Investigation of Anomaly-based Passive Localization with Received Signal Strength for IEEE 802.15.4

Marco Cimdins*, Mathias Pelka* and Horst Hellbrück*

*Lübeck University of Applied Sciences, Germany
Department of Electrical Engineering and Computer Science
Email: marco.maris.cimdins@stud.fh-luebeck.de, mathias.pelka@fh-luebeck.de, hellbrueck@fh-luebeck.de

Abstract—Localization has important applications, for instance intrusion detection and elderly care. Such applications benefit from Device-free passive (DfP) localization systems, which employ received signal strength measurements (RSSM) to detect and track entities that neither participate actively in the localization process nor emit signals actively. RSSMs include received signal strength indicator (RSSI), energy detection (ED) and link quality indicator (LQI) measurements. This paper compares different packet-based RSSMs for DfP localization and presents detection results of a DfP anomaly-based detection system employed by IEEE 802.15.4 compliant devices. Furthermore, we investigate techniques for anomaly detection with continuous RSSM measurements.

Index Terms—Device-free passive localization, IEEE 802.15.4 anomaly detection, received signal strength

I. INTRODUCTION AND RELATED WORK

Device-free passive (DfP) localization systems detect, track and identify entities with the help of wireless networks e.g. IEEE 802.11 [1]. DfP localization systems assume that entities e.g. humans or objects in the target area influence radio frequency (RF) signals which are measured in return. Entity motion within the target area causes fluctuations of received power which are recorded by received signal strength measurements (RSSMs). Further processing of the values identifies anomalous behavior of the RF signal. We introduce RSSM as a general term for input values of an DfP localization system. RSSMs are commonly available for IEEE 802.15.4 RF chips: Received signal strength indicator (RSSI), energy detection (ED) and link quality indicator (LQI). DfP localization systems such as Horus [2] and Nuzzer [3] were proposed in the past. They employ fingerprinting for localization of an entity within a target area. The main disadvantage of fingerprinting is that it requires a training, such as a creation of a passive radio map. Changes of the environment e.g. temperature or humidity result in different RSSMs compared to measurements of the training period. This results in an overall reduced system performance.

The RASID system [4] introduced anomaly-based detection, which was later adopted and enhanced with the ability to track entities via a particle filter algorithm in Ichnaea [5]. RASID requires a short training period where a silence profile is measured in the room without the entity. Continuous adaption of the silence profile with measurements with absence of an entity in the target area, increases robustness for changes in the environment. This approach has been implemented and tested with IEEE 802.11 devices.

In our work, we investigate anomaly-based DfP localization with IEEE 802.15.4 compliant devices. And we aim to find the best packet-based RSSM for DfP systems and to improve the ability to detect the presence of an entity within the target area of the system.

We implement two different systems for different purposes: The first one serves to find the best RSSM for our DfP localization system and contains several IEEE 802.15.4 tranceivers that send packets and measure the RSSM on arrival. The second one investigates continuous RSSM measurements in order to opportunistically use RF signals sent out by other wireless systems for the use in DfP localization systems. This system contains IEEE 802.15.4 receivers and an IEEE 802.11 access point (AP). The contributions of this paper are:

- Comparison and evaluation of RSSMs e.g. RSSI, ED and LQI values for DfP localization systems.
- Implementation and evaluation of an anomaly-based detection for DfP localization with IEEE 802.15.4.
- Comparison and evaluation of continuously measured received signal strength (RSS) values in comparison with packet-based RSSM.

The rest of the paper is organized as follows, Section II introduces different RSSMs, principles of DfP systems and the approach of the underlying anomaly-based DfP localization system. In Section III the implementations with IEEE 802.15.4 are described and compared with each other. Section IV presents the preliminary evaluation results. Finally, we provide a summary and an outlook for future work in Section V.

II. APPROACH & SYSTEM DESCRIPTION

This section describes how entity motion affects RSSMs, introduces the experimental setup and finally explains the DfP anomaly detection system.

A DfP system assumes that received RF signal power changes – either increases or decreases – when an entity moves within a target area. During RF signal propagation, reflection, scattering and diffraction occurs and results in multi-path phenomena. Devices receive signals from different paths and therefore measure different RSSM values. In Figure 1a each dashed line indicates the line-of-sight (LOS) between the transmitter and monitoring point (MP) which are transceivers within the system. An entity near to the LOS of the stream typically changes the RSSM and therefore causes large changes in the values.
Common parameters for IEEE 802.15.4 radios for RSSM include RSSI, ED and LQI. RSSI is an integer value that represents the RSS measured by the radio chip. ED is the mean of RSSI values over 8 symbol periods. LQI is a measure of the link quality. Section IV-B shows the comparative results for suitability in DfP localization systems.

Current DfP localization systems e.g. RASID or Ichneumon, employ packet-based RSSMs. On reception of a packet, RSSMs such as the RSSI, are created by the radio chip and processed further. For a continuous transmission of packets, a stream of RSSM values is available. Figure 1a shows the testbed that is used to find the best packet-based RSSM for our IEEE 802.15.4 DfP localization system.

In contrast to existing work, we investigate opportunistic signals that are transmitted by other wireless systems, for instance from a 2.4 GHz IEEE 802.11 AP and determine the change of the RF signal levels while only listening to a channel. We record the RSSI to identify transmitted packets and use those values to detect motion of an entity within the target area. This investigation is motivated by employing already available RF signals for the DfP localization system instead of transmitting new packets in the already crowded 2.4 GHz ISM-band. Figure 1b shows the testbed for the investigation and Section IV-A presents preliminary results.

![Testbed for packet-based RSS measurements.](image1)

![Testbed for continuous RSSI measurements.](image2)

(a) Testbed for packet-based RSS measurements.
(b) Testbed for continuous RSSI measurements.

Fig. 1: Setup of the two testbeds.

Anomaly detection was first introduced by Kosba et al. for DfP localization systems in [4] and is described in more detail in [5]. We implemented the same steps, namely: 1. Calculate the variance from a time window $W_{j,t}$. 2. Estimate the probability density function (PDF) $\hat{f}_j$ of the silence period. 3. Calculate an upper bound $u_{j,t}$ based on the PDF of the silence period. 4. Calculate the anomaly score $a_{j,t}$. 5. Calculate the (smoothed) global anomaly score $B_t$.

Every step is done for each stream $j$, where $s_{j,t}$ is the RSSM at time $t$ for stream $j$. Instead of calculating the variance from a sliding window as described in [4], we calculate the variance in blocks. This reduces the number of calculations significantly. A window of size $l$ that ends at time $t$ is studied, so $W_{j,t} = [s_{j,t-l+1}, s_{j,t}]$. The function $g(W_{j,t})$ calculates a single feature $x_{j,t}$ for every window $W_{j,t}$. We follow the recommendation of [4], [5] and limit the investigation to the variance. Literature suggest the variance as a feature for processing of the raw RSSM. Variance is a suitable indicator for the change of the values caused e.g. by entity motion [1], [3], [4], [5]. As suggested in [4] a silence profile needs to be recorded in order to detect the motion of an entity. The silence profile is created by measuring the distribution of the variances for each stream in the target area. For each stream $j$ with a set of windows $n$, we calculate the variance $x_{j,t}$ for the time window $W_{j,t}$ of the signal. With $f_j$ as the density function, the estimated density function $\hat{f}_j$ is given by:

$$\hat{f}_j(x) = \frac{1}{nh_j} \sum_{t=1}^{n} V \left( \frac{x - x_{j,t}}{h_j} \right).$$ (1)

With $h_j$ as the bandwidth and $V(\cdot)$ the kernel function. A kernel density estimator is used to calculate the estimate of the PDF of the silence period. As stated in [4], an exact estimate of the PDF is not necessary so for the kernel function the Epanechnikov kernel was chosen, because it is bounded and efficient to integrate:

$$V(q) = \begin{cases} \frac{3}{4}(1-q^2), & \text{if } |q| \leq 1, \\ 0, & \text{otherwise.} \end{cases}$$ (2)

To determine whether an entity is present an upper bound is calculated from the PDF of the silence period [4], [5]. Assume $F_j$ is the cumulative distribution function (CDF) of $\hat{f}_j$ with $\alpha$ as the significance parameter. The upper bound $u_j$ is calculated as $u_j = F_j^{-1}(1-\alpha)$. It is the $100(1-\alpha)$th percentile of the CDF $F_j$. The detection works as follows: According to [4], [5], a stream $j$ is considered anomalous when $x_{j,t} > u_j$. To measure the significance of the anomalous activity for each stream $j$, the anomaly score $a_{j,t}$ is calculated as follows:

$$a_{j,t} = \frac{x_{j,t}}{u_j}, \quad \text{where} \quad \begin{cases} a_{j,t} < 1, & \text{if no anomaly is detected}, \\ a_{j,t} \geq 1, & \text{if anomaly is detected}. \end{cases}$$ (3)

The anomaly score also serves as a normalization between the measurements of the different MPs and their own upper bounds. Different from [4], [5], we calculate the global anomaly score by averaging all the anomaly scores for each stream (in comparison by summing up all the anomaly scores from each stream $j$). This simplifies the detection of anomalous behavior, because this enables to compare the values to a normalized threshold (e.g. $a_t \leq 1$). In order to use the history of entity activities, and smoothing the possibly noisy signal samples, exponential smoothing is used [4], [5]:

$$B_t = (1-\beta)B_{t-1} + \beta a_t, \quad B_0 = a_0.$$ (4)

III. IMPLEMENTATION

Our testbed contains IEEE 802.15.4 compliant devices with an Atmel AT86RF233 radio chip that is controlled by an ATXmega128A1. For the tests, the MPs are connected to a laptop via a serial port. Figure 1 shows the floor plan of the area of interest. The target area is a laboratory room of the
Fachhochschule Lübeck with tables and lab equipment — that produce multipath conditions.

The implementation for a packet-based measurement (Figure 1a) is as follows: The MPs wait for the transmitter to send a message. When an MP detects a start of a packet, it measures the RSSI and generates the ED and LQI automatically. Note: For a better comparison the ED and RSSI values will be converted into RSS values in dBm. At the end of the packet, the RSSM and the source address of the corresponding packet are saved and the MP enters the listen state.

For a continuous measurement (Figure 1b), a different implementation is used: Note: For the measurement it is important that devices listen on an IEEE 802.15.4 channel that overlaps with a WLAN channel. So the MPs listen on IEEE 802.15.4 Channel 17, while the laptop creates traffic on WLAN Channel 6. Every 33 µs the RSSI is continuously measured and finally sent via the serial port to the laptop, which results in approx. 30000 values per MP each second. This high measurement rate is necessary to detect and display the packets that have been sent by e.g. WLAN AP.

IV. EVALUATION

This section presents preliminary measurement results of continuous RSSI measurements, followed by a comparison of the different RSSMs. Finally, we discuss the anomaly detection system on our IEEE 802.15.4 compliant hardware.

A. Evaluation of continuous RSSI measurements

![Fig. 2: The RSSI values from the measured WLAN packets over time.](image)

![Fig. 3: Variance of the continuous RSSI measurement.](image)

In this section we evaluate the continuous RSSI measurement from the testbed shown in Figure 1b. Figure 2 shows RSS values of the measured packets. Current DfP localization systems transmit signals in order to measure a change in the RSSM when an entity is present. Thus, establishing high traffic for DfP localization might block the channel for other communication purposes.

Processing continuously measured RSSMs is a challenging task: For each MP, we measure the target area with and without entity motion. It is not possible to create a silence profile, because it is not possible to determine if a packet was sent, which results in a high variation of the RSS. The variances are calculated out of a time window over the raw data with the length $l$ — in our case $l$ was chosen heuristically as 100. The variances from the silence period doesn’t differentiate from the variances of the normal operation — as already explained. This is shown in Figure 3, from 0 s – 100 s was the silence period and a person was moving in the room from 100 s – 150 s.

A way of detecting a packet would be required, such events could be noted by a reference node and sent to the other MPs. Doing so, the devices need to be synchronized — empirical measurements determined that for our setup a sync needs to be done every 100 ms. This results in a number of sync messages that are in the same magnitude as packet-based RSSMs. A different approach is to guess the range of the RSS coming from the AP and to process those values that are above this threshold. Still, there are use cases such as the handling of many APs and other technologies transmitting on the same channel, as well as the need for processing this huge amount of raw data on the node, which makes this approach challenging.

B. Evaluation of different RSS measurements within the Anomaly Detection

![Fig. 4: Comparison of ED and RSSI within the silence period of stream (Tx1,MP4).](image)

![Fig. 5: The Measurement of the LQI of stream (Tx1,MP4).](image)

In this section, we evaluate the packet-based RSSMs and their impact on the anomaly detection with the testbed shown in Figure 1a. The first 15 s of the test were used to start the test, to ensure that everything was working properly and to leave the room. The silence period was from 15 s – 180 s. 180 s – 420 s a person moved within the target area. Between 420 s – 480 s the room was vacant, and for the last 60 s a person walked to a place left from the transmitter Tx1 and sat down.

Figure 4 shows a close-up of the RSSI and ED values during the silence period for the stream (Tx1,MP4) (the complete measurement is shown in Figure 6a). In our implementation the RSSI has a measurement resolution of 3 dB. As expected the 1 dB measurement resolution of the ED results in a lower change of the variances which can be seen in Figure 6b and finally in a higher anomaly score shown in Figure 6c. The higher the anomaly score, the higher the probability that an entity is present at the stream. Figure 5 shows the LQI over the duration of the measurement. It shows that the LQI measured by the AT86RF233 radio chip (a measure of the link quality, which can be described with the packet error rate [6]) is not suited as a RSSM for DfP localization systems. Neither during the silence period, nor with an moving entity within the target area, the measured values show different behavior compared to e.g. the ED values in Figure 6a.
Figure 6 shows the progress from the raw RSSM over the signal feature — in our case the variance — to the anomaly score of the stream (Tx1,MP4). Figure 6 also shows the comparison of the different RSSMs. The ED value serves as the best input, followed by the RSSI value. The LQI does not result in a detection of an entity motion.

C. Evaluation of the Anomaly Detection

In this section we evaluate the three different packet-based RSSMs with the testbed shown in Figure 1a. Each transmitter broadcasts a message every 10 ms, \( l \) was chosen as 100 so the time window for the variance covers a period of 1 s. We chose \( \alpha \) as 0.05 and \( \beta \) as 0.1, which is within the range of the values employed in [4, 5]. Those values were chosen heuristically and will be optimized in the future.

Figure 7 shows the result of the anomaly detection. Values that are higher than a threshold (e.g., \( B_t > 1 \)) indicate that an entity is present within the target area. When a person moved within the target area, the LQI values do not increase reliably — different from the ED and RSSI values, which respond to the movement of the entity continuously. The ED and the RSSI values are nearly equal during the silence period, when an entity in moving within the target area, the ED values are higher than the RSSI values. We conclude that the ED value serves as the best parameter for the DfP detection system. The LQI does not indicate motion of an entity reliably.

V. CONCLUSION AND FUTURE WORK

In this work we demonstrated entity detection with DfP localization systems based on IEEE 802.15.4. We compared different RSSMs namely the RSSI, ED and LQI and found that detection of a person within the testbed was possible. The higher measurement resolution of the ED value is better suited than the RSSI value. The LQI value did not result in detection. In general, we recommend using the RSSM that has the best resolution. Measuring the RSSI continuously on a single channel is a very challenging task and does not result in a detection without further processing.

In the future, we will adapt the upper bounds for each stream to the dynamic radio environment. Furthermore, we will enhance the anomaly detection with a localization estimation via a particle filter. Moreover, we will investigate additional metrics compared to the variance to provide a more robust base for further processing.

ACKNOWLEDGMENTS

This publication is a result of the research work of the Center of Excellence CoSA in three projects m:flo,LOCIC and RosiE which are funded by German Federal Ministry for Economic Affairs and Energy (BMWi), FKZ KF3177201ED3, FKZ KF3177202PR4, FKZ ZF4186102ED6.

REFERENCES