Moves like Jagger: Exploiting variations in instantaneous gait for spontaneous device pairing*

Dominik Schürmann[a], Arne Brüsch[a], Ngu Nguyen[b], Stephan Sigg[b], Lars Wolf[a]

[a] *Connected and Mobile Systems, Institute of Operating Systems and Computer Networks, TU Braunschweig, Mühlenpfordtstr. 23, Braunschweig, Germany*
[b] *Ambient Intelligence, Department of Communications and Networking, Aalto University, Maarintie 8, Espoo, Finland*

Abstract

Seamless device pairing conditioned on the context of use fosters novel application domains and ease of use. Examples are automatic device pairings with objects interacted with, such as instrumented shopping baskets, electronic tourist guides (e.g. tablets), fitness trackers or other fitness equipment. We propose a cryptographically secure spontaneous authentication scheme, BANDANA, that exploits correlation in acceleration sequences from devices worn or carried together by the same person to extract always-fresh secure secrets. On two real world datasets with 15 and 482 subjects, BANDANA generated fingerprints achieved intra- (50%) and inter-body ($>75\%$) similarity sufficient for secure key generation via fuzzy cryptography. Using BCH codes, best results are achieved with 48 bit fingerprints from 12 gait cycles generating 16 bit long keys. Statistical bias of the generated fingerprints has been evaluated as well as vulnerabilities towards relevant attack scenarios.

Keywords: gait, authentication, fuzzy cryptography, ad-hoc secure pairing

1. Introduction

With increasing importance of short-term spontaneous interaction, ad-hoc device pairing promises seamless secure interaction in smart environments.

We envision short-term spontaneous pairing such that co-presence, i.e. devices worn or carried by the same person, suffices for autonomous, spontaneous secure connection establishing (not assuming any prior shared secret, not involving any trusted third party and without leaking information on the key via any communication channel). Pervasive Computing applications for such protocol are numerous and include, for example, the pairing between a personal device worn on the body, and other pervasive, computing, and sensing capable devices. For instance, a shopping basket carried by the same person, or even instrumented items carried inside the basket. Such pairing could enable synchronization of a shopping list on the personal device with items in the basket, or the display of advertisements on the personal device, tailored to match items in the basket.

Furthermore, in a Pervasive Computing setting, computing and sensing capable fitness equipment in a gym could spontaneously pair with a fitness app on a personal device during the context of use to provide accurate information on the intensity and performance of a specific workout.

Also, tablet-based electronic tourist guides could pair spontaneously with a personal on-body device in order to inquire information on language preferences, interest and background to tailor the provided experience on the respective user.

*This paper is an extended version of "D. Schürmann, A. Brüsch, S. Sigg, L. Wolf, BANDANA – Body Area Network Device-to-device Authentication using Natural gAit".

Email addresses: schuermann@ibr.cs.tu-bs.de (Dominik Schürmann), bruesch@ibr.cs.tu-bs.de (Arne Brüsch), le.ngu.nguyen@aalto.fi (Ngu Nguyen), stephan.sigg@aalto.fi (Stephan Sigg), wolf@ibr.cs.tu-bs.de (Lars Wolf)

Preprint submitted to Pervasive and Mobile Computing on May 2017, revised Oct 2017 and Feb 2018, corrected Aug 2019

There exist many further examples and in all cases the spontaneous pairing shall break in the very moment that the device (e.g. basket, fitness equipment or tourist guide) is discarded or handed to another person, so that no privacy-related information is disclosed unwittingly. We present BANDANA, a spontaneous secure pairing scheme based on gait, which allows frequent re-pairing (restricted to the time-of-use), and ad-hoc implicit (no manual interaction required) secure authentication bound to an individual. Our solution does not require a trusted third party. In particular, we utilize instantaneous variations in gait sequences for implicit generation of a shared secret among all devices on the same body. Our contributions are (1) a secure ad-hoc pairing scheme for devices worn on the same body, (2) experimental verification of the protocol on two large gait datasets, and (3) security analysis on the pairing approach covering statistical bias, and attack scenarios.

Compared to [1], we integrate BANDANA with Password-Authenticated Key Agreements (PAKEs), such as in Bluetooth's Secure simple Pairing (SSP) to reduce extracted the gait fingerprint to $M = 48$ bits, while retaining security guarantees (cf. Section 4–6.) A new dataset and a consideration of new activities (running, ascending and descending stairs) was added to the evaluation (cf. Section 3.3, and Figures 10, 9), correlation distances for various body parts (cf. Figures 7–9), and a detailed threat model including video attacks have been added (cf. Section 7).

2. Related Work

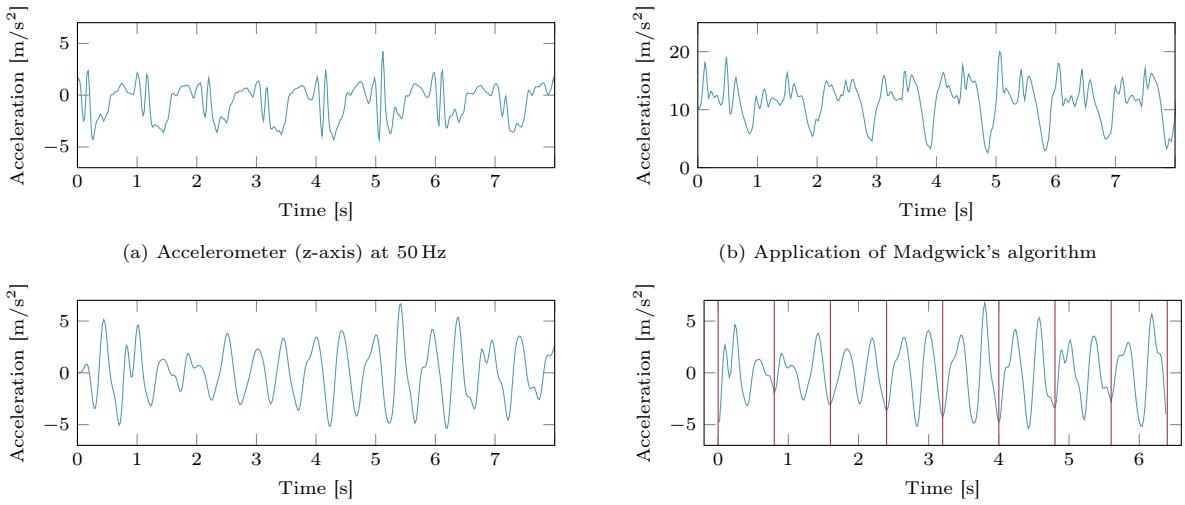
A popular sensor to detect co-presence is the accelerometer. For instance, [2, 3] present a process to generate shared keys via a threshold-based protocol conditioned on the magnitude of co-aligned acceleration processes. [4, 5, 6] further improve this protocol with respect to success probability, different sample rates and starting points as well as differing rotation. Implementations of this protocol have been presented in [7, 8].

For authentication based on arbitrary co-aligned sensor data, the candidate key protocol is proposed in [9]. It interactively exchanges hashes from feature sequences as short secrets and concatenates the key from the secrets with matching hashes. All above implementations require that pairing patterns are explicitly generated (e.g. devices are shaken together). In contrast, we propose to exploit derivation from mean acceleration (where the mean serves as a sort of normalization among devices) to pair devices implicitly conditioned on co-presence on the same body.

Other sensor modalities that can be used for unattended co-presence-based device pairing [10] are magnetometer [11], RF-signals [12, 13] luminosity [14] or audio [15]. For these, in contrast to our approach, pairing is not constrained by co-presence on the same body but, more generally, by proximity.

Acceleration sequences from devices worn or carried by the same person differ in orientation and placement [16]. To receive placement independent features one can (A) calculate norm or magnitude $m_i = \sqrt{x_i^2 + y_i^2 + z_i^2}$ (discarding information on acceleration along individual axes [17]), (B) to first detect the location and then to try to deal with changes that occur due to placement [16], or (C) to tackle disorientation and misplacement errors by calculating the rotation matrix from magnetometer readings [18]. Even though after (A), the resulting signal still differed greatly due to inherently differing movement of underlying body parts (e.g. arm vs. head vs. legs) [19], Cornelius et al. [20] succeeded to show good correlation among all body locations. We implement (C) to remove additional uncertainty and noise due to the merged acceleration angles.

For many daily activities, upper body and lower body movements are only weakly or not correlated. We therefore propose to use gait, which can be well recognized over the whole body [21]. For instance, identical step patterns have been utilized for co-location detection [22]. The authors in [23, 18] employ gait cycles to authenticate a user on his smart-phone by matching the current walking pattern against a previously saved walking template exploiting a fuzzy commitment scheme [24]. In [25], it was shown that gait as a biometric feature is robust against an attacker mimicking the victims gait. In their study, professional actors with matching physical properties have been chosen. [23] recently presented an approach to generate a key fingerprint from the difference of a mean world gait (spanning the complete population) to the mean gait of an individual. By computing the mean gait over the whole population, the authors assured that the resulting sequence is well balanced and uniformly distributed.



(a) Accelerometer (z-axis) at 50 Hz

(b) Application of Madgwick's algorithm

(c) Type-II Chebyshev bandpass filter

(d) Resample and Gait Cycle Detection.

Figure 1: Pre-processing and gait cycle detection (z-axis, accelerometer at the forearm).

We also exploit this idea of using the difference to a mean for normalization, but, in contrast, we are not interested in a mean gait over a world population but instead, we derive a mean gait over few preceding gait cycles for all devices on the same body. This is important since the protocol shall generate always fresh instantaneous keys for ad-hoc pairing based on the recent gait history.

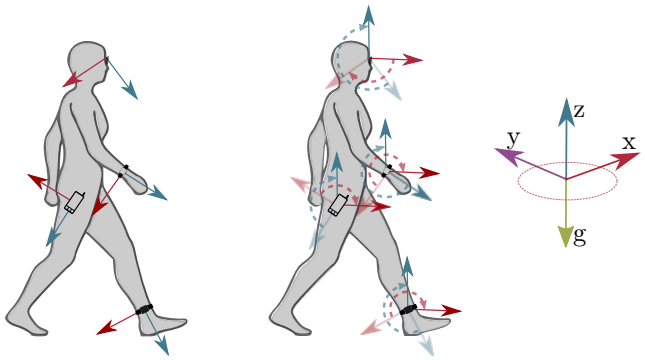
Summarizing, the related work on device pairing from on-body features does, in contrast to our work, (1) not address the impact of different on-body locations and sensor orientation, (2) require devices in close proximity and with strong, purpose-generated acceleration sequences, and (3) use biometric features for distinguishing distinct individuals, rather than instantaneous characteristic movement patterns that change over time. In contrast, we generate always-fresh authentication keys from instantaneous acceleration sequences for arbitrary location on the body. Muaaz et al. [26] confirmed the significant challenge of (1) but demonstrated gait-based authentication for selected related locations on the human body (from one to the other side of the hip), accepting a high error rate.

A work closely related to our study has been presented in [27]. The authors exploit independent component analysis to obtain meaningful gait sequences and extract binary patterns for device pairing by applying a threshold to the data. In contrast, our quantization exploits difference of an instantaneous gait to the mean gait of a respective body location. In addition, we demonstrate that our method is feasible on two freely available benchmark gait databases. In particular, the body locations considered by us cover, in contrast to [27], also lower body-parts, which are more challenging to pair as detailed in Section 6.3.

3. Fundamentals

3.1. Data Pre-Processing

Body-worn sensors feature dynamically changing orientations due to body part movement (cf. Figure 2a). To derive a correlated acceleration independently of the on-body location every data point must be rotated such that one of the axes is facing in the opposite direction of gravity as depicted in Figure 2b. We employ the algorithm proposed by Madgwick et al. [28] to rotate all measurements z_i accordingly, resulting in a signal for the z-axis as indicated in Figure 1b (Orientation and gravity are derived from gyroscope and accelerometer [29]). Compared to sensor fusion based on Kalman filters, Madgwick's algorithm is less computationally expensive due to its linearity and is thus suitable for mobile devices [28]. Afterwards, correlation between records taken simultaneously from devices worn or carried by the same person exists (cf. Figure 3). To remove additional noise for correlations in high and low frequencies, we apply a Type II



(a) Before (b) After Madgwick

Figure 2: Body-worn sensors' coordinate systems before and after application of Madgwick's algorithm. Note the remaining degree of freedom along the xy-plane.

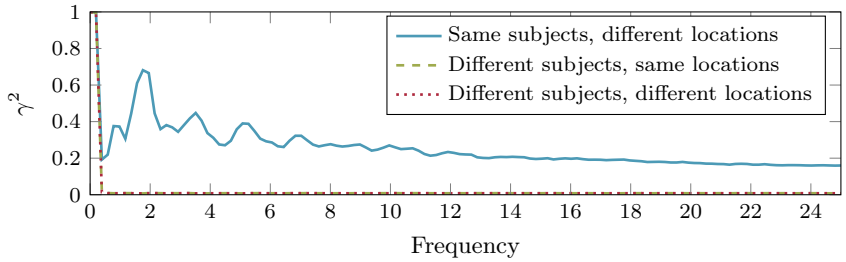


Figure 3: Average spectral coherence for the Mannheim dataset (same and different subject).

Chebyshev bandpass filter with passband between 0.5 Hz and 12 Hz. The choice for these cutoff frequencies was taken since human motion does not affect frequencies significantly above 10 Hz [30] (cf. Figure 1c).

3.2. Gait Cycle Detection

A gait cycle is the time interval between two successive steps [31]. As discussed in the related work, our algorithm is based on ideas by Hoang et al. [18] providing a reliable method for segmentation. The algorithm's input is a vector of amplitude values $\boldsymbol{z} = (z_1, \ldots, z_n)$ of the accelerometer z-axis (cf. Figure 1a). Its output is a gait sequence of consecutive gait cycles with normalized length.

To find repetitive parts in the signal, clearly separated cycles are extracted based on autocorrelation and distance calculation. The discrete autocorrelation at time lag k and with variance σ^2 is estimated as

$$A_{corr}(k) = \frac{1}{(n-k)\sigma^2} \sum_{t \in \mathbb{Z}} z_{t+k} \cdot \overline{z}_t$$

where $\overline{z}_t$ is the conjugate of z_t. The resulting autocorrelation $\boldsymbol{a} = (a_1, \ldots, a_n)$ leads to m non-ambiguous local maxima in $\boldsymbol{a}$, stored as $\boldsymbol{\zeta} = \{\zeta_1, \ldots, \zeta_i, \ldots \zeta_m\}$. The distances between these indices and a mean distance

$$\delta_{mean} = \left\lceil \frac{\sum_{i=1}^{m-1} \zeta_{i+1} - \zeta_i}{m-1} \right\rceil$$

are then calculated. δ_{mean} can now be used to select indices of minima from $\boldsymbol{z}$ that represent clear cycles with the same length:

$$\begin{aligned} \boldsymbol{\mu} &= \{\mu_1, \ldots, \mu_i, \ldots, \mu_{m-1}\}; \\ \mu_i &= \arg\min(z_{\zeta_i - \tau}, z_{\zeta_i - \tau + 1}, \ldots, z_{\zeta_i + \delta_{mean} + \tau}). \end{aligned}$$

Every μ_j represents the index of a minimum in $\boldsymbol{z}$ limited to the range of δ_{mean} where τ defines an additional correction factor to account for small deviations in gait duration. The indices in $\boldsymbol{\mu}$ are used to split raw data $\boldsymbol{z}$ into gait cycles

$$\begin{aligned} \boldsymbol{Z} &= \{Z_1, \ldots, Z_i, \ldots, Z_q\}; \\ Z_i &= (z_{\mu_{\frac{i}{2}}}, \ldots, z_{\mu_i}, \ldots, z_{\mu_{\frac{i+1}{2}}-1}); \\ &\quad \text{with } i = \{2, 4, ..., q\}. \end{aligned}$$

Finally, the length of gait cycles are normalized by resampling every Z_i using a Fourier method to ρ samples per gait cycle so that $|Z_i| = \rho$ ($Z_i = \{Z_{i1}, \ldots, Z_{i\rho}\}$; cf. Figure 1d). The choice of ρ depends on factors such as sample rate and requirements of the quantization algorithm discussed in Section 4.

3.3. Datasets

In order to verify that our approach is able to establish gait-based short-term spontaneous pairing for devices worn or carried jointly by the same person we employ two real-world datasets that feature specific characteristics well aligned with this aim. In particular, we utilize the *Mannheim* dataset presented in detail in [32] for the use in position aware activity recognition. It features 15 subjects (8 male, age 31.9 ± 12.4, height 173.1 ± 6.9, weight 74.1 ± 13.8), which are equipped with 7 sensors on different body parts (head, upper arm, chest, waist, forearm, thigh, shin), and which performed different activities (walking, running, ascending, descending stairs, ...) for a time period of 10 - 12 minutes each. It is well suited because it features several relevant sensor positions for on-body device pairing, multiple activities and complete ground truth is available from video recordings.

A single limitation of the *Mannheim* dataset is the limited number of participants. We therefore, in addition, verified our approach on the *Osaka* OU-ISIR Gait Database [33]. This dataset features acceleration recordings from a total of 496 subjects from which 482 have been used in this paper after removing samples with missing sensor locations or short duration. Samples are taken from three triaxial accelerometers and gyroscopes worn on different parts of the waist (left, right, center). Subjects traversed a course comprising a straight path, upstairs and down a slope. A conceptual issue in our case lies in the fact that all sensor units were located on rather close locations on the body and mounted to the same harness, potentially introducing an error.

4. BANDANA

For BANDANA's device-to-device authentication, shared secrets are generated based on acceleration sequences independently on participating devices and, in particular, without disclosing information on the gait sequence on the communication channel. For this, we generate binary fingerprints from the gait and utilize fuzzy cryptography to derive unique key sequences. Following Figure 4, we summarize the novel parts of our protocol.

Gait cycle detection is applied on accelerometer data recorded on A and B and corrected by Madgwick's algorithm and Type-II Chebyshev bandpass filter.

We propose a quantization algorithm inspired by [23], but instead of exploiting the difference to a mean world gait, we calculate differences to the mean of a specific gait sequence. The mean gait is thus defined as

$$\boldsymbol{A} = (A_1, \ldots, A_j, \ldots A_\rho); \quad A_j = \frac{\sum_{i=1}^{q} Z_{ij}}{q}$$

and compared to each gait cycle Z_i (Figure 5).

The mean normalizes differences in acceleration patterns at distinct body locations. To extract b bit per gait cycle Z_i, each Z_i is split into b parts of identical length ρ/b. A binary fingerprint $\tilde{\boldsymbol{f}} = (\tilde{f}_1, \ldots, \tilde{f}_M)$ is

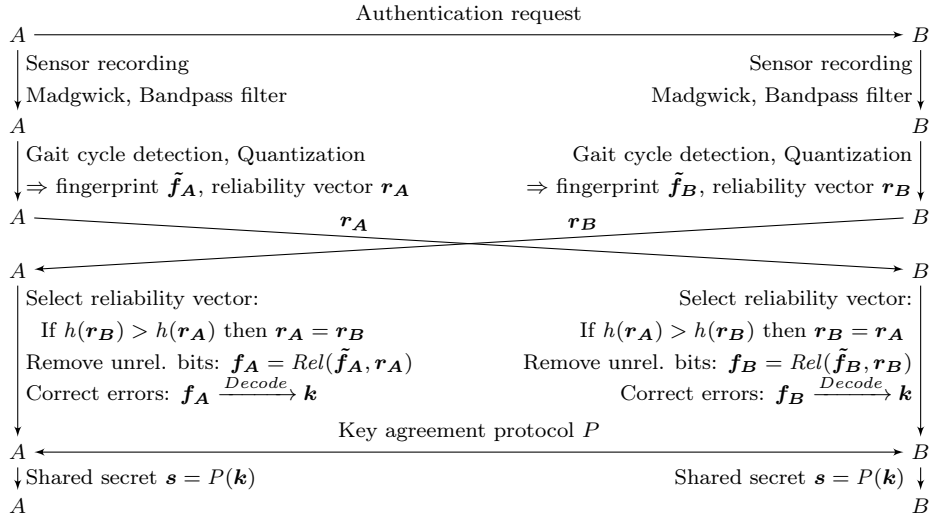


Figure 4: Protocol sequence between two devices A and B worn on the same body.

given by

$$\begin{aligned}\tilde{\boldsymbol{f}} &= (\tilde{f}_{11}, \ldots, \tilde{f}_{1\frac{\rho}{b}}, \ldots, \tilde{f}_{b1}, \ldots, \tilde{f}_{b\frac{\rho}{b}}) \\ \tilde{f}_{ij} &= \begin{cases} 1, & \delta_{ij} > 0 \\ 0, & \text{otherwise.} \end{cases} \\ \delta_{ij} &= \sum_{k=0}^{\rho/b} A_{i+k} - Z_{i+k,j}.\end{aligned}$$

The differences of the quantization are

$$\boldsymbol{\delta} = (\delta_{11}, \ldots, \delta_{1b}, \ldots, \delta_{q1}, \ldots, \delta_{qb}).$$

Larger δ_{ij} indicate higher probability to be identical for arbitrary body locations.

The indices of $\boldsymbol{\delta}$ are sorted in descending order by the absolute value $|\delta_{ij}|$ to retrieve the *reliability vector* $\boldsymbol{r} = (r_1, \ldots, r_M)$ with $r_i \geq r_{i+1}$. The independently generated vectors $\boldsymbol{r_A}$ and $\boldsymbol{r_B}$ are exchanged. While their ordering is similar, it is decided that the one with a higher hash value generated by $h()$, e.g., SHA-256, is selected on both sides. Using $Rel(\tilde{\boldsymbol{f}}, \boldsymbol{r})$, the least reliable bits are disregarded for the fingerprint, so that the first N constitute the fingerprint $\boldsymbol{f} = (f_{r_1}, \ldots, f_{r_N})$ (cf. Figure 5 (c)).

After reliability ordering, the remaining differences in the derived secrets are corrected with fuzzy cryptography. We choose the codespace $\mathcal{C}$ of an error correcting code (We propose to use BCH codes over the Galois field $\mathbb{F}_2$; A BCH code can be parameterized to correct up to p errors) such that we can directly map a fingerprint $\boldsymbol{f}$ into this codespace. By decoding it with $\boldsymbol{f} \xrightarrow{Decode} \boldsymbol{k}$ into the message-space of the error correcting code, a binary key $\boldsymbol{k}$ is derived that is identical for a pair of on-body devices. Using $\boldsymbol{f} \xrightarrow{Decode} \boldsymbol{k}$, a (N, K)-error correcting code can correct up to $p = \lfloor \frac{N-K}{2} \rfloor$ errors. The minimal percentage such that all errors are corrected, i.e. the threshold for a successful pairing, is $u = 1 - \frac{p}{N}$.[1] Based on the targeted bit size K of the key $\boldsymbol{k}$ and u, the required fingerprint size is therefore $N = \frac{K}{2u-1}$.

Finally, a shared secret $\boldsymbol{s}$ can be derived by executing a key agreement protocol $\boldsymbol{s} = P(\boldsymbol{k})$.

[1] 2019-08-14: Errors have been corrected and an additional explanation has been added (changes marked in blue).

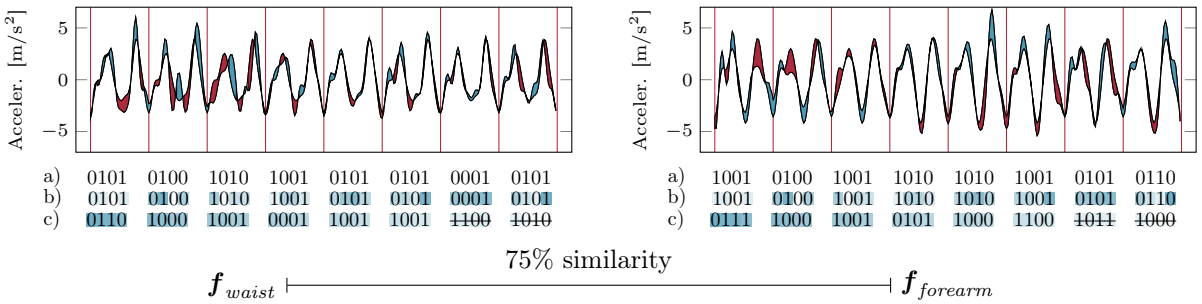


Figure 5: Fingerprint generation on waist and forearm: Energy above average gait cycle in blue and below red. a) after quantization; b) reliability for each bit (darker colors → more reliable); c) sorted by decreasing reliability of forearm and removing least reliable $M - N$ bits

5. Key Agreement

BANDANA can be applied in conjunction with various key agreement protocols. To provide a large security margin, we propose to use protocols with a two-party adversarial model, where the attacker is reduced to a one-shot Man-in-the-Middle attacker. A typical design constrains the attacker to only one try by extending a Diffie-Hellmann key exchange. One possible implementation is to use a hash commitment before revealing public values over the channel (cf. Vaudenay [34]). Other protocols, called Password Authenticated Key Exchanges (PAKE), have been proposed with similar goals: The chance of a successful attack should not depend on an attackers offline computing power, but solely on the interaction during the protocol execution. Important standards implementing these primitives include Bluetooth Secure Simple Pairing (SSP), IPSec, and ZRTP [35, 36, 37].

PAKEs can roughly be categorized by (a) their way of storing the password, (b) encrypting transmitted public-keys, and (c) their number of participants [38]. In BANDANA, a "balanced" PAKEs should be used to derive a shared secret on both sides because either party can initiate an exchange (a). Whether public-keys are transmitted encrypted or not can independently be chosen as it is not influenced by BANDANA's threat model (b). We focus on a two-party adversarial model (c). Besides this categorization, a modern PAKE should provide resilience to dictionary attacks, replay attacks, Unknown Key-Share attack, and Denning-Sacco attack [39]. As security attributes it should provide mutual authentication, key control, known-key security and forward secrecy. However, we note that BANDANA does not require passkey secrecy of a previous authentication attempt, as discussed in Section 7.2. While any modern PAKE within this category could be chosen, we focus on the integration of BANDANA into real-world applications and thus on the Bluetooth standard. Bluetooth 4.2 with *Secure Connection* and *Secure Simple Pairing* fits well into BANDANA's threat model. BANDANA can be integrated as an additional Out of Band (OoB) mode besides NFC providing $\boldsymbol{k}$ as the Bluetooth passkey. This is considered secure under the PE(i) model in [40]. In Section 6.1 we discuss our choice of an appropriately short key size with a negligible success probability for an attacker (also cf. Section 7.3).

6. Length of Fingerprints and Keys in BANDANA

As sketched in Figure 4, BANDANA utilizes fuzzy cryptography and reliability amplification, both of which shorten the extracted bit sequence so that the final key length is smaller. In the following, we argue on a reasonable size of the key (Section 6.1) as well as on a suggestive number of bits to disregard for reliability amplification (Section 6.2). Finally, we discuss the discriminability of fingerprints (Section 6.3), which defines the parameters of the error correcting code. Final parameters are proposed in Section 6.4.

6.1. Key Size

PAKEs, as discussed in Section 5, prevent offline attacks and can thus provide a sufficiently large security margin even with short key sizes K. Most PAKEs allow for multiple parallel protocol runs per node, such

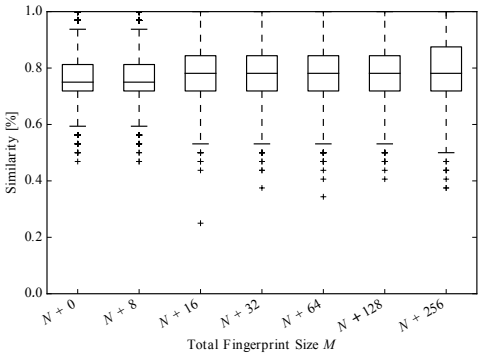


Figure 6: All possible similarities of simultaneous recordings from two *differing* sensor locations on the same subject (intra-body) in the Mannheim dataset (cutoff $N = 32$). Fingerprints are generated by a sliding window with 50% overlap.

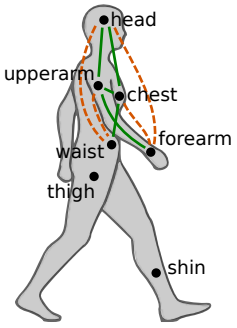


Figure 7: Correlation between on-body sensor locations (Mannheim dataset). green: $\sim 81\%$, dashed orange: $\sim 78\%$, other: $\sim 75\%$

as 2^{10} [34]. In BANDANA we suggest to forbid parallel protocol runs, as this would allow an attacker to boost her success probability by pretending to be multiple devices.

In addition, threat models, such as [41], choose a relatively high $K = 24$ to even have a negligible attacker's success probability if only 16 out of 24 bits are compared correct. Similar margins have been chosen in Bluetooth for PIN comparison with $K = \sim 20$ and ZRTP for word comparison with $K = 20$. In contrast, we can keep a tighter margin as $\boldsymbol{k}$ is generated automatically. Thus, we propose to target a bit size of $K = 16$ with a one-shot success probability for the attacker of 2^{-16}.

6.2. Reliability

We evaluated the number of unreliable bits that could be removed by testing different sequence lengths M with cutoff at $N = 32$ bit using the Mannheim dataset (cf. Figure 6). For $M = 2^i$ the mean-similarity improves by approximately 3% for $i \to i+1$ and settles around $M = N+16$. Thus, we chose $M = N+16$ for our configuration. When repeating this test for $N = 64, 128$, we were able to observe a similar improvement always settling around $M = N + \frac{1}{2}N$.

6.3. Discriminability of Intra- and Inter-body Fingerprints

We observe that upper body locations share a greater similarity than lower body locations. In particular, we identify three similarity groups shown in Figure 7: torso and head ($\sim 81\%$ similarity), upper body with respect to more distant pairs ($\sim 78\%$ similarity), and lower-body locations ($\sim 75\%$ similarity).

Figure 8 illustrates the discriminability between intra-body and inter-body fingerprints. While the intra-body case tests only similarities between differing sensor location on the same body (8037 similarities), each inter-body location case contains 11968975 similarities[2]. As expected, the similarity between different subjects is centered at 50%.

Intra-body similarities for other actions are shown in Figure 9. Due to the strong acceleration during running, which effect the whole body, we observed more homogeneous mean values for this action (cf. Figure 9a). Unfortunately, these are less unique. In contrast, climbing stairs up and down has been shown to generate very unique fingerprints for the upper body (cf. Figure 9b,9c).

In addition to the Mannheim dataset, we evaluated BANDANA using the Osaka dataset, which contains just three sensor locations around the waist, but provides recordings of 482 subjects. Figure 10 illustrates the discriminability between intra-body and inter-body fingerprints. For Osaka, the intra-body test case contains 1446 similarities, while the inter-body case comprises 8694075 similarities.

[2]Note that an attacker is constrained to only ~ 3600 tries per day (cf. Section 7).

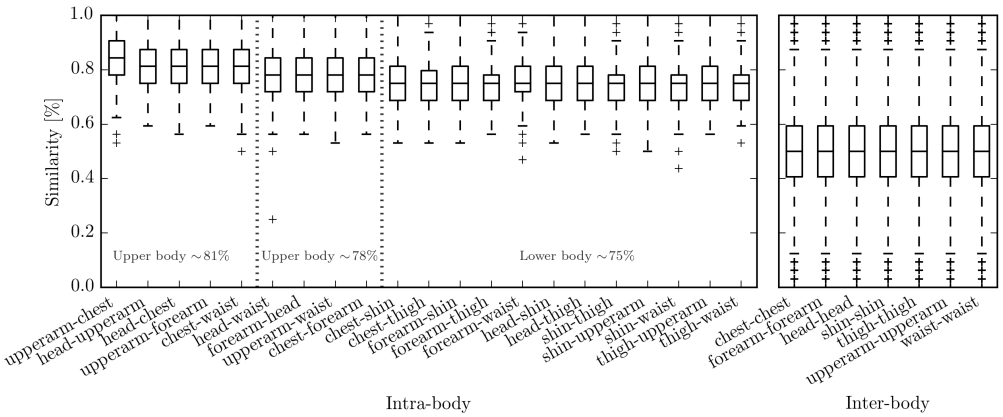


Figure 8: Mannheim (walking): Comparison of intra-body against inter-body similarity. Each value in the *intra-body* boxplot is defined by the similarity of two *different* sensor locations on the same subject (all possible combinations within each subject). For *inter-body*, each boxplot defines a different sensor location. Only *different* subjects are tested against each other with the *same* sensor location. Fingerprint length: $M = 48$ with cutoff at $N = 32$.

In the inter-body case, a number of fingerprints (4.64% (Mannheim); 2.47% (Osaka)) match with above 75% similarity. We attribute these collisions to gait sequences with low entropy due to the design of the quantization scheme. To guard against this, we suggest to disregard gait sequences with low entropy.

6.4. Choice of Parameters

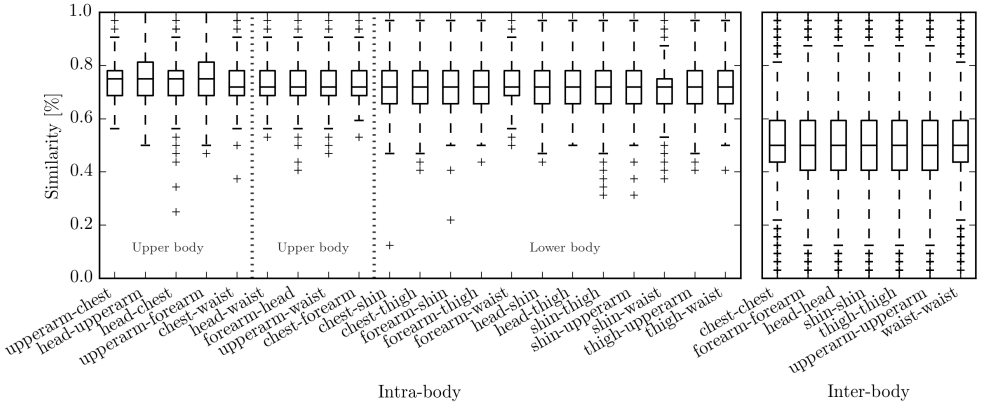
We propose the following configuration for a deployment of BANDANA. As detailed in our security discussion in Section 7, the length K of the resulting key $\boldsymbol{k}$ should be $K = 16$. Following the results depicted in Figure 8, we chose to parameterize the BCH codes to allow correction of at maximum 25% of the bits in the fingerprint. Thus, calculating the error correction rate shows that $N = 32$ bit fingerprints are required: $N = \frac{K}{2u-1} = \frac{16}{2 \cdot 0.75 - 1} = 32$. When using an accelerometer resolution of 50 Hz, we propose a resampling rate of $\rho = 40$ for bit extraction of $b = 4$ bits per gait cycle R_i. Conditioned on ρ and b, we define the correction factor $\tau = \rho / b = 10$. As shown in Figure 6, removing $\frac{1}{3}$ of unreliable bits (i.e. $M = 48$ bit sequences from $q = 12$ gait cycles) provides the best trade-off. We estimate an upper bound for the required length of the recording $\boldsymbol{r}$ as $12 \cdot {\sim}1\ s \approx 12\ s$[3].

7. Security Discussion

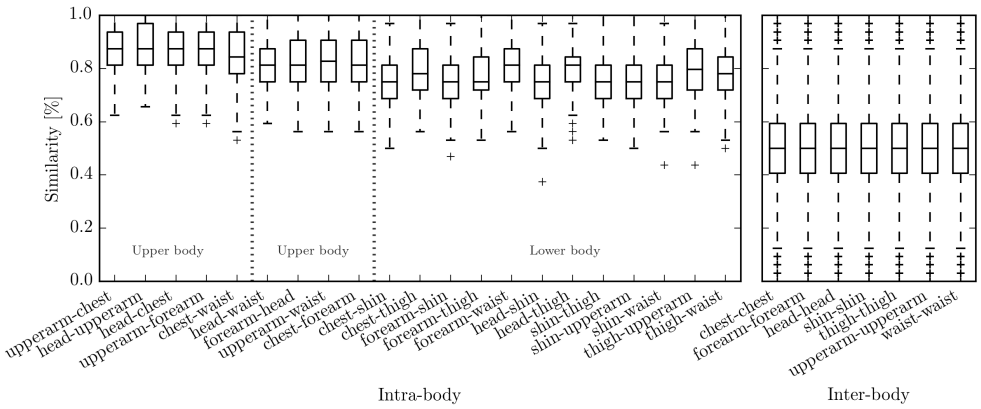
In the following, we analyze BANDANA's security model by discussing possible attack scenarios and properties of the fingerprints. In particular, we focus on the risk that an adversary obtains a gait acceleration sequence that is sufficiently similar to pair with a device located on the subjects body following the BANDANA protocol (cf. figure 4). Since BANDANA corrects 8 bits from the 32 bit fingerprints derived, an adversary would be able to successfully pair with an on-body device provided that she is able to establish a 32 bit fingerprint in which at least 24 bits are identical to the fingerprint generated for the on-body device.

For instance, after successful pairing, an adversary might be able to access private information that shall be restricted to body-worn personal devices only. Considering the example applications specified in the introduction, this might be information related to a subject's shopping list (e.g. for user profiling or also dietary or health related), access to health related data from on-body bio sensors or workout performance, as well as demographics and personal interests.

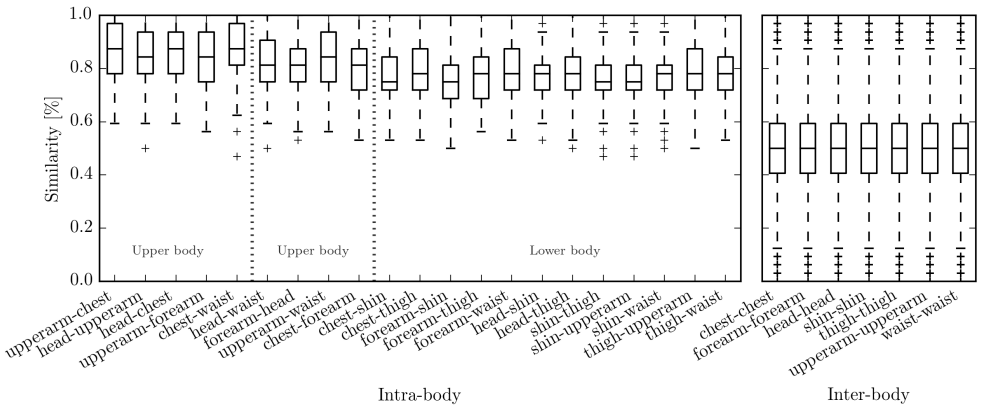
[3]Dall et al. [42] found a mean cadence of 109 steps/minute = 0.91 cycles/second.



(a) Running: Mean values between 75% (upper body) and 71% (lower body)



(b) Climbing down: Mean values between 87% (upper body) and 75% (lower body)



(c) Climbing up: Mean values between 87% (upper body) and 75% (lower body). Subject 2 has been excluded due to missing locations

Figure 9: Intra- vs. inter-body similarity for other actions of the Mannheim dataset. Fingerprint length: $M = 48$ with $N = 32$.

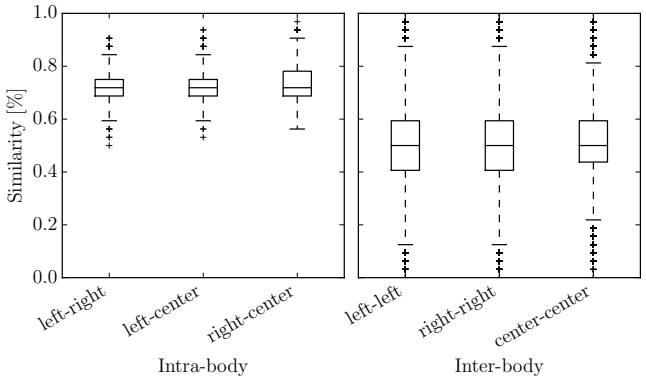


Figure 10: Osaka: Intra- vs. inter-body similarity. Fingerprint length: $M = 48$ with $N = 32$.

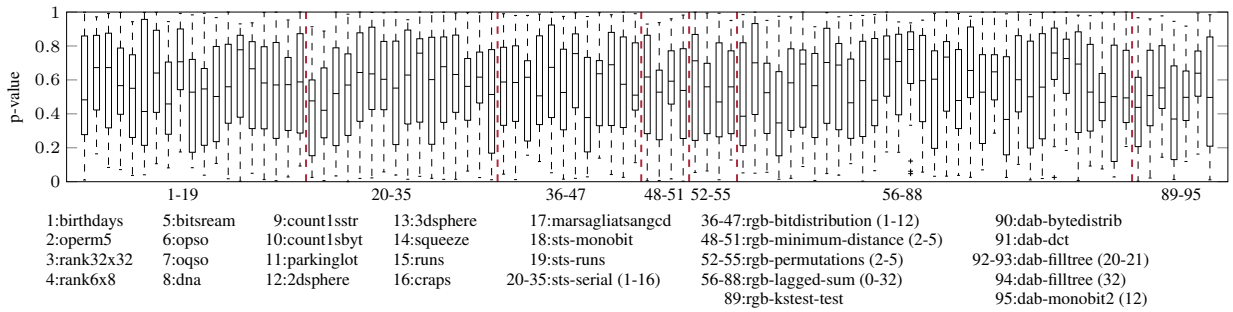


Figure 11: Distribution of p-values achieved for BANDANA fingerprints in 21 runs of the various statistical tests of the dieHarder set of statistical tests.

7.1. Statistical Bias

BANDANA is basically a pseudo random number generator (PRNG) conditioned on instantaneous gait acceleration sequences. As for any PRNGs, it is essential that the generated binary sequences are unbiased since the adversary could else exploit knowledge on the bias of the PRNG to boost her chances to guess the same binary fingerprint. We rigorously tested the keys generated against statistical bias via the dieHarder battery of statistical tests [43], to uncover bias and dependency in the pseudo random sequence. Test runs produce a value that is compared to the theoretical outcome. A p-value, describing the probability that a real Random Number Generator (RNG) would produce this outcome, between 0 and 1 is computed. A good RNG features uniformly distributed p-values. A p-value below a fixed significance level $\alpha = 0.001$ indicates a failure of the PRNG with probability $1-\alpha$. For instance, a p-value ≤ 0.05 is expected 5% of the time. Our results are depicted in Figure 11. Observe that the p-values are well distributed over the complete range and clustered in the center which indicates a good random distribution.

7.2. No Passkey Secrecy Required

In general, for a pairing scheme, an adversary might consider to exhaust the key-space via multiple repeated attacks. This is not possible for BANDANA though, since $\boldsymbol{k}$ changes with each attempt so that previously learned parts cannot be reused. The adversary is confined to challenge one-shot success probability in each new attempt. This is similar, for instance, to Bluetooth 4.2, which implements *Secure Connection* and *Secure Simple Pairing* (SSP). SSP realizes bit commitment, in which the individual bits of the key are iteratively validated in an interactive protocol. Because each Bluetooth pairing uses a new ephemeral passkey, by design SSP does not provide passkey secrecy [35, 40].

7.3. One-Shot Success Probability

Without requiring additional knowledge about the victim's gait, an attacker may want to exhaust the key-space $\mathcal{C} = \mathbb{F}_{2^{16}}$. However, in BANDANA, after each single try, a completely new authentication process (new $\boldsymbol{k}$ independent from the previous one) is started, thus making it impossible to exhaust $\mathcal{C}$. For $M = 48$ bit long sequences, BANDANA's full process takes about $\sim 12\,\mathrm{s}$. Thus, an optimal imposter is constrained to not more than ~ 7200 tries per day. From each 48 bit sequence, 16 bit are disregarded for reliability amplification. From the remaining 32 bit fingerprints, up to 8 bit are corrected by BCH codes, resulting in $|\boldsymbol{k}| = 16$ bit long keys (cf. Section 6.4). The success probability of a single randomly drawn fingerprint is therefore

$$\sum_{k=0}^{8} \left(\begin{array}{c} 32 \\ k \end{array} \right) / 2^{32} = \frac{\sum_{k=0}^{8} \left(\frac{32!}{(32-k)! \cdot k!} \right)}{2^{32}} \approx 0.0035 \tag{1}$$

7.4. Mimic Gait

A frequently envisioned attack on gait-based authentication and pairing schemes is that an adversary would walk next to the victim, thereby mimicing the victims gait so that a device on the body of the adversary would be able to establish a successful pairing to a device on the body of the victim.

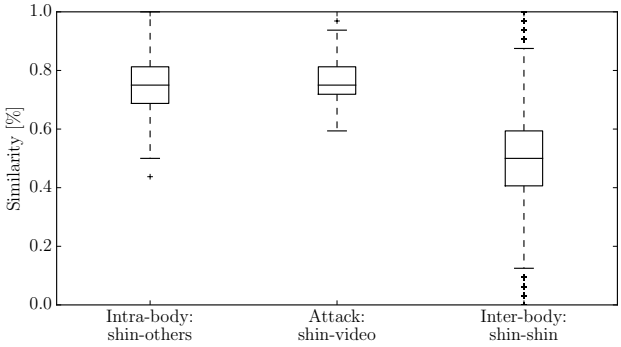
Multiple studies have demonstrated that the success probability of an imposter trying to mimic a subjects gait are low [44] even when trained professionals with similar physical characteristics are employed [25].

For instance, Mjaaland et al [45] trained seven individuals to imitate one specific victim. Even after intensive training over two weeks (5 hours every day), and for one subject even for six weeks, it was not possible for the subjects to accurately imitate the walking pattern of the victim. Also, the provision of continuous visual feedback did not suffice to assist imitators in [46]. Furthermore, the authors of [44] investigated the success probability of an attacker towards a particular subject on a database of 100 subjects and concluded that it is unlikely for an adversary to mimic the subjects gait with sufficient accuracy. This result has been confirmed by [25] who employed professional actors to mimic the gait of 15 subjects with close physical properties. Indeed, the attempt to mimic gait incorporates the risk of asymmetric gait cycles and thus even lowers the chance of success. However, as indicated in [44], the probability of random matches significantly exceeds the expected probability in the birthday paradoxon. An attacker with knowledge to her closest person poses a serious threat to gait-based authentication, and does not even have to impersonate his or her nearest target. This is confirmed in [21, 47] who report an equal error rate (EER) (Equal rates for false acceptance and false rejection) of 20% for gait authentication. In addition, given the gait features of the victim and exploiting a treadmill to control speed, length of steps, thigh lift, hip movement and width of steps, the authors in [48] could reach a false acceptance rate (FAR) of 46.66%.

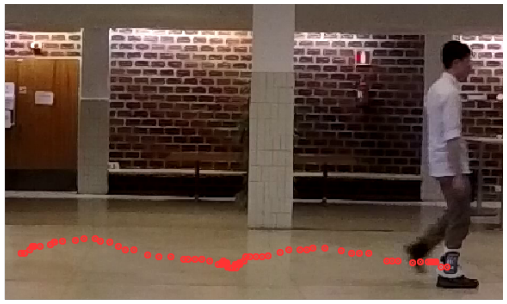
7.5. Video Recording

An attacker with access to surveillance cameras could create a video recording of the victim's gait for the timespan during which the device-to-device authentication happens in order to pair with an on-body device. To investigate this attack, we captured user's movement by a wearable inertial measurement unit (smartphone) attached to the subjects shin, and simultaneously with a high-speed camera at 90 fps. We chose the position shin as this location has clearly distinguishable movement from video. With automated video-tracking software, we have not been able to extract the gait from the video with sufficient accuracy. We therefore utilized Tracker[4] to manually track the smartphone on a frame-to-frame basis (cf. Figure 12b). Then, we estimated acceleration data of the smartphone from the tracking result. Figure 12a illustrates the results. The figure shows that a powerful attacker might achieve successful pairing. We considered optimal conditions (stationary high-speed camera at optimal height & subject passing in straight line). We did not succeed to adhere BANDANAs real-time constraints, but a powerful attacker might achieve this.

[4] http://physlets.org/tracker/



(a) Mannheim: Intra-body (shin wrt to all same-body pairs); video vs. acceleration at shin; inter-body shin-shin (all pairs)



(b) Tracking the z-axis acceleration by manually annotated video recordings (90 fps).

Figure 12: Approximating the acceleration reading from video.

7.6. Attach Malicious Device

In order to establish a pairing with an on-body device, an attacker could attach a malicious device to the body of the victim, e.g. by slipping a small sensor node into the victim's jacket or by selling a compromised device to the victim. This device could create a second communication channel to forward traffic from inside the BAN to an outsider. Due to the fact that BANDANA works without explicit user interaction, this attack could succeed if executed properly and unnoticed. We would like to remark, though, that this physical attack also contains significant risk for the attacker to be revealed when such malicious device is detected.

8. Conclusion

We have discussed and analyzed implicit secure device-to-device authentication via the BANDANA protocol for devices worn on the same body. Shared secrets are implicitly extracted for fingerprints generated from the user's gait. The protocol accounts for errors without comparing the fingerprints directly, but utilizes fuzzy cryptography based on error correcting codes. A quantization method for independently generating similar fingerprints at differing sensor locations has been proposed and evaluated. By selecting only reliable bits, we were able to boost the similarity by 3%. Our fingerprints between devices worn on the same body have a minimum similarity of $\geq 75\%$ in contrast to devices worn on different bodies (50%). The protocol was verified on two large gait datasets and for various gait types (walking, running, descending and ascending stairs). The security properties of the protocol have been discussed. BANDANA enables novel pervasive applications such as the pairing between a personal device and a shopping basket in order to synchronize a shopping list on a personal device with items already placed in the basket, as well as for means to advertise offers tailored to a persons shopping items from the basket on a personal device.

Furthermore, fitness equipment in a gym could spontaneously pair with a fitness app on a personal device during the context of use in order to provide accurate information on the intensity and performance of a specific workout.

Also, tablet-based electronic tourist guides could pair spontaneously with a personal on-body device in order to inquire information on language preferences, interest and background to tailor the provided experience on the respective user.

The list of further examples is countless and in all cases the spontaneous pairing would break in the very moment that the device is discarded or handed to another person, so that no privacy-related information is disclosed unwittingly.

Acknowledgments

We appreciate partial funding from an EIT Digital HII Active project, Academy of Finland and the German Academic Exchange Service (DAAD).

References

[1] D. Schürmann, A. Brüsch, S. Sigg, L. Wolf, BANDANA – Body Area Network Device-to-device Authentication using Natural gAit, in: IEEE International Conference on Pervasive Computing and Communications (PerCom), 2017, pp. 190–196.

[2] D. Bichler, G. Stromberg, M. Huemer, M. Löw, Key generation based on acceleration data of shaking processes, in: International Conference on Ubiquitous Computing, Springer, 2007, pp. 304–317.

[3] R. Mayrhofer, H. Gellersen, Shake well before use: Authentication based on accelerometer data, in: Pervasive computing, Springer, 2007, pp. 144–161.

[4] B. Groza, R. Mayrhofer, SAPHE: simple accelerometer based wireless pairing with heuristic trees, in: Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia, ACM, 2012.

[5] Y. Liu, J. Niu, Overlapped-shaking: A local authentication method for mobile applications, in: 2014 IEEE Computing, Communications and IT Applications Conference (ComComAp), IEEE, 2014, pp. 93–97.

[6] R. Mayrhofer, H. Hlavacs, R. D. Findling, Optimal derotation of shared acceleration time series by determining relative spatial alignment, International Journal of Pervasive Computing and Communications 11 (4).

[7] R. D. Findling, M. Muaaz, D. Hintze, R. Mayrhofer, Shakeunlock: Securely unlock mobile devices by shaking them together, in: Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia, ACM, 2014, pp. 165–174.

[8] T. Van Goethem, W. Scheepers, D. Preuveneers, W. Joosen, Accelerometer-Based Device Fingerprinting for Multi-factor Mobile Authentication, in: International Symposium on Engineering Secure Software and Systems, Springer, 2016, pp. 106–121.

[9] R. Mayrhofer, The candidate key protocol for generating secret shared keys from similar sensor data streams, in: European Workshop on Security in Ad-hoc and Sensor Networks, Springer, 2007, pp. 1–15.

[10] S. Sigg, D. Schürmann, Y. Ji, PINtext: A Framework for Secure Communication Based on Context, 2012.

[11] R. Jin, L. Shi, K. Zeng, A. Pande, P. Mohapatra, MagPairing: Pairing Smartphones in Close Proximity Using Magnetometers, IEEE Transactions on Information Forensics and Security 11 (6) (2016) 1306–1320.

[12] A. Varshavsky, A. Scannell, A. LaMarca, E. De Lara, Amigo: Proximity-Based Authentication of Mobile Devices, Springer, Berlin, Heidelberg, 2007, pp. 253–270.

[13] D. A. Knox, T. Kunz, Wireless fingerprints inside a wireless sensor network, ACM Transactions on Sensor Networks (TOSN) 11 (2) (2015) 37.

[14] M. Miettinen, N. Asokan, T. D. Nguyen, A.-R. Sadeghi, M. Sobhani, Context-based zero-interaction pairing and key evolution for advanced personal devices, in: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2014, pp. 880–891.

[15] D. Schürmann, S. Sigg, Secure communication based on ambient audio, IEEE Transactions on Mobile Computing 12 (2) (2013) 358–370.

[16] K. Kunze, Compensating for on-body placement effects in activity recognition, Ph.D. thesis, Citeseer (2011).

[17] M. Muaaz, R. Mayrhofer, Orientation independent cell phone based gait authentication, in: Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia, ACM, 2014, pp. 161–164.

[18] T. Hoang, D. Choi, V. Vo, A. Nguyen, T. Nguyen, A lightweight gait authentication on mobile phone regardless of installation error, in: IFIP International Information Security Conference, Springer, 2013, pp. 83–101.

[19] E. A. Heinz, K. S. Kunze, S. Sulistyo, H. Junker, P. Lukowicz, G. Tröster, Experimental evaluation of variations in primary features used for accelerometric context recognition, in: European Symposium on AI, 2003.

[20] C. Cornelius, D. Kotz, Recognizing whether sensors are on the same body, in: Proceedings of the 9th International Conference on Pervasive Computing (Pervasive'11), Springer-Verlag, Berlin, Heidelberg, 2011, pp. 332–349.

[21] M. Muaaz, R. Mayrhofer, An analysis of different approaches to gait recognition using cell phone based accelerometers, in: International Conference on Advances in Mobile Computing & Multimedia, ACM, 2013.

[22] A. Srivastava, J. Gummeson, M. Baker, K.-H. Kim, Step-by-step detection of personally collocated mobile devices, in: 16th International Workshop on Mobile Computing Systems and Applications, 2015.

[23] T. Hoang, D. Choi, T. Nguyen, Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme, International Journal of Information Security 14 (6) (2015) 549–560.

[24] A. Juels, M. Wattenberg, A fuzzy commitment scheme, in: 6th ACM conference on Computer and communications security, 1999, pp. 28–36.

[25] M. Muaaz, R. Mayrhofer, Smartphone-based gait recognition: From authentication to imitation, IEEE Transactions on Mobile Computing PP (99) (2017) 1–1.

[26] M. Muaaz, R. Mayrhofer, Cross Pocket Gait Authentication Using Mobile Phone Based Accelerometer Sensor, in: International Conference on Computer Aided Systems Theory, Springer, 2015, pp. 731–738.

[27] W. Xu, G. Revadigar, C. Luo, N. Bergmann, W. Hu, Walkie-talkie: Motion-assisted automatic key generation for secure on-body device communication, in: 2016 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), 2016.

[28] S. O. Madgwick, A. J. Harrison, R. Vaidyanathan, Estimation of IMU and MARG orientation using a gradient descent algorithm, in: 2011 IEEE International Conference on Rehabilitation Robotics, IEEE, 2011, pp. 1–7.
[29] GSMArena.com, Phone finder results for accelerometer and gyrometer, http://www.gsmarena.com (2016).
[30] J. Lester, B. Hannaford, G. Borriello, "Are You with Me?"–Using Accelerometers to Determine If Two Devices Are Carried by the Same Person, in: Pervasive, 2004.
[31] M. W. Whittle, Chapter 2 - Normal gait, in: M. W. Whittle (Ed.), Gait Analysis (Fourth Edition), fourth edition Edition, Butterworth-Heinemann, Edinburgh, 2007, pp. 47–100.
[32] T. Sztyler, H. Stuckenschmidt, Localization of Wearable Devices: An Investigation of Position-Aware Activity Recognition, in: PerCom, 2016.
[33] T. T. Ngo, Y. Makihara, H. Nagahara, Y. Mukaigawa, Y. Yagi, The largest inertial sensor-based gait database and performance evaluation of gait-based personal authentication, Pattern Recognition 47 (1) (2014) 228–237.
[34] S. Vaudenay, Secure Communications over Insecure Channels Based on Short Authenticated Strings, Springer Berlin Heidelberg, Berlin, Heidelberg, 2005, pp. 309–326.
[35] J. Suomalainen, J. Valkonen, N. Asokan, Security Associations in Personal Networks: A Comparative Analysis, Springer Berlin Heidelberg, Berlin, Heidelberg, 2007, pp. 43–57.
[36] C. Kaufman, P. E. Hoffman, Y. Nir, P. Eronen, T. Kivinen, Internet Key Exchange Protocol Version 2 (IKEv2), RFC 7296 (Oct. 2014).
[37] P. Zimmermann, A. Johnston, J. Callas, ZRTP: Media Path Key Agreement for Unicast Secure RTP, RFC 6189 (Informational) (Apr. 2011).
[38] J.-M. Schmidt, Requirements for Password-Authenticated Key Agreement (PAKE) Schemes, RFC 8125 (Apr. 2017).
[39] M. Toorani, Security analysis of j-pake, in: IEEE Symposium on Computers and Communications (ISCC), 2014, pp. 1–6. doi:10.1109/ISCC.2014.6912576.
[40] R. C.-W. Phan, P. Mingard, Analyzing the secure simple pairing in bluetooth v4.0, Wireless Personal Communications 64 (4) (2012) 719–737.
[41] M. Farb, Y.-H. Lin, T. H.-J. Kim, J. McCune, A. Perrig, Safeslinger: Easy-to-use and secure public-key exchange, in: MobiCom'13, ACM, New York, NY, USA, 2013, pp. 417–428.
[42] D. P. Margaret, M. P. R. Walker, G. M. Howard, S. B. William, Step Accumulation per Minute Epoch Is Not the Same as Cadence for Free-Living Adults, Medicine & Science in Sports & Exercise 45 (10).
[43] R. G. Brown, Dieharder: A random number test suite, http://www.phy.duke.edu/∼rgb/General/dieharder.php (2011).
[44] D. Gafurov, E. Snekkenes, P. Bours, Spoof attacks on gait authentication system, IEEE Trans. on Information Forensics and Security 2 (3).
[45] B. B. Mjaaland, P. Bours, D. Gligoroski, Walk the walk: attacking gait biometrics by imitation, in: International Conference on Information Security, Springer, 2010, pp. 361–380.
[46] Ø. Stang, Gait analysis: Is it easy to learn to walk like someone else?, Master's thesis (2007).
[47] M. O. Derawi, C. Nickel, P. Bours, C. Busch, Unobtrusive user-authentication on mobile phones using biometric gait recognition, in: Intelligent Information Hiding and Multimedia Signal Processing, Sixth International Conference on, IEEE, 2010, pp. 306–311.
[48] R. Kumar, V. V. Phoha, A. Jain, Treadmill attack on gait-based authentication systems, in: 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), 2015.