Beck, Nils; Zuo, Si; Sigg, Stephan

BCG ECG-based secure communication for medical devices in Body Area Networks

Published in:
2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events, PerCom Workshops 2021

DOI:
10.1109/PerComWorkshops51409.2021.9430964

Published: 25/05/2021

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

Please cite the original version:
Beck, N., Zuo, S., & Sigg, S. (2021). BCG ECG-based secure communication for medical devices in Body Area Networks. In *2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events, PerCom Workshops 2021* (pp. 207-212). Article 9430964 (IEEE international conference on pervasive computing and communications workshops). IEEE. https://doi.org/10.1109/PerComWorkshops51409.2021.9430964

BCG & ECG-based secure communication for medical devices in Body Area Networks

Nils Beck
Aalto University, Finland
nils.beck@protonmail.com

Si Zuo
Aalto University, Finland
si.zuo@aalto.fi

Stephan Sigg
Aalto University, Finland
stephan.sigg@aalto.fi

***Abstract*—An increasing amount of medical devices, such as pacemakers or insulin pumps, can communicate in wireless Body Area Networks (BANs). While this facilitates the interaction between users and medical devices, something that was previously more complicated or - in the case of implanted devices - often impossible, it also raises security and privacy questions. We exploit the wide availability of ballistocardiographs (BCG) and electrocardiographs (ECG) in consumer wearables and propose MEDISCOM, an ad-hoc, implicit, and secure communication protocol for medical devices in local BANs. Deriving common secret keys from a body's BCG or ECG signal, MEDISCOM ensures confidentiality and integrity of sensitive medical data. It also continuously authenticates devices, requiring no explicit user interaction and maintaining a low computational overhead. We consider relevant attack vectors and show how MEDISCOM is resilient towards them. Also, we validate the security of our protocol's secret keys on BCG and ECG data from 29 subjects.**

***Index Terms*—usable security, protocol, health data, pervasive computing, embedded and mobile devices**

I. Introduction

Medical devices and sensors that used to be exclusive for health care professionals, like ballistocardiographs (BCG) and electrocardiographs (ECG), are becoming smaller, more affordable, and more ubiquitous [1]. Wrist bands and other mobile devices targeted at users of any background now feature accelerometers to measure BCG signals and some even feature ECG capability. While ECG is the traditional method to measure the heart's activity, BCG is comparable in capability, yet of lower complexity, lower cost, wider availability as well as easier to operate.

With BCG and many other sensors being distributed increasingly ubiquitously, collecting and interpreting medical data becomes feasible, without needing to reach out to health care professionals. At the same time, broad access to health-related data also raises privacy and security concerns as sensitive data is exposed to threats such as third parties manipulating or acquiring this data without permission [2].

Recently, the use of the sensor data itself has been proposed to protect and secure device-to-device access to it. In particular, medical data, such as ECG or BCG was employed as a seed to pseudo-random number generators that feed key generation for secure device pairing [3] [4]. These protocols proposed in the literature focus on the establishing of device pairing but disregard continuous pairing and de-authentication routines, which are essential in practical use.

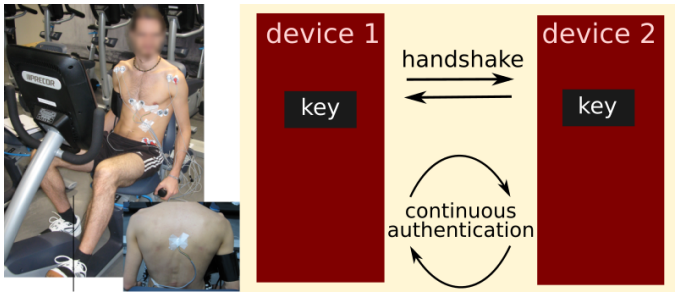

Fig. 1: Subject with BCG and ECG sensors (left) and protocol scheme (right). After retrieving the BCG or ECG signal the devices extract a common secret key for encryption. They then use the signal to continuously authenticate with each other and to provide message integrity.

We propose a novel communication protocol, MEDISCOM (medical devices' implicit and secure communication protocol). MEDISCOM exploits implicit pairing from ECG or BCG data and further features the complete lifetime of a secure connection, including continuous pairing, secure information exchange as well as unobtrusive de-authentication. As illustrated in figure 1, the protocol achieves a handshake between previously unacquainted devices, utilizing a key which is extracted from biometric traits. Continuous authentication is achieved by continuously sharing and validating snippets from BCG or ECG signals. Specifically, MEDISCOM is
implicit: no explicit user interaction required
light-weight: for low-power small medical devices
robust: regarding noise and fluctuations in the signal
anonymous: does not identify individual persons
private: does not leak sensitive personal data
local: does not need an internet connection or trusted authority

We analyze the properties of BCG and ECG data from 29 subjects to show that both fulfil the requirements to be used as a seed for a pseudo-random number generator in MEDISCOM. Furthermore, we analyse and discuss possible attack vectors for the proposed protocol.

II. Related Work

With device and sensor manufacturing costs decreasing steadily, and many sectors – among them health care – taking interest in health-related applications, there has been considerable work in determining implicit keys for secure

communication in local Body Area Networks (BANs) in recent years. The approaches differ in the type of human behavior that they observe, the sensors that they use to derive a shared secret, the computational ways of mapping the sensor data to fixed size bit sequences, and their focus on authenticity as opposed to confidentiality or integrity of data. Groza and Mayrhofer propose the SAPHE protocol for authenticated key-exchanges between devices that observe the same secure secret, using hash functions and heuristic search trees [5]. The authors demonstrate SAPHE for exploiting the correlation between acceleration sensors' signals. A continuous authentication process as in MEDISCOM is not included in SAPHE.

For ECG-based on-body device pairing, Rostami et al. propose a method of deriving keys for symmetric encryption between medical devices as well as an in-depth security analysis of their approach. Like we do, they exploit inter-pulse-interval values (IPI) for this, but measure solely ECG and no BCG signals. Also, they assume a secure Transport Layer Security (TLS) channel to be present, demanding a considerably complex security and internet infrastructure, which we do not [6]. Recently, Lin et al. [4] suggested the use of ballistocardiograph signals measured by vibration sensors for device pairing, focusing on key generation as opposed to continuous authentication or integrity. Using acceleration sensors, our approach exceeds their key generation rate with an average of 3.13 bits entropy per IPI (cf. figure 10) rather than the previous 2.9. They also considered video-based attacks, where an adversary retrieves the same BCG signal from video.

Another domain where pairing based on acceleration from behavior-biometrics has been employed is gait-based pairing [7]–[9]. The authors of [8] suggest a protocol similar to MEDISCOM, which does not assume any central trusted authority. In contrast to MEDISCOM, they focus less on privacy, while we specifically aim to rule out identification possibilities as they are not necessary to secure a Body Area Network. Sun et al. focus on gait as well, exploiting features derived from the length of gait cycles [9]. Another gait-based protocol has been proposed in [3]. The authors propose to integrate a password-authenticated key exchange into the protocol. We remark that this choice increases the required computing capacity of involved devices. Since they focus on pairing but not on confidentiality, their approach is vulnerable to man-in-the-middle attacks.

Venkatasubramanian et al. propose an implicit one-time key agreement method for BANs [10]. Their actual symmetric key is, however, not directly derived from data that the human body generates, but rather autonomously by the device. The authors focus on a key agreement and not on continuous authenticity and de-authentication. Another similar work is [11]. The authors focus on an implicit key agreement in BANs, but not on the devices' interactions after this agreement. In Shen et al.'s work, a light-weight and secure communication protocol is proposed specifically for BANs in the medical domain [12]. The work focuses on confidentiality and integrity of data, establishing group keys based on elliptic curve cryptography and hash chains. In contrast to MEDISCOM, they do not generate keys implicitly from a body signal, but build upon asymmetric cryptography, demanding a preexisting infrastructure for this.

Zeng et al. leverage acceleration in devices to establish a continuous authenticity mechanism [13]. They also investigate energy consumption. Although aiming for an implicit method, the authors actually require users to train their sensors and even to label data, basing the continuous authentication on machine learning calculations on a cloud server. In contrast, we propose a less complex and decentralized approach.

III. A PROTOCOL FOR IMPLICIT AD-HOC SECURITY

In this section, we first outline a representative setting for MEDISCOM, before specifying its core functionality. We then consider possible attack vectors and counter measures.

A. Setting

Consider Elise, a person with Diabetes. For monitoring her blood sugar level and responding with insulin if necessary, she resorts to contemporary devices that sacrifice physical buttons and interfaces for a small form factor and remote interaction via, e.g., smart watches.

While convenient, the intuitive interface of a smart watch and the possibility to gather and analyze all data in one place, comes at the price of considerable privacy and security risks. The wireless interfaces provide an attack surface that might leak sensitive medical data. Moreover, software vulnerabilities might allow an adversary to reprogram or control her medical equipment remotely. Furthermore, protection against accidental information leaks (e.g., reusing older smart devices by family members) or curious spouses is lacking.

MEDISCOM addresses these kinds of threats: We assume two or more benign devices to be paired for the context of use. We also assume these devices to use wireless body-area communication, as this is the predominant use case. After sketching the protocol, we discuss threats posed by adversarial parties, such as interception of communication.

B. Description of the protocol

Let *Bob* (d_b) and *Alice* (d_a) be two devices jointly worn on a Elise's (e's) body and *Eve* be a remote device capable to communicate via the same wireless medium. According to MEDISCOM, Bob and Alice first retrieve and confirm a common secret key (figure 2). They then use the secret key k to ensure data integrity (figure 3). Finally, they implement a continuous authentication mechanism (figure 4).

1) Handshake for confidential communication: After being placed on e's body and registering a corresponding signal, e.g. BCG or ECG, Bob exploits the randomness in this signal to retrieve a cryptographic key k_b from it, for instance, extracting binary keys from heart-rate variability (cf. figure 2). Being located on es body too, Alice is capable of accessing the same random process to derive her key k_a.

To establish secure communication only with devices co-present on e's body, Bob generates a random challenge (e.g. $12 - 8$). This challenge is concatenated to a 'Hello' message, encrypted using k_b, and wirelessly broadcast.

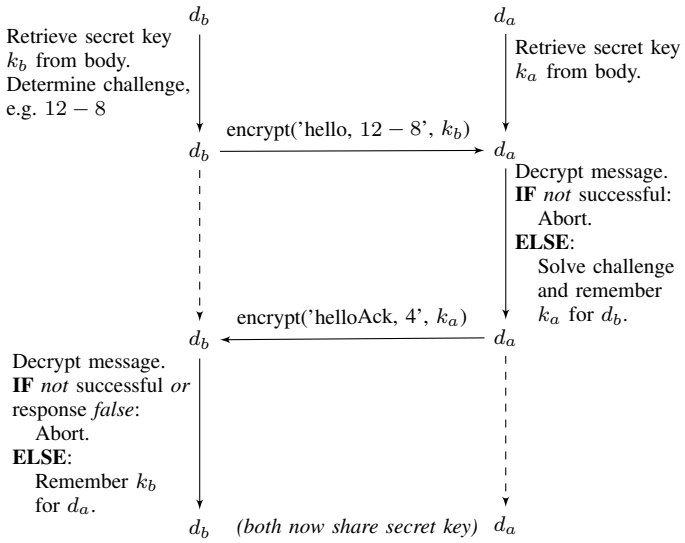

Fig. 2: Handshake between Bob (d_b) and Alice (d_a)

After receiving Bob's message, Alice decrypts it using her key k_a, and broadcasts her encrypted 'Hello' concatenated with the solution to Bob's challenge. Alice now remembers k_a as a symmetric encryption key for future communication with Bob. Bob receives Alice's message and successfully decrypts it using k_b. He verifies that her response to his challenge was correct and remembers k_b as a symmetric encryption key for future communication with Alice.

Alternatively, Alice and Bob could also implement a password-authenticated key agreement (PAKE) to agree upon a common key. This way, they could work with fewer key components while maintaining the same level of security. For the sake of simplicity, we, however, directly derive a key locally on both devices without further exchanges in that phase.

2) Ensuring data integrity: To prevent data tampering, the protocol further integrates sequence numbers and digital signatures (cf. figure 3).

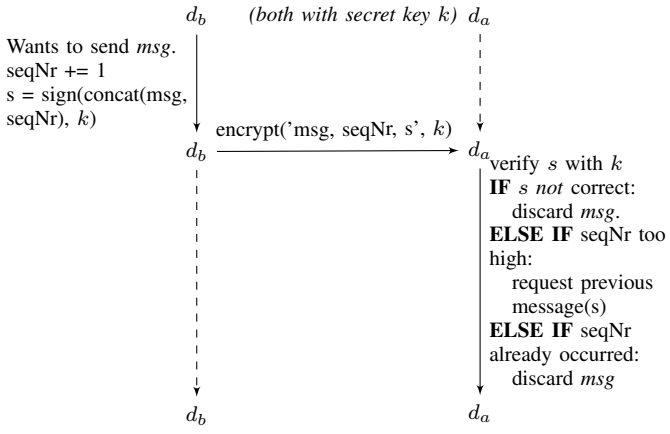

Fig. 3: Ensuring integrity between Bob (d_b) and Alice (d_a)

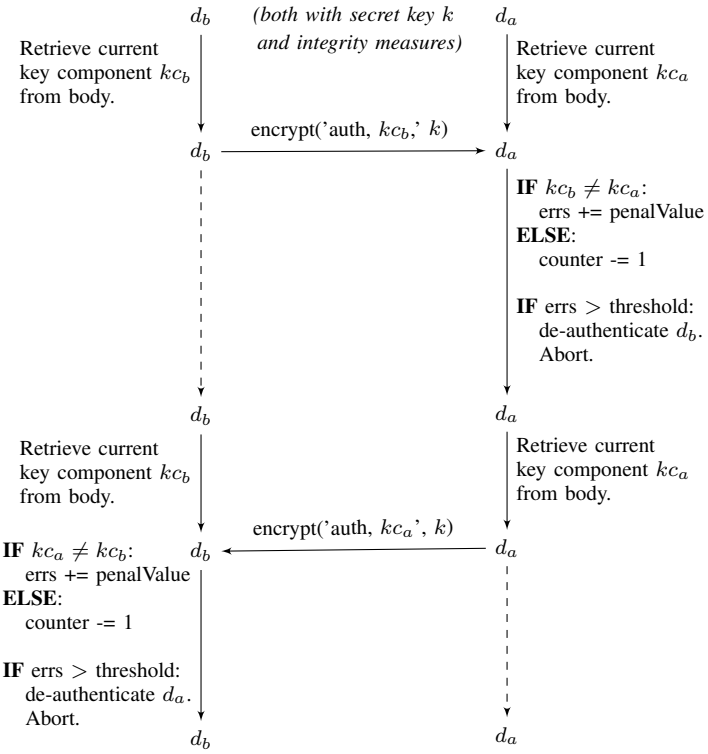

Fig. 4: Continuous authentication between Bob (d_b) and Alice (d_a)

Bob concatenates any message msg that he sends via the secure channel with a sequence number $seqNr$ and signs it with the common secret key k. The resulting signature s is appended to the message. Knowing k, Alice is able to verify the signature s and discards the message in case the signature is incorrect. Missing messages trigger a resend request, messages with already received $seqNr$ are discarded.

3) Continuous authentication: After having established a secure communication channel, Bob and Alice confirm their co-presence at repeated intervals by retrieving and exchanging authentication requests including time-sensitive key components kc_b and kc_a from e's body signal. In the case of BCG or ECG signals, these key components correspond to e's most recent heart beat (cf. figure 4).

The communication is closed by either side if kc_b or kc_a can not be confirmed with a sufficiently low error rate.

C. Considerations regarding relevant attacks

We now discuss possible attack vectors and resilience of MEDISCOM against them. In particular, figure 5 summarizes possible attack vectors on the left and mitigation mechanisms on the right.

The protocol does not mitigate attacks by an adversary with physical or remote access to the device, as these lie out of the scope of a communication protocol. The respective attacks are discussed in the following.

1) Eavesdropping: A common attack is to listen in to a conversation, i.e., to eavesdrop. MEDISCOM prevents this by

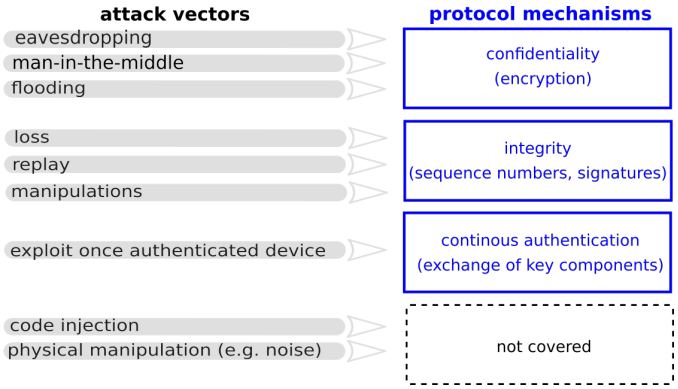

Fig. 5: Attack vectors for the MEDISCOM protocol

encrypting any communication. Since the secret encryption key is derived from a person's BCG or ECG signal, it can only be derived by those devices that are placed on this body. A malicious actor Eve will thus not be able to interpret the communication between Bob and Alice, since she does not have access to the secret decryption key.

Even if Eve would replay any of Bob and Alice's messages during the handshake, pretending to share their secret key k, she would not reap any benefits from this, as this does not bring her closer to interpreting the exchanged data.

The strength of the encryption scheme depends on how hard it is to guess the key. We assume that the BCG/ECG features utilized behave randomly. This assumption is supported by our analysis of BCG and ECG data in section IV. The protocol is thus resilient towards brute-force guessing as well as dictionary-attacks, which take into consideration the probability distribution of the key components.

2) Man-in-the-middle attacks: Man-in-the-middle attacks can be ruled out in our setting, which is essentially a symmetric encryption scheme. Eve is unable to pretend to be Bob or Alice, as she does not have access to their shared secret. In contrast to other protocols which are based on asymmetric encryption, this is an advantage.

3) Flooding: Eve might try to prevent Bob and Alice from communicating altogether by flooding the communication medium. This attack is feasible, although challenging to maintain by Eve, as MEDISCOM is a protocol for local Body Area Networks, which significantly reduces the attack space (e.g., spatial area in proximity to p) of scalable attacks such as flooding (accessibility, flexibility and scalability constraints).

4) Loss: Messages might get lost by physical interference of the communication medium, be it intentional or not [14]. Via sequence numbers, this attack can, however, be mitigated through resend requests for missing messages.

5) Replay attacks: Eve might decide to resend an intercepted message. This message is then considered integer in the sense that the signature is correct, but the duplicate would be detected from the sequence number and discarded.

6) Manipulation: Eve might manipulate a message on its way to Alice without even understanding it. In this case, Alice would notice that the signature and the message are not coherent and thus ask Bob to resend it.

7) Attacks outside our scope: We limit this work to securing the communication channel between Bob and Alice. But attacks that compromise the devices themselves, such as code injections, as well as attacks in which Eve generates audio signals of sufficient loudness to impact the BCG readings [15] may also need further consideration.

IV. Experimental validation of security

We investigate the randomness of keys derived from 29 subjects' BCG and ECG signals. Further, we show that additional properties, as mentioned in section I, hold for MEDISCOM.

A. Description of data

We use data that was gathered during various sessions in a period of two weeks. 29 subjects were measured while sitting. Some subjects were measured multiple times, leading to a total of 80 measurement sessions. The subjects wore three BCG sensors, i.e., accelerometers, and one ECG sensor. From each measurement we extracted 80 seconds of data from the BCG sensor placed on the person's cardiac apex as well as the ECG sensor. We used this data to derive key components as described in section III-B1, i.e. calculating the IPI values corresponding to individual heart beats and then extracting 4-bit sequences from their least significant bits. This way, we computed roughly 6000 BCG key components and 4000 ECG key components. This difference can be attributed to some of the measurements not featuring an ECG signal. This large set of key samples allows us to make quantitative arguments about the behavior and suitability of these key sequences for MEDISCOM. We visualize the distribution of the key components' values $\in \{0, 1, \ldots, 15\}$ in figures 6 (BCG) and 8 (ECG). The individual bits' behavior is shown in figures 7 (BCG) and 9 (ECG).

B. Randomness in key components

We examine the key samples with a focus on both overall randomness and randomness in the samples tied to one person. Our hypothesis is that the observed values can be understood as a random variable. We first consider the distribution of key component values and then quantify randomness in terms of Shannon entropy.

1) Distribution of key component values: As figure 6 and 8 show, the overall distribution of values is fairly even. It is not easy to just guess a key, since even the best guess among our BCG samples (value 3 in figure 6, being the most frequent value) only has a chance of approximately 9% of being correct. The optimal probability would be 6.25%, corresponding to a uniform distribution amongst 16 values. For a key that is comprised of, e.g., 32 key components (i.e., 128 bits long), the chance of guessing it using a dictionary-based method would thus be $0.09^{32} < 4 \cdot 10^{-34}$.

Although the key component value might be a sufficiently random variable, we caution that it is not uniformly distributed. For both BCG and ECG data, the hypothesis that the given

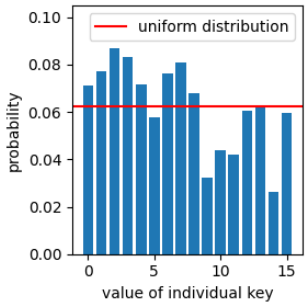

Fig. 6: BCG key components

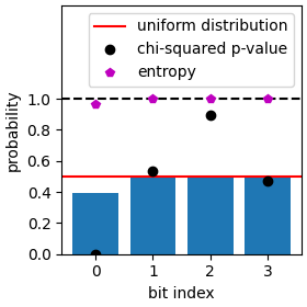

Fig. 7: BCG individual bits

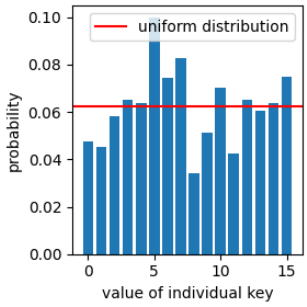

Fig. 8: ECG key components

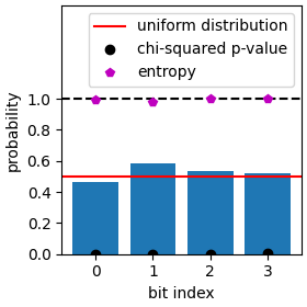

Fig. 9: ECG individual bits

observation has been generated from a uniformly distributed random variable can be rejected with certainty, as the chi-square test's [16] p-value, which is smaller than 0.05 indicates. A p-value smaller than 0.05 means that we can reject the hypothesis (uniform distribution) at a significance level of 5%. Since we have a much lower p-value, we can actually reject the hypothesis with even higher confidence.

These overall observations cannot be transferred to the distribution of keys among a single measurement or person. All individual measurements show that their key values are less evenly distributed. Their chi-square tests' p-values are equally low, leading us to discard the hypothesis of uniform distribution for individual subjects' key component values.

2) Distribution of individual bit values: The presumption arises that the lack of complete randomness is due to some the individual bits of a key component not behaving randomly. We therefore looked at the behavior of every single bit in the 4-bit key component to see how equally distributed they behave.

In the BCG data, one of the four bits of a key sequence is not behaving like a uniformly distributed random variable, but rather like a biased coin, as figure 7 shows. Bits 1,2 and 3's chi-squared test's p-values do, however, not allow us to discard the hypothesis that they behave randomly, since they exhibit very high p-values. This observation explains the not-fully-random behavior of the BCG key values. We can observe similar behavior in the ECG key component's bit distributions in figure 9. According to the chi-squared test that we applied, all four bits can be said not to behave fully randomly. Again, we point out that we were not able to retrieve ECG data for all measurements for which we display BCG data. Hence, a direct comparison to the BCG results can not be made.

3) Entropy as a measure of randomness: Our findings suggest that a quantifiable measure of randomness is needed to evaluate how secure keys from the BCG signal are. Given our BCG-conditioned random variable X, we compute the Shannon Entropy

$$H(X) = -\sum_{i=1}^{n} P(x_i) \cdot log_2(P(x_i)),$$

where $\{x_i | i \in \{0, 1, \ldots, 16\}\}$ is the discrete set of possible values that X can assume, and P is the probability function.

The Entropy $H(X)$ can be interpreted as the amount of fully random bits that X' behavior is equivalent to. Assume that we intend to generate a secret s , e.g. of length $l_s = 128$, so that it can be used in the AES symmetric encryption scheme. Using X of length l_x bits, we need to stretch that variable X' length by the factor $\frac{l_x}{H(x)}$ to achieve the desired amount of entropy.

As figure 10 shows, a 4-bit BCG key component behaves on average like a purely random sequence that is 3.13 bits long. To achieve the randomness of n purely random bits we have to use a key that is $\frac{4}{3.13} = 1.780$ times as long. We conclude that the key values can thus be made to behave sufficiently random with an acceptable overhead on the length of the random sequence. Figures 7 and 9 also support this assessment. Drawing an analogy to password security, it is not necessary for a 'good' password to be fully random as long as it is long enough. Rather, length and randomness or entropy can be seen as interplaying in determining whether a password, or an encryption key for that matter, are 'good'.

Notable, however, is the variance in entropy that the different subjects' measurements - both BCG and ECG - in figure 10 exhibit. While a great majority produce entropy values around 3 bits, a couple of measurements only exhibit around 1 bit of entropy, considerably less than the average. This finding presents a challenge for MEDISCOM. The sample size of only 29 subjects is too small to derive general claims and this property is to be investigated further in future work. Our results indicate that the number of 'outlier subjects' that produce key components with little entropy is small. If this can be confirmed in a larger study with several hundred subjects, the guessing of keys will remain a sufficient challenge for an adversary. Furthermore, we remark that the protocol might involve a test on the randomness of keys and fall back to an alternative pairing scheme, such as PAKE, in such a case. Alternatively, stretching key length by a larger factor is another possibility to ensure sufficient randomness in the presence of adversarial devices.

We remark that we expect MEDISCOM not to be able to identify individuals in the way that a biometric scheme would. This becomes harder to guarantee when entropy levels drop.

C. Justification of properties

In section I we presented properties that MEDISCOM possesses. We here reason why these properties hold. MEDISCOM is

implicit: devices are able to use implicit signals, such as

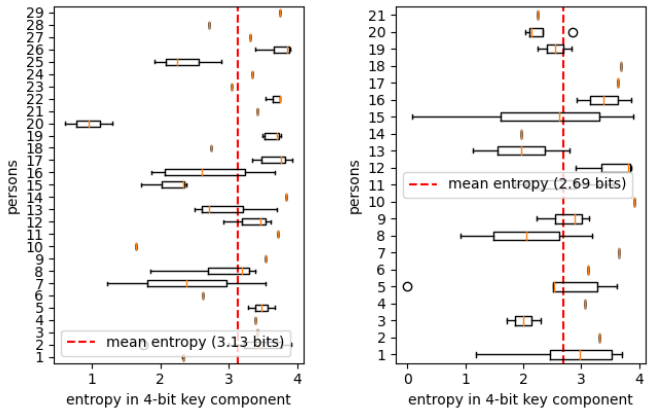

Fig. 10: Subjects' mean entropy values, *BCG* (left) and *ECG* (right)

the BCG signal to generate and agree upon common secret keys without any user interaction. They also stop sensitive communications just as implicitly once they are detached from the respective signal.

light-weight: does not require any preexisting infrastructure to work. Also, apart from the one-time handshake between two devices the protocol's security measures produce no large continuous overhead.

robust: includes mechanisms that allow devices to deal with incorrect incoming data, be it due to loss, manipulation or incorrect authentication messages, caused by a noisy signal.

anonymous: key components behave randomly, as shown in section IV. Hence, they serve to distinguish individual subjects from one another at a given time, but cannot be used to identify them over periods of time.

private: key components behave randomly. Therefore they do not contain personal information, meaning no sensitive medical data or other personal data is leaked by MEDISCOM.

local: MEDISCOM is designed to be implemented in wireless near-field communication, not in, e.g., internet communication. It does not require a central or trusted authority to function and therefore avoids unnecessary exposure of communications.

V. Conclusion

In this paper, we presented MEDISCOM, a novel implicit communication protocol for Body Area Networks, especially suitable for medical devices. We used keys derived from the ballistic forces generated by the heart (BCG) or from the heart's electrical activity (ECG) to extract a secret key for confidential and authenticated communication between wearable devices. We defined security requirements for this protocol and used data from 29 subjects to validate that MEDISCOM can provide the required security.

Limitations include the positioning of BCG sensors on the body, which can lead to large amounts of noise and the handling of this noise in general. This challenge is present in the data set that we used, leading us to focus only on the measurements that we were able to free to a sufficient degree from this noise. Compared to ECG sensors, BCG sensors will continue to need more work on removing and reducing noise, as they are much more sensitive to it. Future work may include the validation of the protocol on a larger or cleaner data set, as well as the derivation of more features from IPI values in a given amount of time, thus improving the protocol's usability or hardening its security.

References

[1] J. Zheng, Y. Shen, Z. Zhang, T. Wu, G. Zhang, and H. Lu, "Emerging wearable medical devices towards personalized healthcare," in *Proceedings of the 8th international conference on body area networks*, pp. 427–431, 2013.

[2] H. Almohri, L. Cheng, D. Yao, and H. Alemzadeh, "On threat modeling and mitigation of medical cyber-physical systems," in *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, pp. 114–119, IEEE, 2017.

[3] D. Schürmann, A. Brüsch, N. Nguyen, S. Sigg, and L. Wolf, "Moves like jagger: Exploiting variations in instantaneous gait for spontaneous device pairing," *Pervasive and Mobile Computing*, vol. 47, pp. 1–12, 2018.

[4] Q. Lin, W. Xu, J. Liu, A. Khamis, W. Hu, M. Hassan, and A. Seneviratne, "H2b: Heartbeat-based secret key generation using piezo vibration sensors," in *Proceedings of the 18th International Conference on Information Processing in Sensor Networks*, pp. 265–276, 2019.

[5] 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*, pp. 161–168, 2012.

[6] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (h2h) authentication for implanted medical devices," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pp. 1099–1112, 2013.

[7] A. Bruesch, L. Nguyen, D. Schürmann, S. Sigg, and L. C. Wolf, "Security properties of gait for mobile device pairing," *IEEE Transactions on Mobile Computing*, 2019.

[8] 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)*, pp. 1–12, IEEE, 2016.

[9] Y. Sun, C. Wong, G.-Z. Yang, and B. Lo, "Secure key generation using gait features for body sensor networks," in *2017 IEEE 14th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, pp. 206–210, IEEE, 2017.

[10] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "Pska: Usable and secure key agreement scheme for body area networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 1, pp. 60–68, 2009.

[11] D. Oberoi, W. Y. Sou, Y. Y. Lui, R. Fisher, L. Dinca, and G. P. Hancke, "Wearable security: Key derivation for body area sensor networks based on host movement," in *2016 IEEE 25th International Symposium on Industrial Electronics (ISIE)*, pp. 1116–1121, IEEE, 2016.

[12] J. Shen, H. Tan, S. Moh, I. Chung, Q. Liu, and X. Sun, "Enhanced secure sensor association and key management in wireless body area networks," *Journal of Communications and Networks*, vol. 17, no. 5, pp. 453–462, 2015.

[13] Y. Zeng, A. Pande, J. Zhu, and P. Mohapatra, "Wearia: Wearable device implicit authentication based on activity information," in *2017 IEEE 18th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pp. 1–9, IEEE, 2017.

[14] L. Kong, M. Xia, X.-Y. Liu, G. Chen, Y. Gu, M.-Y. Wu, and X. Liu, "Data loss and reconstruction in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 11, pp. 2818–2828, 2013.

[15] S. Eberz, N. Paoletti, M. Roeschlin, M. Kwiatkowska, I. Martinovic, and A. Patané, "Broken hearted: How to attack ecg biometrics," 2017.

[16] R. Lowry, "Chi-square procedures for the analysis of categorical frequency data part," *Therapy*, vol. 24, no. 40.0, pp. 40–0, 1999.