Noise robustness of communications provided by coupling-function-encryption and dynamical Bayesian inference

Tomislav Stankovski*,† Peter V. E. McClintock*, and Aneta Stefanovska*,‡
*Department of Physics, Lancaster University, Lancaster LA1 4YB, UK
†Faculty of Medicine, Ss Cyril and Methodius University, Skopje 1000, Macedonia
‡Correspondence: aneta@lancaster.ac.uk

***Abstract*—In addition to the need for security, everyday information exchange must be able to cope with noise and interference. We discuss the noise robustness of a recently-introduced communications protocol inspired by the human cardiorespiratory interaction, based on analysis methods originally developed for reconstructing coupling functions between oscillatory processes underlying the biological signals. Security is assured by use of multiple, time-varying, coupling functions between two or more dynamical systems, and the protocol allows for multiplexing of the information transfer. We focus on the exceptional noise-robustness that arises from the application of dynamical Bayesian inference to the stochastic differential equations. A particular advantage of the protocol is that it facilitates an effective separation between the deterministic information signals and the dynamical (channel) noise perturbations. We define reliability in terms of the bit-error-rate (BER) as a function of noise strength, expressed as the signal-to-noise ratio (SNR). We present results confirming that the coupling function protocol is highly noise robust, and that it outperforms other known communications protocols. In the broader context, we point out that this use of coupling functions between dynamical systems is a modular construct that can be extended to implement a range of different encryption concepts. Similarly, the method of dynamical Bayesian inference carries wider implications for future applications to noise reduction in communications using other protocols.**

I. Introduction

The ever-increasing use of non-local communications brings an associated requirement for methods enabling secure and reliable exchange of information [1]–[5] transmitted e.g. over wires, optically, or by radio. In addition to withstanding human attacks, the communications protocols must cope with noise and with a range of other forms of interference, including interruptions arising from the technical infrastructure. They all tend to affect adversely the quality of communication, acting mostly within the communication channels and media.

We discuss here the noise aspects of a secure communications protocol [6], [7] based on the *coupling functions* between dynamical systems, a method that results in an unbounded number of encryption key possibilities. The information signals are encrypted as the time-variations of linearly-independent coupling functions; the transmission and reception of more than one signal simultaneously is allowed. Using predetermined forms of coupling function, we can apply Bayesian inference at the receiver end to detect and separate the information signals, while simultaneously eliminating the effect of external noise. In principle, this procedure makes the protocol particularly noise-robust.

A coupling function describes in great detail the physical rule defining *how* interactions occur and manifest themselves. Much attention is now being focused on their functional *form*, which provides direct insight into the mechanisms of interaction. In this way a coupling function can determine the possibility of qualitative transitions between states of the systems e.g. routes into and out of synchronization, even with an invariant coupling strength [8]. Consequently, coupling functions can be even used to predict the onset of synchronization [9]. Different methods for coupling function detection have been applied widely in chemistry [10], [11], in cardiorespiratory physiology [12], [13], in neuroscience [14]–[16], in mechanical interactions [17] and in the social sciences [18]. In the present work we use coupling functions to provide an effective nonlinear mixing of information, thereby achieving encryption with extensive key possibilities.

II. From Biology to secure communications

The interactions between the oscillatory activities of the heart and the lungs carry important implications for the wellbeing of the human cardiovascular system [19]–[22]. The genesis of the secure communication protocol that we discuss originated in an early discovery that the coupling functions of the cardiorespiratory interactions are time-varying. A method based on dynamical Bayesian inference, applied to reconstruct and follow these time-variations, revealed that the cardiorespiratory coupling function can be decomposed into a number of independent functions, [23]. It was studies of this complex biomedical problem that initiated the idea of a new secure protocol to encrypt information as the time-variability of multiple, non-linear, coupling functions between dynamical systems.

The protocol starts with a number of information signals coming from different channels or communications devices (e.g. mobile phone, sensor networks or wireless broadband) that need to be transmitted simultaneously. Each of the signals s_i is encrypted as a coupling scale parameter in the nonlinear coupling functions between two self-sustained oscillatory systems in the transmitter. Two signals, one from each system, are transmitted through the public channel. At the receiving end,

978-1-5090-2760-6/17/$31.00

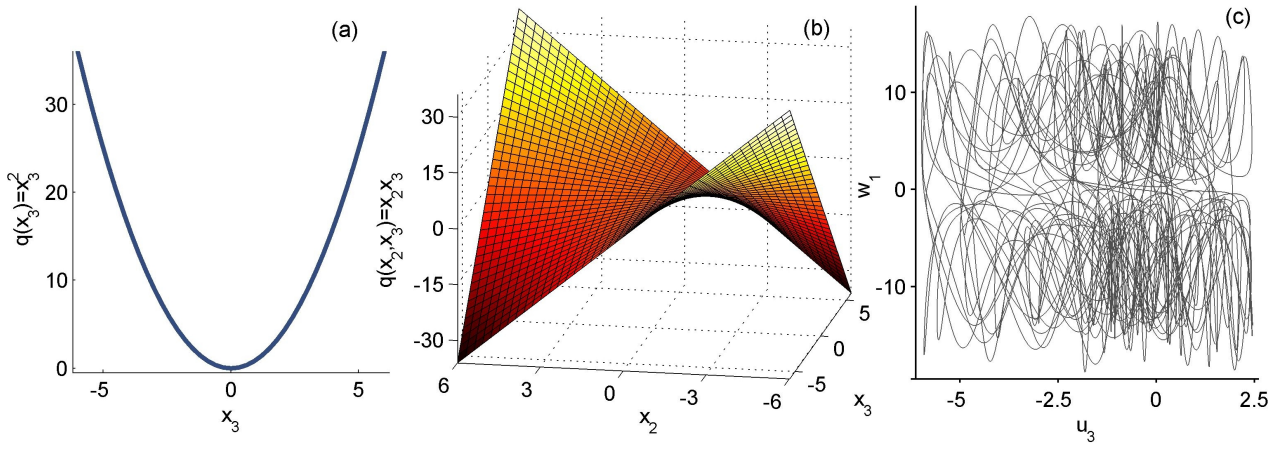

Figure 1. The coupling functions and the encrypted information space. (a) The quadratic univariate coupling function for encrypting the first information signal. (b) The multiplicative bivariate coupling function for encryption of the second signal. (c) The Lissajous curve qualitatively demonstrating the complicated information mixing.

two similar systems are enslaved, i.e. completely synchronized [24], by the two transmitted signals. Finally, by applying time-evolving Bayesian inference to the reconstructed systems one can infer the model parameters and decrypt the information signals s_i.

The number of coupling functions in use will always be finite, depending on the specific number of information channels that are needed. However the choice of *forms* available for the coupling functions constituting the private key has an unbounded continuum of possible variations. Because the protocol allows a number of information streams to be encrypted simultaneously, it inherently provides for multiplexing. The other key advantage of the protocol is the Bayesian inference of stochastic processes, which is what makes the procedure so noise resistent.

III. Technical aspects of the realization

A. The general systems model and an illustrative example

The coupled dynamical systems consist of (at least) two noisy M-dimensional interacting systems given in general by the following stochastic differential equation:

$$\dot{\mathbf{x}}_i = \mathbf{f}(\mathbf{x}_i, \mathbf{x}_j|\mathbf{c}) + \sqrt{\mathbf{D}}\xi_i = \mathbf{g}(\mathbf{x}_i|\mathbf{c}_1) + \mathbf{q}(\mathbf{x}_i, \mathbf{x}_j|\mathbf{c}_2) + \sqrt{\mathbf{D}}\xi_i \tag{1}$$

where $i \neq j = 1, 2$, $\mathbf{c}$ is a parameter vector and $\mathbf{f}(\mathbf{x}_i, \mathbf{x}_j|\mathbf{c})$ are base functions describing both the autonomous dynamics $\mathbf{g}(\mathbf{x}_i)$ and the coupling functions $\mathbf{q}(\mathbf{x}_i, \mathbf{x}_j)$. The noise is assumed to be white, Gaussian, and parameterized by a noise diffusion matrix $\mathbf{D}$. The dynamical systems $\dot{\mathbf{x}}_{i,j}$ need to be self-sustained for optimal security. For example, they can be limit-cycle oscillators or chaotic attractors. Chaotic properties are not essential for the protocol, but they add additional complexity with their random-like but deterministic signals.

In order to illustrate the protocol and its characteristics, we use an example of the transmitter consist of a Rössler systems (left, below) coupled to a Lorenz (right) system:

$$\begin{aligned} \dot{x}_1 &= 2 + x_1(x_2 - 4) + \xi_1 & \dot{y}_1 &= 10y_2 - 10y_1 + \xi_2 \\ \dot{x}_2 &= -x_1 - x_3 & \dot{y}_2 &= -y_1y_3 - y_2 + s_0(t)y_1 + \\ \dot{x}_3 &= x_2 + 0.45x_3 & & + s_1(t)x_2x_3 + s_2(t)x_3^2 \\ & & \dot{y}_3 &= y_1y_2 - 2.67y_3 + \xi_3. \end{aligned} \tag{2}$$

Only the signals x_1 and y_2 are transmitted, and they completely synchronize [24] the Rössler and Lorenz systems at the receiver:

$$\begin{aligned} u_1 &= x_1 & \dot{w}_1 &= 10y_2 - 10w_1 + \xi_4 \\ \dot{u}_2 &= -x_1 - u_3 & w_2 &= y_2 \\ \dot{u}_3 &= u_2 + 0.45u_3 & \dot{w}_3 &= w_1y_2 - 2.67w_3 + \xi_5. \end{aligned} \tag{3}$$

In this way the coupled systems at the receiver are completely restored. The information signals acting as time-dependent non-autonomous terms are given by binary pseudorandom sequence signals $s_0(t) = \{0, 28\}$, $s_1(t) = \{1.6, 2.4\}$ and $s_2(t) = \{0, 0.6\}$, while the noises have same intensity $D = 0.05$. In our implementation, the differentiation was rescaled to $d/d\tau$ with $\tau = t/2000$ for the Rössler and $\tau = t/1000$ for the Lorenz oscillator. The signals were generated by numerical simulation, but analogue electrical circuits [25], [26] can equally be used. Finally, dynamical Bayesian inference was applied to the receiver signals $\mathbf{u}$ and $\mathbf{w}$ using the same base functions as the rhs of the transmitter model (2).

In the example systems, three coupling functions are used to provide nonlinear complicated "scrambling" of the information signals. The first coupling function $q(\mathbf{x}) = y_1$ is univariate and linear, and can act more as a control function, for example to mutually synchronize the two systems in the transmitter. The other two functions are nonlinear and are the ones that provide for the complex mixing of information. The $q(x_3) = x_3^2$ coupling is a quadratic univariate function, Fig. 1(a), that shows how the information signal $s_2(t)$ is included in the dynamics

through dependence on the x_3 variable. Similarly, Fig. 1(b) shows the bivariate coupling function $q(x_2, x_3) = x_2 x_3$ that encrypts the $s_1(t)$ information signal as the scale of a product dependence based on the x_2 and x_3 variables. The resultant coupled dynamics that an intruder would face, for example as observed in the Lissajous curves in Fig. 1(c), demonstrates complex information mixing that, without knowledge of which coupling functions to use (i.e. the information of the private key) is extremely difficult, if not impossible, to break.

B. Dynamical Bayesian inference

After the information has been encrypted numerically at the receiver, the signals sent over the channel, and the systems reconstructed at the receiver, dynamical Bayesian inference [23], [27] is applied for decryption of the information and separation of the interfering noise. If $2 \times M$ time-series $\mathcal{X} = \{\mathbf{x}_n \equiv \mathbf{x}(t_n)\}$ $(t_n = nh)$ are provided as inputs, the fundamental task for the Bayesian dynamical inference is to reveal the unknown model parameters $\mathcal{M} = \{\mathbf{c}, \mathbf{D}\}$. The inference uses Bayes' theorem to calculate the so-called *posterior* density $p_{\mathcal{X}}(\mathcal{M}|\mathcal{X})$ of the unknown parameters $\mathcal{M}$, given a *prior* density $p_{\text{prior}}(\mathcal{M})$ that encloses previous knowledge of the unknown parameters based on observations, and the *likelihood* function $\ell(\mathcal{X}|\mathcal{M})$ which is the conditional probability density to observe $\mathcal{X}$ for a given choice $\mathcal{M}$ of the dynamical model (1).

The log-likelihood can be derived to have a specific quadratic form to be used with multivariate normal distributions for the prior and posterior. Given such a distribution as a prior for the parameters $\mathbf{c}$, with mean $\bar{\mathbf{c}}$, and covariance matrix $\mathbf{\Sigma}_{\text{prior}} \equiv {\mathbf{\Xi}^{-1}}_{\text{prior}}$, the stationary evaluation within the method can be calculated recursively using only the following four equations:

$$
\begin{aligned}
\mathbf{D} &= \frac{h}{N}\left(\dot{\mathbf{x}}_n - \mathbf{c}_k \mathbf{f}_k(\mathbf{x}^*_{\cdot,n})\right)^T \left(\dot{\mathbf{x}}_n - \mathbf{c}_k \mathbf{f}_k(\mathbf{x}^*_{\cdot,n})\right), \\
\mathbf{c}_k &= (\mathbf{\Xi}^{-1})_{kw}\, \mathbf{r}_w, \\
\mathbf{r}_w &= (\mathbf{\Xi}_{\text{prior}})_{kw}\, \mathbf{c}_w + h\, \mathbf{f}_k(\mathbf{x}^*_{\cdot,n})\, (\mathbf{D}^{-1})\, \dot{\mathbf{x}}_n + \\
&\quad - \frac{h}{2} \frac{\partial \mathbf{f}_k(\mathbf{x}_{\cdot,n})}{\partial \mathbf{x}}, \\
\mathbf{\Xi}_{kw} &= (\mathbf{\Xi}_{\text{prior}})_{kw} + h\, \mathbf{f}_k(\mathbf{x}^*_{\cdot,n})\, (\mathbf{D}^{-1})\, \mathbf{f}_w(\mathbf{x}^*_{\cdot,n}),
\end{aligned}
\tag{4}
$$

where summation over $n = 1, \ldots, N$ is assumed and the summation over repeated indices k and w is again implicit. The initial prior is set to be the non-informative flat normal distribution given by $\mathbf{\Xi}_{\text{prior}} = 0$ and $\bar{\mathbf{c}}_{\text{prior}} = 0$. A special procedure is used to propagate information from the previous prior to the new posterior, thereby enabling the method to follow the time-evolution of the parameters i.e. the encrypted signals. More details about the method, its implementation and coding can be found in [28], [29].

IV. The noise robustness

The channel noise affects the transmitted signals, which are then incorporated into the dynamical systems i.e. they are introduced into the differential equations. In this way channel noise acts as a dynamical noise in the reconstructed systems, and the dynamics turns into stochastic processes. Hence, dynamical Bayesian inference is ideally fitted to treat such stochastic differential equations and to separate out the noise effects.

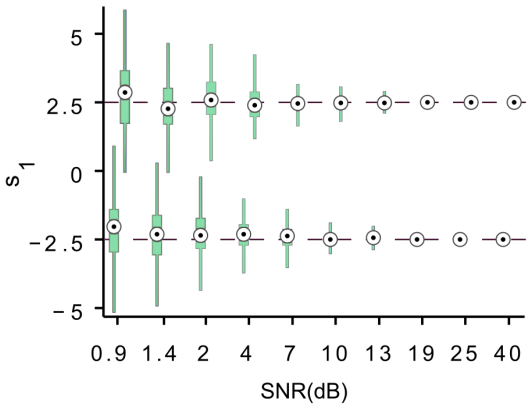

Figure 2. Deviations of the demodulated signal from the initial binary states due to noise, presented as compact boxplots (in terms of descriptive statistics: median, quartiles, max., and min.) plotted as functions of the signal-to-noise-ratio (SNR). The transmitted signal has the two binary values $s_1(t) = \{-2.5, 2.5\}$.

To test and demonstrate the noise robustness of the protocol, we studied the reliability of communications by gradually increasing the noise level. Fig. 2 illustrates the resultant distributions of deviations from the as-sent binary values, plotted as functions of the signal-to-noise-ratio (SNR). Note that, as the noise increases i.e. the SNR decreases, the boxplots and the deviations enlarge. For some values below 4dB SNR, the boxplots start to overlap, meaning that they cannot be separated, and corresponding to communications failure.

We also quantified the erroneous communications in terms of the bit-error-rate (BER) as a function of gradually increasing noise strength, as shown in Fig. 3. First, in Fig. 3(a) we present the case of our coupling-function-based protocol. Note that the communications are quite noise robust, with insignificant BER above SNR=4dB. Secondly, in order to compare our scheme with other encryption methods, we investigated how noise affects signal-masking [3] communication. This case can act as a general example of a whole class of secure communications schemes based on dynamical systems and complete synchronization [24]. It also corresponds to how we transmit and recover the systems in the coupling-function scheme, before the Bayesian inference is applied. For this reason we masked the y_2 signal at the transmitter with a binary signal $s_3(t) = \{0, 5\}$ as: $\dot{y}_2 = -y_1 y_3 - y_2 + 28 y_1 + s_3(t)$, and we applied the relevant recovery procedure [3]. The results for this protocol, presented in Fig. 3(b), show that erroneous detection occurs at around and below $\sim$ 20dB, representing significantly lower than the noise-tolerance when compared to 4dB for the coupling function protocol.

V. Conclusion

We have confirmed that the communication scheme [6] based on coupling functions is exceptionally noise resistant,

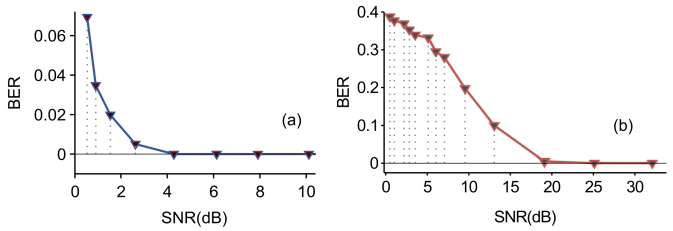

Figure 3. Variation of erroneous communication with noise intensity. (a) Bit-error-rate (BER) of the coupling-function scheme as a function of SNR. (b) For comparison, BER of the signal-masking scheme as a function of SNR. In each run, 10^3 randomly-ordered binary symbols were sent.

in addition to being secure and allowing multiplexing. In the present case, we used three coupling functions but, in principle a larger number (e.g. ten) could be used. Our focus was on the noise tolerance conferred by the use of dynamical Bayesian inference.

Applied to the coupled chaotic systems, our demonstration showed that the noise resistance of around 4dB SNR provided by the coupling function protocol is well below the 15dB SNR of a typical digital transmission, or the 40dB SNR of a wireline communication channel in a real environment [5]. The coupling-function scheme's 4dB, was also greatly superior to the 20dB of signal-masking schemes, clearly illustrating the advantage of Bayesian inference in providing robust communications in a noisy environment.

Our results imply that the combination of dynamical systems and dynamical Bayesian inference provides a powerful tool that can be used to confer high noise-robustness on other communications protocols and logic schemes.

ACKNOWLEDGMENT

We are grateful to Robert J. Young and Christopher Anderson for helpful discussions. The work was funded by the EPSRC (UK) through Lancaster University's Impact Acceleration Account.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Tech. J*, vol. 28, no. 4, pp. 656–715, 1949.

[2] C. E. Shannon , "Communication in the presence of noise," *Proc. IRE*, vol. 37, no. 1, pp. 10–21, 1949.

[3] K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.*, vol. 71, pp. 65–68, 1993.

[4] L. B. Kish, "Totally secure classical communication utilizing Johnson (-like) noise and Kirchoff's law," *Phys. Lett. A*, vol. 352, no. 3, pp. 178–182, 2006.

[5] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Intern. J. Bifurc. Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[6] T. Stankovski, P. V. E. McClintock, and A. Stefanovska, "Coupling functions enable secure communications," *Phys. Rev. X*, vol. 4, p. 011026, 2014.

[7] T. Stankovski, A. Stefanovska, R. J. Young, and P. V. E. McClintock, "Encoding data using dynamic system coupling," *US Patent App. 14/910,547*, 2014.

[8] T. Stankovski, "Time-varying coupling functions: Dynamical inference and cause of synchronization transitions," *Phys. Rev. E*, vol. 95, no. 2, p. 022206, 2017.

[9] I. Z. Kiss, Y. Zhai, and J. L. Hudson, "Predicting mutual entrainment of oscillators with experiment-based phase models," *Phys. Rev. Lett.*, vol. 94, p. 248301, Jun 2005.

[10] I. Z. Kiss, C. G. Rusin, H. Kori, and J. L. Hudson, "Engineering complex dynamical structures: Sequential patterns and desynchronization," *Science*, vol. 316, no. 5833, pp. 1886–1889, 2007.

[11] J. Miyazaki and S. Kinoshita, "Determination of a coupling function in multicoupled oscillators," *Phys. Rev. Lett.*, vol. 96, p. 194101, May 2006.

[12] B. Kralemann, M. Frühwirth, A. Pikovsky, M. Rosenblum, T. Kenner, J. Schaefer, and M. Moser, "In vivo cardiac phase response curve elucidates human respiratory heart rate variability," *Nat. Commun.*, vol. 4, p. 2418, 2013.

[13] D. Iatsenko, A. Bernjak, T. Stankovski, Y. Shiogai, P. J. Owen-Lynch, P. B. M. Clarkson, P. V. E. McClintock, and A. Stefanovska, "Evolution of cardio-respiratory interactions with age," *Phil. Trans. R. Soc. Lond. A*, vol. 371, no. 1997, p. 20110622, 2013.

[14] T. Stankovski, V. Ticcinelli, P. V. E. McClintock, and A. Stefanovska, "Coupling functions in networks of oscillators," *New J. Phys.*, vol. 17, no. 3, p. 035002, 2015.

[15] T. Stankovski, S. Petkoski, J. Raeder, A. F. Smith, P. V. E. McClintock, and A. Stefanovska, "Alterations in the coupling functions between cortical and cardio-respiratory oscillations due to anaesthesia with propofol and sevoflurane." *Phil. Trans. R. Soc. A*, vol. 374, no. 2067, p. 20150186, 2016.

[16] J. Wilting and K. Lehnertz, "Bayesian inference of interaction properties of noisy dynamical systems with time-varying coupling: capabilities and limitations," *Eur. Phys. J. B*, vol. 88, no. 8, pp. 1–11, 2015.

[17] B. Kralemann, L. Cimponeriu, M. Rosenblum, A. Pikovsky, and R. Mrowka, "Phase dynamics of coupled oscillators reconstructed from data," *Phys. Rev. E*, vol. 77, no. 6, Part 2, p. 066205, 2008.

[18] S. Ranganathan, V. Spaiser, R. P. Mann, and D. J. T. Sumpter, "Bayesian dynamical systems modelling in the social sciences," *PloS one*, vol. 9, no. 1, p. e86468, 2014.

[19] A. Stefanovska and M. Bračič, "Physics of the human cardiovascular system," *Contemp. Phys.*, vol. 40, no. 1, pp. 31–55, 1999.

[20] A. Stefanovska, H. Haken, P. V. E. McClintock, M. Hožič, F. Bajrović, and S. Ribarič, "Reversible transitions between synchronization states of the cardiorespiratory system," *Phys. Rev. Lett.*, vol. 85, no. 22, pp. 4831–4834, 2000.

[21] Y. Shiogai, A. Stefanovska, and P. V. E. McClintock, "Nonlinear dynamics of cardiovascular ageing," *Phys. Rep.*, vol. 488, pp. 51–110, 2010.

[22] D. A. Kenwright, *et al.*, "The discriminatory value of cardiorespiratory interactions in distinguishing awake from anaesthetised states: a randomised observational study," *Anaesthesia*, vol. 70, no. 12, pp. 1356–1368, 2015.

[23] T. Stankovski, A. Duggento, P. V. E. McClintock, and A. Stefanovska, "Inference of time-evolving coupled dynamical systems in the presence of noise," *Phys. Rev. Lett.*, vol. 109, p. 024101, 2012.

[24] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821–824, Feb 1990.

[25] D. G. Luchinsky and P. V. E. McClintock, "Irreversibility of classical fluctuations studied in analogue electrical circuits," *Nature*, vol. 389, no. 6650, pp. 463–466, 1997.

[26] T. Stankovski, P. V. E. McClintock, and A. Stefanovska, "Dynamical inference: Where phase synchronization and generalized synchronization meet," *Phys. Rev. E*, vol. 89, no. 6, p. 062909, 2014.

[27] V. N. Smelyanskiy, D. G. Luchinsky, A. Stefanovska, and P. V. E. McClintock, "Inference of a nonlinear stochastic model of the cardiorespiratory interaction," *Phys. Rev. Lett.*, vol. 94, no. 9, p. 098101, 2005.

[28] A. Duggento, T. Stankovski, P. V. E. McClintock, and A. Stefanovska, "Dynamical Bayesian inference of time-evolving interactions: From a pair of coupled oscillators to networks of oscillators," *Phys. Rev. E*, vol. 86, p. 061126, 2012.

[29] T. Stankovski, A. Duggento, P. V. E. McClintock, and A. Stefanovska, "A tutorial on time-evolving dynamical Bayesian inference," *Eur. Phys. J. Special Topics*, vol. 223, no. 13, pp. 2685–2703, 2014.