Interference Effect on Localization Solutions: Signal Feature Perspective

Arash Behboodi*, Niklas Wirström†, Filip Lemic*, Thiemo Voigt†, Adam Wolisz*
* Dept. of Telecommunication Systems, Technische Universität Berlin
† SICS Swedish ICT

***Abstract*—We study the effect of interference on localization algorithms through the study of the interference effect on signal features that are used for localization. Particularly, the effect of interference on packet-based Received Signal Strength Indicator (RSSI), reported by IEEE 802.11 and IEEE 802.15.4 technologies, and on Time of Flight (ToF), reported by IEEE 802.15.4 technology, is studied using both theoretical discussions and experimental verifications. As for the RSSI values, using an information theoretic formulation, we distinguish three operational regimes and we show that the RSSI values, in dBm, remain unchanged in the noise-limited regime, increase almost linearly with interference power in dBm in the interference-limited regime and cannot be obtained due to packet loss in the collision regime. The maximum observable RSSI variation is dependent on the transmission rate and Signal to Noise Ratio (SNR). We also show that ToF is, interestingly, decreased under interference which is caused in the symbol synchronization procedure at the receiver. After providing the experimental results, we discuss how the localization algorithms are affected by interference.**

I. Introduction

The precise location of things, indoor or outdoor, is an enabler of various applications in future networks. Among variety of localization algorithms, Radio Frequency (RF)-based localization algorithms are particularly interesting due to the large scale availability of hardwares and infrastructures. RF-based localization algorithms use different technologies such as Wireless Fidelity (WiFi), ZigBee, Bluetooth, Ultra-Wideband (UWB), RFID or mobile telephony, and different RF characteristics for localization, including Time of Flight, Angle of Arrival (AoA) and Received Signal Strength (RSS). The location is then extracted either using methods such as fingerprinting procedures [1].

Although interference is known to degrade the performance of RF wireless systems by reducing the Signal to Interference plus Noise Ratio (SINR), a little is known about the interference effect on the performance of localization algorithms. The problem is that localization solutions are often complex systems and their performance is dependent on various elements including infrastructure, used technology, estimation methods and propagation environment. Moreover, the very same interference can have different effects on different technologies (IEEE 802.11, IEEE 802.15.4, etc.) and on the localization parameters reported by each technology. The manufacturer dependence of certain features of technologies makes an exhaustive study of interference effect on all these technologies very difficult. For instance, there is no standard rule for converting the measured received power into RSSI reported in IEEE 802.11 standard [2]. Inter- and intra-technology interference have also different effect for a technology. The performance of localization algorithms cannot be evaluated under interference without a clear choice of technology and precise characterization of the interference.

The impact of beacon packet losses on the RSSI-based fingerprinting algorithms is discussed in [3]. In [4], the authors show how the interference between Access Points (APs) degrades the performance of localization solutions. The authors in [5] performed a set of measurements using telosB with CC2420 radio where, according to their observations, the interference effect on RSSI values is additive. Similar empirical work has been done in [6]. Corresponding RSSIs have shown to be distorted by interference, which typically manifests as an additive increase in RSSI values.

This work serves as the first step toward the characterization of interference effect on localization algorithms by studying the way the interference affects the signal features used for localization. In particular, we choose packet based RSSI, reported by IEEE 802.11 and IEEE 802.15.4 technologies, and the ToF, measured by IEEE 802.15.4 nodes. First the interference effect on the received power is studied using an information theoretic perspective. Later on, these conclusions are examined through experimental evaluation and under different types of interference. We will see that the interference starts to change the RSSI value only if its power in dBm increases and passes a certain threshold, and afterward the RSSI values change almost linearly with the interference power in dBm. This is only possible if the packets are received correctly and the SINR is large enough. In some cases, as soon as the interference effect on RSSI starts to appear, it is no longer possible to receive the packets correctly. We verify these claims through experimental results. ToF, measured by IEEE 802.15.4 sensor nodes, is interestingly decreased under interference. The reason stems from the symbol synchronization process in which the receiver decides where in time each symbol starts in terms of discrete clock ticks. The probability of deciding an earlier clock tick is higher for signals under interference and, moreover, this probability seems to increase gradually with interference.

The paper is organized as follows. In Section II the interference effect is studied through theoretical discussions. In the sections that follow we provide experimental results and finally we discuss the interference effect on the performance of localization algorithms.

II. Theoretical Analysis of Interference Effect

RF-based localization algorithms can be categorized based on their used signal feature as RSSI, ToF and AoA-based. On the other hand, there are some interference characteristics which are particularly important for the used localization solutions, namely the transmission power, used modulation and coding schemes, Medium Access Control (MAC) mechanisms and transmitted traffic pattern. In this section, we focus on RSS and ToF values and we assume that they can only be obtained based on the correct reception of packets. This fact couples the problem of signal feature extraction to decoding problem and therefore we have to consider both simultaneously.

One should not confuse the RSS value at the receiver's antenna with RSSI value. It is known that the received total power at the receiver, in mW, is increased by a statistically independent interference and proportional to the received interference power. The RSSI, on the other hand, is a discrete value reported by different technologies and architectures, usually only reported when a packet has been received correctly. It is also an indicator of the total received power, however, without a universally accepted procedure for converting the measured received power to the RSSI values. In this work, we do not consider the effect of MAC mechanisms. However, it should be noted that the interference avoidance schemes in MAC layers of communication systems can, to a certain extent, mitigate the effect of interference, specifically when the interference comes in bursts and the sender does not transmit all the time. For the rest of this paper, we assume that RSSI is the quantized version of the RSS. In the next section we use an information theoretic framework to study the effect of interference on received power.

A. Information Theoretic Perspective

In this part, we discuss the problem using a basic information theoretic framework. Consider a simple Additive White Gaussian Noise (AWGN) channel with interference, from now on AWGN-interference channel, defined as $Y = X + X_I + Z$, where X is the transmitted channel code with power P_X, X_I is the interference with power P_I and Z is Gaussian noise with power N. The channel code is used to transmit messages with rate r. The communication bandwidth is assumed to be W. From here, if the interference X_I is statistically independent of X, then the received power is the sum of the individual powers, namely $P_R = P_X + P_I + N$. Therefore, the received power increases linearly with the interference power. Note that the powers are measured in W, and not in dB. If the signal powers are expressed in dB, then the received power is equal to $P_R[dB] = 10\log(10^{\frac{P_X[dB]}{10}} + 10^{\frac{P_I[dB]}{10}} + 10^{\frac{N[dB]}{10}})$. Keeping P_X and N fixed, if the interference power increases exponentially, i.e. linearly in dB scale, then the received power in dB changes as the function $y = \log(1 + 10^x)$. This means that, when the interference power is negligible compared to P_X and N, one does not observe any significant change in received power.

The situation is more complicated if the received power is reported only upon the correct reception of the message. In this case, the increase in interference power will gradually decrease the capacity of the channel, until the moment it creates an outage and the message cannot be decoded anymore with an arbitrarily small probability of error. Since the channel is memoryless, the error probability will tend to one when operating beyond capacity and therefore there is a sharp transition when interference makes the capacity to drop below the transmission rate. The interference effect on received power is only observable below this outage threshold. Therefore the variation of received power due to RSSI is only observable when the interference is strong enough but not too strong to cause an outage. It is possible that, whenever the interference is strong enough to affect the received power, it also causes the outage. In this case, whenever the message is received correctly, we can assume that the received power in dB is reliable and it is not getting affected by interference. The following proposition describes when we can observe variation of the received power and correctly receive the message.

Proposition 2.1: For AWGN-interference channel introduced above, the maximum observable change of received power in dB for messages of rate r (in bit-per-second) is obtained as follows:

$$\delta_{max} = 10\log(\frac{\mathsf{SNR} - \gamma_{snr}}{\mathsf{SNR} + 1}\frac{1}{\gamma_{snr}} + 1),$$

where SNR is the SNR $\frac{P_X}{N}$ and γ_{snr} is the minimum required SINR to achieve the rate r given by $\gamma_{snr} = 2^{\frac{r}{W}} - 1$. In the high SNR-regime the previous equation is simplified as follows:

$$\delta_{max} = 10\log(1 + \frac{1}{\gamma_{snr}}). \tag{1}$$

Proof: The Shannon capacity of the AWGN-interference channel is $W\log_2(1 + SINR)$, where $SINR$ is the signal-to-interference noise ratio, i.e. $\frac{P_X}{P_I + N}$. Note that the channel satisfies the strong converse and therefore the probability of error for a code with rate beyond capacity is one. Now, if the message with rate r is successfully decoded, then $W\log_2(1 + SINR)$ is not smaller than r, i.e. $r \leq W\log_2(1 + SINR)$. In other words, to correctly receive a message, the following inequality should be satisfied:

$$SINR \geq 2^{\frac{r}{W}} - 1 \implies P_I \leq \frac{P_X}{\gamma_{snr}} - N, \tag{2}$$

where $\gamma_{snr} = 2^{\frac{r}{W}} - 1$ is the minimum SINR to achieve the rate r. On the other hand, the variation of received power by interference is as follows:

$$\begin{aligned}\delta &= 10\log(P_I + P_X + N) - 10\log(P_X + N)\\ &= 10\log(1 + \frac{P_I}{P_X + N}).\end{aligned}$$

To observe this variation, the message should be decoded correctly. The maximum variation occurs if the interference power is its maximum. But it cannot exceed the value in Equation 2. Therefore the maximum interference power is

$P_I = \frac{P_X}{\gamma_{snr}} - N$, the maximum variation of received power in dB is as follows:

$$\delta_{max} = 10\log(1 + \frac{\frac{P_X}{\gamma_{snr}} - N}{P_X + N}) = 10\log(1 + \frac{\mathsf{SNR} - \gamma_{snr}}{\mathsf{SNR} + 1}\frac{1}{\gamma_{snr}})$$

If SNR is too high, then we can see that the fraction inside the logarithm can be estimated with one and we get Equation 1. ■

We call δ_{max} *maximal power variation* of a wireless system and this is the maximum amount of change we can expect in the received power under interference. The previous proposition leads to a very interesting conclusion that the received power is at most changed by a value which is independent of actual SNR and the interference power. As it can be seen in Equation 1, if the rate r is big, and hence γ_{snr} is big, then δ_{max} is small and one does not see that much variation in received power. Therefore, when higher rates are transmitted in high SNR regime, the received power measured in dB is more robust to interference. However, it is also more likely that the message cannot be received due to the high SINR requirement. As the maximum interference power P_{max} is $\frac{P_X}{\gamma_{snr}} - N$, it can be seen that higher rates require smaller interference for maximum power variation, however the variation may turn out to be small at the end. In Proposition 2.1 we have determined the maximal power variation. However, it is interesting to see when we start to observe any significant change in the received power due to the increase in the interference power. If even the slightest change in received power is obtained only by a very strong interference, then in *normal* conditions the received power should remain unchanged. Therefore, it is of practical interest to see when the received power starts to vary due to the interference power. To this purpose we introduce the notion of $\delta-$*critical power*, which is defined as the minimum interference power necessary in order to achieve δ dB variation in received power. It is possible that the $\delta-$critical power P_δ does not exist for some δ, because it may necessitate so high interference power that the message cannot be correctly received anymore. From Proposition 2.1 we know that δ cannot exceed δ_{max}. The following proposition provides the value of $\delta-$critical power and summarizes the current discussion.

Proposition 2.2: For AWGN-interference channel introduced above, $\delta-$critical power, P_δ, for a message of rate r (in bit-per-second) exists if $\delta \leq \delta_{max}$ and is as follows:

$$10\log(P_X + N) + 10\log(10^{\frac{\delta}{10}} - 1) \approx 10\log(P_X + N) + \delta.$$

Proof: We already argued about $\delta \leq \delta_{max}$. In order to cause a variation of δ dB in the reported received power, the interference power should satisfy $10\log(1+\frac{P_I}{P_X+N}) = \delta$ which implies $P_I = \frac{P_X+N}{\gamma_{rss}}$, where $\gamma_{rss} = \frac{1}{10^{\frac{\delta}{10}} - 1}$. The rest results from straightforward manipulations. ■

As an example, consider $1-$critical power, which is the variation of 1 dB. The interference power should satisfy $P_I \approx \frac{P_X+N}{4}$ in order to cause a variation of 1 dB in the reported received power. The stronger P_X, the stronger should the interference be to change the received power.

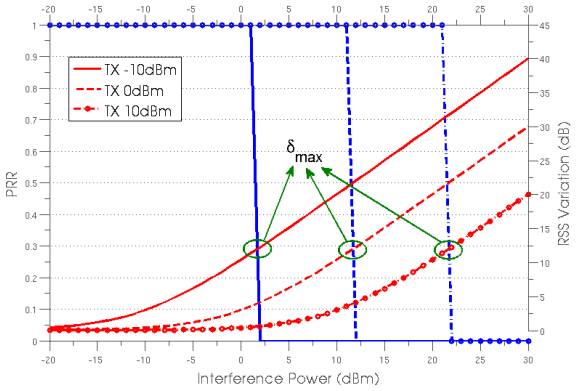

Fig. 1: RSS and PRR change versus Interference Power

B. Interference effect on packet based RSSI

In IEEE 802.11 based systems, RSSI values are numbers extracted from the radio-tap headers and another important point is that RSSI values are converted to dBm. The question, therefore, is whether the RSSI values can change significantly with interference power and yet the SINR is above the reception threshold, i.e. the packets are correctly received. If this is not the case, then we can claim that if the packets are received correctly, then the RSSI values do not change with the interference power and therefore they are robust to interference. This fits exactly the discussion of previous section. Consider an IEEE 802.11 based system where RSSI values are extracted from beacon packets with the rate 2 Mbps. Assume a 20 MHz bandwidth. For such a system, the SNR threshold is $\gamma_{snr} \approx 0.0718$ dB and therefore the maximal power variation is $\delta_{max} \approx 11.7414$ dB. Figure 1 presents the numerical evaluation of our previous results reinterpreted in case of IEEE 802.11 system with packet based RSSI and Packet Reception Rate (PRR). We work with RSS to avoid the quantization effect of RSSI and we plot the variation in RSS values in terms of interference power. It is know that in IEEE 802.11 systems, there is a sharp transition from very high PRR to a very low PRR [7, 8] and therefore the adoption of Shannon capacity and its sharp transition is justified.

As a result of this discussion, three operational regimes can be distinguished in general. As it can be seen in Figure 2, in the first regime, the interference does not change the received power and no packet loss is observed. We call this the noise-limited regime. We then define the interference limited regime as the case where the packet is received correctly, however the received power is changed by interference power. Finally we call the regime where the packet cannot be received correctly, the collision regime. The interference-limited regime appears for interference power between P_δ and $P_{\max}$.

C. Interference in DSSS and OFDM Systems

In the previous section, we did not assume any kind of modulation. After filtering the out-of-band signal and other physical layer processing, such as DFT operation in Orthogonal Frequency Division Multiplexing (OFDM) systems, the

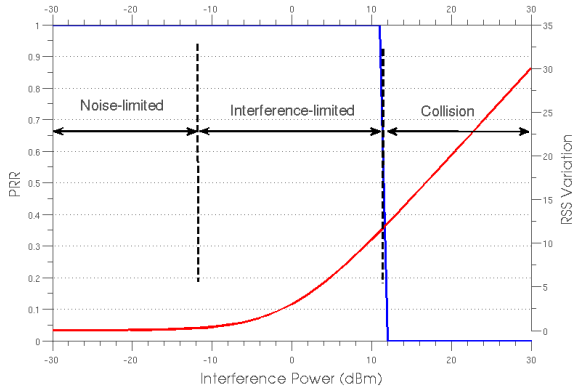

Fig. 2: Operational regimes for RSSI-PRR variation

received signal at the output of the antenna is changed into a new signal where the interference signal is also changed through the processing units. When the received power is measured after the initial processing, the effect of interference on received power is also changed. In this part, we consider an OFDM based physical layer, ex. IEEE 802.11, and Direct Sequence Spread Spectrum (DSSS) based one, ex. IEEE 802.15.4, to see the effect of modulation on the received power.

Consider an OFDM-based system. We chose an OFDM-based system because of its common usage as the PHY layer of many available technologies. In OFDM, the data is modulated over N orthogonal subcarriers and is implemented using a simple inverse DFT operation. $n-$th subcarrier is $w_n = 2\pi f_n$ with $f_n = (f_0 + \frac{n}{N\Delta t})$ with Δt the sampling time of signal.

To avoid inter-symbol interference (Inter Symbol Interference (ISI)) caused by multi-path, Cyclic Prefix (CP) is added to the beginning of the signal whose length in time is chosen bigger that the largest delay of paths. At the receiver side, the cyclic property of CP is used to remove the ISI effect by re-structuring the received signal and taking a N-DFT of the sampled signal. As a result of this procedure the relation of transmitted signal $X[m]$ and received signal $Y[m]$ in the frequency domain for the m-th subcarrier becomes simply $Y[m] = H[m]X[m]+N[m]$, where H and N are respectively the channel fading coefficient and the noise. When interference is present, the ISI cancellation procedure affects the structure of the interference. If the interferer is jamming the whole bandwidth with the same power then it appears as additional noise in the system because it occupies the whole bandwidth around each subcarrier. This means that the received power is increased with the jammer power. Now suppose that the interference is also an OFDM based signal with data modulated on the same N subcarriers. The demodulation procedure suppress the effect of the interference at subcarrier m on its adjacent subcarriers which is resulted naturally from Discrete Fourrier Transform (DFT) operation. Therefore it is expected that the effect of the OFDM-based interferer on the signal strength of OFDM-based systems is partially reduced. Since the interferer signal is re-structured in demodulation process, it is difficult to have precise analysis of interference effect on received power in general.

DSSS modulation is done through multiplication of the original sequence with Pseudo-Noise (PN) sequence of much higher frequency. An important design parameter is called processing gain, say M, defined as the ratio between the original signal period T and the PN sequence period T_c. The effect of themultiplication is that the original signal Power Spectrum Density (PSD), concentrated in bandwidth W, is spread in a larger bandwidth namely $W' = M \times W$. Therefore the signal power is distributed over bandwidth W'. If the processing gain is large then the signal PSD looks like a white noise over W'. If thePN sequence is designed properly, one cannot recover the original signal without the correct PN sequence as the signal looks like the noise. However, with the correct PN, the receiver can multiply the received signal by the PN sequence. This double multiplication will recover the signal PSD in bandwidth W.

In the decoding process, the interference is also multiplied by the PN sequence. But as it is multiplied only once, the power spectral density of the interference signal is changed just like the way original signal was changed at the transmitter. The multiplication spreads the interference signal in a wider spectrum and therefore its PSD becomes much more flat and its main components are attenuated more. That is why DSSS systems are more robust to interference as we will see in the experimental results. The received power is still increased by the interference power, however, the increase is attenuated by the processing gain.

D. Interference Effect on Packet Based ToF Ranging

Here we consider ToF ranging between two low-cost 802.15.4 nodes. The ranging scheme is as described by Mazomenos et al. [9]: A *master* node transmits a packet to a *slave* node that responds with an automatic acknowledgment, a constant delay after reception. The time between the transmission of the initial packet and the reception of the acknowledgment is measured at the master node. Due to the low clock resolution on low-cost hardware, the average of multiple (e.g. 500) measurements has to be used to gain finer distance granularity. The measured time includes several delays other than the actual ToF. These can, however, be regarded as a single constant independent of the distance. Calibration consists in estimating this constant.

A Cramr-Rao Bound (CRB) can be established for ToF as function of the SNR, as described by e.g. Lanzisera et al. [10], and it tells us that the lower bound for measurement variance increases when the SNR decreases. The CRB tells us, however, nothing about any systematic error introduced by interference. In this section we describe how interference can cause the magnitude of range measurements to decrease, and hence result in shorter estimated distances compared to if no interference is present.

Interference can affect the carrier, symbol and frame synchronization steps in the transceiver. On a 2.4 GHz receiver, the effect on carrier synchronization is however comparatively small and can have a maximum error (for a full period)

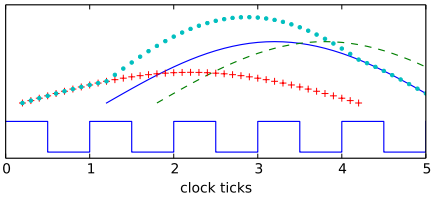

Fig. 3: Example of when interference can cause early reception.

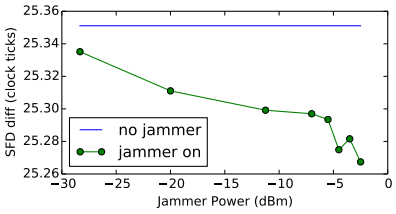

Fig. 4: Time difference between sender and receivers SFD interrupts for different levels of interference.

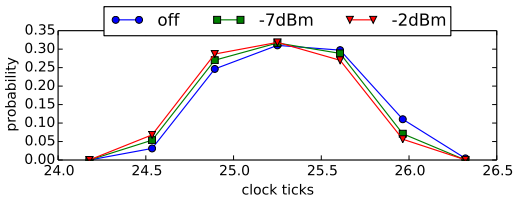

Fig. 5: PDF for the time difference between sender and receivers SFD interrupts.

corresponding to 12.5 cm for a single measurement. On low-cost transceivers, the Analog to Digital Converters (ADCs) used to sample the analog baseband signals, may be sourced by clocks with significantly lower frequency than the carrier frequency, e.g. 8 or 12 MHz.

The ADC frequency determines the resolution for symbol synchronization and hence also for frame synchronization. A deviation of one clock tick in symbol and frame synchronization results in a deviation in distance with 37.5 m for a single one-way measurement using an 8 MHz clock.

The following is a simplified discussion, but describes well how systematic errors can be introduced under interference. If no interference is present, and the first chip of a signal arrives at time t which corresponds to transceiver clock tick $n = \lfloor t f_{clock} \rfloor$, the synchronization process may determine that the chip starts at either clock tick n or $n+1$ depending on the phase difference between the clock and the incoming signal. Under interference, on the other hand, the chip may be determined to start at clock tick $n-1$, n, or $n+1$, and can therefore result in an earlier reception than for no interference. Figure 3 shows an example. The square wave represents the receiver's clock. The half sine waves represent the first I-phase chip component from incoming signals. The solid and dashed lines represent two signals without interference. The solid one would most likely be determined to start at clock tick 1 because no signal is present at clock tick 0, and a significantly large segment is present during clock tick 1. The dashed may be determined to start at either clock tick 1 or 2. The dotted sine is the result of the solid sine being interfered by the crossed sine, and may be considered to start at clock tick 0 or 1, though the desired signal starts at clock tick 1.

Early reception will result in that the acknowledgment is transmitted one clock tick earlier. At the reception of the acknowledgment, there is again the possibility of early reception. Moreover, it is likely that the frequency of early receptions increase with the interference power. We perform two types of experiment that support this theory in Section III. In the first one we perform one-way transmissions under different levels of interference, and measure the time difference between the transmitter's and receiver's Start of Frame Delimiter (SFD) interrupts. In the second experiment we perform ToF measurements under different levels of interference.

Different approaches can be used to overcome, or avoid, the effect of interference on ToF measurements. A simple way is to use measurements from multiple channels, or simply avoid channels with high interference. Using multiple channels also has benefits regarding compensation for multi-path effects [11]. A second approach is to learn how ToF measurements are affected under different interference conditions, and use it to improve measurements based on current interference conditions.

III. Experimental Results on Interference Effect

A. Packet Pased Ranging Experiments

We now turn to study the effect of interference on symbol and frame synchronization in IEEE 802.15.4. We perform one-way transmissions using two telosB nodes, under different levels of interference, and measure the time difference between the transmitter's and receiver's SFD interrupts using a logic analyzer. The two nodes are placed on a table approximately 40 cm apart. The interference source is a third telosB node, 1 m away from the other nodes, that outputs a continuous randomly modulated signal. The order of the power levels are randomized to remove temperature dependent changes in the clocks' frequencies. Figure 4 shows the SFD time difference for the different interference levels. The SFD times are averaged over approximately 4000 packets. The figure shows a clear correlation between SFD time difference and interference power. The difference in SFD times between no interference and the highest interference levels is approximately 0.08 clock ticks using the 8 MHz ADC clock of the CC2420. Figure 5 shows the probability for measuring x clock ticks for a given level of interference in the experiment. Low interference results in higher probabilities for higher number of clock ticks, and lower probability for lower number of clock ticks, and vice versa for high interference.

We perform a second set of experiment to evaluate the effect of early reception in a full two-way ToF setup. Here we also measure packet RSSI. A master and a slave, as defined in Section II-D, are placed 3 m from each other. The master transmits an empty IEEE 802.15.4 packet to the slave that answers with an hardware ACK. The packet RSSI of the ACK is collected, and the number of clock ticks passed between the event of transmitting the empty packet, and that of receiving the ACK is measured to compute ToF values based on the round-trip time. In the middle a third node is placed which we refer to as the *jammer*. The jammer transmits a continuous randomly modulated carrier wave at the same

channel as the master and slave are operating (channel 26). We perform two experiments which differ only in the type of hardware used for the master node. In one, a telosB node (with a MSP430 MCU and a CC2420 radio) is used, and in the other an STM32W which is a System On Chip (SOC) with an integrated radio. The slave and jammer nodes, are telosB nodes in both experiments. The transmission power of the jammer cycles through the 32 different available transmission power levels of the CC2420, including switching off the radio completely. For each power level 1,000 packets are sent by the master. The cycle is repeated 10 times, and the mean ToF and RSSI are computed over the 10,000 packets corresponding to each jammer transmission power. Figure 6 shows the result together with the PRR for each jammer transmission power level. The ToF values are shown as the measured number of clock ticks normalized by subtracting the number of clock ticks for the case in which the jammer is turned off.

Both experiments resulted in a decrease in the measured number of clock ticks for higher level of interference. There is, however, a clear difference in magnitude of the decrease between the two experiments. The two platforms use different clock frequencies, 12 MHz and 8 MHz, for the STM32W and telosB, respectively. But the maximum decrease is approximately 1 clock tick for STM32W, and 0.1 for telosB, which corresponds to 83 μs and 13 μs, respectively. One possible explanation can be that the faster clock results in higher probability for early reception. We also note that the decrease does not seem to be correlated with the PRR. For the packet RSSI measurements, the results from the two platforms are more coherent, showing that the packet RSSI increases with the jammer transmission power, however, the increase of RSSI is small because of processing gain of DSSS system used in IEEE 802.15.4, smearing the PSD of the interferer.

B. Interference in OFDM 802.11

In this part, we conduct a similar experiment to understand the effect of interference on packet based RSSI in OFDM based IEEE 802.11 systems. The receiver is a laptop with an Intel Centrino wireless card from which the RSSI of beacon packets are sniffed using a python script. The AP has a unique SSID and is regularly transmitting its beacon packets with 100 mW transmission power on channel 11 of IEEE 802.11. The beacon packets are captured for 5 minutes in this case and the mean RSSI value is calculated. The number of correctly received packets is counted as an indicator of PRR. The interferer is a signal generator which can create three types of jamming signals. The first type is an unmodulated signal with constant power on the channel 11, the second type is an OFDM modulated signal with WiFi-like traffic on the same band and the third one is a narrow band IEEE 802.15.4 jammer.

In the first experiment setup, the jammer is 8 m from the AP and 1 m from the receiver, which is itself 6 m from the AP. As it can be seen, the RSSI value increases proportionally with the interference transmission power after a threshold until the packet transmission is no longer possible due to insufficient SINR, having verified that packets are still being

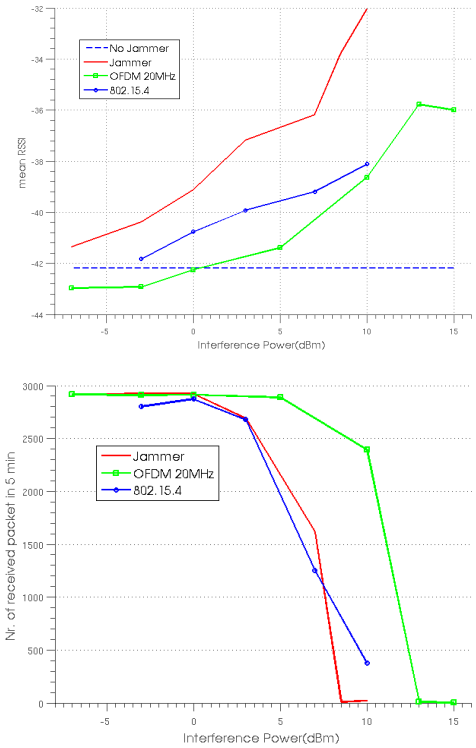

Fig. 7: RSSI and PRR change with interference power

transmitted. Figure 7 shows how the RSSI value and PRR changes with interference power. The power increase of around 10 dB causes an increase in RSSI values of around 10 dB too. For an OFDM modulated jammer, as it was explained in Section II-C, the interference effect is mitigated at the receiver due to OFDM's demodulation procedure and therefore the increase in RSSI is smaller and packet reception ratio is larger. Since the IEEE 802.15.4 jammer is a narrow-band jammer, the increase in RSSI values is more than with the OFDM interferer but less than with the wide band jammer. To examine the low SNR regime of Section II-A, the wideband jammer and the receiver, with the same distance, are brought far from the original AP such that the normal RSSI without interference is around -88 dBm. In Figure 8, one can observe at most 7 dB variation in RSSI, smaller than the high SNR case because we fall into the collision regime rapidly.

IV. Effect on Localization Algorithms

There are two main localization algorithms that use RSSI values, ranging algorithms and fingerprinting algorithms. It is obvious that the variation of RSSI values will have negative effects on the ranging algorithms. Each RSSI value obtained from an AP determine by power-law path loss model a set of points in the space that provide the same RSSI. The RSSI variation amounts to change of location of possible points corresponding to the RSSI value. The higher variation in RSSI values results in higher geometric error. This means that a small change in position of the points closer to the AP will cause larger variation in RSSI values or in other words, the

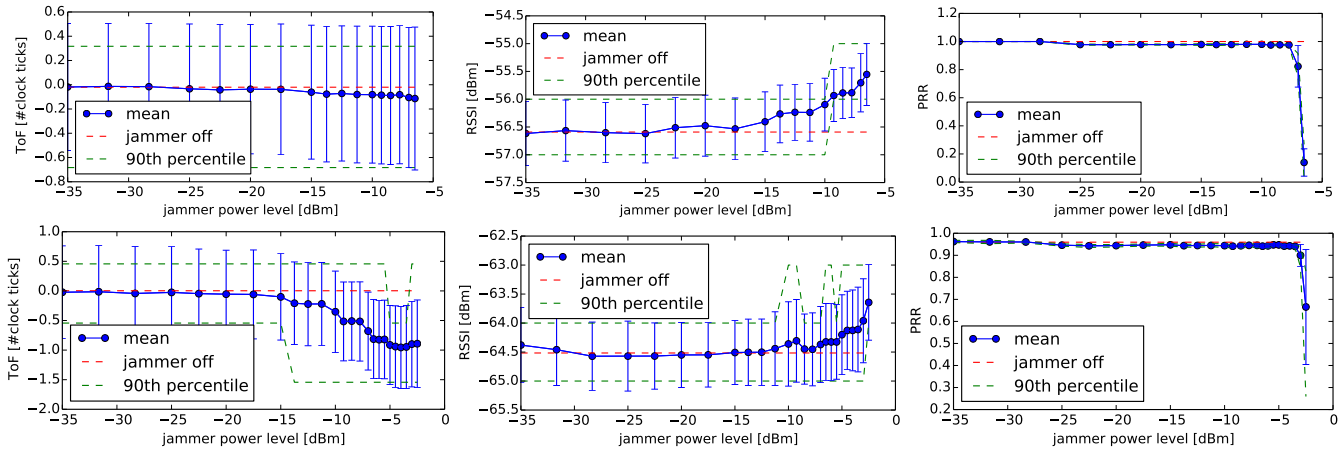

Fig. 6: ToF, RSSI, and packet reception rate (PRR) for telosB (top row) and stm32w (bottom row) in an outdoor environment.

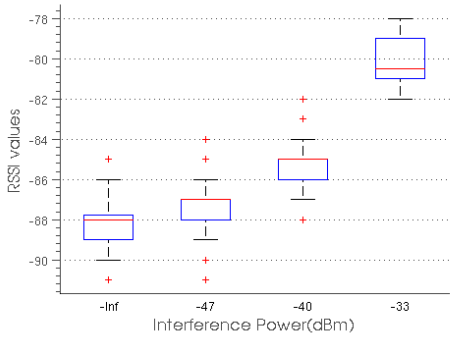

Fig. 8: RSSI change with interference power: low SNR

variation of RSSI values cause smaller geometric error for those points closer to the AP. The same discussion is true about ToF ranging. Since the ToF is related to the distance by the electromagnetic wave propagation speed, the ToF variation uniformly causes the geometric error and moreover the small variation in ToF can cause a significant geometric error.

The situation is different for fingerprinting based algorithms as the estimated position is not directly related to the RSSI values. The variation of RSSI values definitely changes the fingerprint of a given point however it is more complicated to establish a relation between the geometric error and RSSI variation. One reason is that if RSSI values are taken in dBm then different APs vary differently with the same interference depending on their SNR. For the fixed interference power, the RSSI values of stronger APs, i.e. with higher SNR, are changed less than the APs with smaller SNR and the points closer to APs suffer less geometric error under interference.

V. Conclusion and Future Works

In this work we have discussed how interference affects the packet-based RSSI values of IEEE 802.11 and IEEE 802.15.4 and ToF measured by IEEE 802.15.4 based system. It has been confirmed both theoretically and experimentally that the interference significantly changes the signal features. Future work consists of using these results in development of interference robust localization algorithms.

VI. Acknowledgement

This work has been partially funded by the European Commission (FP7-ICT-FIRE) within the project EVARILOS (grant No. 317989).

References

[1] V. Honkavirta *et al.*, "A Comparative Survey of WLAN Location Fingerprinting Methods," in *WPNC 2009*, IEEE, 2009, pp. 243–251.

[2] G. Lui *et al.*, "Differences in rssi readings made by different wi-fi chipsets: a limitation of wlan localization," in *Localization and GNSS (ICL-GNSS), 2011 International Conference on*, 2011, pp. 53–57.

[3] T.-H. Lin *et al.*, "Impact of beacon packet losses to rssi-signature-based indoor localization sensor networks," in *Mobile Data Management: Systems, Services and Middleware, 2009. MDM '09. Tenth International Conference on*, 2009, pp. 389–390.

[4] E. Chan *et al.*, "Effect of channel interference on indoor wireless local area network positioning," in *Wireless and Mobile Computing, Networking and Communications (WiMob), 2010 IEEE 6th International Conference on*, Oct. Pp. 239–245.

[5] R. Maheshwari *et al.*, "On estimating joint interference for concurrent packet transmissions in low power wireless networks," in *Proceedings of the Third ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization*, ser. WiNTECH '08, San Francisco, California, USA, 2008, pp. 89–94.

[6] D. Son *et al.*, "Experimental study of concurrent transmission in wireless sensor networks," in *Proceedings of the 4th International Conference on Embedded Networked Sensor Systems*, ser. SenSys '06, Boulder, Colorado, USA: ACM, 2006, pp. 237–250.

[7] D. Halperin *et al.*, "Predictable 802.11 packet delivery from wireless channel measurements," *SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 4, pp. –, Aug. 2010.

[8] C. Reis *et al.*, "Measurement-based models of delivery and interference in static wireless networks," in *Proceedings of the 2006 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, Pisa, Italy, 2006, pp. 51–62.

[9] E. Mazomenos *et al.*, "A two-way time of flight ranging scheme for wireless sensor networks," in *European Conference on Wireless Sensor Networks*, Bonn, Germany, Feb. 2011.

[10] S. Lanzisera *et al.*, "Rf time of flight ranging for wireless sensor network localization," in *International Workshop on Intelligent Solutions in Embedded Systems*, Jun. 2006.

[11] P. Pettinato *et al.*, "Multi-channel two-way time of flight sensor network ranging," in *Proceedings of the 9th European conference on Wireless Sensor Networks*, Trento, Italy, 2012, pp. 163–178.