Received Signal Strength Quantization for Secure Indoor Positioning via Fingerprinting

P. Richter*, Z. Yang†, O. Tkachenko,‡, H. Leppäkoski*, K. Järvinen†, T. Schneider,‡ and E. S. Lohan*
*Tampere University of Technology, Tampere, Finland
†University of Helsinki, Helsinki, Finland
‡TU Darmstadt, Darmstadt, Germany
Email: philipp.richter@tut.fi

***Abstract*—The increasingly connected world magnifies the threats to users' location privacy. Encryption protocols offer solutions to privacy concerns, but they are computationally very demanding. A reduction of the bit-length of the Received Signal Strength (RSS) measurements is required for a realistic, privacy-preserving positioning system based on fingerprinting. This paper studies the practical design of quantizers for RSS fingerprinting data and analyses the effect of the quantization on the positioning performance, with several real data sets and positioning algorithms. Our results show that a 4-bit quantization of RSS yields the same positioning accuracy as with unquantized RSS and that 1-bit approaches (i.e. proximity based positioning) are also feasible for certain applications.**

***Index Terms*—Received Signal Strength (RSS), quantization, secure protocols, privacy-preserving positioning, fingerprinting**

I. Introduction and motivation

The Received Signal Strength (RSS) information in a wireless system is nowadays used in a variety of applications, ranging from link-budget computations and optimizations of the communication chain to RSS-based localization and tracking. Typically, the RSS are used without any quantization, but a quantized RSS approach would bring in significant benefits in terms of lowering the energy consumption and communication bandwidths [1] and increasing the security of the positioning protocol for RSS-based positioning. In this paper we address the latter case, namely the quantization of RSS values for the purpose of enabling low-complexity security protocols in positioning for an increased user privacy. Indeed, in a RSS-based positioning approach, there are two main threats to user's location privacy if the RSSs heard by the user are sent in "clear" (i.e. without any encryption mechanism):

- The location server in charge with computing the user's location can also track the users' position and could disclose it unwittingly to third parties.
- An attacker with the access to a fingerprint database of a particular building can intercept the user's signalling towards the location server (Medium Access Control (MAC) addresses of the Access Nodes (AN) and their corresponding RSS) and infer the user's location information.

User's position privacy infringements can bring in significant threats, as outlined recently in [2]. In order to offer solutions to the user's privacy problem, privacy-preserving protocols have to be derived. Security against external adversaries intercepting signals between the user and server is relatively easy to solve by encrypting the channel, e.g., with TLS. Privacy problems originating from the server's ability to track users is significantly harder to solve, but a few attempts are available in the literature [3]–[8]. Many of them use secure multiparty computation (MPC) based on partially homomorphic encryption that allows limited operations with encrypted data. Unfortunately, weaknesses have been identified recently in some of them [8]. The schemes also introduce significant computation and communication overheads compared to basic privacy-violating protocols. Nevertheless, some promising schemes have been identified in [8] based on MPC built from garbled circuits and additively homomorphic encryption. Their complexities are directly related to the precision (bits) of RSS values used in the protocols. Consequently, significant efficiency improvements could be received by using fewer bits in the quantized RSS values, both used in the fingerprint database and measured by the user's device.

While RSS quantization decreases the complexity of the privacy-preserving protocol, it will also decrease the accuracy of the location estimate. The goal of this paper is to investigate the impact of RSS quantization on the positioning accuracy.

Most related work about RSS quantization can be found in the research on sensor node localization in densely deployed wireless sensor networks, where sensors are low-cost with limited energy, communication and sensing ability. The authors of [9]–[11] use quantized RSS to localize a target in a sensor network, but they are not concerned about the trade-off between quantization and positioning accuracy.

In [12] a quantizer is proposed whose output level is a function of the number of spatial grid cells, in order to minimize the number of beacons while pertaining the positioning accuracy. The basic path loss model with log-normal shadowing is used in simulations to evaluate the method.

The studies [13] and [14] derive the Cramér-Rao lower bound (CRLB) to analyse the performance of a RSS-based localization system with quantized RSS. The principal objective in these studies are the optimal quantization thresholds based on the CRLB. Both works conclude that a small number of quantization levels suffices to achieve a good localization performance. Patawari et al. [13] state that eight levels (3 bit) suffice to achieve a performance comparable with that of systems using unquantized RSS. These contributions were later extended by [1] to a distributed estimation of the target

978-1-5386-6984-6/18/$31.00

location. They found that 5-bit quantized RSS achieve a similar CRLB as using raw RSS.

These theoretical studies derive the optimal quantization thresholds for specific networks, network configurations and particular assumptions (a-priori knowledge of the sensor locations, isotropic signal attenuation model, reception of target's signals at all nodes, access nodes communicate with each other). This limits the validity of their findings and renders the transfer of the outcomes uncertain for positioning systems that do not reflect these assumption.

In [15] a genetic algorithm is used to find the partitions of a RSS quantizer. From experiments with EMSPCC 11 nodes in an $8 \times 12\,\mathrm{m}^2$ environment, they conclude that a 2-bit representation of RSS yields an adequate compromise between data compression and positioning accuracy.

Our study outlines privacy-preserving fingerprinting localization in WLANs and investigates the trade-off between positioning accuracy and quantization bit-length using real-field measurements in large multi-floor spaces (office and mall buildings with areas larger than $100 \times 100\,\mathrm{m}^2$ per floor). We design several practical quantizers, derived empirically from the fingerprint data, and we evaluate them with k-Nearest Neighbour (k-NN) algorithms using three different distance metrics for five different WLAN RSS data sets.

II. Indoor positioning with privacy constraints

Indoor positioning methods rely commonly on inertial measurements or on radio signals, as those used in WLAN and Bluetooth [16]–[18]. Among the possible positioning techniques, fingerprinting with RSS measurements has been widely adopted, because of the ease with that the necessary data can be acquired and because of its low complexity. In addition, alternative techniques based on signal propagation times suffer severely from shadowing and multipath propagation effects and yield typically poorer accuracy. With fingerprinting localization, a positioning accuracy of a few meters can be achieved, which is sufficient for many location based services.

RSS-based fingerprinting uses a pattern matching technique that finds the user's position by comparing an observed RSS signature, a set of RSS values from all ANs in range, with previously collected RSS signatures in a database. During an off-line phase, RSSs and the positions at which the RSSs have been recorded, are collected and stored in a database. In an on-line phase a RSS signature is measured and compared with the RSS signatures in the database. The position associated to RSSs that match best with the observed RSSs serves as an estimate for the user position. For that comparison we use the k-NN method with the following commonly used metrics:

a) Gaussian-kernel distance:

$$d_i = \sum_{m=1}^{M} \frac{1}{\sqrt{2\pi\sigma_s^2}} \exp\Big(-\frac{(s_m - \hat{s}_{m,i})^2}{2\sigma_s^2}\Big) \tag{1}$$

b) Euclidean distance:

$$d_i = \sqrt{\sum_{m=1}^{M} (s_m - \hat{s}_{m,i})^2} \tag{2}$$

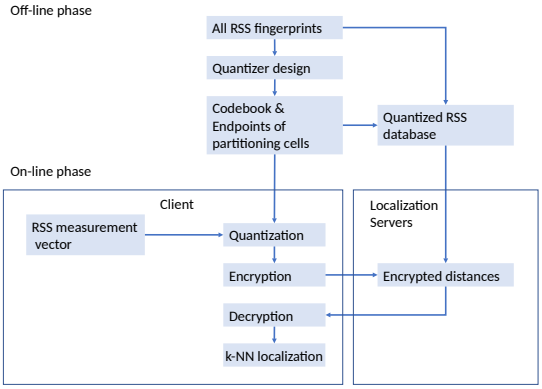


Fig. 1. Privacy preserving fingerprinting localization using quantized RSS.

c) Sørensen distance:

$$d_i = \frac{\sum_{m=1}^{M} |s_m - \hat{s}_{m,i}|}{\sum_{m=1}^{M} (s_m + \hat{s}_{m,i})}, \tag{3}$$

where $\{s_m\}_{m=1}^{M}$ is the observed RSS signature, $\{\hat{s}_{m,i}\})_{m=1}^{M}$ the ith entry in the database and M denotes the number of ANs.

To preserve the users' location privacy its RSS measurements need to be protected. Fig. 1 shows a flow chart of the privacy-preserving positioning system that integrates quantization and encryption. In Sect. III, we describe possible privacy-preserving protocols and Sect. IV details the quantization of RSS.

III. Security protocols for positioning

In privacy-preserving RSS-based localization the problems are twofold: (1) how to prevent the server from learning the user's RSS measurements and, consequently, the user's location and (2) how to prevent the user from obtaining the server's database. Secure multi-party computation (MPC) are cryptographic protocols that allow two (or more) parties to jointly perform computations without revealing their inputs to each other. Yang and Järvinen [8] surveyed different possibilities to use MPC for efficient privacy-preserving RSS-based localization. They identified garbled circuits and additively homomorphic (Paillier) encryption as the main enabling techniques. In the following, we discuss the benefits of reducing the number of bits per RSS value in both of them.

A. Garbled Circuits

Garbled circuits introduced by Andrew Yao [19] allow two parties to jointly evaluate a function $f(x, y)$ without revealing their inputs (x and y, respectively) to each other. The simplest way to use this for privacy-preserving RSS-based localization is to let x be the user's RSS measurements and y be the server's database, but other more efficient ways have been proposed [8].

In MPC using garbled circuits, the main problem is the size of the garbled circuits that is proportional to the communication between the parties. The function f is first represented as a Boolean circuit and then this circuit is scrambled into a garbled circuit so that each non-XOR gate in the circuit becomes a 2λ-bit table [20], where $\lambda = 128$ is a typical value, and XORs

are for free [21]. For instance, an addition (subtraction) of two b-bit integers requires a $2b\lambda$-bit garbled circuit whereas a schoolbook multiplication requires a $2(2b^2 - b)\lambda$-bit garbled circuit (see, e.g., [22]). Given this, it is clear that the size of the garbled circuit for computing, for example, Eq. (2) depends heavily on the precision of RSS values.

Example: Consider constructing a garbled circuit for Eq. (2) (but omitting the square root because it does not affect the ordering) with $M = 500$ and $\lambda = 128$. With 8-bit RSS values, $s_m - \hat{s}_m$ requires 256 B. Squaring the result requires 3840 B. To simplify, we assume that accumulating the 500 squares (16-bit values) is done with 25-bit additions[1] (each 800 B) and, then, we get that the total circuit becomes about 2.33 MB. The corresponding numbers with 2-bit RSS values are 64 B (2-bit addition), 192 B (2-bit multiplication), 416 B (13-bit addition), and 0.32 MB.

Above, we considered only computing a single instance of Eq. (2) but, in reality, we need to compute several distances and, then, find the shortest of them, e.g., as shown in [23].

B. Paillier Encryption

In the following, we use Paillier's additively homomorphic public key encryption scheme [24] as an example of how reducing the precision of RSS values can significantly reduce the number of ciphertexts that needs to be communicated. We discuss Paillier encryption because it is used in [8] for privacy-preserving localization, but similar advantages can be achieved for most additively homomorphic encryption schemes.

In Paillier encryption, the encryption and decryption functions with a key pair (sk, pk) are as follows:

$$c = \text{Enc}(pk, m) \tag{4}$$

$$m = \text{Dec}(sk, c), \tag{5}$$

where $m \in \mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, where n is a large integer (more than 2000 bit), m is the plaintext message, c is the ciphertext, sk is the secret key, and pk is the public key. Paillier encryption is additively homomorphic and, therefore, given two ciphertexts c_1 and c_2, which are encryptions of m_1 and m_2, there is an operator $\star$ for the ciphertexts such that $c_3 = c_1 \star c_2$ and $\text{Dec}(sk, c_3) = m_1 + m_2$. For Paillier, $\star$ is multiplication modulo n^2. This allows the server to compute Euclidean distances using the user's encrypted RSS measurements without learning their real values [3], [8].

As shown above, Paillier encryption allows encrypting very large numbers because n is large. Hence, it is not immediately obvious how reducing the precision of RSS values plays any role. However, as shown in [25], it is possible to reduce the number of ciphertexts sent from the server to the user by packing several b-bit Euclidean distances into one ciphertext. The packing can be done by, first, scaling the ciphertext of d_i by $2^{(i-1)b}$ via repeated homomorphic additions with itself and, second, by adding several scaled ciphertexts together homomorphically. Fig. 2(a) shows how most of the $\log_2(n)$-bit plaintext space of a Paillier ciphertext is wasted if only one b-bit distance is stored in a ciphertext. Fig. 2(b) demonstrates how $T = \lfloor \log_2(n)/b \rfloor$ distances can be packed in one ciphertext for efficient use of the plaintext space. Obviously, the number of distances that fit into a ciphertext depends on b, the number of bits per distance, which in turn depends on the RSS values.

[1] In practice, the first additions can use a smaller precision.

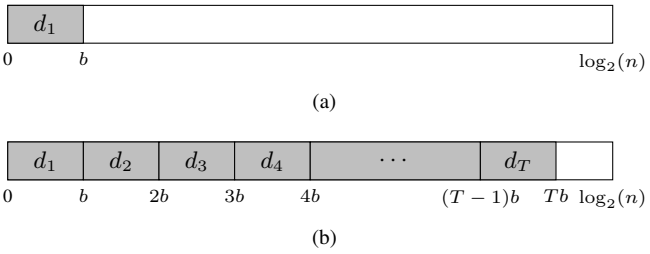


Fig. 2. (a) Only one b-bit distance per ciphertext that could store a $\log_2(n)$-bit plaintext (b) T distances packed in one ciphertext for efficient use of the plaintext space

Example: Let $\log_2(n) = 2048$ and assume that Euclidean distances are computed with Eq. (2) by omitting the square root (not possible with Paillier but also no effect on the ordering). Let the number of ANs be $M = 500$ and the number of reference points be $N = 1000$. If only one distance is stored in one ciphertext, then 2 048 000 bit need to be transmitted regardless of b. With 8-bit RSS values, we have that each $(s_m - \hat{s}_m)^2$ can be a 16-bit value and as we have $M = 500$, one distance can be at maximum a 25-bit value. Hence, $T = \lfloor 2048/25 \rfloor = 81$ values can be packed in one ciphertext resulting in $\lceil 1000/81 \rceil \cdot 2048 = 26\,624$ bit to be transmitted. With 2-bit RSS values, each distance is only a 13-bit value and $T = 157$ which gives that only 14 336 bit need to be transmitted leading to a 46.5 % saving compared to 8-bit values (and 99.3 % compared to the non-packed version). This clearly shows that the precision plays an important role.

IV. RSS QUANTIZATION

This section details the fix bit-length quantization of RSS for secure multi-party computation in support of privacy preserving localization systems.

A quantizer is specified by a codebook and a partition. The codebook defines a finite set of L output levels, $\{y_1, y_2, \ldots, y_L\}$, and the partition defines the L cells that form the input range of the quantizer. The partition cells are specified by their endpoints $\{x_1, x_2, \ldots, x_L\}$, also called boundary points or decision levels. Quantizers are typically regular, that is, each partition cell is an interval of the corresponding boundary points (x_{i-1}, x_i) and $y_i \in (x_{i-1}, x_i)$.

The overall goal when designing a quantizer is to minimize the (squared) error that the quantization $y = Q(x)$ introduces: $d = |x - y|^2$ [26]. The performance of a quantizer depends on the quantizer itself, but also on the data, X, which we model as random variable with a probability density function (pdf) $f_X(x)$. A more general and informative measure of a quantizer's overall performance is then the average distortion $D = \mathbb{E}[d(X, Q(X)]$ [26], where $\mathbb{E}$ denotes the expectation. To find an optimal quantizer, the codebook and the partitions need to be found at the same time.

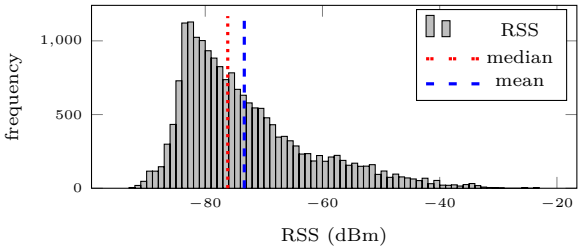


Fig. 3. Histogram of RSS of fingerprint database.

The RSS in a fingerprint database are spatio-temporal samples of an underlying random process whose analytic model is unknown. We design therefore the quantizer based on the empirical distribution of a RSS data set, considering all RSS in a fingerprint database. Fig. 3 illustrates the histogram of the RSS for a three-floor university building. We consider two principle options in this study: uniform quantization and nonuniform quantization. The motivation of studying also the nonuniform quantizers comes from the fact that the RSS probability distribution is not uniform, as shown in Fig. 3.

A. Uniform and nonuniform quantization

Uniform quantization is characterized by an input-output function that lies on a line with unit slope. That implies equally spaced boundary points and also output levels, $\Delta = y_i - y_{i-1}$. Thus, the output levels are given as the midpoints of the quantization intervals, $y_i = (x_i + x_{i-1})/2$ [26]. This limits the maximum quantization error to $\Delta/2$ regardless the distribution of the input data. We denote such a design by *Q1′*.

A nonuniform quantizer that is adapted to the input pdf quantizes frequent values fine and less frequent values coarse. This results in smaller errors for frequent input values, which may compensate the larger errors yielded from less frequent values, and thus decreases the average distortion compared to an uniform quantizer. This enables higher dynamic ranges without an increase of the distortion. We use *Q2′* to refer to this type of quantizer.

RSS measurements are in logarithmic scale, thus, the distortion of the quantizer may not be the crucial factor for the positioning accuracy. We evaluate additionally a quantizer that takes into account the exponential decay of the RSS as a function of distance. For this quantizer we choose smaller quantization levels for large RSSs and coarse quantization levels for low RSSs. This quantizer design is denoted by *Q3′*.

B. Codebook and partition choice

In order design a quantizer, the optimal partitions for a given codebook must be found. We first compute the codebook based on the complete set of RSS of a fingerprint database and then we fix the partitions. The number of bits, ℓ, determines the number of output levels $L = 2^\ell$.

The codebook of the *Q1′* quantizer is simply determined by picking L equally spaced values from the interval defined by the maximum and minimum of the RSSs: $y_i = y_{i-1} + \Delta$, where $y_1 = \min X$ and $\Delta = (\max X - \min X)/(L-1)$.

The codebook of the *Q2′* quantizer is determined in two steps: First, we determine a vector of L equally spaced ordinal numbers starting at one and ending at the cardinality of the RSS fingerprint data set, $\mathbf{v} = (1, \lfloor |X|/(L-1) \rfloor, \ldots, |X|)$. The $\lfloor \cdot \rfloor$ is the rounding operator and $|\cdot|$ is the cardinality. Second, we rank the set of RSSs. The codebook is then the ordered set of RSS that corresponds to the ranks contained in $\mathbf{v}$.

For *Q3′* we proceed as for *Q2′*, but instead of equally spaced ordinal numbers we determine L exponentially spaced (base 10) ordinal numbers in the same interval as for *Q2′*, $[1, |X|]$.

An optimal partition for a given codebook should minimize the distortion. Thus, the input values in the range of the partition cell i should be closer to y_i than to any other output level. This is equivalent to choosing the partition boundary points as midpoints of the neighbouring output levels $x_{i-1} = (y_{i-1} - y_i)/2$, also known as the nearest neighbour condition [26]. We choose the partitions of the three quantizers according to that rule.

In a last step we encode the quantizer outputs with a simple binary code. As only the difference between the RSSs matters (see metrics in Sect. II), the binary number does not have to reflect the actual RSS value as long the same encoding is used on the server and client side, recall Fig. 1.

C. Modified (combined) quantizer

Furthermore, we introduce a modification of the three quantizers described in the Sect. IV-A. The modified quantizers reserve an extra bit for the ANs whose signals could not be received. This information is either directly or indirectly contained in a fingerprint database: indirectly, if the identifiers of certain ANs do not appear in a fingerprint but in other fingerprints; directly, if the RSS values of every AN are included in the database but are set to some invalid value.

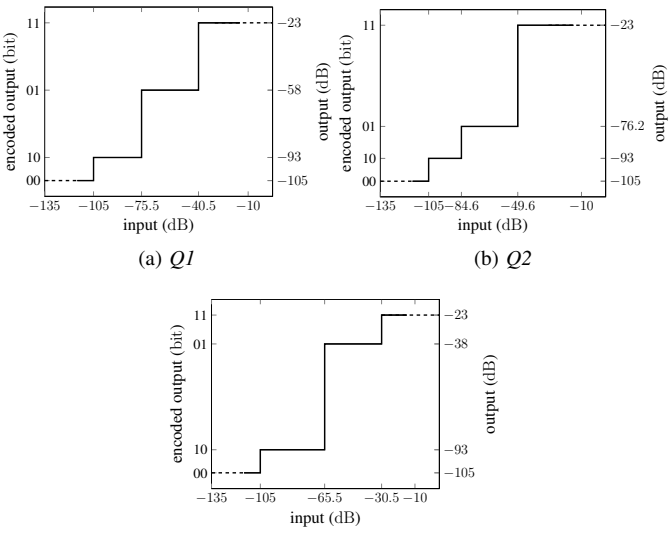
We compute the codebook of these modified quantizers as described before, but with a number of output levels $L = 2^\ell - 1$. Based on these codebooks, we determine the partition, also as described before, and then add an extra output level and boundary point to accommodate the retained *zero-bit*. We use a value below the lowest RSS of $s_{\text{th}} = -105\,\text{dB}$ for the not heard RSS. The resulting quantizers *Q1*, *Q2* and *Q3* are depicted for the same data set in Fig. 4(a) to (c).

V. Positioning results with quantization

This section presents the experimental set-up, data sets and fingerprinting positioning results with quantized RSS. To evaluate the positioning with quantized RSS we use fingerprinting with WLAN RSS. Nonetheless, we expect similar results for RSS-based fingerprinting methods in other networks, such as Bluetooth. We set $k = 3$ for the k-NN.

A. Measurement environments

We use RSS data from five different data sets, collected in different buildings, with different devices. Details about the different environments can be found in Tab. I. Among the buildings there are three typical university buildings with primarily office and lab use (Data-set-1 to Data-set-3), but



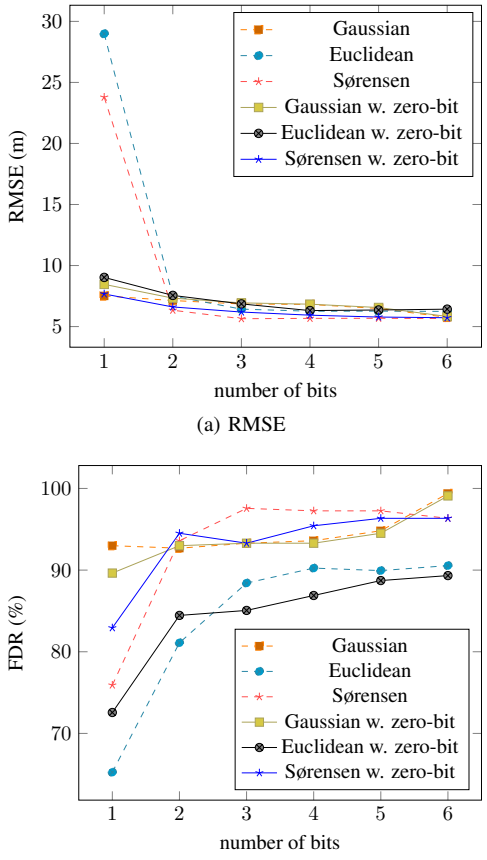
(a) *Q1* (b) *Q2*

(c) *Q3*

Fig. 4. Quantizers with zero-bit for the same RSS data set. The threshold for the zero-bit is $s_{\text{th}} = -105\,\text{dBm}$.

TABLE I
CHARACTERISTICS OF FINGERPRINT (FP) DATABASES USED IN THE EXPERIMENTS. THE BASE AREA IS ROUGHLY ESTIMATED FROM THE POSITIONS OF THE FINGERPRINTS.

	base area (m^2)	# AN	# FP	# floors
Data-set-1	176 × 73	509	628	4
Data-set-2	176 × 73	331	360	5
Data-set-3 [27]	166 ×199	489	446	3
Data-set-4	183 ×163	653	406	3
Data-set-5 [28]	395 ×275	465	19861	5



(a) RMSE

(b) FDR

Fig. 5. Positioning performance of the k-NN with Gaussian kernel-, Euclidean- and Sørensen distance for the quantizers *Q1′* and *Q1*, without and with the zero-bit, respectively, for the not heard values.

also a shopping mall (Data-set-4). Data-set-5 consists of three university buildings. Data-set-1 and Data-set-2 were collected in the same building, but with different devices.

B. Positioning accuracy with quantized RSS values

Fig. 5 shows the Root Mean Square Error (RMSE) and the Floor Detection Rate (FDR) for Data-set-3 for different bit sizes and for different k-NN metrics, Eqs. (1)–(3). It compares the positioning performance that results from the use of the zero-bit when quantizing the RSS with *Q1*.

Noticeable is first of all the high RMSE and FDR of the k-NN with Euclidean and Sørensen distance at 1-bit quantization, when zero-bit was not used. Interestingly, the Gaussian distance does not show that behaviour, it outperforms the other two metrics if the RSS are quantized with 1-bit, regardless of the zero-bit. For bit-lengths larger than four, the difference between the quantizer with zero-bit and without it is almost negligible. If two or more bits are spent, the Sørensen distance performs better than the Gaussian distance. The Euclidean distance yields consistently the highest RMSE and lowest FDR.

Next, the three quantizers *Q1*, *Q2* and *Q3* are studied. All three quantizers use the zero-bit and the positions are estimated for all five data sets, with the k-NN employing the Sørensen distance. Fig. 6 depicts the RMSE for different bit-lengths and shows the RMSE obtained from unquantized RSS for comparison.

The use of RSSs quantized with only 4-bit achieves, and eventually falls below, the positioning accuracy of raw, unquantized RSSs. That means for WLAN, where RSSs are quantized with eight bit, that four bits can be saved in any case without compromising the localization performance. The RSSs quantized with *Q3* lead to a lower positioning error than the RSSs quantized with *Q1* or *Q2*, particularly for bit-lengths larger than three. According to the path loss curve, large RSSs discriminate distances better than low RSSs. Thus, spending more bits for large RSSs (*Q3*) yields lower positioning error than spending many bits for low RSSs values (*Q2*).

A final remark is on the positioning accuracy of Data-set-4, whose fingerprints were collected sparsely in an environment that consists of only a few separations: An accuracy of 15 m is too high for a practical indoor localization system. However, despite the accuracy deviation also this data set conforms with the general pattern regarding the effect of quantization.

VI. CONCLUSIONS AND FURTHER STUDIES

Through the design of different quantization schemes and the subsequent use of quantized RSSs in WLAN positioning

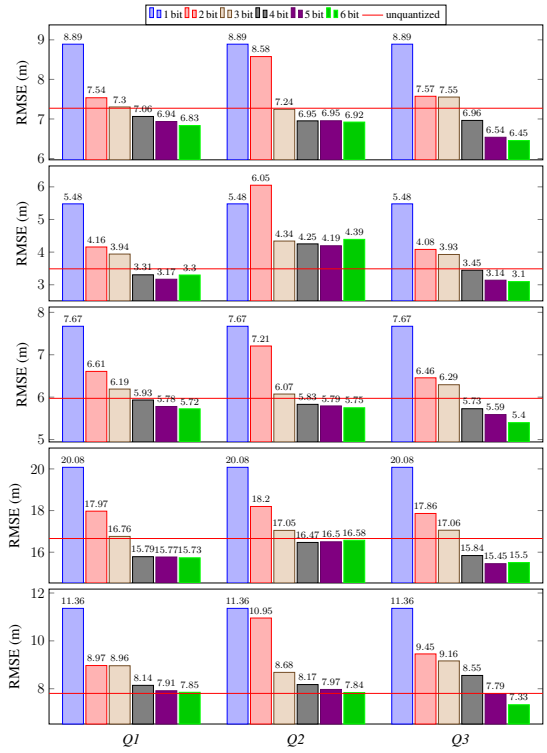


Fig. 6. Positioning performance of k-NN with Sørensen distance with RSS for three different quantizers, *Q1–Q3*, and multiple RSS fingerprint data sets. The data sets from top to bottom correspond the order in Tab. I.

methods, we found that quantizing the RSSs with $\ell = 4\,\mathrm{bit}$ yields comparable positioning accuracies than with unquantized RSSs. Thus, 4 bit can be saved, which improves the practicability of privacy preserving WLAN positioning. We recommend to spend available bits on large RSSs; anyhow, the accuracy resulting from different quantizers is quite small. It was shown that the zero-bit is only beneficial for localization with binary quantized RSSs and that although the Gaussian distance proved to be robust for proximity based positioning (1-bit quantized RSSs), the Sørensen distance yielded the best overall performance. We would also like to point out that for certain applications the accuracy of proximity based positioning might actually suffice. For such applications the computational and storage costs would be decreased significantly.

Acknowledgements

The authors express their warm thanks to the Academy of Finland (project 303576) for its financial support for this research work. This work has been co-funded by the DFG as part of project E4 within CROSSING and by the BMBF and the HMWK within CRISP.

References

[1] Z. Li, P.-J. Chung, and B. Mulgrew, "Distributed target localization using quantized received signal strength," *Signal Process.*, vol. 134, no. C, pp. 214–223, May 2017.

[2] E. Lohan, P. Richter, V. Lucas-Sabola, J. Lopez-Salcedo, G. Seco-Granados, H. Leppkoski, and E. S. Santiago, "Location privacy challenges and solutions part 2: Hybrid and non-GNSS localization," *Inside GNSS magazine*, Nov/Dec 2017.

[3] H. Li, L. Sun, H. Zhu, X. Lu, and X. Cheng, "Achieving privacy preservation in WiFi fingerprint-based localization," in *INFOCOM*, Apr. 2014, pp. 2337–2345.

[4] T. Shu, Y. Chen, J. Yang, and A. Williams, "Multi-lateral privacy-preserving localization in pervasive environments," in *INFOCOM*, 2014.

[5] J. H. Ziegeldorf, N. Viol, M. Henze, and K. Wehrle, "Poster: Privacy-preserving indoor localization," *WiSec*, 2014.

[6] A. Konstantinidis, G. Chatzimilioudis, D. Zeinalipour-Yazti, P. Mpeis, N. Pelekis, and Y. Theodoridis, "Privacy-preserving indoor localization on smartphones," *IEEE Trans. Knowl. Data Eng.*, vol. 27, no. 11, pp. 3042–3055, 2015.

[7] T. Zhang, S. S. M. Chow, Z. Zhou, and M. Li, "Privacy-preserving Wi-Fi fingerprinting indoor localization," in *IWSEC*, 2016.

[8] Z. Yang and K. Järvinen, "The death and rebirth of privacy-reserving Wifi fingerprint localization with Paillier encryption," in *INFOCOM*, 2018, https://eprint.iacr.org/2018/259, accessed Mar. 20, 2018.

[9] O. Ozdemir, R. Niu, and P. K. Varshney, "Channel aware target localization with quantized data in wireless sensor networks," *IEEE Trans. Signal Process.*, vol. 57, no. 3, pp. 1190–1202, Mar. 2009.

[10] H. Shi, X. Li, Y. Shang, and D. Ma, "Cramer-rao bound analysis of quantized RSSI based localization in wireless sensor networks," in *ICPADS*, vol. 2, 2005, pp. 32–36.

[11] X. Li, H. Shi, and Y. Shang, "A sorted RSSI quantization based algorithm for sensor network localization," in *ICPADS*, vol. 1, 2005, pp. 557–563.

[12] M. Mizmizi and L. Reggiani, "Design of RSSI based fingerprinting with reduced quantization measures," in *IPIN*, Oct. 2016.

[13] N. Patwari and A. O. Hero, III, "Using proximity and quantized RSS for sensor localization in wireless networks," in *WSNA*. ACM, 2003, pp. 20–29.

[14] R. Niu and P. K. Varshney, "Target location estimation in sensor networks with quantized data," *IEEE Trans. Signal Process.*, vol. 54, no. 12, pp. 4519–4528, Dec. 2006.

[15] W. Gao, I. Nikolaidis, and J. J. Harms, "RSSI quantization for indoor localization services," in *PIMRC*. IEEE, Oct. 2017, pp. 1–7.

[16] M. Passafiume, S. Maddio, and A. Cidronali, "An improved approach for RSSI-based only calibration-free real-time indoor localization on IEEE 802.11 and 802.15.4 wireless networks," *Sensors*, vol. 17, no. 4, 2017.

[17] S. Yiu, M. Dashti, H. Claussen, and F. Perez-Cruz, "Wireless RSSI fingerprinting localization," *Signal Process.*, vol. 131, pp. 235–244, 2017.

[18] P. Davidson and R. Piché, "A survey of selected indoor positioning methods for smartphones," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1347–1370, Secondquarter 2017.

[19] A. C.-C. Yao, "How to generate and exchange secrets," in *FOCS*. IEEE, 1986, pp. 162–167.

[20] S. Zahur, M. Rosulek, and D. Evans, "Two halves makes a whole — reducing data transfer in garbled circuits using half gates," in *EUROCRYPT*, ser. LNCS, vol. 9057. Springer, 2015, pp. 220–250.

[21] V. Kolesnikov and T. Schneider, "Improved garbled circuit: Free XOR gates and applications," in *ICALP*, ser. LNCS, vol. 5126. Springer, 2008, pp. 486–498.

[22] T. Schneider, *Engineering Secure Two-Party Computation Protocols: Design, Optimization, and Applications of Efficient Secure Function Evaluation*. Springer, 2012.

[23] E. M. Songhori, S. U. Hussain, A.-R. Sadeghi, and F. Koushanfar, "Compacting privacy-preserving k-nearest neighbor search using logic synthesis," in *DAC*. ACM, 2015, pp. 36:1–36:6.

[24] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *EUROCRYPT*, ser. LNCS, vol. 1592. Springer, 1999, pp. 223–238.

[25] A.-R. Sadeghi, T. Schneider, and I. Wehrenberg, "Efficient privacy-preserving face recognition," in *ICISC*, ser. LNCS, vol. 5984. Springer, 2009, pp. 229–244.

[26] A. Gersho and R. M. Gray, *Vector quantization and signal compression*. Kluwer Academic Publishers, 1992.

[27] P. Richter, E. S. Lohan, and J. Talvitie, "WLAN (WiFi) RSS database for fingerprinting positioning," Jan. 2018. [Online]. Available: https://doi.org/10.5281/zenodo.1161525

[28] J. Torres-Sospedra, R. Montoliu, A. Martnez-Us, J. P. Avariento, T. J. Arnau, M. Benedito-Bordonau, and J. Huerta, "Ujiindoorloc: A new multi-building and multi-floor database for WLAN fingerprint-based indoor localization problems," in *IPIN*, Oct. 2014, pp. 261–270.