Spying on chaos-based cryptosystems with reservoir computing

Antonik, Piotr; Gulina, Marvyn; Pauwels, Jael ; Rontani, Damien ; Haelterman, Marc; Massar, Serge

Published in:
2018 International Joint Conference on Neural Networks, IJCNN 2018 - Proceedings

DOI:
10.1109/IJCNN.2018.8489102

Publication date:
2018

Document Version
Peer reviewed version

Cracking chaos-based cryptography with reservoir computing

Piotr Antonik [1,2], Marvyn Gulina[3], Jaël Pauwels[4,5], Damien Rontani[1,2], Marc Haelterman[6], and Serge Massar[4,5]

[1] Chaire Photonique, CentraleSupélec, Université Paris-Saclay, F-57070 Metz, France
[2] LMOPS EA 4423 Lab, CentraleSupélec & Université de Lorraine, F-57070 Metz, France
[3] Namur Institute for Complex Systems, Université de Namur, B-5000 Namur, Belgium
[4] Applied Physics Research Group, Vrije Universiteit Brussels, B-1050 Brussels, Belgium
[5] Laboratoire d'Information Quantique, Université libre de Bruxelles, B-1050 Brussels, Belgium
[6] Service OPERA-Photonique, Université libre de Bruxelles, B-1050 Brussels, Belgium
Email: piotr.antonik@centralesupelec.fr

Is it possible to emulate a non-linear chaotic dynamical system with a fundamentally different non-linear dynamical system? This question has been answered positively in the context of reservoir computing – a machine learning approach to designing artificial neural networks [1, 2]. Despite the significant simplification of the training process, the performance of such systems is comparable to other digital algorithms on a series of benchmark tasks. Reservoir computing was originally used for forecasting the trajectories of chaotic dynamical systems, where it reached record forecasting horizons [1].

In the first part of this work, we demonstrate that a trained reservoir computer captures a large part of the characteristics of the dynamics of the original system. That is, if weakly driven by the original system, the reservoir computer will synchronise with it. We illustrate this phenomenon on two examples, the Lorenz and Mackey-Glass systems. The phenomenon of synchronisation is one of the most surprising aspects of chaos theory, and has been extensively studied, see e.g. the review [3]. However, our results appear in great contrast with what was known about synchronisation of chaotic systems, in the sense that two twin physical systems were required to achieve similar properties of the generated chaotic time series.

After the discovery of chaos synchronisation, considerable effort was devoted to trying to use this effect and the unpredictability of chaotic systems to hide secret messages. In this type of systems, a message is embedded within a chaotic carrier in the emitter, and recovered after transmission by a receiver upon synchronisation with the emitter [4]. The security of chaos-based transmissions relies on the fact that the emitting and receiving parties must have similar copies of a chaotic attractor, that is very challenging to manufacture for a third party, without any knowledge of its internal structure and parameters. However, a potential eavesdropper could crack the chaotic masking with a device capable of emulating a chaotic system, such as the reservoir computer.

In the second part of this work, as an application of our results on chaos synchronisation, we consider using the reservoir computer to crack two chaos-based encryption schemes with Mackey-Glass and Lorenz chaotic carriers. The successful results we obtain suggest that hardware chaos-based cryptosystems could be cracked by hardware reservoir computers, as these have been implemented physically with good performance and high speed, see [5] for a review.

Acknowledgements

This work was supported by the Interuniversity Attraction Poles Program (Belgian Science Policy) Project Photonics@be IAP P7-35, by the Fonds de la Recherche Scientifique (FRS-FNRS), by the Action de Recherche Concertée of the Fédération Universitaire Wallonie-Bruxelles through Grant No. AUWB-2012-12/17-ULB9, by the Research Foundation - Flanders (FWO, Ph. D. fellowship), and by the Université de Namur. P.A. and D.R gratefully acknowledge the support of AFOSR (grants No. FA-9550-15-1-0279 and FA-9550-17-1-0072) and Région Grand-Est.

References

[1] H. Jaeger and H. Haas, "Harnessing nonlinearity: Predicting chaotic systems and saving energy in wireless communication," *Science*, vol. 304, pp. 78–80, 2004.

[2] P. Antonik, M. Haelterman, and S. Massar, "Brain-inspired photonic signal processor for generating periodic patterns and emulating chaotic systems," *Phys. Rev. Applied*, vol. 7, p. 054014, May 2017.

[3] S. Boccaletti, J. Kurths, G. Osipov, D. Valladares, and C. Zhou, "The synchronization of chaotic systems," *Physics reports*, vol. 366, no. 1, pp. 1–101, 2002.

[4] J.-M. Liu and L. S. Tsimring, *Digital communications using chaos and nonlinear dynamics*. Springer Science & Business Media, 2006.

[5] G. Van der Sande, D. Brunner, and M. C. Soriano, "Advances in photonic reservoir computing," *Nanophotonics*, vol. 6, no. 3, pp. 561–576, 2017.