Data Trustworthiness for UWB Ranging in IoT

Philipp Peterseil, Bernhard Etzlinger, David Märzinger, Roya Khanzadeh, Andreas Springer

Johannes Kepler University, Linz, Austria, {firstname.lastname}@jku.at

***Abstract*—UWB is one of the main technologies for localization in IoT applications. For range-based localization, it is crucial to secure UWB ranging by a suitable mechanism. Thereby, trustworthiness measures appear to be specifically attractive for constraints posed by IoT applications. In this work, a measure for data trustworthiness of the double-sided two-way-ranging estimate is proposed. The measure relies on features obtained from the channel impulse response and applies two machine learning techniques, namely a modified k nearest neighbour and a modified random forest, to infer an error correction term together with a trust value. To increase the number of trusted measurements, a more accurate stepwise labeling of the training data is used, and an optimum combination scheme of the resulting stepwise trust values is proposed. The results on experimental data show an improvement of 34% RMSE on the test set with 61% of the measurements considered trustworthy.**

***Index Terms*—Trustworthiness, data trust, UWB, double-sided two-way ranging, location enabled IoT.**

I. Introduction

The internet of things (IoT) is a network of billions of connected hardware-constrained devices, which enable smart scenarios in different contexts [1], [2]. To protect the increasing amount of security-critical and privacy-sensitive data processed by IoT, trustworthiness is seen as a main pillar [3]. Trustworthiness jointly covers the aspects of security, trust, resilience, and agility [4]. Hence, it is used to handle IoT system challenges, such as malicious attacks by external agents, system threats such as vulnerabilities and faults, and unexpected system behaviour [5].

In IoT, localization techniques are a core technology to aquire spatial data and a foundation of location-enabled IoT [6]. The most widespread state-of-the art option to obtain accurate location information even in complex indoor environments is ultra-wideband (UWB) wireless communications [7], [8].

A main challenge in location-enabled IoT which is addressed in recent UWB research, is localization error sources [6], such as multipath and non-line-of-sight [9]–[11] or human body effects [12]. These methods rely on the channel impulse response (CIR), which is available in commercial transceivers (e.g., [13]). While these methods improve the localization performance, they are sensitive to environmental changes. Trustworthiness is a measure to early detect resulting misbehavior.

Yet, the main body of research focuses on mitigating localization error sources rather than considering trustworthiness [14]. In localization, trustworthiness was recently leveraged in [15], [16]. While [15] focuses on beacon trust in range free systems, [16] reformulates the problem by adding probabilities of untrusted range estimates as latent variable in the iterative localization algorithm to identify if one or more range estimates to neighboring nodes are untrusted.

In this work we consider the trustworthiness for a single link in the localization scenario, i.e., for ranging between a tag-anchor node pair. We rely on features that represent channel characteristics, measured during a double-sided two-way-ranging (DSTWR) [17] cycle. DSTWR is currently the most widespread ranging principle in industrial applications.

To derive a trustworthiness value, machine learning methods, namely modified versions of the k nearest neighbor (KNN) and the random forest (RF) are applied. While conventional error mitigation techniques use these methods to find a single estimate–either a binary identification value (e.g., LOS/NLOS) or a correction value [18]–we apply a simple modification to additionally measure the uncertainty of the estimate to capture data trust [19].

As the DSTWR consists of three packet exchanges, a recently introduced stepwise labeling approach [20] is necessary to assess the trustworthiness of each individual packet. To obtain the overall trustworthiness of the DSTWR result, an optimum combination of the individual values is found.

To evaluate the proposed scheme, the measurement set from [21] with 400k ranging cycles is used, which includes localization error sources such as changing environments, multipath and obstruction of the line-of-sight (LOS) path.

II. UWB Measurements

A. DSTWR Features

The DSTWR message exchange is essential to perform ranging with asynchronous hardware. It is extremely popular due to its simple mechanism, as ranges can be estimated from measuring the exchange of three packets, referred to as packets a, b and c, as depicted in Fig. 1(a) for N measurement cycles. For each packet, a feature vector $\mathbf{x}_{i,k}$, $i \in \{\text{a,b,c}\}$, $k \in \{0, \dots, N-1\}$, is recorded. The feature vector includes the local timestamps from tag and anchor, denoted by $t_{i,n}$ and $\tau_{i,n}$, respectively, and channel related features that are direct outputs of the transceiver or calculated from the channel

This research was funded in part by InSecTT project that has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 876038. The JU receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Sweden, Spain, Italy, France, Portugal, Ireland, Finland, Slovenia, Poland, Netherlands, Turkey. The document reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains.
This work was also supported in part by the Linz Center of Mechatronics (LCM) in the framework of the Austrian COMET-K2 programme. The first and the second author have contributed equally to this work.

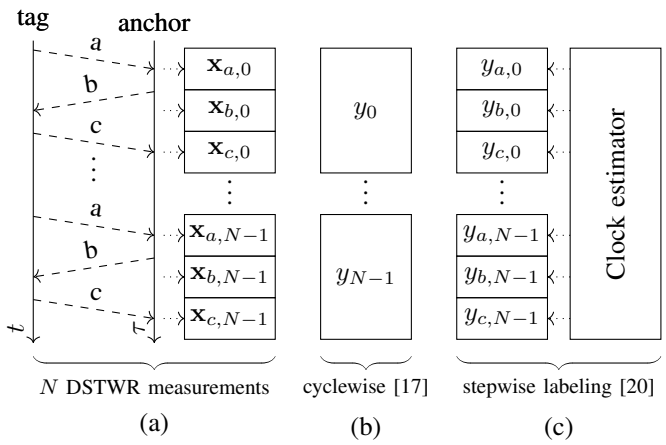


Fig. 1: DSTWR feature labeling: (a) message exchange for N rounds and recorded features; (b) cyclewise labeling; (c) stepwise labeling.

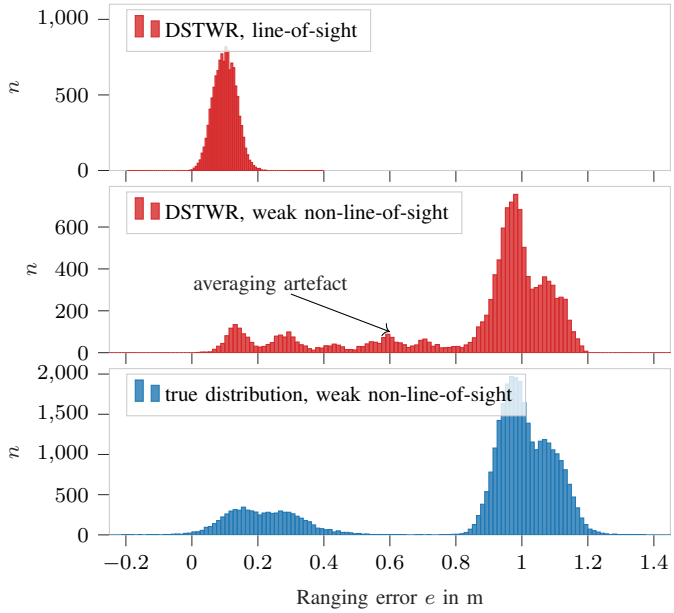


Fig. 2: Histogram of ranging error in LOS and weak NLOS in indoor environments. Ranging error (Top:) DSTWR results in LOS, (Center:) DSTWR results in weak NLOS with a person on the direct path; (Bottom:) distribution of individual packet errors in weak NLOS, evaluated through stepwise ToF estimation [20].

impulse response (CIR). As the dimension of the feature vector correlates with the computational complexity of the implemented algorithms, it is beneficial to use a limited number of features only.

In this work, 10 commonly used features are considered: three power features - received signal power level P_{RX}, first path power level P_{FP} [13] and accumulator saturation M_c [22]; calculated from the CIR, four physical features - maximum amplitude h_{max}, mean excess delay τ_{MED}, delay spread σ_{DS} and Kurtosis κ [23, Eqs. (2)-(7)]; two probabilistic features - probability of NLOS p_{NLOS} and probability of undetected early path p_{UEP} [22] as well as the receive timestamp `RX_STAMP`.

B. DSTWR Ranging

To estimate the range between a tag-anchor node pair, the recorded transmit timestamps and the measured receive timestamps are used to determine the time-of-flight (ToF). The estimation occurs cyclewise, i.e., requiring a full DSTWR cycle with the three packets $i \in \{\text{a,b,c}\}$, as [17]

$$\widehat{\text{ToF}}_n = \frac{(\tau_{\text{c},n} - \tau_{\text{b},n})(t_{\text{b},n} - t_{\text{a},n}) - (\tau_{\text{b},n} - \tau_{\text{a},n})(t_{\text{c},n} - t_{\text{b},n})}{-t_{\text{a},n} - \tau_{\text{a},n} + t_{\text{c},n} + \tau_{\text{c},n}}, \tag{1}$$

where $t_{\text{a},n}, \tau_{\text{b},n}, t_{\text{c},n}$ are transmit times and $\tau_{\text{a},n}, t_{\text{b},n}, \tau_{\text{c},n}$ are receive times in round n. Note that this estimation can be considered as a weighted average of the ToF of the three packets in round n. From the ToF, the estimated range is obtained by

$$\hat{d}_n = v_c \, \widehat{\text{ToF}}_n \,, \tag{2}$$

where v_c is the propagation speed of the electromagnetic wave.

The sensitivity of (1) to time-of-flight errors of the individual packets is measured by the first order Taylor expansion w.r.t. the receive time stamps by $\Delta\tau_{\text{a},n}$, $\Delta t_{\text{b},n}$, $\Delta\tau_{\text{c},n}$, i.e.,

$$\Delta\widehat{\text{ToF}}_n \approx \underbrace{\frac{\partial\widehat{\text{ToF}}_n}{\partial\tau_{\text{a},n}}}_{\triangleq w_{\text{a},n}} \Delta\tau_{\text{a},n} + \underbrace{\frac{\partial\widehat{\text{ToF}}_n}{\partial t_{\text{b},n}}}_{\triangleq w_{\text{b},n}} \Delta t_{\text{b},n} + \underbrace{\frac{\partial\widehat{\text{ToF}}_n}{\partial\tau_{\text{c},n}}}_{\triangleq w_{\text{c},n}} \Delta\tau_{\text{c},n} \,. \tag{3}$$

C. Problem Statement

It is generally known that the propagation channel strongly influences the ToF estimation quality, and hence poses a vulnerability of the localization system. Fig. 2 depicts the histogram of ranging errors in an indoor environment, at a ground-truth distance of $d_{\text{true}} = 3\,\text{m}$. While LOS conditions (top figure) show low ranging errors $e_n = \hat{d}_n - d_{\text{true}}$ of up to 20 cm, the obstruction of the direct path by a person (middle figure) increases the DSTWR ranging error by the factor 6 to up to 1.2 m. Through evaluating and deciding upon the data trustworthiness of the measurements, we aim to overcome this vulnerability.

D. Data Labeling

The recorded feature values are labeled in the training set. In this work we aim to identify the ranging error e while additionally quantifying the trust into this estimate. Therefore, we choose the ranging error as label value.

The ranging error can be determined straightforward by comparing the DSTWR result (2) of the training data set with the true distance d_{true}, i.e., we obtain the label $y_n = e_n = \hat{d}_n - d_{\text{true}}$. Conventionally, a label is assigned for all three packets in a cyclewise manner (c.f. Fig.1(b)). The cyclic approach has the disadvantage that it causes an averaging of the errors, which occur in the individual packets. These averaging artefacts, as visible in Fig. 2 (center), significantly degrade the labeling performance, as detailed in [20].

An alternative method to assign individual labels to each of the three DSTWR packets was recently proposed in [20], which is applied in this work. Thereby, packets from multiple

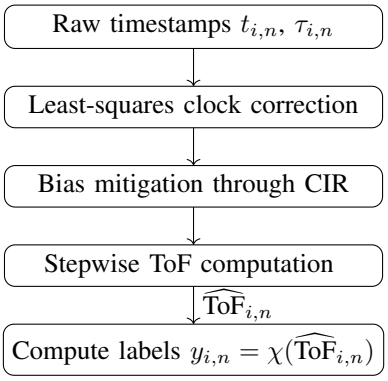


Fig. 3: Flowchart of packetwise ToF estimation for stepwise labeling according to [20]

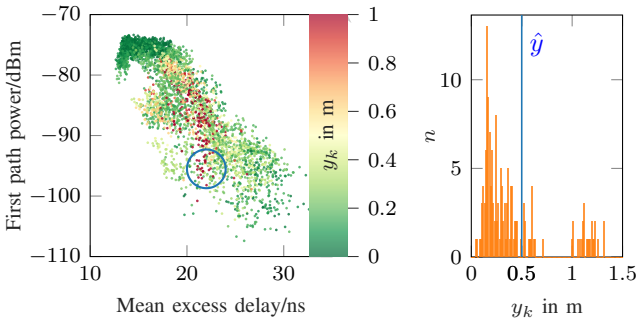
DSTWR cycles are combined for clock synchronization and precise ToF computation for each transmitted packet. The principal steps of the procedure are summarized in Fig. 3. In a first step, the time basis of tag and anchor are roughly aligned by least-square estimation based clock correction. In the second step, a fine adjustment of the clock offset is performed by comparing the shifts of the CIR. Having a precise time alignment, the ToF of each packet can be computed and then used to determine the stepwise labels (cf. Fig. 1(c)) by $y_{i,n} = v_c \widehat{\text{ToF}}_{i,n} - d_{\text{true}}$.

III. Infering Range Error and Uncertainty

Data trustworthiness is directly related to, how uncertain the estimation algorithm is about the result. We quantify the uncertainty by a standard deviation parameter $\hat{\sigma}$ which measures the variation of the intermediate results used for the primary estimate of ML algorithm, i.e., of the range error estimate $\hat{y}$.

A. Modified KNN

From a new feature measurement $\mathbf{x}_{i,n}$, conventional k nearest neighbour regression searches the k nearest neighbours



(a) (b)

Fig. 4: Modified KNN: (a) feature space with circle around example feature measurement to depict neighborhood; (b) histogram of label values from neighborhood.

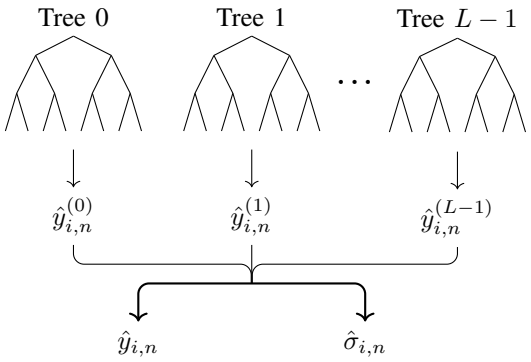


Fig. 5: Random forest regression, extended by standard deviation as uncertainty measure.

in feature space $\mathcal{X}'$ of the training data. The estimate $\hat{y}$ is obtained by averaging the labels y'_k of the k neighbors

$$\hat{y}_{i,n} = \frac{1}{k} \sum_k y'_k \,. \tag{4}$$

If the labels y'_k of the k nearest neighbors are similar to each other, the estimate $\hat{y}$ can be considered as reliable. In contrast, if the labels are contradicting, the estimate is considered as unreliable. Such a case is illustrated in Fig. 4 for a simplified 2 dimensional feature space. In Fig. 4, the detected neighborhood is indicated by the blue circle, and in Fig. 4(b) the histogram of the neighbor labels and the mean value estimate $\hat{y}$ (blue line) are depicted. In the histogram it can be seen that the neighborhood labels are separated into two groups and thus contradicting, resulting in a poor estimate.

To capture the spread of the neighboring labels, the KNN regression is extended by the label standard deviation

$$\hat{\sigma}_{i,n} = \sqrt{\frac{1}{k} \sum_k (y'_k - \hat{y}_{i,n})^2} \,. \tag{5}$$

B. Modified Random Forest

For RF regression, L decision trees are constructed during the training phase. In the online phase, each tree computes an estimate $\hat{y}_{i,n}^{(l)}$ for a new feature $\mathbf{x}_{i,n}$. The regression estimate is obtained from the mean value

$$\hat{y}_{i,n} = \frac{1}{l} \sum_l \hat{y}_{i,n}^{(l)} \,, \tag{6}$$

which we extend (as for KNN) by the standard deviation of the intermediate results

$$\hat{\sigma}_{i,n} = \sqrt{\frac{1}{l} \sum_l (\hat{y}_{i,n}^{(l)} - \hat{y}_{i,n})^2} \,, \tag{7}$$

as a measure of the uncertainty. The approach is summarized in Fig. 5.

IV. Trustworthiness of DSTWR Measurement

To convert the ML results $\hat{\mathbf{y}}_{i,n} = [\hat{y}_{i,n}, \hat{\sigma}_{i,n}]^{\mathrm{T}}$ to a trustworthiness value and a correction term, a mapping function

$$\mathbf{\Pi}(\hat{\mathbf{y}}_{i,n}) \triangleq \begin{bmatrix} \Pi(\hat{\sigma}_{i,n}) \\ \hat{y}_{i,n} \end{bmatrix} = \begin{bmatrix} \hat{T}_{i,n} \\ \hat{y}_{i,n} \end{bmatrix} \,, \tag{8}$$

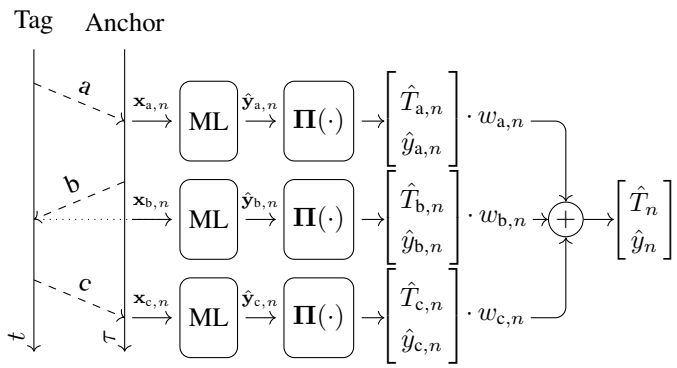


Fig. 6: Combination of packet-wise trust values to the nth DSTWR trustworthiness.

is used. While the correction term is passed directly, a soft-thresholding function $\Pi(\cdot) : \mathbb{R}^+ \to [0,1]$ is used to convert $\hat{\sigma}_{i,n}$ to a trust value $\hat{T}_{i,n} = \Pi(\hat{\sigma}_{i,n})$.

In this paper, two soft thresholding functions for data trust are utilized, namely raised cosine and exponential function. While soft values are beneficial for the combination of several trust values, a binary decision has to be made at the final stage if an estimate is trustworthy or not. Thus, in the context of this paper, a hard decision is made either to apply the estimated correction term or to eliminate the measurement.

A. Raised Cosine Mapping

A raised cosine function can be used for mapping $\hat{\sigma}$ to trust values in the interval $[0,1]$ as

$$\Pi_{\mathrm{rc}}\big(\hat{\sigma};\beta,\zeta\big) \triangleq \begin{cases} 1 & \text{if } \hat{\sigma} \le a_l \\ \cos^2\left(\frac{\pi}{4\beta\zeta}(\hat{\sigma}-a_l)\right) & \text{if } a_l < \hat{\sigma} \le a_u \\ 0 & \text{otherwise} \end{cases} \quad (9)$$

with $a_l \triangleq (1-\beta)\,\zeta$ and $a_u \triangleq (1+\beta)\,\zeta$, where β is the roll-off factor and ζ the threshold level.

B. Exponential Mapping

Alternatively, the assigned data trust values can be estimated using an Exponential function as follows:

$$\Pi_{\mathrm{exp}}\big(\hat{\sigma};\zeta\big) \triangleq e^{-\left(\frac{\hat{\sigma}^2}{\zeta}\right)} \quad (10)$$

where ζ is a normalization factor.

The raised cosine and exponential functions are used here to make sure that the driven data trust value is a real number between zero and one. They also ensure that as $\hat{\sigma}$ grows the corresponding data trust value decreases smoothly.

C. DSTWR Combination

The trust and the regression values from each packet have to be combined to obtain an overall estimate for the DSTWR cycle, and hence for the range estimate in the localization. The combination follows the sensitivity given by the partial derivatives in (3), i.e., the weigths $w_{i,n}$, with

$$\hat{T}_n = \sum_{i\in\{\mathrm{a,b,c}\}} w_{i,n}\hat{T}_{i,n}\,, \quad (11)$$

$$\hat{y}_n = \sum_{i\in\{\mathrm{a,b,c}\}} w_{i,n}\hat{y}_{i,n}\,. \quad (12)$$

The approach is depicted in Fig. 6.

For evaluation, a hard decision on $\hat{T}_n$ is done, i.e., the estimate $\hat{y}_n$ and the range estimate $\hat{d}_n$ in (2) are considered trustworthy if $\hat{T}_n$ is larger than a given threshold. In this case, the range estimate is corrected with the regression estimate to $\hat{d}_{\mathrm{corr},n} = \hat{d}_n - \hat{y}_n$.

D. Selection of Mapping Parameters

The critical parameter for the mapping functions is the cut-off parameter ζ. A heuristic method to choose this parameter from the training data set is described in the following steps:

1) Define a ranging error until which measurements appear trustworthy.
2) Count the number of measurements that are below the defined ranging error, compute the ratio to entire training set.
3) Apply the ML method from Sec. III to the training data set to obtain $\hat{\sigma}$ for all training points.
4) Apply the treshold function on $\hat{\sigma}$ and vary ζ until same ratio of trustworthy measurements appears as in 1).

V. Evaluation

The proposed approach for jointly estimating data trustworthiness together with error correction is evaluated on measurement data and compared with uncorrected DSTWR method.

A. Evaluation Data

To capture the vulnerability of UWB ranging, in total 400k DSTWR cycles were collected and structured in 36 data sets (available at [21]). The data sets differ in multipath environment (15 in corridor, 12 in lab, 5 outdoors, 4 in anechoic chamber), in ground truth distance (1, 3, 5 and 8 m), and in obstacle on the LOS path (none, non-conductive wooden wall, conductive flipchart, human). Per data set, 20 relative angular orientations differing by 18° were adjusted and for each 200 DSTWR cycles between 3 node pairs were performed. For each DSTWR packet 10 features are recorded, as detailled in Sec. II-A.

The evaluation data is partitioned into two disjoint data set groups for training and testing consisting of n_{train} and n_{test} data sets, as indicated by the $n_{\mathrm{train}}/n_{\mathrm{test}}$ tuples in Tab. I. All 24 data sets from the training group are referred to as the *training set*, while all 12 data sets from the testing group are reffered to as the *test set*.

TABLE I: Composition of training and testing data sets.

#datasets $n_{\text{train}}/n_{\text{test}}$	anechoic chamber	corridor	lab	outdoor	Σ
LOS	2/2	2/2	2/2	2/1	8/7
human	0/0	3/1	0/1	2/0	5/2
wood	0/0	3/1	2/0	0/0	5/1
flipchart	0/0	2/1	2/0	0/0	4/1
monitor	0/0	0/0	2/1	0/0	2/1
Σ	2/2	10/5	8/4	4/1	24/12

B. Weights for Trust Combination

The weights for combining the trust parameters (c.f. Fig. 6) depend on programmed response times of tag and anchor. In the asymmetric implementation as used in this paper, the weights are found through numerical evaluation to be $w_{\text{a},n} = w_{\text{c},n} = 0.2$ and $w_{\text{b},n} = 0.6$. The detailed results, which include mean, standard deviation and min and max values, are collected in Tab. II.

C. Elimination of Untrusted Ranges

To illustrate the elimination of untrusted values, the modified KNN with raised cosine function is applied to a undisrupted LOS measurement set, a measurement set with LOS obstruction and to the entire test data set. The cut-off parameter is selected as described in Sec. IV-D, yielding $\zeta = 0.06$, and the roll-off factor is fixed to $\beta = 0.5$. As trustworthiness threshold we select 75% and 99%.

In perfect channel conditions, i.e., LOS from multipath-free measurements in an anechoic chamber, a sharp histogram of raw DSTWR ranging errors can be seen in Fig. 7(a). For $\hat{T}_n > 0.75$, 94% of the measurements are identified as trustworthy. Thereby, the error compensation yields to a slight increase of the root-mean-square error (RMSE) from 3 cm of the raw estimates to 5 cm of the corrected estimates. This is due to a slight overcompensation of the method. For $\hat{T}_n > 0.99$, only 55% are identified as trustworthy, whereas also the RMSE reduces to 4 cm.

In bad channel conditions, i.e., an lab room enviornment where the LOS is obstructed by a monitor, only a very little number of trustworthy measurements survive (see ig. 7(b)). The RMSE reduces from 43 cm to 20 cm (39% surviving) and 21 cm (11% surviving), respectively, for 0.99 and 0.75 trust threshold. Thus, a low rate of trustworthy measurements is obtained as expected.

The histogram of the overall test dataset in Fig. 7(c) validates that trustworthy measurements only remain close to the origin. Obstructions on the channel, which is a major vulnerability as they yield significant ranging error, are excluded. The RMSE reduces from 36 cm to 21 cm and 17 cm, while 41 % and 17 % of the measurements are kept.

TABLE II: Weights numerically evaluated from 429970 DSTWR cycles of the evaluation data.

	w_{a}	w_{b}	w_{c}
mean	0.200021	0.5999581	0.200021
std	4.4165e-07	9.7605e-07	6.0485e-07
min	0.2000197	0.5999546	0.2000191
max	0.2000224	0.5999611	0.200023

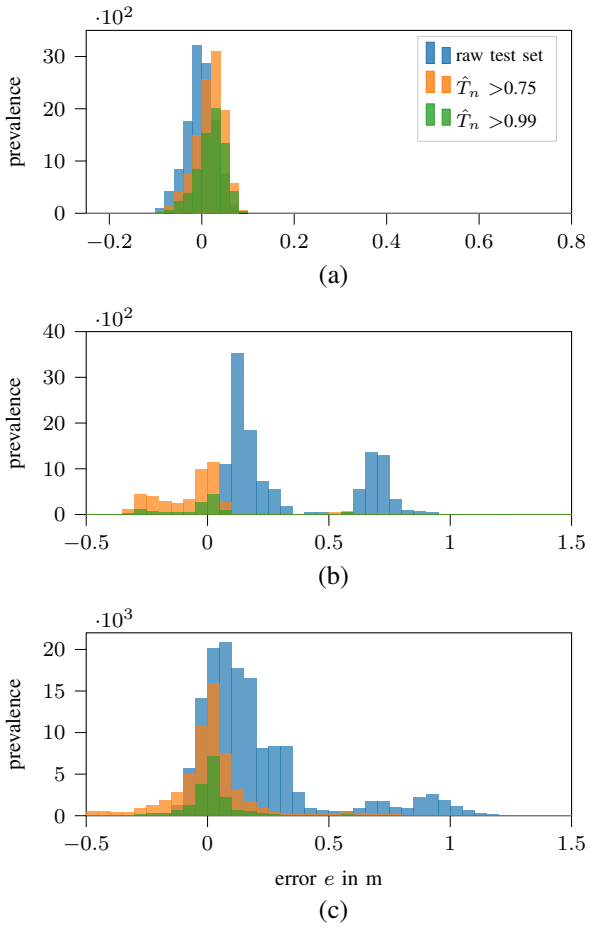


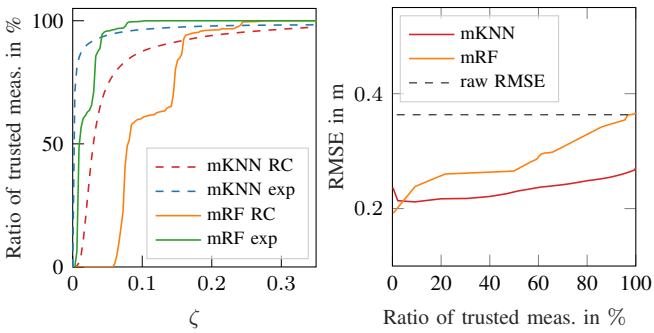
Fig. 7: Measured DSTWR estimates vs. trusted and corrected DSTWR estimates: (a) example set without interference, (b) example set with interference, (c) all test data sets.

D. Variation of Cut-Off Value

A main tuning parameter for determining trustworthiness is the cut-off parameter ζ. It defines the selectivity of trustworthy values.

In Fig. 8(a), the parameter ζ for raised cosine and exponential trust mapping for the training set was varied. It was investigated how many measurements were classified trustworthy, i.e. have trust values of $T > 0.5$. From this, a rough upper and lower bound on how to choose ζ can be concluded. The upper bound can be identified where all measurements are considered to be trusted, while the lower bound is where all measurements are dropped, e.g. for the modified KNN with raised cosine mapping upper and lower bounds are found to be 0.01 and 0.4.

In Fig. 8(b) the RMSE of the corrected measurements is depicted over the percentage of trusted measurements. The correction term of the modified KNN algorithm shows significant improvements of approximately 15cm RMSE over the full range. The modified RF algorithm as well shows improvements in RMSE over a wide range, however, the corrected RMSE is equal to the raw RMSE if all measurements are considered as trustworthy. It has to be noted, that the RMSE curves for raised cosine and exponential mapping



(a) (b)

Fig. 8: (a) Percentage of training set measurements considered trusted as a function of ζ. This relation is used to tune the cut-off parameter ζ. (b) RMSE of corrected test set measurements considered trustworthy w.r.t to percentage of measurements trusted. Both algorithms show an improvement in RMSE over wide ranges.

function are equivalent, and thus are not distinguished in this plot.

VI. Conclusion

For dependable range-based localization in location enabled IoT, it is crucial to secure vulnerabilities of UWB ranging against intended or unintended attacks, and to improve reliability in challenging channel conditions. Hence, to secure the ranging process, we introduced a machine learning based method which jointly estimates data trustworthiness together with an error correction. For trustworthiness estimation of measurements, the proposed method leverages intermediate results from the inference method to quantify the certainty of the estimate for modified k nearest neighbours and random forest implementations. The proposed method is able eliminate measurements that contribute to major ranging errors. In future work, the here presented data trustworthiness can be combined with other trust measures, such as behaviorial trust, to form a more inclusive trust notion.

References

[1] S. Li, L. D. Xu, and S. Zhao, "The internet of things: a survey," *Information systems frontiers*, vol. 17, no. 2, pp. 243–259, 2015.

[2] K. Rose, S. Eldridge, and L. Chapin, "The internet of things: An overview," *The internet society (ISOC)*, vol. 80, pp. 1–50, 2015.

[3] N. S. Labib, M. R. Brust, G. Danoy, and P. Bouvry, "Trustworthiness in iot–a standards gap analysis on security, data protection and privacy," in *2019 IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE, 2019, pp. 1–7.

[7] S. Gezici, Z. Tian, G. B. Giannakis, H. Kobayashi, A. F. Molisch, H. V. Poor, and Z. Sahinoglu, "Localization via ultra-wideband radios: a look at positioning aspects for future sensor networks," *IEEE signal processing magazine*, vol. 22, no. 4, pp. 70–84, 2005.

[4] J.-H. Cho, S. Xu, P. M. Hurley, M. Mackay, T. Benjamin, and M. Beaumont, "Stram: Measuring the trustworthiness of computer-based systems," *ACM Computing Surveys (CSUR)*, vol. 51, no. 6, pp. 1–47, 2019.

[5] F. M. R. Junior and C. A. Kamienski, "A survey on trustworthiness for the internet of things," *IEEE Access*, vol. 9, pp. 42 493–42 514, 2021.

[6] Y. Li, Y. Zhuang, X. Hu, Z. Gao, J. Hu, L. Chen, Z. He, L. Pei, K. Chen, M. Wang *et al.*, "Toward location-enabled iot (le-iot): Iot positioning techniques, error sources, and error mitigation," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4035–4062, 2020.

[8] D. Minoli and B. Occhiogrosso, "Ultrawideband (uwb) technology for smart cities iot applications," in *2018 IEEE international smart cities conference (ISC2)*. IEEE, 2018, pp. 1–8.

[9] J. Khodjaev, Y. Park, and A. Saeed Malik, "Survey of nlos identification and error mitigation problems in uwb-based positioning algorithms for dense environments," *annals of telecommunications-annales des télécommunications*, vol. 65, no. 5, pp. 301–311, 2010.

[10] Q. Zhang, D. Zhao, S. Zuo, T. Zhang, and D. Ma, "A low complexity nlos error mitigation method in uwb localization," in *Int. Conf. Commun. China (ICCC)*. IEEE, 2015, pp. 1–5.

[11] T. Wang, K. Hu, Z. Li, K. Lin, J. Wang, and Y. Shen, "A semi-supervised learning approach for uwb ranging error mitigation," *Wireless Commun. Letters*, vol. 10, no. 3, pp. 688–691, 2020.

[12] T. Wilding, E. Leitinger, U. Muehlmann, and K. Witrisal, "Modeling human body influence in uwb channels," in *2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications*. IEEE, 2020, pp. 1–6.

[13] *DW1000 Data Sheet*, DecaWave Ltd., 2014, version 2.04.

[14] H. Kuusniemi, E. S. Lohan, K. Järvinen, P. Korpisaari, S. Thombre, M. Z. Bhuiyan, H. Leppäkoski, L. Chen, S. Bu-Pasha, A. Alen-Savikko *et al.*, "Information security of location estimation-increasing trustworthiness," in *ESA Workshop Satellite Navigation Technologies and Europ. Workshop GNSS Signals and Signal Process. (NAVITEC)*. European Space Agency, Dec. 2016, pp. 1–8.

[15] R. Goyat, G. Kumar, M. K. Rai, R. Saha, R. Thomas, and T. H. Kim, "Blockchain powered secure range-free localization in wireless sensor networks," *Arabian Journal for Science and Engineering*, vol. 45, no. 8, pp. 6139–6155, 2020.

[16] Z. Wang, S. Wang, Z. Zhao, and M. Sun, "Trustworthy localization with em-based federated control scheme for iiots," *Trans. Industrial Inf.*, 2022.

[17] D. Neirynck, E. Luk, and M. McLaughlin, "An alternative double-sided two-way ranging method," in *13th Workshop Pos., Navig. Commun. (WPNC)*. IEEE, 2016, pp. 1–4.

[18] C. L. Sang, B. Steinhagen, J. D. Homburg, M. Adams, M. Hesse, and U. Rückert, "Identification of nlos and multi-path conditions in uwb localization using machine learning methods," *Applied Sciences*, vol. 10, no. 11, p. 3980, 2020.

[19] G. Han, J. Jiang, L. Shu, J. Niu, and H.-C. Chao, "Management and applications of trust in wireless sensor networks: A survey," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 602–617, 2014.

[20] P. Peterseil, D. Märzinger, B. Etzlinger, and A. Springer, "Labeling for uwb ranging in weak nlos conditions," in *2022 International Conference on Localization and GNSS (ICL-GNSS)*. IEEE, 2022, pp. 1–6.

[21] P. Peterseil, D. Märzinger, and B. Etzlinger. (2022, Jun.) UWB weak-NLOS structured dataset. [Online]. Available: https://github.com/ppeterseil/UWB-weak-NLOS-structured-dataset

[22] *DW1000 metrics for estimation of non line of sight operating conditions*, DecaWave Ltd., 2016, aPS006 Part 3 Application Note, version 1.1.

[23] S. Marano, W. M. Gifford, H. Wymeersch, and M. Z. Win, "NLOS identification and mitigation for localization based on UWB experimental data," *IEEE Journal on selected areas in communications*, vol. 28, no. 7, pp. 1026–1035, 2010.