Nguyen, Ngu; Kaya, Çağlar Yüce; Brüsch, Arne; Schürmann, Dominik; Sigg, Stephan; Wolf, Lars

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

Published in:
2018 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2018

DOI:
10.1109/PERCOMW.2018.8480248

Published: 02/10/2018

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Please cite the original version:
Nguyen, N., Kaya, Ç. Y., Brüsch, A., Schürmann, D., Sigg, S., & Wolf, L. (2018). Demo of BANDANA - Body Area Network Device-to-device Authentication using Natural gAit. In *2018 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2018* (pp. 421-423). Article 8480248 IEEE. https://doi.org/10.1109/PERCOMW.2018.8480248

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

Ngu Nguyen†, Çağlar Yüce Kaya*, Arne Brüsch*, Dominik Schürmann*, Stephan Sigg†, Lars Wolf*
*Technische Universität Braunschweig
{c.kaya, bruesch, schuermann, wolf}@ibr.cs.tu-bs.de
†Aalto University
{le.ngu.nguyen, stephan.sigg}@aalto.fi

***Abstract*—We demonstrate the BANDANA gait-based ad-hoc device pairing scheme. Our quantization approach extracts binary fingerprints from the deviation of acceleration sequences representing instantaneous gait vs. mean gait and establishes identical keys for fingerprints generated at distinct locations on the same body via a fuzzy commitment scheme. The separation between device-pairs on same-body and distinct body is possible as the fingerprint similarity exceeds 70% for same-body device pairs but on average reaches only 50% (random guess) for different body device pairs. The application of the BANDANA ad-hoc pairing will be demonstrated on a pair of Nexus 5X android phones and with a Huawei Watch 2.**

I. Introduction

Recent technological advances allow on-body appliances to pervade our daily life. For instance, smart-watches become fashionable gadgets that can communicate to your phones. Sensor-equipped shoes help sportsmen to monitor and evaluate their performance. In health-care, implant devices have been standardized and employed for a long time. Furthermore, research community in smart-textile envisions the future popularity of intelligent platforms embedded in clothes. The increasing number of device types with various use cases for spontaneous interaction has posed a challenge: securely pairing them to form an ad-hoc network but for the duration only of the context of use. Applications for ad-hoc secure pairing are manyfold (cf. figure 1). For instance, ad-hoc spontaneous pairings for a fixed duration is found in intelligent shopping cards tht share a purchase list from a smart personal device for he context of use, or fitness equipment such as a treadmill that synchronizes training data (e.g. physiological information) securely with the on-body worn fitness equipment. Furthermore, devices worn on the same body are spontaneously paired with always-fresh keys. Whenever a device is detached from the user, pairing stops automatically without requiring an explicit *log-out* command. Finally, the unobtrusive pairing schemes release users from remembering passwords. Since the keys are generated dynamically, there is no need to update them manually. The third scenario extends the use of ad-hoc pairing to equipment that interact with users.

PIN-based device pairing was a common solution but it is obtrusive because of required user's input. Moreover, it is difficult to use with appliances that lack interactive interfaces. Other common authentication approaches on mobile devices, such as biometric or pattern-based input, also require the users' attention and feature security weaknesses for frequent-use systems: Biometrics are inherently observable and easily stolen [1] while pattern-based input is vulnerable to shoulder surfing or smudge attacks [2].

Recently proposed protocols for ad-hoc pairing of devices co-present on the same body [3]–[7] leverage sensor data to form characteristic sequences, called fingerprints, in each wearable device. These fingerprints can be collated with a template database to identify legitimate users or detect impostors. In device pairing, they are exploited to generate secret keys for device-to-device communication.

The existing approaches [3]–[7] utilized the correlation of movement data to generate fingerprints. It is observed that fingerprints on devices carried or worn by the same individual are more similar than those attached to distinct users. To handle a limited number of errors in fingerprints, error correcting codes and fuzzy cryptography can be applied to create identical secret keys. Mayrhofer [3] proposes the candidate key protocol in which a user is required to shake devices together for several seconds. One device hashes the acceleration readings and then sends the hashed values along with random salt to the other. If the latter discovers a match in its own processed data, the vector is appended to a candidate key pool. As soon as a sufficient number of matched entries is reached, the pool itself is hashed to create the shared secret key. Groza and Mayrhofer [4] later improved the protocol with heuristic tree and hashed heuristic tree to counteract the attacker's analysis over hashed values. Walkie-Talkie [5] is another scheme that exploits correlated signals captured by accelerometers when the user is walking. The authors applied independent component analysis and low-pass filtering to remove undesired movements. Acceleration amplitudes are then quantized as binary sequences based on whether they are lower or higher than a threshold region. The Inter-Pulse-Interval protocol [7] exploits the random residual by which individual steps (left and right) differ from the mean gait cycle in time domain. The key is formed from first bits of the graycode representing gait fingerprints.

We have implemented the BANDANA protocol for Android and will showcase the implementation to demonstrate gait pairing from acceleration conditioned on co-presence on the same body. The application operates on the Android platform as a background service. It continuously collects sensor data,

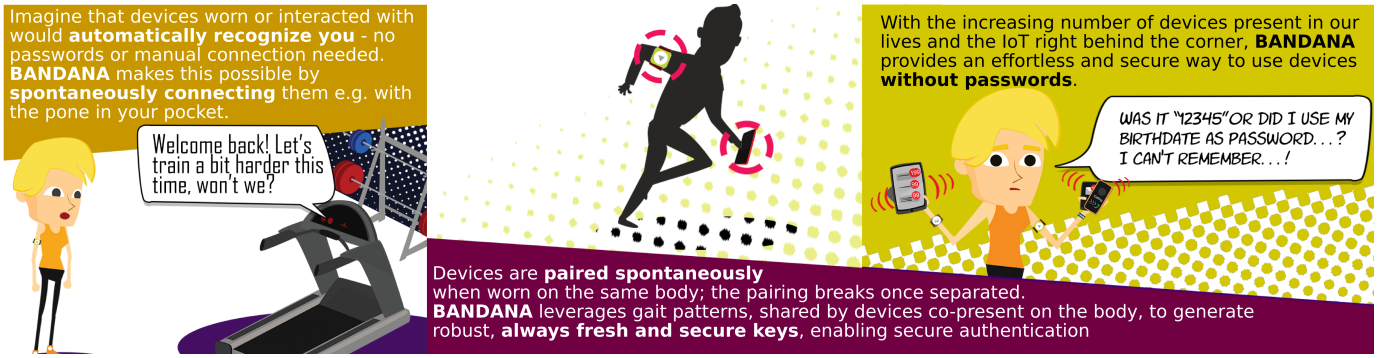


Fig. 1. BANDANA enables seamless ad-hoc device pairing based on acceleration sequences

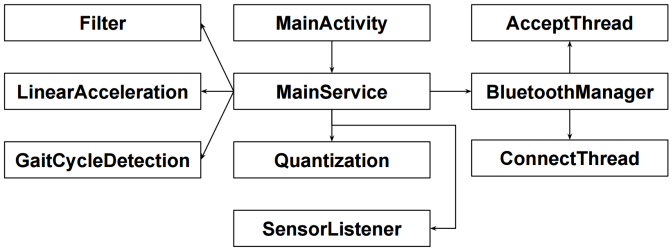


Fig. 2. Simplified class diagram of BANDANA Android prototype

extracts gait fingerprints, and issues notification whenever on-body devices change their status (e.g leaving user's body or being carried by another user). When running continuously as a background application on our experiment phones in two days, it utilized 4% of total app battery usage (for comparison, Google background services leveraged 34%). The energy consumption can be reduced by initiating BANDANA only when necessary (e.g. movement detection). A simplified class diagram of our prototype is displayed in Figure 2. The main component is a background service to continuously collect sensor data (SensorListener), generate gait fingerprints (Linear Acceleration, Filter, and GaitCycleDetection), and communicate with another device for demonstration purposes only (DeviceManager, AcceptThread, and ConnectThread).

II. BANDANA Gait-based Device Pairing

In BANDANA [6], secret keys reflect variations between mean and instantaneous gait cycles. Algorithm 1 summarizes all of the steps performed in each device partner in the pairing procedure. The approach exploits only acceleration along the gravity direction corrected by Madgwick's algorithm [8]. We first detect gait cycles from these enhanced values. Then, we quantize the difference of mean and instantaneous gait cycles into binary sequences. Figure 3 visualizes the process of obtaining bits from cumulative disparity of gait cycles. To further increase similarity of fingerprints generated on the same body, we discard unreliable bits produced from low difference between mean and instantaneous gait.

Our approach was assessed on two public datasets: *Mannheim* dataset [9] of 15 subjects and *Osaka* OU-ISIR Gait Database [10] of 496 subjects. Each user in the former dataset was equipped with seven smartphones on different body parts and performed several activities (walking, running, ascending, descending stairs, ...) for a period of 10 - 12 minutes each. The latter dataset was recorded with three triaxial accelerometers and gyroscopes worn on different parts of the waist (left, right, center). Experimental subjects traversed a parcours comprising a straight path, upstairs and down a slope.

Figure 4 depicts the similarity of intra- and inter- body fingerprints for the walking activity for all subjects and sensor locations in the *Mannheim* dataset. They are produced from seven locations [1] on human body [9]. Intra-body similarity is calculated from comparison of fingerprints from various positions on the same subject while inter-body values are the similarity of gait fingerprints of different subjects. Our experimental results encourage the use of error correcting codes to transform fingerprints of sufficient similarity into a pairing key whenever their similarity is high enough.

Algorithm 1: Extracting the secret key from walking acceleration

1. Collect acceleration readings from the z-axis;
2. Correct rotation w.r.t. gravity (using gyroscope);
3. Bandpass filter between 0.5Hz and 12Hz;
4. Resampling (40 samples/gait) and gait detection;
5. Compute mean gait;
6. Transform difference between mean and instantaneous gait to binary sequence;
7. Calculate reliability of bits, disregard least reliable;
8. Share reliability ordering;
9. Create fingerprint (see Figure 3);
10. Fuzzy cryptography: Get key from fingerprint

III. Demonstration

For the demonstration, we will need a table, a monitor and a power strip. If space is available, we can also bring a poster featuring the technical concept of the gait-based quantization and pairing utilized in BANDANA. We will

[1] Chest, forearm, head, shin, thigh, upper arm, and waist

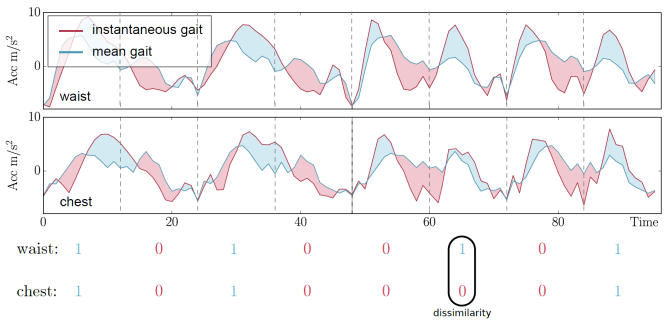


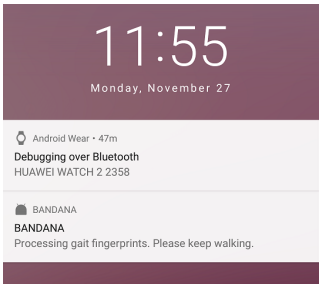
Fig. 3. BANDANA gait fingerprinting scheme

Fig. 4. Similarity of gait-based fingerprints extracted from body locations of the same (intra-body) and different users (inter-body). The results are obtained from *Mannheim* dataset [9]

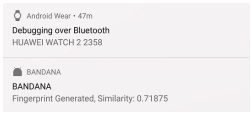
continuously play a video introducing the BANDANA gait-based pairing concept (processing of the acceleration data, quantization and fingerprint extraction, key generation and pairing) and captured example use cases.

The main part of the demo constitutes a life-experimentation with the implemented application on two Nexus 5X phones and on a Huawei Watch 2 smartwatch. One to two people will be constantly present during the demo and first demonstrate that a pairing based on gait is established continuously as long as all three devices are co-present at any pair of locations on the same body. Next, one of the devices is given to a by-stander to demonstrate that the pairing to this device breaks as soon as the devices are no longer co-present on the same body. If also the second phone is handed to another person, all connections break. Next, we invite two spontaneous volunteers visiting the demo to try and achieve successful pairing by mimicking gait. Finally, handing both devices to one spontaneous by-stander, pairing is again successful. Figure 5 displays screenshots of our prototype running on Nexus 5X phones. For demonstration purposes only, the application shows similarity of gait fingerprints when the devices are hold by one user (see Figure 5b) and when one of them lies upon a table and the other is carried (see Figure 5c). The similarity in the latter case is significantly lower.

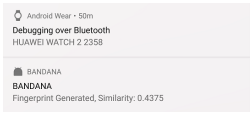
The demonstration shall showcase that robust pairing is possible for arbitrary locations on the same body while it is not possible to establish a pairing when devices are worn by different persons. Further, it shall demonstrate that straightforward attacks like gait mimicry are not successful for our implementation of the BANDANA protocol. In addition, at our demo session, users are welcomed to suggest potential attacking strategies (e.g. a couple walking together holding hands).



(a) Collecting sensor data and computing fingerprints



(b) Connected case



(c) Disconnected case

Fig. 5. Screenshots of our Android prototype running as a background service

IV. Conclusion

This paper introduces a demonstration for an on-body device pairing mechanism based on natural body movements. Specifically, we extract gait fingerprints from acceleration data through comparing mean and instantaneous gait cycles. Our technique is evaluated on seven locations, including upper and lower body parts. The similarity of gait fingerprints on the same user is consistently higher than those on different subjects. Thus, an error correcting code can be applied to derive secret communication keys. We implemented the scheme on Android platform to demonstrate it in realistic scenarios.

References

[1] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE*, 2003.

[2] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," in *Proceedings of the 4th USENIX Conference on Offensive Technologies*, 2010.

[3] 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*, 2007.

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

[5] W. Xu, G. Revadigar, C. Luo, N. Bergmann, and 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.

[6] D. Schürmann, A. Brüsch, S. Sigg, and L. Wolf, "BANDANA – Body Area Network Device-to-device Authentication using Natural gAit," in *IEEE PerCom*, Mar. 2017, pp. 190–196.

[7] Y. Sun, C. Wong, G.-Z. Yang, and B. Lo, "Secure key generation using gait features for body sensor networks," in *IEEE BSN*, 2017.

[8] 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*, 2011.

[9] 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)*. IEEE, 2016, pp. 1–9.

[10] T. T. Ngo, Y. Makihara, H. Nagahara, Y. Mukaigawa, and Y. Yagi, "The largest inertial sensor-based gait database and performance evaluation of gait-based personal authentication," *Pattern Recognition*, 2014.