BANDANA – Body Area Network Device-to-device Authentication using Natural gAit

Dominik Schürmann*, Arne Brüsch*†, Stephan Sigg† and Lars Wolf*
*Institute of Operating Systems and Computer Networks, TU Braunschweig
†Ambient Intelligence, Comnet, Aalto University

***Abstract*—Secure spontaneous authentication between devices worn at arbitrary locations on the same body is a challenging, yet unsolved problem. We propose BANDANA, the first-ever implicit secure device-to-device authentication scheme for devices worn on the same body. Our approach leverages instantaneous variations in acceleration patterns from the user's gait to extract always-fresh secure secrets. It enables secure spontaneous pairing of devices worn on the same body or interacted with. The method is robust against noise in sensor readings and active attackers.**

I. Introduction

Device pairing mostly comprises one-time manual pairing of a limited number of devices. However, the personal device-network in the Internet of Things (IoT) is expected to experience frequent fluctuation in device count and identity as devices are added and discarded in the context of use [1]. While seamless device pairing without user interaction promises new personalized services, the user's privacy must be protected. This requires novel secure pairing schemes that scale.

We propose BANDANA, enabling convenient interaction-free secure pairing of devices conditioned to the context of use. As depicted in Figure 1, potential devices are any wearables, for instance, glasses, watches, smartphones, tablet computers or notebooks, smart textile, shoes or devices worn in bags or backpacks. In professional environments, further devices include helmets, Virtual Reality headsets and any co-used tools and wearables shared among workers. In addition, external devices such as a treadmill in a gym can be temporarily and spontaneously paired and BANDANA might be extended to pair with shopping carts, bicycles or cars.

BANDANA exploits common movement patterns to generate robust secure keys for pairs of devices worn at arbitrary locations on the same body. In contrast to previous work, proximity of devices on the body is not necessary as gait can be extracted at arbitrary body locations. The protocol is flexible in the strength of the generated key and can, for instance, replace Bluetooth PIN authentication with 24 seconds of gait while highly secure device pairing with 128 bit keys requires about 96 seconds of gait. We exploit instantaneous variations in gait sequences for implicit shared secrets among all devices on the same body. The contributions of our work are (A) a secure ad-hoc pairing scheme for devices worn on the same body, and (B) the experimental verification of the protocol on a large-scale gait dataset.

In a nutshell, a device (1) records acceleration sequences, (2) corrects their rotation error, (3) computes the mean gait from the previous gait cycles, and (4) generates a binary feature vector as the difference between this mean gait and the individual gait cycles. The feature vector reflects the pattern in which the mean gait exceeds or falls below the individual gait. Although individual and mean gait differ for various body locations, BANDANA exploits the correlation in the deviation from the mean. Utilizing fuzzy cryptography, device pairs are then able to (5) generate identical secret keys from similar binary fingerprints without disclosing any information about the fingerprints or keys on the wireless channel.

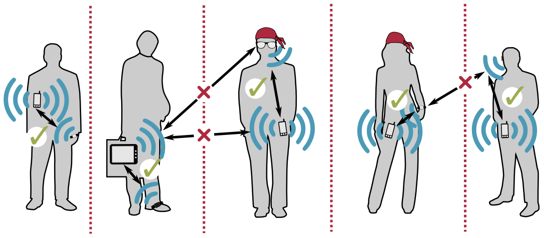
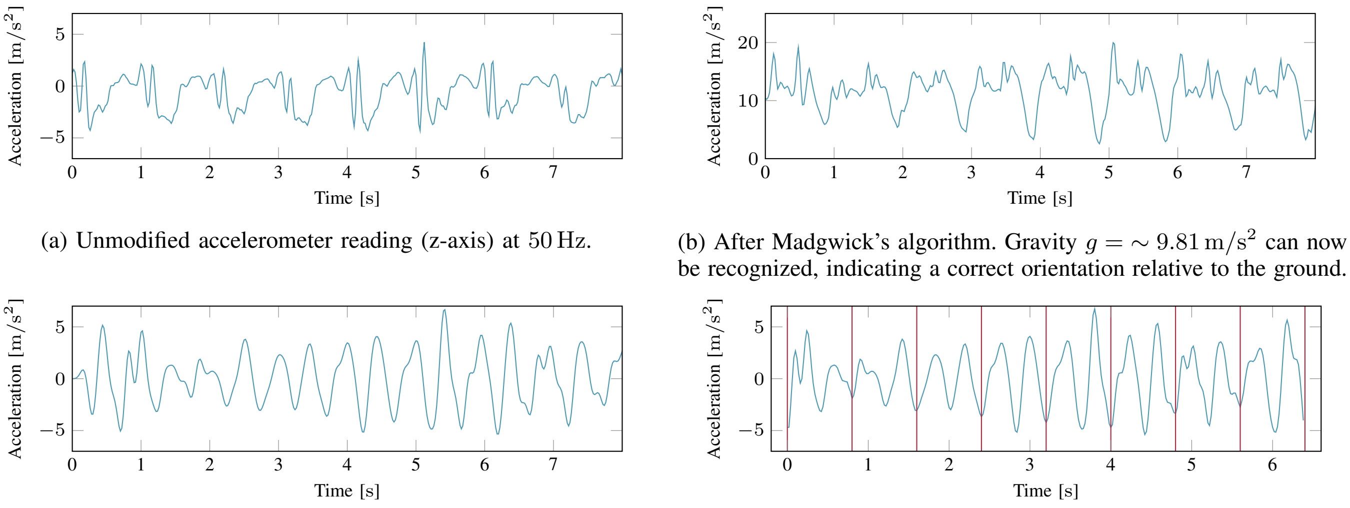


Fig. 1: BANDANA creates implicit security barriers towards devices in proximity, while establishing ad-hoc spontaneously secure connections between devices worn on the same body.

II. Related Work

For authentication based on arbitrary co-aligned sensor data, Mayrhofer [2] proposes the candidate key protocol. It interactively exchanges hashes from feature sequences as short secrets and concatenates the key from the secrets with matching hashes. Based on this protocol, unlocking of a mobile device can be achieved by shaking it simultaneously with a smartwatch [3], [4]. Their approach, however, requires that acceleration sequences are exchanged and compared via an established secure channel and also that both devices are spatially close in order for acceleration sequences to be sufficiently similar. Sensor modalities suited for unattended co-presence-based device pairing extend to magnetometer [5], RF-signals [6], [7] luminosity [8] or audio [9]. In contrast to our study, however, these allow pairings not to the same body but only to devices in proximity.

Cornelius et al. [10] identified devices co-located on the same body via correlated acceleration readings. Even though after abstracting to the magnitude, the resulting signal still differed greatly due to inherently differing movement of underlying body parts (e.g. arm vs. head vs. legs) [11], the



(a) Unmodified accelerometer reading (z-axis) at 50 Hz.

(b) After Madgwick's algorithm. Gravity $g = \sim 9.81\,\mathrm{m/s^2}$ can now be recognized, indicating a correct orientation relative to the ground.

(c) Application of Type-II Chebyshev bandpass filter.

(d) Resampling to $\rho = 40$ and gait detection with $q = 8$ cycles.

Fig. 2: Pre-processing and gait cycle detection. Z-axis of an accelerometer attached to the forearm is depicted.

authors showed good correlation among all body locations from mean, standard deviation, variance, mean absolute deviation and interquartile range as well as signal's energy. This is a strong indication that secure keys conditioned on co-location on the same body exist. However, as correlation can be alternating positively and negatively, it remains unsolved how this can be exploited for the generation of keys, when the sequences shall not be disclosed to an adversary listening to any communication between nodes.

An activity well recognized over the whole body is walking [12]. For instance, identical step patterns from acceleration were utilized for co-location detection [13]. Hoang et al. [14] generated a key from the difference of a mean world gait (spanning the complete population) to the individual's mean gait. In this way, the authors assured that the resulting sequence is well balanced and uniformly distributed.

Recent studies on gait-based authentication, however, (1) do not address the impact of different on-body locations and sensor orientation and (2) use gait as a unique biometric feature that does not change for an individual over time. In contrast, we generate always-fresh keys from instantaneous accelerations for arbitrary locations on the human body.

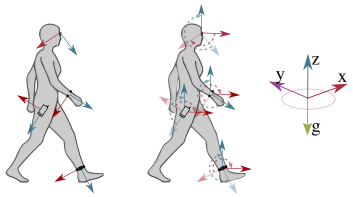
III. Fundamentals

In this section, our gait cycle detection algorithm is presented which builds on ideas by Hoang et al. [14], [15]. In addition, we also utilize gyroscope readings to normalize the sensor's orientation and keep only the z-Axis that points in the opposite direction of gravity. A gait cycle is defined as the "time interval between two successive steps" [16]. The algorithms input is a vector of amplitude values $\boldsymbol{z} = (z_1, \ldots, z_n)$ of the accelerometer z-axis (cf. Figure 2a). Its output is a gait sequence of consecutive gait cycles with normalized length.

To find repetitive parts in the signal, we extract the local minima with similar distance to each other to define clearly separated cycles. Our filtering method is based on autocorrelation and distance calculation. The discrete autocorrelation at time lag k and with variance σ^2 is estimated as $Acorr(k) = \frac{1}{(n-k)\sigma^2}\sum_{t\in\mathbb{Z}} z_{t+k} \cdot \overline{z}_t$ where $\overline{z}_t$ represents 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 calculated. δ_{mean} defines the length of *half* a cycle, i.e., the time between the initial contact of the starting foot followed by the initial contact of the subsequent foot. Thus, for q describing the number of gait cycles, $m = q \cdot 2$. For the gait-cycle extraction, we assume healthy subjects, where the movement of the right foot is sufficiently similar to the left foot and thus have nearly the same distance. δ_{mean} can now be used to select indices of minima from $\boldsymbol{z}$ that represent clear cycles with the same length: $\boldsymbol{\mu} = \{\mu_1, \ldots, \mu_i, \ldots, \mu_{m-1}\}$; $\mu_i = \arg\min(z_{\zeta_i - \tau}, z_{\zeta_i - \tau + 1}, \ldots, z_{\zeta_i + \delta_{mean} + \tau})$. Every μ_j represents the index of a minimum in $\boldsymbol{z}$ limited to the range of δ_{mean} where τ defines an additional user defined factor to account for small deviations in the gait duration. The indices in $\boldsymbol{\mu}$ can now be used to split the raw data $\boldsymbol{z}$ into full gait cycles $\boldsymbol{Z} = \{Z_1, \ldots, Z_i, \ldots, Z_q\}$; $Z_i = (z_{\mu_{\frac{i}{2}}}, \ldots, z_{\mu_i}, \ldots, z_{\mu_{\frac{i+1}{2}} - 1})$. Finally, the length of gait cycles are normalized by resampling every Z_i using a Fourier method to a fixed number of samples ρ per gait cycle so that $|Z_i| = \rho$ (cf. Figure 2d). For ease of presentation, we will, in the following, describe such normalized gait cycle with $Z_i = \{Z_{i1}, \ldots, Z_{i\rho}\}$. The choice of ρ depends on factors such as sample rate and requirements of the quantization algorithm discussed in Section IV.

A. Dataset

We used the real-world dataset by Sztyler et al. [17] for position-aware activity recognition. 15 subjects performed different actions for approximately 10 - 12 minutes each. They



(a) Before (b) After Madgwick

Fig. 3: Effect of applying Madgwick's algorithm.

were equipped with 7 sensors on different body locations. These locations were chosen in order to gather data from every part of the body that behaves different during human motion.

B. Data Pre-Processing

In real-world settings, sensors locations differ, which introduces changing orientations due to body part movements (cf. Figure 3a). For best results, it is crucial to rotate every data point such that at all time one of the axes is facing in the direction opposite of gravity (cf. Figure 3b).

Nowadays, most mobile devices contain gyroscopes in addition to accelerometers [18]. We therefore posses information about the initial device orientation (since the force of gravity is included in every measurement recorded by the accelerometer) as well as the angular velocity of the sensor platform itself. Thus, it is possible to correct the ongoing orientation error. We employ the algorithm proposed by Madgwick et al. [19] to rotate all measurements z_i accordingly, resulting in a signal as shown in Figure 2b. Note that the output is only guaranteed to be aligned along the z-axis. When comparing two readings, both other axes may point in different directions as no other fixed direction as, e.g., the direction of North is obtainable.

For noise removal, we apply a Type II Chebyshev bandpass filter with passband chosen between $0.5\,\mathrm{Hz}$ and $12\,\mathrm{Hz}$ (cf. Section V-B). The resulting signal is shown in Figure 2c.

IV. BANDANA

After correcting orientations from accelerometer and gyroscope data together with applying a band-pass filter, the gait cycle detection algorithm produces a periodic signal. Shared secrets need to be generated based on these signals on different devices independently without disclosing them on the channel.

A. Quantization

To generate binary fingerprints from the continuous gait sequence, we propose a quantization algorithm inspired by Hoang et al. [14]. Recall the definition of Z_i with the normalized gait cycle $|Z_i| = \rho$ and $Z_i = \{Z_{i1}, \dots, Z_{i\rho}\}$. We define the average gait cycle as $\boldsymbol{A} = (A_1, \dots, A_j, \dots A_\rho)$; $A_j = \frac{\sum_{i=1}^{q} Z_{ij}}{q}$. Fingerprint bits are extracted by calculating the energy difference between each gait cycle Z_i and $\boldsymbol{A}$ as depicted in Figure 4. To extract b bit per Z_i, each Z_i is split into b parts of the same length ρ/b. Thus, a binary fingerprint is defined by $\tilde{\boldsymbol{f}} = (\tilde{f}_{11}, \dots, \tilde{f}_{1\frac{\rho}{b}}, \dots, \tilde{f}_{b1}, \dots, \tilde{f}_{b\frac{\rho}{b}});.$

$$\tilde{f}_{ij} = \begin{cases} 1, & \delta_{ij} > 0 \\ 0, & \text{otherwise.} \end{cases}$$

as exemplary shown in Figure 4a. In the following, the fingerprint vector is written as $\tilde{\boldsymbol{f}} = (\tilde{f}_1, \dots, \tilde{f}_M)$.

B. Reliability

To calculate the reliability of the extracted bits, the differences of the quantization algorithm are stored as $\boldsymbol{\delta} = (\delta_{11}, \dots, \delta_{1b}, \dots, \delta_{q1}, \dots, \delta_{qb})$. The indices of $\boldsymbol{\delta}$ are sorted in descending order by their absolute value $|\delta_{ij}|$ to retrieve the reliability ordering $\boldsymbol{r} = (r_1, \dots, r_M)$ with $r_i \geq r_{i+1}$. We refer to $\boldsymbol{r}$ as the *reliability vector* containing indices which experienced the highest difference between the mean gait $\boldsymbol{A}$ and an instantaneous normalized gait Z_j. These bits are most reliable since they have high probability to be identical at arbitrary body locations. In Figure 4b colors to indicate the associated reliability. The elements of $\tilde{\boldsymbol{f}}$ are then sorted according to their values of $\boldsymbol{r}$ and the most reliable first N are the fingerprint $\boldsymbol{f} = (f_{r_1}, \dots, f_{r_N})$ (cf. Figure 4c).

C. Fuzzy Cryptography

To derive unique shared secrets on two devices without disclosing the fingerprint, error correcting codes are used, which encode messages from the messagespace $m \in \mathcal{M}$ into codewords of the (larger) codespace $c \in \mathcal{C}$ introducing redundancies. Then, errors from transmission of c over lossy channels are corrected before decoding back to m.

In a sense, our fingerprints $\boldsymbol{f}$ are lossy as they are not entirely equal on the devices trying to mutually authenticate. Here, the codespace $\mathcal{C}$ is chosen in a way that we can directly pick a fingerprint $\boldsymbol{f}$ from this codespace and apply the *Decode*-method to derive a binary key $\boldsymbol{k}$ that is error corrected. Due to the usage of binary fingerprints we propose the usage of BCH codes over the Galois field $\mathbb{F}_2$. A BCH code can be parameterized to correct up to t errors, which in our case must be chosen carefully to allow for errors within different locations on the same body but not for correction of errors between different bodies. As with the other parameters, t is chosen based on our evaluation in Section V.

D. Protocol

Figure 5 specifies the BANDANA protocol. For two co-aligned devices A and B, fingerprints $\boldsymbol{f_A}$, $\boldsymbol{f_B}$ and reliability vectors $\boldsymbol{r_A}$, $\boldsymbol{r_B}$ are derived on both devices independently. The vector with the higher hash is used for reliability ordering on both sides. To account for errors, we apply the BCH decoding-method to reduce both $\boldsymbol{r_A}$ and $\boldsymbol{r_B}$ to a unique $\boldsymbol{k}$, which is then used as the password for a Password-Authenticated Key Agreement (PAKE). Both devices now share the same secret $\boldsymbol{s}$ protected by a key agreement authenticated by their gait fingerprints. We propose the usage of a modern non-patented PAKE that feature additional countermeasures for low entropy passwords, such as J-PAKE [20] or SRP [21].

For devices with high clock drift, the protocol can be extended to allow for multiple tries with shifted fingerprints.

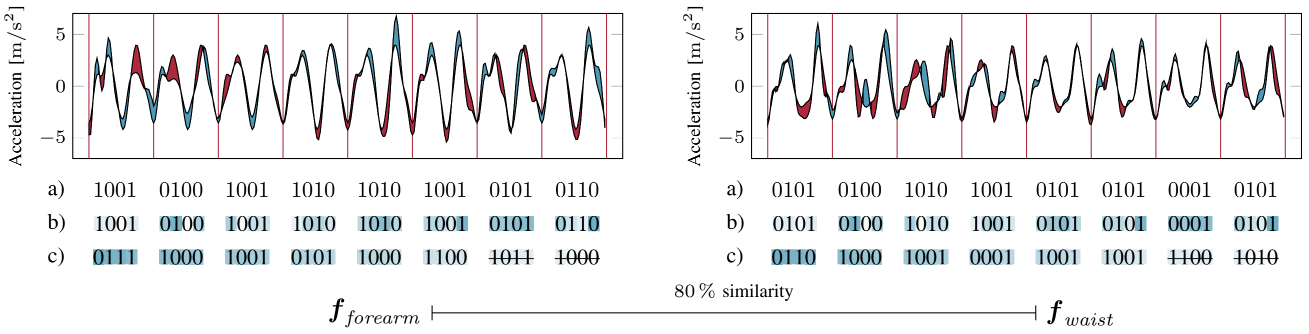


Fig. 4: Independent fingerprint generation on forearm and waist (forearm pre-processing is shown in Figure 2): Energy levels above the average gait cycle $\boldsymbol{A}$ are blue and below red. After quantization in a), reliabilities are calculated and assigned to each bit in b). Darker color, indicates higher reliability. In c) the fingerprint is sorted by reliability vector of the forearm.

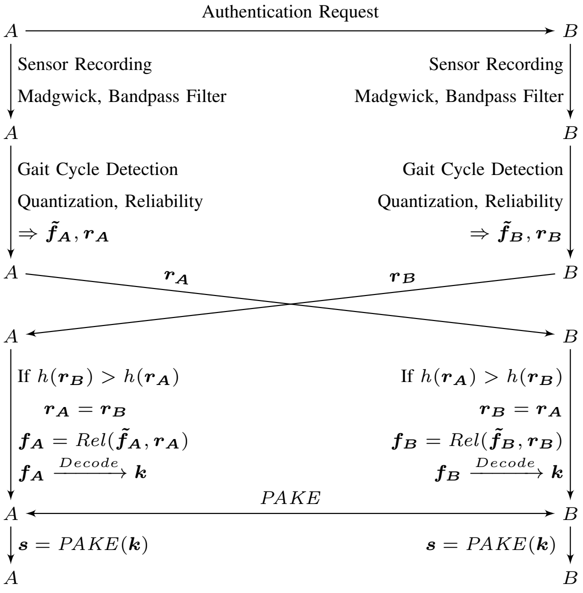

Authentication Request
A
B
Sensor Recording
Madgwick, Bandpass Filter
Sensor Recording
Madgwick, Bandpass Filter
A
B
Gait Cycle Detection
Quantization, Reliability
$\Rightarrow \tilde{\boldsymbol{f}}_{\boldsymbol{A}}, \boldsymbol{r}_{\boldsymbol{A}}$
Gait Cycle Detection
Quantization, Reliability
$\Rightarrow \tilde{\boldsymbol{f}}_{\boldsymbol{B}}, \boldsymbol{r}_{\boldsymbol{B}}$
A
$\boldsymbol{r}_{\boldsymbol{A}}$
$\boldsymbol{r}_{\boldsymbol{B}}$
B
A
B
If $h(\boldsymbol{r}_{\boldsymbol{B}}) > h(\boldsymbol{r}_{\boldsymbol{A}})$
$\boldsymbol{r}_{\boldsymbol{A}} = \boldsymbol{r}_{\boldsymbol{B}}$
$\boldsymbol{f}_{\boldsymbol{A}} = Rel(\tilde{\boldsymbol{f}}_{\boldsymbol{A}}, \boldsymbol{r}_{\boldsymbol{A}})$
$\boldsymbol{f}_{\boldsymbol{A}} \xrightarrow{Decode} \boldsymbol{k}$
If $h(\boldsymbol{r}_{\boldsymbol{A}}) > h(\boldsymbol{r}_{\boldsymbol{B}})$
$\boldsymbol{r}_{\boldsymbol{B}} = \boldsymbol{r}_{\boldsymbol{A}}$
$\boldsymbol{f}_{\boldsymbol{B}} = Rel(\tilde{\boldsymbol{f}}_{\boldsymbol{B}}, \boldsymbol{r}_{\boldsymbol{B}})$
$\boldsymbol{f}_{\boldsymbol{B}} \xrightarrow{Decode} \boldsymbol{k}$
$PAKE$
A
B
$\boldsymbol{s} = PAKE(\boldsymbol{k})$
$\boldsymbol{s} = PAKE(\boldsymbol{k})$
A
B

Fig. 5: BANDANA protocol sequence between two devices A and B worn on the same body.

V. Evaluation

A. Signal Coherence

After applying Madgwick's algorithm (cf. Section III-B), we end up with sensor readings where the z-axis points to the ground. This allows to examine their relation. For this, we calculate the spectral coherence for different sensor combinations to test whether any causality between readings taken simultaneously by sensors located at different locations on the same body exists – apart from just the correlation for the motion in general. Figure 6 shows that there is high correlation between records taken simultaneously. Between arbitrary records, there is only correlation between 0 Hz up to 0.5 Hz. This leaves us with two major results: (a) There is a measurable causality between sensor readings taken simultaneously on the same body; (b) Some correlation at lower frequencies still exists.

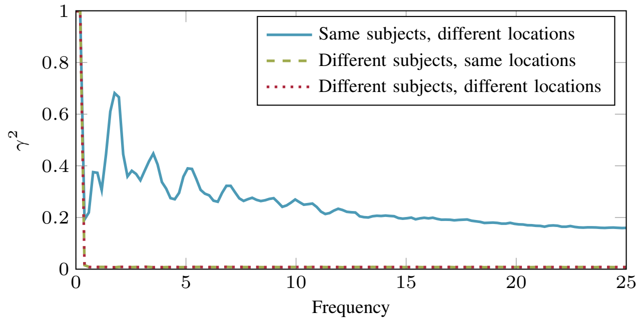


Fig. 6: Average spectral coherence over full sensor readings of the Mannheim dataset for same and different subject.

B. Bandpass Filter

As visualized in Figure 6, there still exists some unexpected correlation between arbitrary readings on low frequencies. As these frequencies - up to approximately 0.5 Hz - only add noise, we filter them out while keeping all the frequencies above. We thus employ a Type-II Chebyshev filter, which is known to have a very steep drop at the cutoff frequency. Furthermore, in contrast to Type-I, Type-II Chebyshev filters do not have any ripple in the passband. Researchers in the domain of Activity Recognition report that human motion does not affect frequencies significantly above 10 Hz [22]. Based on this observation and the coherence depicted in Figure 6, we decided to choose an upper cutoff frequency of 12 Hz.

C. Reliability

Our quantization scheme defines that iff $\delta_{ij} > 0$ for fixed i, j is true for A, the same has to apply for B for at least 80 %. Some Z_{ij} are less prone to leading to different bits between sensors at different body locations than others, namely those with a higher difference δ_{ij} to the mean gait $\boldsymbol{A}$. Both A and B keep a reliability value for each bit of the fingerprint. According to the protocol sequence (cf. Figure 5), one of these reliability vectors is chosen and the fingerprint is sorted by each party following the vector's order of indices (cf. Figure 4). In a last step, the fingerprint's most unreliable bits

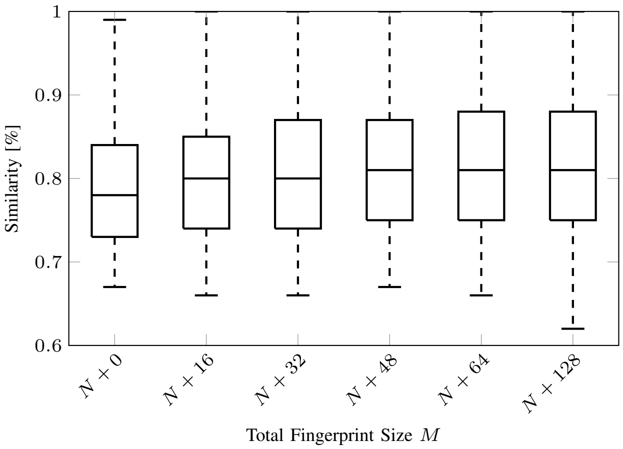


Fig. 7: Fingerprint similarity of different sizes M with cutoff at $N = 128$ to evaluate the influence of *Rel*(). Each boxplot value is defined by the similarity between two fingerprints at *different* sensor locations within the same subject (intra-body). All possible similarities over all combinations of sensor locations within each subject are evaluated. Fingerprints are generated by a sliding window over the sensor data with half-overlapping windows. Only fingerprints from the same window are matched against each other.

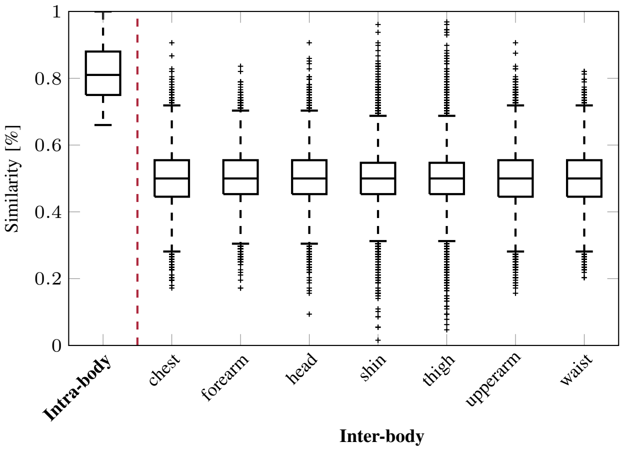


Fig. 8: Intra-body and inter-body fingerprint similarity. For *intra-body*, each boxplot value is defined by the similarity between two *different* sensor locations (all possible similarities over all combinations of sensor locations within each subject). For *inter-body*, each boxplot defines a different sensor location. Only *different* subjects are tested against each other with the *same* sensor locations. Fingerprints are generated by a sliding window over the sensor data with half-overlapping windows for $M = 192$ with cutoff at $N = 128$.

are discarded. To show the method's viability, we calculated the fingerprints' similarity over all 15 subjects and all 7 sensor locations. As shown in Figure 7, we chose different fingerprint sizes M with cutoff at $N = 128$ to test how many additional bits should be discarded to gain the best similarity. The mean-similarity improves with greater values of M and settles around $N+64$ with an average improvement of approximately $4\,\%$. Thus, we chose $N + 64$ for our configuration.

D. Discriminability of Intra- and Inter-body Fingerprints

Figure 8 illustrates the discriminability between intra-body and inter-body fingerprints. While the intra-body case tests only similarities between different sensor locations on the same body (315 similarities), the inter-body case is much larger (8880300 similarities). The mean similarity between different subjects is $50\,\%$, which is indistinguishable from a similarity between random bit sequences. In comparison, the inter-body similarity exhibits a clear security margin with $82\,\%$. It is important to note that this test evaluates the worst case of brute forcing all possible combinations between subjects. In reality, an attacker is constrained to ~ 900 tries per day since BANDANA's process takes up to $\sim 96\,$s with $M = 192$ bit long fingerprints. In the inter-body case, it can be seen that a small number of fingerprints match with unexpected high similarity values (outliers). We assume that these collisions happen in case of gait sequences with very low entropy still exhibiting specific pattern due to the design of the quantization scheme. While this should be investigated further, only $0.0642\,\%$ of these collisions show similarity values above $80\,\%$.

TABLE I: Fingerprint similarity between locations on the same body (intra-body). Shown is the mean over all 15 subjects.

	chest	forearm	head	shin	thigh	upperarm	waist
chest	1.0	0.82	0.74	0.78	0.78	0.88	0.81
forearm	0.82	1.0	0.8	0.81	0.88	0.89	0.89
head	0.74	0.8	1.0	0.8	0.76	0.77	0.78
shin	0.78	0.81	0.8	1.0	0.77	0.78	0.8
thigh	0.78	0.88	0.76	0.77	1.0	0.85	0.84
upperarm	0.88	0.89	0.77	0.78	0.85	1.0	0.88
waist	0.81	0.89	0.78	0.8	0.84	0.88	1.0

E. Similarities between Sensor Location-Combinations

Table I illustrates how well different sensor locations authenticate against each other. We found out that chest against other locations and head against other locations perform worse while forearm and waist perform best.

F. Statistical Bias

For the robustness against a potent adversary, it is important that the keys generated from gait sequences are random. For instance, Figure 10 exemplarily depicts 64 keys we extracted using BANDANA with fingerprint length $N = 256$ bits for an intuitive illustration of the randomness of the generated fingerprints. We tested the keys generated by BANDANA against statistical bias and employed the dieHarder battery of statistical tests for this end [23]. While these tests can not replace cryptanalysis, they are designed to uncover bias and

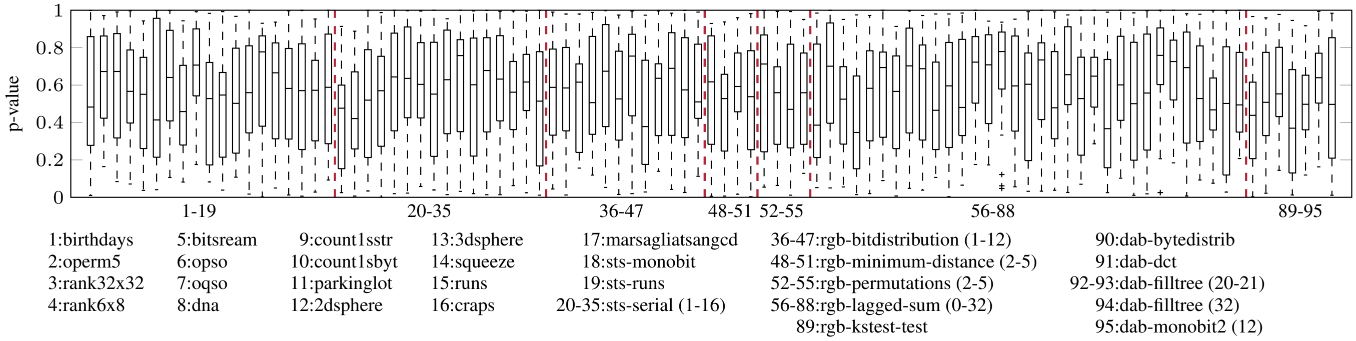


Fig. 9: Distribution of p-values achieved for 128 bit keys (fingerprint length $M = 192$, 64 unreliable bits removed) in 21 runs of the various statistical tests of the dieHarder set of statistical tests.

Fig. 10: Illustration of 64 binary keys. Each row contains one 256 bit fingerprint with $1 =$ black and $0 =$ white.

dependency in the pseudo random sequence. Every test has an expected distribution of outcomes. A p-value, between 0 and 1, describes the probability that a real Random Number Generator (RNG) would produce this outcome. A good RNG will have a range of p-values that follows a uniform distribution. A p-value below a significance level $\alpha = 0.001$ indicates a failure of the RNG with probability $1 - \alpha$. For instance, a p-value ≤ 0.05 is expected $5\,\%$ of the time. Our results in Figure 9 depict well distributed p-values clustered in the center which indicates a good random distribution.

VI. Conclusion

We have presented BANDANA, a secure device-to-device authentication scheme for devices worn on the same body. By generating unique fingerprints from the user's gait, we were able to establish shared secrets implicitly without user interaction. The protocol accounts for errors without comparing the fingerprints directly, instead it utilizes fuzzy cryptography based on error correcting codes. A novel quantization method for independently generating similar fingerprints at different sensor locations has been proposed and evaluated. By selecting only reliable fingerprint bits, we were able to boost the similarity by $4\,\%$. We evaluated the security by generating all possible fingerprints in our dataset for sensors worn on the same body (intra-body) in comparison to sensors worn on different bodies (inter-body). While intra-body similarity is indistinguishable from similarity between random bit sequences $(50\,\%)$, inter-body similarity exhibits a clear security margin with $82\,\%$. Based on our evaluation, the final specification of BANDANA is depicted in Figure 11.

Parameters: We used a resampling rate of $\rho = 40$ to extract $b = 4$ bits per gait cycle R_i resulting in $\tau = \rho/b = 10$. For $N = 128$ bit keys we used $M = 192$ bit fingerprints ($q = 48$ gait cycles), disregarding 64 least reliable bits. Fuzzy pairing corrected at most $20\,\%$ (cf. Figure 8) dissimilar bits ($t = \lfloor 128 \cdot 0.2 \rfloor = 25$). Consequently, at least $80\,\%$ similarity between the fingerprints is required. This results in a 103-bit security level for the PAKE password $\boldsymbol{k}$.

Time to generate a secure key: The key-strength depends on the number of gait cycles. Our parameters $b = 4, \rho = 40, M = 192$ result in the worst-case duration of $\boldsymbol{r} = 96\,\mathrm{s}$ assuming that gait cycles do not exceed 2 seconds. Clearly, by extracting more bits from each cycle or requiring shorter key sequences, generation time can be reduced linearly.

Time after which secure key generation fails: After removal from the body, the gait-history is bit by bit replaced so that similarity in fingerprints gradually deteriorates from about $80\,\%$ to $50\,\%$ (cf. Figure 8). A fuzzy cryptography scheme requiring at least $75\,\%$ similarity (which is weaker than $80\,\%$ in our results), then fails after 9.6 gait cycles or 19.2 seconds ($0.8 \cdot 80\,\% + 0.2 \cdot 50\,\% \approx 74\,\%$).

Adaptive security levels: The key-length determines its strength. E.g. manual Bluetooth pairing (4-digit PIN) is equivalent to a 32 bit key, generated in 24 seconds ($b = 4, \rho = 40, M = 48$). Key generation after removing the device from the body would then fail after 5 seconds. An adaptive security protocol can alter security levels (and granted rights) conditioned on the co-presence duration.

Pairing in the absence of gait: For some activities, gait is not available. We did not consider this case in our study. The primary challenge in such a case is then to identify a feature recognizable from arbitrary locations on the same body, since else, device pairing is constrained to proximate body parts (e.g. in [24]).

Technical requirements: Devices should feature accelerometer and gyroscope. While instrumentations without gyroscope might also be feasible in some scenarios, continuous correction of accelerometer orientation works most reliable with gyroscope information. Given its low price and since most contemporary wearables with acceleration sensors also include a gyroscope, this is not a limitation.

Fig. 11: Technical specification and limitations of BANDANA.

REFERENCES

[1] M. K. Chong, R. Mayrhofer, and H. Gellersen, "A survey of user interaction for spontaneous device association," *ACM Computing Surveys (CSUR)*, vol. 47, no. 1, p. 8, 2014.

[2] 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.

[3] R. D. Findling, M. Muaaz, D. Hintze, and 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.

[4] R. D. Findling, M. Muaaz, D. Hintze, and R. Mayrhofer, "ShakeUnlock: Securely Transfer Authentication States Between Mobile Devices," *IEEE Transactions on Mobile Computing*, vol. PP, no. 99, pp. 1–1, 2016.

[5] R. Jin, L. Shi, K. Zeng, A. Pande, and P. Mohapatra, "MagPairing: Pairing Smartphones in Close Proximity Using Magnetometers," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1306–1320, 2016.

[6] A. Varshavsky, A. Scannell, A. LaMarca, and E. De Lara, "Amigo: Proximity-based authentication of mobile devices," in *UbiComp 2007: Ubiquitous Computing: 9th International Conference*. Berlin, Heidelberg: Springer, 2007, pp. 253–270.

[7] D. A. Knox and T. Kunz, "Wireless fingerprints inside a wireless sensor network," *ACM Transactions on Sensor Networks (TOSN)*, vol. 11, no. 2, p. 37, 2015.

[8] M. Miettinen, N Asokan, T. D. Nguyen, A.-R. Sadeghi, and 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.

[9] D. Schürmann and S. Sigg, "Secure communication based on ambient audio," *IEEE Transactions on Mobile Computing*, vol. 12, no. 2, pp. 358–370, 2013.

[10] C. Cornelius and D. Kotz, "Recognizing whether sensors are on the same body," in *Proceedings of the 9th International Conference on Pervasive Computing (Pervasive'11)*, San Francisco, USA: Springer-Verlag, 2011, pp. 332–349.

[11] E. A. Heinz, K. S. Kunze, S. Sulistyo, H. Junker, P. Lukowicz, and G. Tröster, "Experimental evaluation of variations in primary features used for accelerometric context recognition," in *European Symposium on Ambient Intelligence*, Springer, 2003, pp. 252–263.

[12] M. Muaaz and R. Mayrhofer, "An analysis of different approaches to gait recognition using cell phone based accelerometers," in *Proceedings of International Conference on Advances in Mobile Computing & Multimedia*, ACM, 2013, p. 293.

[13] A. Srivastava, J. Gummeson, M. Baker, and K.-H. Kim, "Step-by-step detection of personally collocated mobile devices," in *Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications*, ACM, 2015, pp. 93–98.

[14] T. Hoang, D. Choi, and T. Nguyen, "Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme," *International Journal of Information Security*, vol. 14, no. 6, pp. 549–560, 2015.

[15] T. Hoang, D. Choi, V. Vo, A. Nguyen, and T. Nguyen, "A Lightweight Gait Authentication on Mobile Phone Regardless of Installation Error," in *Security and Privacy Protection in Information Processing Systems: 28th IFIP TC 11 International Conference, SEC 2013, Auckland, New Zealand, July 8-10, 2013. Proceedings*, L. J. Janczewski, H. B. Wolfe, and S. Shenoi, Eds. Berlin, Heidelberg: Springer, 2013, pp. 83–101.

[16] M. W. Whittle, "Chapter 2 - Normal gait," in *Gait Analysis (Fourth Edition)*, M. W. Whittle, Ed., Fourth Edition, Edinburgh: Butterworth-Heinemann, 2007, pp. 47–100.

[17] T. Sztyler and H. Stuckenschmidt, "On-body Localization of Wearable Devices: An Investigation of Position-Aware Activity Recognition," in *IEEE International Conference on Pervasive Computing and Communications (PerCom'16)*, (Sydney, Australia, Mar. 14–18, 2016), IEEE Computer Society, 2016, pp. 1–9.

[18] GSMArena.com, *Phone finder results for accelerometer and gyrometer*, http : / / www . gsmarena . com / results . php3 ? chkAccelerometer=selected&chkGyro=selected (accessed on 09/2016), 2016.

[19] S. O. Madgwick, A. J. Harrison, and 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.

[20] F. Hao and P. Ryan, "J-PAKE: Authenticated Key Exchange without PKI," in *Transactions on Computational Science XI: Special Issue on Security in Computing, Part II*, M. L. Gavrilova, C. J. K. Tan, and E. D. Moreno, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 192–206.

[21] T. D. Wu *et al.*, "The Secure Remote Password Protocol," in *Network and Distributed System Security Symposium (NDSS'98)*, 1998, pp. 97–111.

[22] J. Lester, B. Hannaford, and G. Borriello, ""Are You with Me?"–Using Accelerometers to Determine If Two Devices Are Carried by the Same Person," in *Pervasive Computing: Second International Conference (Pervasive'04)*. Berlin, Heidelberg: Springer, 2004, pp. 33–50.

[23] R. G. Brown, *Dieharder: A Random Number Test Suite*, http://www.phy.duke.edu/~rgb/General/dieharder.php, 2011.

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