Insider-Resistant Context-Based Pairing for Multimodality Sleep Apnea Test

Yao Zheng* (ID)   Shekh Md Mahmudul Islam*   Yanjun Pan†   Marionne Millan*   Samson Aggelopoulos*
Brian Lu*   Alvin Yang*   Thomas Yang*   Stephanie Aelmore*   Willy Chang*
Alana Power*   Ming Li†   Olga Borić–Lubecke*   Victor Lubecke*   Wenhai Sun‡

*University of Hawai'i at Mānoa, USA   †University of Arizona, USA   ‡Purdue University, USA

Email: *{yao.zheng,shekh,marionne,saggelop,lubrian,ayang27,thomasy4,saelmore,changw,afpower,olgabl,lubecke}@hawaii.edu
† {yanjunpan,lim}@email.arizona.edu   ‡whsun@purdue.edu

Abstract—**The increasingly sophisticated at-home screening systems for obstructive sleep apnea (OSA), integrated with both contactless and contact-based sensing modalities, bring convenience and reliability to remote chronic disease management. However, the device pairing processes between system components are vulnerable to wireless exploitation from a non-compliant user wishing to manipulate the test results. This work presents SIENNA, an insider-resistant context-based pairing protocol. SIENNA leverages JADE-ICA to uniquely identify a user's respiration pattern within a multi-person environment and fuzzy commitment for automatic device pairing, while using friendly jamming technique to prevent an insider with knowledge of respiration patterns from acquiring the pairing key. Our analysis and test results show that SIENNA can achieve reliable (> 90% success rate) device pairing under a noisy environment and is robust against the attacker with full knowledge of the context information.**

I. Introduction

Over twenty-five million adults in the US suffer from obstructive sleep apnea (OSA), an airway muscle-related breathing condition that involuntarily causes respiratory cessations during sleep. Poor treatment can lead to excessive daytime fatigue, high blood pressure, cardio-metabolic conditions, along with a myriad of health problems [1]. A traditional diagnostic procedure, known as polysomnography (PSG), requires the patient to be in a laboratory overnight with instruments of multiple sensors/electrodes to track various sleep-related physiological parameters. However, PSG is highly obtrusive, expensive, and scarce.

At-home OSA monitoring systems leverage contactless and/or contact-based sensing technologies to monitor respiratory symptoms related to OSA. They allow users to conduct self-administered tests prescribed by their doctors and are considered economical alternatives for PSG. However, At-home OSA tests are subject to test fraud, as several professions within the patient population are deeply concerned that positive OSA test results will jeopardize their careers. As a result, an OSA patient may exploit the unsupervised at-home environment to manipulate the OSA test results. Specifically, the device pairing processes between the OSA screening system components are often the target of eavesdropping and spoofing from a non-compliant user.

To combat these malicious behaviors, we introduce SIENNA: in**SI**der r**E**sista**N**t co**N**text-based p**A**iring for unobtrusive at-home OSA screening. SIENNA works with a multi-modality OSA screening system consisting of one data aggregate, e.g., the user's mobile phone, and two sensing modalities, e.g., a respiratory belt and a physiological radar monitoring system (PRMS). It leverages the respiration patterns collected by the respiratory belt to allow automatic pairing between the PRMS and the phone. The design of SIENNA uses a novel combination of JADE-ICA [2], [3], fuzzy commitment, [4], and friendly jamming [5], [6], [7]. The JADE-ICA allows the PRMS to identify the unique patterns of a person's breathing from a multi-person environment. The fuzzy commitment leverages the user's breathing patterns to establish a shared secret key between the PRMS and the mobile phone. And the friendly jamming prevents insiders, e.g., a non-compliant and unsupervised user with knowledge of the breathing patterns, from learning the security key.

We formally analyzed the security of SIENNA based on the attacker's knowledge of the context information, and implemented a laboratory prototype consisting of a mmWave PRMS (implemented with SDR and mmWave radio heads), a wireless respiratory belt, and a Android-based OSA app. We conducted an evaluation consisting of 20 subjects spanning over one month. The results show that SIENNA achieves reliable device pairing within a noisy at-home environment with multiple free moving persons in the background. It also prevents unauthorized receivers from retrieving the secret key, regardless of their locations or knowledge of the user's respiration patterns.

II. Preliminary

Before introducing SIENNA, we briefly review the mechanisms of two common at-home OSA screening modalities: respiratory belt and non-contact PRMS. An external motion respiratory belt sensor utilizes a transducer to generate a substantial linear signal in response to changes in thoracic circumference associated with respiration (Fig. 1a). The linear signal is first sampled by a analog-to-digital converter (commonly at 100 Hz), then transmitted to a mobile OSA app.
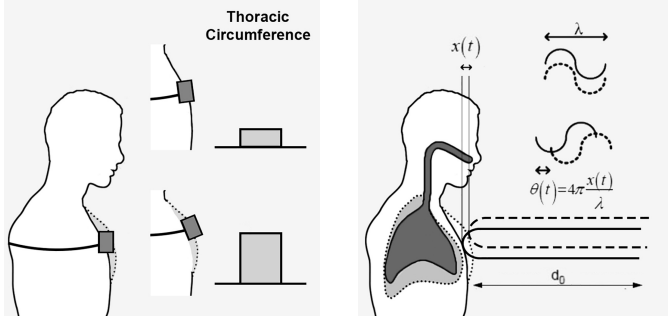
Fig. 1: Left to right: (a) The respiratory belt detects chest displacement (breathing) through changes in thoracic or abdominal circumference; (b) The PRMS detects displacement (breathing) in patient's chest through phase offset between the TX and RX signal.

The PRMS (Fig. 1b) utilizes Continuous Wave (CW) Doppler radar technology to detect the phase shift of reflected signals from the patient's chest movements. Let the distance offset due to chest movements be $x(t)$, and the in-phase (I) and quadrature phase (Q) can expressed as:

$$B_I(t) = A_I \cos \left(\theta_0 + \frac{4\pi x(t)}{\lambda} + \delta\theta(t) \right)$$
$$B_Q(t) = A_Q \sin \left(\theta_0 + \frac{4\pi x(t)}{\lambda} + \delta\theta(t) \right)$$

where λ is the signal wavelength, θ_0 is the phase delay due to the nominal distance between the radar transmitter and the user's torso, surface scattering, and radar's RF chains, and $\delta\theta(t)$ is the residual phase noise. The phase shift corresponds to the respiratory movement and can be computed via arctangent demodulation:

$$\theta(t) = \theta_0 + \frac{4\pi x(t)}{\lambda} = \arctan \left(\frac{A_I B_Q(t)}{A_Q B_I(t)} \right).$$

III. PROBLEM DESCRIPTION

A respiratory belt and a PRMS need to pair with the user's mobile phone before an OSA test. A respiratory belt is often paired with the user's phone by a medical technician during a clinic visit. The PRMS is usually shipped directly to the user's home and paired without supervision. The unsupervised pairing process is subject to exploitation from a non-compliant user. Assuming the respiratory belt has successfully paired with the phone, we aim to enable automatic device paring between the PRMS and the phone via the shared context information, e.g., the user's respiratory patterns observed by the belt and PRMS. Unlike previous works on context-based zero-effort pairing, our pairing protocol must pair two devices securely in the presence of a co-located adversary who can also observe the context information.

A. System Model

We consider a multimodality OSA screening system with three modules: (1) A mobile phone that aggregates the screening data, a PRMS, and a wireless respiratory belt, and assume the following. (1) Wireless interface: The phone, PRMS, and belt are equipped with radio interfaces such as Bluetooth. (2) Computation: The PRMS and belt can perform computational inexpensive cryptographic algorithms, such as SHA-256 hash and AES. (3) Tamper-proof: The phone, PRMS, and belt are tamper-proof. Any attempts to physically modify the circuit would nullify the test. (4) Security: The phone, PRMS, and belt do not have any prior security associations. Secret keys are established between the belt and the user's phone by a medical technician (Fig. 2a).

B. Adversary Model

A distinguishing feature of our adversary model is that the system's legitimate user could also be an insider attacker (non-compliant user). The attacker's objective is to either eavesdrop on the communication between the system modules or manipulate the system into accepting false data.

Eavesdrop. A non-compliant user may seek to eavesdrop on the pairing communication between the PRMS and the phone, aiming to extract the security context. For instance, the patient may intercept the key exchanged between the PRMS and the phone to decrypt and review all data records before a doctor examines. If patterns related to OSA symptoms were found, the patient would have time to come up with false excuses.

Spoofing. A non-compliant user may leverage the eavesdropped key to transmit false data to the mobile device and manipulate the OSA test outcome. For instance, the patient may use a third device to collect normal patterns prior to the test and replay the normal data records to the phone during the test.

IV. SIENNA

We present SIENNA: in**SI**der r**E**sista**N**t co**N**text-based p**A**iring. SIENNA leverages the user's respiratory patterns observed by both the respiratory belt and the PRMS. To defense against an insider attack, SIENNA employs a combination of fuzzy matching and friendly jamming to prevent a non-compliant user from obtaining the pairing key using the same context.

A. Overview

The pairing procedure of SIENNA is shown in Fig. 2. It begins when the user visits a doctor to obtain the test authorization. During the visit, the doctor attaches a respiratory belt to the patient, and pairs it to the user's mobile device OSA app (Fig. 2a). Once arriving home, the user lies in bed and the PRMS automatically pairs with the mobile device based on the respiration pattern observed by both the PRMS and the respiratory belt (Fig. 2b). Once the pairing completes, both links from the PRMS and respiratory belt to the mobile device are secure. The user can freely choose either the respiratory belt or PRMS for OSA screening, and the selected modality communicates encrypted OSA data to the mobile device (Fig. 2c). Once testing is completed, the user revisits the doctor and uploads the OSA screening from the mobile device. The doctor runs a compliance check and examines whether there were any significant gaps or inconsistencies with the OSA data. Based
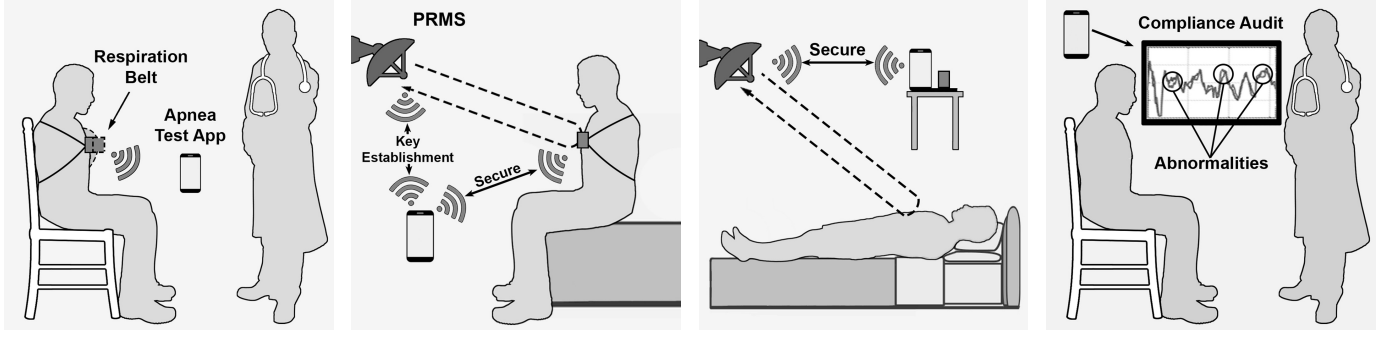
Fig. 2: Left to right: (a) In hospital: a medical technician places a respiratory belt on a user and pairs it with the user's phone; (b) At home: a user pairs the PRMS with the user's phone; (c) User switches to PRMS for OSA screening; (d) Doctor verifies OSA data for any abnormalities.

on the compliance check report, the doctor decides whether to accept or reject the OSA screening (Fig. 2d).

B. Insider Resistant Device Pairing

The core of SIENNA is a context-based secure key establishment (Fig. 3), which allows two devices, a and b, to securely exchange and update a symmetric key in the presence of a nearby eavesdropper by utilizing the context (user's breathing patterns) observed by both devices at the moment of exchange. In the OSA scenario above, a represents the mobile device connected to a respiratory belt, b represents the PRMS.
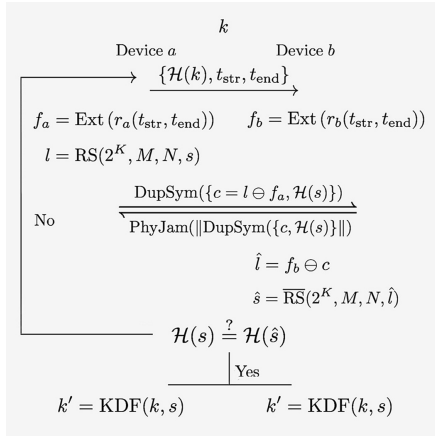

Fig. 3: Pairing protocol for two devices observing similar data to establish a symmetric key in the presence of an adversary.

Traditional context-based key establishment protocols are not secure when eavesdroppers are nearby to observe the context. Many of such protocols assume that the adversary cannot be near paring devices over extended periods of time [8]. SIENNA addresses this shortcoming through a cross-layer design that employs two security primitives: fuzzy commitment [4] and and dialog-codes-based friendly jamming [5], [6], [7]. The former is a cryptographic scheme that allows secure commit and de-commit of a secrete similar-but-not-identical open value. The latter is a friendly jamming scheme at the receiver by jamming the transmitted signal to flip specific bits in the message. Together, this ensures that an eavesdropper

with the right context will not be able to recover the key exchanged between the pairing devices.

First we define the fuzzy commitment scheme [4]. Let σ be a secret value. A fuzzy commitment transforms a secret value σ into a commitment $\{\chi, \mathcal{H}(\sigma)\}$ using an opening feature, ϕ, and a hash function, $\mathcal{H}(\cdot)$:

$$\{\chi, \mathcal{H}(\sigma)\} = \text{COMMIT}(\sigma, \phi),$$

such that χ appears random and devoid of any information about σ. And all open features $\hat{\phi}$ reveals σ via

$$\sigma = \text{OPEN}(\chi, \hat{\phi}),$$

if and only if the Hamming distance $\text{HAM}(\phi, \hat{\phi}) \leq \tau$, where τ is a parameter denoting the maximum allowable Hamming distance between $\hat{\phi}$ and ϕ to reveal σ.

To initiate the key establishment protocol, a broadcasts a message, $\{\mathcal{H}(k), t_{\text{str}}, t_{\text{end}}\}$, where k denotes the key of the previous iteration. t_{str} and t_{end} denotes the starting and ending timestamps of a and b's captures of the respiratory patterns. During the first round, $\mathcal{H}(k)$ is replaced with a public parameter known to all parties.

From respiratory patterns $r_a(t_{\text{str}}, t_{\text{end}})$ and $r_b(t_{\text{str}}, t_{\text{end}})$ captured within the specified time interval, the two devices extract breathing fingerprints $f_a = \text{EXT}(r_a(t_{\text{str}}, t_{\text{end}}))$ and $f_b = \text{EXT}(r_b(t_{\text{str}}, t_{\text{end}}))$, via a fingerprint extraction function $\text{EXT}(\cdot) : \{1, 0\}^* \mapsto \{1, 0\}^{M*2^K}$ (detailed in Sec. IV-D). In case a, e.g., PRMS, observes a breathing mixture of multiple subjects, the mixture is first separated into the breathing patterns of individual subjects (detailed in Sec. IV-C), which are processed by $\text{EXT}(\cdot)$ to create multiple fingerprints, one for each subject.

Once the breathing fingerprints are generated, a randomly selects a key salt, $s \in \{1, 0\}^{N*2^K}$, and transforms it into a commitment $\{c \in \{1, 0\}^{M*2^K}, \mathcal{H}(s)\}$ using the breathing fingerprint, f_a. Specifically, a encodes s via the Reed-Solomon (RS) encoding function

$$l = \text{RS}(2^K, M, N, s) \in \mathbb{F}_{2^K}^M$$

and compute:

$$c = l \ominus f_a,$$

with $\ominus$ denoting exclusive OR (XOR).

Henceforth, a and b exchange c through dialog codes to defend against insider attack. First, a converts the commitment,

$$\{c, \mathcal{H}(s)\},$$

into OFDM symbols, duplicates each symbol back-to-back,

$$\text{DUPSYM}\left(\{c, \mathcal{H}(s)\}\right),$$

and broadcasts all the symbols. In parallel to a's broadcast, b randomly jams either the original symbol or its repetition [6], [5],

$$\text{PHYJAM}\left(\|\text{DUPSYM}\left(\{c, \mathcal{H}(s)\}\right)\|\right),$$

To jam a symbol, b transmits a signal that is drawn randomly from a zero-mean Gaussian distribution whose variance is the same as the OFDM signal with the same modulation. Since b knows which symbols are jammed, it stitches the unjammed symbols together to create a clean version of the OFDM transmission and decodes the signal to obtain the clear message.

Upon receiving $\{c, \mathcal{H}(s)\}$, b computes

$$\hat{l} = f_b \ominus c$$

and decommits the salt by decoding $\hat{l}$ using the Reed-Solomon (RS) decoding function:

$$\hat{s} = \overline{RS}(2^K, M, N, \hat{l}).$$

Due to the error correction capability of Reed–Solomon codes, s equals to $\hat{s}$ if and only if l and $\hat{l}$ differ in less than $2^{K-1}(M-N)$ bits. Since $l = f_a \ominus d$ and $\hat{l} = f_b \ominus d$, it is equivalent in saying that f_a and f_b must differ in less than T bits for b to retrieve s.

To confirm whether the retrieval were successful, b computes $\mathcal{H}(\hat{s})$ and compares it with $\mathcal{H}(s)$. Depending on whether they were equal, an ACK or a NAK message is transmitted from b to a, with the former initiating the final step of the key establishment protocol and the latter initiating the reattempts.

To conclude the key establishment, both a and b applies a key derivation function

$$k' = \text{KDF}(k, s),$$

to obtain the new key.

C. Breathing Separation with JADE-ICA

Home environments are noisy and unpredictable, with the possibility of irrelevant individuals in close vicinity from the user. To retrieve the correct context in an environment with potentially multiple subjects, SIENNA augments the PRMS modality with a breathing separation module, which reconstructs the breathing signals of multiple co-located individuals to select the correct target. The goal of the separation module is to reconstruct a set of source signals from a set of mixtures, without knowing the properties of the sources and the mixing proportion. Since respiration signals are non-Gaussian and independent from individuals, whilst mixed linearly at the PRMS receiver, one can recover the source signals using

independent component analysis (ICA) [9], which is formulated as the following: assume N independent time varying sources $s_i(t)$, $i = 1 \ldots N$, and M different observations $x_i(t)$, $i = 1 \ldots M$. For T time units ($t = 1 \ldots T$), we can define the source signal as a $N \times T$ matrix,

$$\mathbf{S}_{N \times T} = \begin{bmatrix} s_{11} & s_{12} & \cdots \\ \vdots & \ddots & \\ s_{N_1} & & s_{N_T} \end{bmatrix},$$

and the observed mixtures as a $M \times T$ matrix,

$$\mathbf{X}_{M \times T} = \begin{bmatrix} x_{11} & x_{12} & \cdots \\ \vdots & \ddots & \\ x_{M_1} & & x_{M_T} \end{bmatrix}.$$

The mixtures are produced as the product of the source and a mixing matrix $\mathbf{W}_{M \times N}$, e.g.,

$$\mathbf{X}_{M \times T} = \mathbf{W}_{M \times N} \times \mathbf{S}_{N \times T}.$$

The goal of ICA is to recover $\mathbf{S}_{N \times T}$ and $\mathbf{W}_{M \times N}$ given only $\mathbf{X}_{M \times T}$, assuming the $s_i(t)$, $i = 1 \ldots N$ are independent and non-Gaussian. We employ the joint approximate diagonalization of eignematrices (JADE) algorithm [2] to perform ICA, with the details omitted to conserve space??.

D. Fingerprinting with Level-Crossing Quantization

Once the devices obtain breathing patterns of individual targets, they apply $\text{EXT}(\cdot)$ to extract the binary breathing fingerprints. The binary strings must meet two criteria for the two to agree on the patient's identity and evolve the shared security key: (1) they should look sufficiently similar in Hamming space if they represent the breathing process of the same person, and (2) they should preserve the uniqueness of the breathing dynamic that distinguishes among individuals.

To achieve these objectives, $\text{EXT}(\cdot)$ applies level-crossing quantization to sample the continuous breathing patterns with two predefined thresholds. Let q_+, q_- be the thresholds values such that $q_+ > q_-$, we define a quantizer $\text{QTZ}(\cdot)$:

$$\text{QTZ}(x) = \begin{cases} 10 & \text{if } x \geq q_+ \\ 01 & \text{if } x \leq q_- \\ 00 & \text{if } q_- < x < q_+ \end{cases}$$

Let T be the time interval between adjacent sampling instants. The binary sequence obtained by $\text{EXT}(\cdot)$ is

$$f = \text{EXT}\left(r(t_{\text{str}}, t_{\text{end}})\right) = [\text{QTZ}\left(r(t_{\text{str}})\right), ...,$$
$$\text{QTZ}\left(r(t_{\text{str}} + \lfloor \frac{t_{\text{end}} - t_{\text{str}}}{T} \rfloor T)\right)],$$

which can be compared in Hamming space.

However, the result of a single level-crossing quantization loses details in the original breath pattern and fails the second objective. To address this issue, we apply multiple passes of level-crossing binary quatizations, each at a distinct pair of levels, q_{i+}, q_{i-}. Intuitively, it is equivalent to create a pairwise linear approximation of the original breathing pattern, with quantization error equal to the level density.

If the binary fingerprints after the multi-level quantization is longer than $\|l\|$, we pad and divide it into multiple subsequences, $f = [f_1, f_2, ..., f_n]$ to commit

$$c = f_1 \ominus f_2 \ominus ... \ominus f_n \ominus l,$$

and decommit

$$l = f_1 \ominus f_2 \ominus ... \ominus f_n \ominus c.$$

V. Security Analysis

The security of SIENNA can be formally analyzed based on the property of a fuzzy commitment, and extended into three cases according to the attacker's knowledge on the user's breathing fingerprint, f. In the following, we omit the proof of the first two cases and focus on the third one to conserve space.

Attacker without Knowledge of f. When the eavesdropper does not have the correct context, SIENNA inherits the security properties of a fuzzy commitment, in terms of concealment and binding [4].

Attacker with General Knowledge of f. By knowing the distribution of f, the attacker can have computationally less expensive strategies to determine $\hat{l}$. One way to enhance SIENNA's security is to commit and decommit l via multiple samples/segments of f as shown in Section IV-D. Yao's XOR lemma [10] indicates that the attacker's advantage due to bias in f's distribution diminishes as we increase the number of fs in the XOR chain, with the diminishing rate defined in [10].

Attacker with Perfect Knowledge of f. The XOR-chain trick would not prevent an attacker with perfect knowledge of f to retrieve s. For a malicious patient capable of measuring his own breathing patterns. When he is also able to capture the commitment message, $\{c, \mathcal{H}(s)\}$, he can accurately compute $l = c \ominus f$ and decode to obtain s.

To prevent such an insider attack, SIENNA leverages friendly jamming to obfuscate the commit message for any unintended receivers, and we can analyze the security of it based on a wiretap channel model [11]. Consider a non-compliant patient using an unauthorized receiver to intercept the commit message X. We denote the main channel as the wireless channel between a and b and the wiretap channel as the one between the unauthorized receiver and a or b. Then the frequency-domain representation of the main channel and the wiretap channel is,

$$Y_{\text{main}} = X + \frac{P_0}{P_1}\mathcal{N}(0, \sigma_0^2), \quad Y_{\text{tap}} = X + \frac{P}{P_2}\mathcal{N}(0, \sigma^2)$$

respectively, where P_0 and σ_0^2 denote the average power and variance of the intrinsic wireless noise, P_1 and P_2 denote the average powers of the OFDM signal observed by the receiver and the unauthorized receiver, and P and σ^2 denote average power and variance of the jamming signal observed by the unauthorized receiver.

[6] has shown that the jamming scheme works at its optimal when the OFDM system operates with high order modulation (at least QPSK), and $1 < P/P_2 < 9$.[1] Therefore, SIENNA prohibits the transmit in BPSK at any SNR. Due to the FFT/IFFT operations in the OFDM system, X is a pseudorandom Gaussian signal according to the central limit theorem. The bit error probability for such an OFDM system, allowing only M-QAM transmission, is

$$B_{\text{main}} \simeq \frac{4}{\log_2 M} Q\left(\sqrt{\frac{3P_1 \log_2 M}{P_0(M-1)}}\right)$$

for the main channel and

$$B_{\text{tap}} \simeq \frac{4}{\log_2 M} Q\left(\sqrt{\frac{3P_2 \log_2 M}{P(M-1)}}\right),$$

for the wiretap channel, where $Q(\cdot)$ denotes the the tail distribution function of the standard normal distribution. The receiver may adjust P to elevate B_{tap} beyond the error correction capability of the fuzzy commitment, and prevent an insider attack. The issue is that the jamming is only effective when $1 < P/P_2 < 9$, but P_2 depends on the location of the unauthorized receiver and is unknown to the receiver. Our solution is to have the transmitter create L commitments, each with one sub-salt, and transmit them one by one, while the receiver jams at L different power levels, $\{P_{\text{max}}, P_{\text{max}}/9, \ldots, P_{\text{max}}/9^{L-1}\}$. Given the fact that B_{main} is not affected by P, the receiver can recover all sub-salts and XOR them together to obtain the key evolution salt. In contrast, the unauthorized receiver will fail to decode at least one sub-salt, therefore, cannot recover the key evolution salt. The number of jamming levels, L, can be computed based on the upper bound (the maximum power supported by the hardware, P_{max}) and lower bound (the noise floor, P_0) on the OFDM signal power.

VI. Evaluation

We empirically evaluated the performance of SIENNA, which consists of a PRMS implemented with mmWave transceivers/radio heads, one respiratory belt sensor implemented with a piezo-electric respiration transducer, and one Android-based OSA application. We conducted laboratory and field experiments over one month with the SIENNA prototype and 20 subjects selected through a random sample recruitment process. All experiments with human subjects are approved by the Institutional Review Board (IRB).

We designed the eavesdropping and spoofing attacks with BLE sniffer and spoofer, implemented via Ubertooth and Kismet. During each experiment, the subject was asked to wear a respiratory belt and lie under a PRMS. A third party manually executes the pairing process, and the packets communicated between the mobile OSA app and the PRMS were identified based on their Bluetooth Device Addresses (BDAs) obtained before the experiment. During the eavesdropping

---

[1]The jamming signal is too weak to degrade the OFDM signal when $P/P_2 \leq 1$, and too strong to be indistinguishable from the OFDM signal when $P/P_2 \geq 9$.
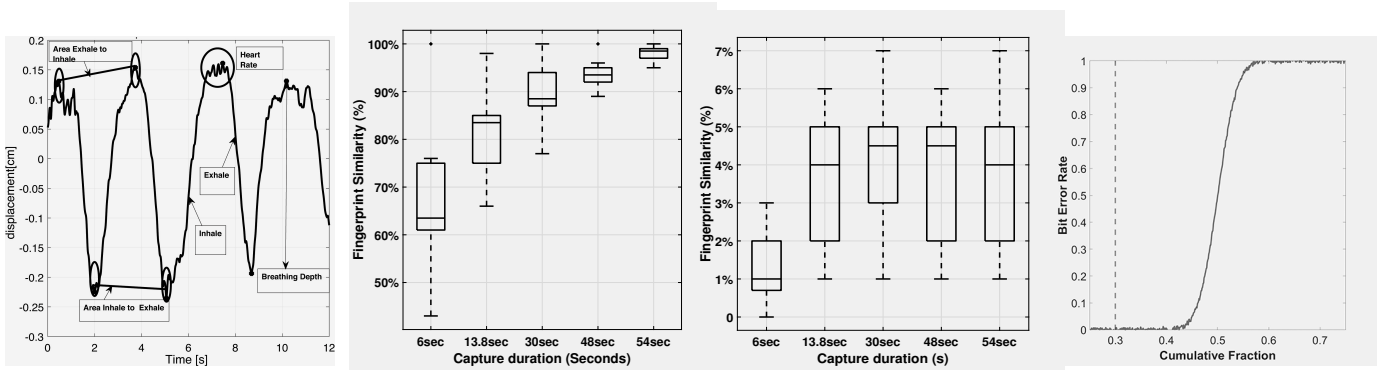
Fig. 4: Left to right: (a) Signal reconstructed after 64-level-crossing quantization with vital related dynamic features preserved; (b) Similarity between belt-based and PRMS-based breathing patterns, measured with the same subject; (c) Similarity between belt-based and PRMS-based breathing patterns, measured with different subjects; (d) Performance of SIENNA against eavesdropper with full knowledge of breathing patterns, measured in aggregated BER.

attack, the host's codes on the BLE sniffer record the packets containing the fuzzy commitment, which were analyzed offline to deduce the keys. During the spoofing attacks, an attacker-generated compliance tracking data encrypted with the deduced key was transmitted at higher power when the PRMS uploads the data to the mobile OSA app to manipulate the latter into accepting the fraudulent data, which was verified during offline analysis.

SIENNA's performance against eavesdropping and spoofing is evaluated by comparing the aggregated bit error rate (BER) at the receiver versus the aggregated BER at the attacker side. Due to the application of fuzzy commitment, the key establishment protocol allows a maximum of 27% BER in the breathing fingerprints (when using $(2^8, 255, 201)$ Reed-Solomon codes) to recover the key salt. Compared to Fig. 4c, such a BER alone prevents any outside attackers who cannot observe and mimic the patient's breathing patterns from stealing the key salt. Our experiment further showed that the jamming signal could suppress the attacker's BER to approximately 50% within the PRMS's transmission range (Fig. 4d). The CDF of the accumulated BERs for attackers at any locations within the PRMS's transmission range concentrated between 41% to 50% (Fig. 4d) and is well beyond the correctable range of the selected Reed-Solomon codes.

VII. CONCLUSION

We presented SIENNA, a novel insider-resistant context-based pairing scheme for multi-modality OSA screening systems. By merging fuzzy commitment, friendly jamming, and JADE-ICA, SIENNA leverages the unique patterns of a person's breathing dynamics for secure pairing with the presence of co-located attackers. We formally analyzed the security of SIENNA according to the attacker's knowledge of the extracted binary sequence. Our results show that the combination of fuzzy commitment, friendly jamming, and JADE-ICA in SIENNA can protect the security key during the pairing process against an attacker equipped with complete knowledge of the context information, and is robust within a noisy at-home environment with multiple persons.

REFERENCES

[1] M. Baboli, A. Singh, B. Soll, O. Boric-Lubecke, and V. M. Lubecke, "Good night: Sleep monitoring using a physiological radar monitoring system integrated with a polysomnography system," *IEEE Microwave Magazine*, vol. 16, no. 6, pp. 34–41, 2015.

[2] L. De Lathauwer, B. De Moor, and J. Vandewalle, "Independent component analysis based on higher-order statistics only," in *Proceedings of 8th Workshop on Statistical Signal and Array Processing*. IEEE, 1996, pp. 356–359.

[3] D. N. Rutledge and D. J.-R. Bouveresse, "Independent components analysis with the jade algorithm," *TrAC Trends in Analytical Chemistry*, vol. 50, pp. 22–32, 2013.

[4] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proceedings of the 6th ACM Conference on Computer and Communications Security*, 1999, pp. 28–36.

[5] A. Arora and L. Sang, "Dialog codes for secure wireless communications," in *2009 International Conference on Information Processing in Sensor Networks*. IEEE, 2009, pp. 13–24.

[6] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *2011 Proceedings IEEE INFOCOM*. Shanghai, China: IEEE, Apr. 2011, pp. 1125–1133.

[7] J. L. Melcher, Y. Zheng, D. Anthony, M. Troglia, T. Yang, A. Yang, S. Aggelopoulos, Y. Pan, and M. Li, "ijam with channel randomization," in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2020, pp. 340–342.

[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*, 2014, pp. 880–891.

[9] S. Yue, H. He, H. Wang, H. Rahul, and D. Katabi, "Extracting multi-person respiration from entangled rf signals," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2, no. 2, pp. 1–22, 2018.

[10] O. Goldreich, N. Nisan, and A. Wigderson, "On Yao's XOR-lemma," in *Studies in Complexity and Cryptography. Miscellanea on the Interplay between Randomness and Computation*. Springer, 2011, pp. 273–301.

[11] Y. Liang, G. Kramer, and H. V. Poor, "Compound wiretap channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 1–12, 2009.