scenario to decide whether a device is co-present or not. However, the imaginary employee who was ill the day before is well again and hence the doors of both offices are open, there is no obstacle between the devices of both offices anymore. We cannot rule out that the CSI received from a device of the other office is now more similar to the CSI from our training set labeled as co-present than to the CSI extracted from a message which had to pass an obstacle (i.e., the door which was formerly closed). In such a situation, it is likely that the classifier will decide incorrectly. But even if the training set contains CSI examples which were recorded with open doors, it may still be hard for a classifier to predict correctly. If messages of both a colocated and a non-colocated device have to travel a similar distance without any door or wall in between, will the resulting CSI differ enough to predict accurately?
In conclusion, we can already presume that the classification task will not be trivial in this scenario. If we aim for high classification accuracy, we will have to take care that the dataset is as extensive as possible, covering many special cases of an office's daily routine. In order to describe the office scenario reliably in CSI, we will have to take a snapshot of the current state from every collection spot at each

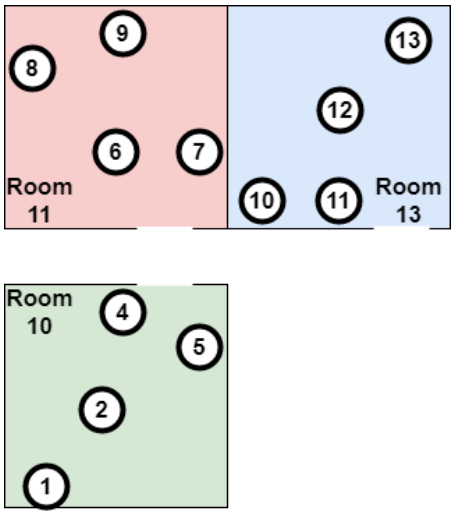

Figure 3.2: Setup of the office scenario

time of the day. In particular, we define four time slots for the collection of CSI: *Morning, afternoon, evening* and *night/weekend*. We expect varying compositions of our scenario in terms of employee density and dynamic, depending on the time slot. Furthermore, we will have to use the whole set of available phones in order to get CSI from as many points of the offices as possible. Considering all these aspects, we create a setup for the experiment which is illustrated in Figure 3.2. Figure 3.2 shows a map of the three offices we conduct our experiments in. Rooms 11 and 13 are on the same side of the hallway, room 12 is opposite of them. We distribute the available devices uniformly over the office rooms we want to observe. Within each office, we look for prominent spots and try to distribute the phones evenly over the available area. Devices placed in these spots represent potential IoT applications. For example, a device close to the window may simulate a smart window sill which regulates the jalousie. A device placed next to a monitor may simulate the controls of a smart screen, which is automatically locked when the user leaves the workstation.
CSI also depends on the elevation as placing devices lower or higher changes the propagation path. Hence, our setup takes different elevations into account. Considering these requirements, we define the following prominent spots for the office experiment:

1. **Window:** One device is placed on a window sill of every office to make sure that our experiment covers the maximum distance between opposite offices. The corresponding spots in Figure 3.2 are 1, 9 and 13.

2. **Table:** Phones lying on tables are ubiquitous in everyday life and must therefore be taken into account. In Figure 3.2, the respective positions are 2, 6 and 12.

3. **Drawer:** The height of the drawers used as prominent spots in our experiment is similar to the height of a phone being carried in a person's hand or pocket. Thus, it is meaningful to collect CSI at this height. The drawers of our office experiment are at positions 5, 7 and 11.

4. **Cupboard:** Eventually, we also want to consider a height on which phones are usually rare. As most obstacles like monitors or drawers are commonly lower, we expect different propagation paths for frames from and to this spot. The respective phones are placed at the spots 4, 8 and 10.

With the setup shown in Figure 3.2, we cover the special case mentioned above: in the case that the doors (illustrated with white gaps in Figure 3.2) of offices 10 and 11 are open, devices 5 and 6, which belong to different offices, are in the line of sight to each other, without any obstacles in between.
In order to record CSI from any of the offices at any time of the day, we need to run experiments on several days, while changing the collection order: on the first day, we start collecting in office 10 in the morning. Subsequently, we run the collection in office 11, covering the afternoon slot. Our final collection round of the first day is performed in office 13 during the time slot in the evening. Acting this way, it takes three days to combine all of our offices with the three time slots *morning*, *afternoon* and *evening*. Additionally, we want to consider the night/weekend as a time slot. Night and weekend are comparable, as there are hardly any employees in the offices and hence there is almost no change. For each experiment, we define a unique name which will be part of any file a *Collector* produces (see Section 4.2.1). Table 3.1 gives an overview of the experiments we will have to conduct in this scenario. All names follow the same scheme. The first number (10, 11 or 13) is the office in which the *Collector* resides. The following letter (**m**orning, **a**fternoon, **e**vening, or **n**ight) determines the time of the day at which the *CSI aggregation round* is performed. Finally, the last part describes the position of the *Collector* within the office. They correspond to the spots presented in the enumeration above.

For the experiments using the 2.4 GHz band, we define 35 minutes as time t of a single *CSI aggregation round* and we reduce t to 25 minutes when using a carrier frequency from the 5 GHz band. The reduction of t for 5 GHz is due to the major bandwidth and the increased amount of data we get from a single CSI record therefore: The bandwidth we use for the 2.4 GHz experiments is 20 MHz, which means that the signal is spread over 64 subcarriers. Our extractor generates CSI on per subcarrier basis, i.e., we get a respective value of magnitude and phase shift for any of them. Hence, a single CSI record contains $2 * 64 = 128$ values for 2.4 GHz. For the 5 GHz experiments, we use a bandwidth of 80 MHz, the signal is spread over 256 subcarriers.

Collector	Day 1	Day 2	Day 3	Night
1	10-m-win	10-a-win	10-e-win	10-n-win
2	10-m-tab	10-a-tab	10-e-tab	10-n-tab
4	10-m-cup	10-a-cup	10-e-cup	10-n-cup
5	10-m-drw	10-a-drw	10-e-drw	10-n-drw
6	11-a-tab	11-e-tab	11-m-tab	11-n-tab
7	11-a-drw	11-e-drw	11-m-drw	11-n-drw
8	11-a-cup	11-e-cup	11-m-cup	11-n-cup
9	11-a-win	11-e-win	11-m-win	11-n-win
10	13-e-cup	13-m-cup	13-a-cup	13-n-cup
11	13-e-drw	13-m-drw	13-a-drw	13-n-drw
12	13-e-tab	13-m-tab	13-a-tab	13-n-tab
13	13-e-win	13-m-win	13-a-win	13-n-win

Table 3.1: Experiment names of the office scenario

Hence, we would ideally obtain $2 * 256 = 512$ values per CSI record which is four times the value of 2.4 GHz.
As we do not expect the office environment to change significantly during the night/weekend experiment, we assume that it is sufficient to set t to 20 minutes for both 2.4 GHz and 5 GHz. All in all, the setup described above results in a total collection time of $3 * 12 * 35\text{min} + 3 * 12 * 25\text{min} + 2 * 12 * 20\text{min} = 2640\text{min} = 44\text{h}$.

3.3.2 *Urban flat scenario*

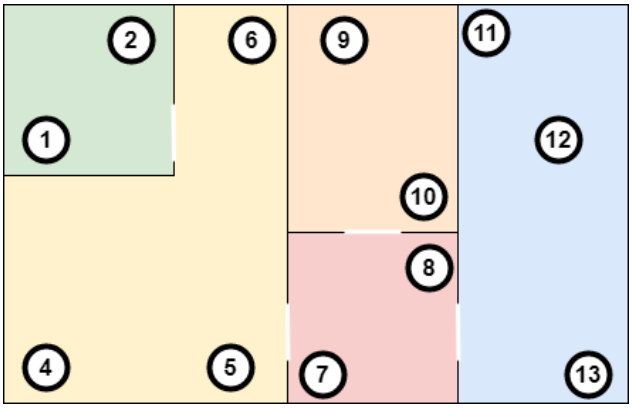

Figure 3.3: Setup of the urban flat scenario

Our second scenario for CSI collection is a flat in Darmstadt. It is inhabited by one person. We assume less environmental changes here compared to the office scenario. However, the flat is located in a densely populated city, and we do not know how a busy environment

affects CSI. We therefore decide to use the full set of available phones again. Figure 3.3 shows the resulting setup for our experiment. The flat consists of five rooms: a small kitchen (green area in Figure 3.3), living room (yellow area), bathroom (orange area), bedroom (blue area), and a hall connecting living room, bathroom, and bedroom (red area). As we want to picture the entire flat in CSI, we place smartphones in every room. The maximum number of available devices is 12, which is not divisible by five. Hence, we place at least two devices in each room. In order to obtain both negatively (label '0') and positively (label '1') labeled data in each *CSI aggregation round*, it is very important to have at least two devices in each room to be pictured. Apparently, a smartphone being the only device in a room would not be able to collect positively (label '1') labeled data during its *CSI aggregation round* as no device is colocated. In the living room and in the bedroom, we place one additional phone respectively because they are the flat's largest rooms.
As in the previous scenario, we look for prominent spots in every room to place the available phones. The device numbers of the following enumeration refer to Figure 3.3:

1. **Kitchen:** We place the devices with numbers 1 and 2 in the kitchen. Device 1 is placed close to the kitchen window, device 2 on a cupboard.

2. **Living room:** Devices 4, 5 and 6 are in the living room. More precisely, device 4 is put on a sofa, device 5 on a wardrobe, and device 6 on a box.

3. **Bathroom:** The devices of this room are placed on the window sill (device 9) and the mirror shelf (device 10).

4. **Bedroom:** We place device 11 on a drawer, device 12 on the bed, and device 13 on a cupboard.

5. **Hall:** One device is put on a wardrobe (device 7), the second device on a shelf (device 8).

Again, we assign unique names to the *CSI aggregation rounds* of every *Collector*. They are shown in Table 3.2. Since we do not consider the time of the day here, the experiment names consist of only two components. The first part is determined by the room of the *Collector*, the second part by its position within the room (as described above).
We use the same setup for our experiments in both bands. However, we can already assume that with this setup, some phones may not be able to receive frames from parts of the other devices. Even if we ignore further obstacles like the furniture, a frame must still pass four walls on its way between devices 2 and 13 for example. Similarly, there are two or three walls on the transmission path between many other devices, as shown in Figure 3.3. We hence expect problems with the

Collector	Experiment name	Collector	Experiment name
1	kitchen-win	2	kitchen-cup
4	living-sofa	5	living-war
6	living-box		
7	hall-war	8	hall-shelf
9	bath-sill	10	bath-mshelf
11	bed-drw	12	bed-bed
13	bed-cup		

Table 3.2: Experiment names of the urban flat scenario

receptivity of some devices, especially for our 5 GHz experiment.
One difficulty of this scenario is the increased number of rooms to be pictured in CSI. We try to cope with this challenge by using all available devices. Apart from that, we consider this scenario less challenging than our office scenario. The flat is only inhabited by one person. Therefore, the setup is less dynamic compared to the office scenario at working hours, which is influenced by an unpredictable number of participants, i.e., persons that are in the offices or walk along the hallway. However, the urban flat scenario has many similarities with the night/weekend experiment of the office scenario in terms of dynamic and setting, i.e., an urban environment. We therefore decide to use the same time t for a single *CSI aggregation round* as in the night/weekend experiment of the office scenario, which is 20 minutes. The time we need to perform a *CSI aggregation round* on each of the 12 phones involved in our setup is $12 * 20\mathrm{min} = 240\mathrm{min}$. Again, we want to conduct experiments in both 2.4 GHz and 5 GHz bands. Hence, the total collection time of the urban flat scenario results in $2 * 240\mathrm{min} = 480\mathrm{min} = 8\mathrm{h}$.

3.3.3 *Rural flat scenario*

In our third scenario, we collect CSI in a flat again, which is also inhabited by only one person. Figure 3.4 shows the flat's outline. In detail, it consists of a larger living area (green area in Figure 3.4) and a small bathroom (red area).
In contrast to the previous scenario, this flat is located in a village in the countryside, not in a densely populated city. Thus, we do not expect many changes in the environment of the flat and in the flat itself. Additionally, the flat consists of only two rooms and has less living space compared to the urban flat of the previous scenario. For these two reasons, we consider the classification task to be the easiest so far. We therefore assume that the classification is feasible with fewer

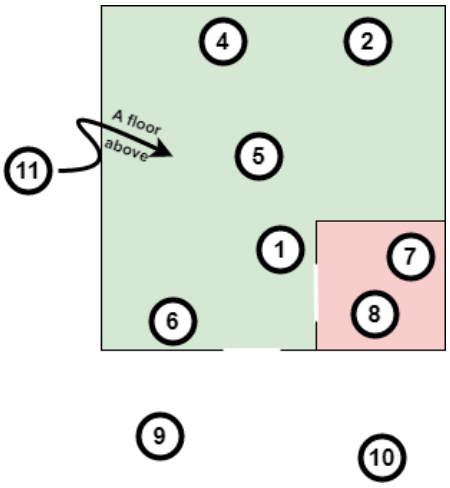

Figure 3.4: Setup of the rural flat scenario

data here, which is why we do not necessarily have to use the full set of available devices. In particular, we place devices as follows (Figure 3.4):

1. **Living area:** All in all, we put five devices here. Device 1 is placed on a box, device 2 on a window sill, device 4 on a desk, device 5 on a table, and device 6 on a shelf.

2. **Bathroom:** Device 7 is put on the closed toilet lid and device 8 on the mirror shelf. We consider two devices sufficient as the bathroom is very small.

3. **Further devices outside the flat:** In order to obtain more negatively labeled data, we place two more devices (numbers 9 and 10) in the stairway in front of the flat's entrance door. Since we have access to the floor above the flat, we also put one device (number 11) there.

Since this is the first experiment we conduct, and since our findings of which channels are reliable come from this scenario, the channel under usage is part of the experiment name. More precisely, the first part of the name is the channel used for collection. As we want to use channel 1 for the 2.4 GHz experiments and channel 157 for the 5 GHz experiments, the respective experiment names start correspondingly. The second part is just *col* (an abbreviation of *Collector*) and the device number. Thus, the experiment names of the *CSI aggregation round* in which device 1 is *Collector* are *1-col1* for 2.4 GHz and *157-col1* for 5 GHz. A more complex naming scheme is not necessary here due to the simplicity of the setup.
We use 20 minutes as time t of a *CSI aggregation round* again. Apparently, we only have to conduct a *CSI aggregation round* for devices inside the flat. This results in a total collection time of $2 * 7 * 20\mathrm{min} = 280\mathrm{min} = 4.7\mathrm{h}$ for our experiments in both bands.

3.3.4 *Automotive scenarios*

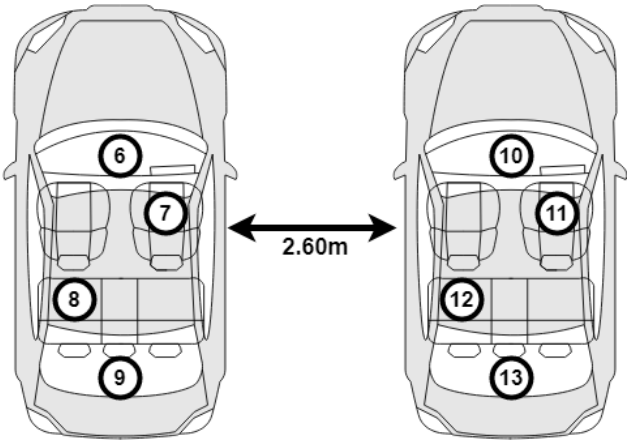

Figure 3.5: Setup of the parking car scenario

In the previous scenarios, static *Collectors* gather CSI from also static *Transmitters* in more or less changing environments. However, we also want to investigate the impact of the movement of *Collectors* and *Transmitters* on the resulting CSI. We consider an automotive scenario for this purpose. In times of smart cars, and possibly soon self-driving cars in everyday life, a ZIA scheme based on CSI may contribute to the further automation of driving, while improving the comfort. For example, we could think of a system that automatically reads the destination after detecting a legitimate user's presence within the car, and that subsequently starts driving to that destination autonomously. In order to determine the influence of the movement on CSI, we start with a static setup (Figure 3.5): two cars are parked side by side, only a few meters apart from each other. We place four devices in prominent spots within each car. These spots are the dashboard (devices 6 and 10 in Figure 3.5), the front passenger's seat (devices 7 and 11), the backseat behind the driver (devices 8 and 12), and the trunk (devices 9 and 13). Table 3.3 shows the unique names we assign to the individual *CSI aggregation rounds*. The name consists of the car number the *Collector* is located in and its position within the car. We use the same naming scheme for our experiments in both bands.

As only eight phones are involved in this setup, and as CSI thus obtained should serve mainly for comparison, time t is 10 minutes per *CSI aggregation round*. The total time we need to conduct the parking car experiments is thus $2 * 8 * 10\text{min} = 160\text{min} = 2.7\text{h}$.

Afterwards, we use the same setup for our experiment with the cars in motion. Both cars drive the same route. We try to keep the distance between them as little as possible. Moreover, we try to stay right behind each other, i.e., with no other car in between. At the end of each *CSI aggregation round*, we stop the cars, reset the phones if necessary, start the *CSI aggregation round* of the next device, and finally start driving

Collector	Experiment name	Collector	Experiment name
6	1-dash	7	1-front
8	1-back	9	1-trunk
10	2-dash	11	2-front
12	2-back	13	2-trunk

Table 3.3: Experiment names of the automotive scenarios

again. Our aim is to collect CSI during a realistic journey, i.e., we drive on different types of roads at appropriate speeds. However, due to safety reasons, cars must keep a certain distance at higher speeds. We hence decide to drive 80 kilometers per hour at most. Even with this limitation, concentrated driving is necessary in order to keep the distance required for our experiment in the presence of obstacles such as traffic lights, and the traffic itself. We set time t to 20 minutes for this setup, resulting in $8 * 20\mathrm{min} = 160\mathrm{min} = 2.7\mathrm{h}$ per experiment in one band.
Ideally, we would conduct identic experiments in both bands again. With the above setup, however, the distances may become too big to receive frames from the other car when using a carrier frequency from the 5 GHz band, due to the reduced transmission range. In this case, we would have to reduce the maximum speed to such an extent that very small distances can be kept without any risk for the drivers. The use of busy roads would therefore be no longer possible. In fact, a test run shows that we hardly receive any frames from the other car when driving as described above. Hence, we reduce the maximum speed to 20 kilometers per hour for the 5 GHz experiment. Since we will have to drive on completely untraveled roads to be able to keep such a low speed for a longer time, we do not expect the cars' relative positions to change significantly during the experiment. Therefore, we assume that 10 minutes per *CSI aggregation round* suffice to describe the scenario in CSI. This results in a collection time of $8 * 10\mathrm{min} = 80\mathrm{min} = 1.3\mathrm{h}$ for the 5 GHz experiment, and $160\mathrm{min} + 80\mathrm{min} = 240\mathrm{min} = 4\mathrm{h}$ for the moving car scenario in total.

3.3.5 *Additional scenarios*

With respect to our threat model, we define two additional scenarios. Since we assume that our adversary possesses the same software and hardware as a legitimate user, she may try to fool the ZIA scheme by sending a different type of frame. Hence, we introduce a *beacon scenario*. In this, we examine the impact of a different frame type on the resulting CSI. More precisely, we want to investigate how the system behaves with heterogeneous frames. The setting is identic with

Collector	Experiment name	Collector	Experiment name
1	10-beac-win	2	10-beac-tab
4	10-beac-cup	5	10-beac-drw
6	11-beac-tab	7	11-beac-drw
8	11-beac-cup	9	11-beac-win
10	13-beac-cup	11	13-beac-drw
12	13-beac-tab	13	13-beac-win

Table 3.4: Experiment names of the beacon scenario

the office scenario. We use the same number of devices and place them according to Figure 3.2. In contrast to the office scenario, the *Transmitters* send beacon frames instead of QoS data frames. Moreover, we do not consider the time of the day and perform only one *CSI aggregation round* per device. In Table 3.4, we define names for the *CSI aggregation rounds* depending on the *Collector*. The naming follows the same scheme as in the office scenario, we only replace the time of the day with *beac*. Furthermore, we assume that our adversary has extensive sensing capabilities. Thus, she knows the power which the legitimate devices use for transmission, and may try to fool the ZIA system by sending with a higher power. The signal strength decreases with a rising distance between *Collector* and *Transmitter*. Sending from a non-colocated position, the adversary can use a higher transmission power to generate a signal strength at the *Collector's* position similar to that of a colocated device.
In order to evaluate whether such an attack is feasible, we define a *power scenario*. Again, it uses a similar setting as the office scenario, i.e., 12 devices distributed over three offices (Figure 3.2). However, we configure only four devices to send with the default transmission power (devices 10-13). These four devices are the only to collect CSI here. The remaining devices are configured to send with higher transmission power. They always send from non-colocated positions: after we have finished all *CSI aggregation rounds* of one office, the collecting devices change positions with the devices from another office. Each device retains its relative position within an office, e.g., a device located on the window sill in office 10 is also placed on the windows sill in office 11. Table 3.5 summarizes the names of the experiments to conduct in this scenario and defines which device is *Collector* in a certain position within an office. The position numbers refer to Figure 3.2.

In both of our additional scenarios, we use 20 minutes as time t of a *CSI aggregation round*. Since it is the same time as in the night sessions of the office scenario, we can compare the obtained datasets afterwards. We conduct experiments in both bands again. In conclusion, this leads

Collector	Experiment name	Collector	Experiment name
13 (pos 1)	10-p-win	12 (pos 2)	10-p-tab
10 (pos 4)	10-p-cup	11 (pos 5)	10-p-drw
12 (pos 6)	11-p-tab	10 (pos 7)	11-p-drw
10 (pos 8)	11-p-cup	13 (pos 9)	11-p-win
10 (pos 10)	13-p-cup	11 (pos 11)	13-p-drw
12 (pos 12)	13-p-tab	13 (pos 13)	13-p-win

Table 3.5: Experiment names and positions of the power scenario

to a total execution time of $2 * 2 * 12 * 20\mathrm{min} = 2 * 480\mathrm{min} = 2 * 8\mathrm{h} = 16\mathrm{h}$.

3.3.6 *Summary*

Table 3.6 summarizes our study design. All in all, we want to conduct experiments in seven different scenarios. We will have to perform 214 *CSI aggregation rounds* of different lengths. The pure collection time which is necessary to conduct all of the experiments is 79.4 hours.

Scenario	Devices	Time per round		Total
		2.4 GHz	5 GHz	
Office	12	35/20min	25/20min	44h
Urban flat	12	20min	20min	8h
Rural flat	10	20min	20min	4.7h
Parking cars	8	10min	10min	2.7h
Moving cars	8	20min	10min	4h
Beacon	12	20min	20min	8h
Power	12	20min	20min	8h
				79.4h

Table 3.6: Summary of study design and collection times