УДК 003.26+004.032.26

О ПРИМЕНЕНИИ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ К РЕШЕНИЮ ЗАДАЧ ЗАЩИТЫ ИНФОРМАЦИИ

М. В. Мальцев, Ю. С. Харин
НИИ прикладных проблем математики и информатики БГУ, Минск

Машинное обучение (machine learning) объединяет в себе методы и алгоритмы, позволяющие автоматически выявлять закономерности в данных и затем использовать обнаруженные закономерности для решения различных задач: прогнозирования, классификации и кластеризации, обнаружения аномалий и т.д. [1]. Одним из наиболее перспективных и активно развивающихся методов машинного обучения являются искусственные нейронные сети (ИНС) [2]. Применение ИНС позволило значительно улучшить качество распознавания речи и изображений, существенно продвинуться в ряде задач биоинформатики, создать системы искусственного интеллекта, способные на сопоставимом с человеком уровне управлять автомобилем и играть в интеллектуальные игры. Закономерно, что интерес к ИНС как к эффективному инструменту решения самых разнообразных задач появился и в криптографическом сообществе.

Идеи использовать машинное обучение в криптологии высказывались еще в начале 90-х годов Ривестом [3], но широкое распространение они получили в последнее десятилетие вследствие развития методов обучения ИНС, появления новых архитектур, роста вычислительных мощностей. ИНС, используя большие объемы информации, позволяют выявлять скрытые закономерности в данных сложной структуры, что способствует их применению в задачах криптоанализа [4–8]. Отметим, что в открытой печати, как правило, анализируются упрощенные версии криптографических алгоритмов. Например, в работе [4] для алгоритма SDES (упрощенная версия алгоритма DES) исследовалось преобразование открытого текста в шифртекст с помощью нейронного криптоанализа. Построенная нейронная сеть смогла выявить уязвимости в одном из используемых *S*-блоков и получить правильные значения для некоторых бит ключа. В работе [5] нейронные сети использовались для повышения эффективности дифференциального криптоанализа алгоритма Speck32/64. В работе [8] – одной из первых, посвященных криптоанализу блочных шифров с помощью нейронных сетей, – исследовалась возможность восстановления ключа для криптосистем, основанных на сети Фейстеля.

Широко применяется машинное обучение в атаках по сторонним каналам, использующих особенности реализации криптосистем на физическом уровне. Для этих задач используется такие методы как глубокие нейронные сети [9], метод опорных векторов [10], генеративно-состязательные нейронные сети [11]. В работе [12] для построения атак по сторонним каналам рассматривались различные архитектуры нейронных сетей, наибольшую эффективность показали сверточные ИНС.

В статье [13] предложен поточный шифр на основе нейронной сети, в [14] – функция хэширования. В [15] нейронные сети применяются для анализа генераторов случайных числовых последовательностей. Ряд статей посвящен применению машинного обучения в стеганографии: работы [16, 17] посвящены методам стегоанализа на основе нейронных сетей, в статьях [18, 19] ИНС применяются для встраивания секретной информации в контейнер.

Таким образом, машинное обучение и ИНС обладают высоким потенциалом для их применения в задачах защиты информации – как за счет повышения эффективности существующих методов, так и путем создания на основе ИНС новых методов анализа.

Список использованных источников

1. Murphy, K. P. Machine Learning: a Probabilistic Perspective. – Cambridge University Press, 2013. – 1104 p.

2. Николенко, С. Глубокое обучение / С. Николенко, А. Кадурин, Е. Архангельская. – СПб.: Питер, 2018. – 480 с.

3. Rivest, R. L. Cryptography and machine learning / R. L. Rivest // Advances in Cryptology. ASIACRYPT 91. – 1991. – P. 427–439.

4. Danziger, M. Improved cryptanalysis combining differential and artificial neural network schemes / M. Danziger, M. Henriques // 2014 Intern. telecommunications symp. (ITS), IEEE, 2014. – P. 1–5.

5. Gohr, A. Improving attacks on round-reduced speck32/64 using deep learning / A. Gohr // Advances in cryptology, CRYPTO-2019. – 2019. – P. 150—179.

6. Laskari, E. Cryptography and cryptanalysis through computational intelligence / E. Laskari, G. Meletiou, Y. Stamatiou, M. Vrahatis // Computational Intelligence in Information Assurance and Security, Springer. – 2007. – P 1–49.

7. Chou, J. On the effectiveness of using state-of-the-art machine learning techniques to launch cryptographic distinguishing attacks / J. Chou, S. Lin, C. Cheng // Proceedings of the 5th ACM workshop on Security and articial intelligence. ACM, 2012.

8. Albassal, A. Neural network based cryptanalysis of a feistel type block cipher / A. Albassal, A. Wahdan // International Conference on Electrical, Electronic and Computer Engineering, 2004. ICEEC'04, 2004. P. 231–237.

9. Lerman, L. Power analysis attack: an approach based on machine learning / L. Lerman, G. Bontempi, O. Markowitch // Intern. J. of Applied Cryptography. – Vol 3(2). – 2014. – P. 97–115.

10.Bartkewitz, T. Ecient Template Attacks Based on Probabilistic Multi-class Support Vector Machines / T. Bartkewitz, K. Lemke-Rust // Springer Berlin Heidelberg – 2013. – P. 263–276.

11. Ping, W. Enhancing the Performance of Practical Profiling Side-Channel Attacks Using Conditional Generative Adversarial Networks / W. Ping, C. Ping, L. Zhimin, D. Gaofeng, Z. Mengce, Y. Nenghai, H. Honggang // Cryptology ePrint Archive, Paper 2020/867. – 2020.

12. Picek, S. On the Performance of Convolutional Neural Networks for Side-channel Analysis / S. Picek, I. P. Saiotis, A. Heuser, J. Kim, S. Bhasin, A. Legay. – Cryptology ePrint Archive, Paper 2018/004. – 2018.

13. Long, H. Stream Cipher Method Based on Neural Network / H. Long // Proceedings of the 2012 National Conf. on Information Technology and Computer Science, CITCS. – 2012. – P. 414–417.

14. Lian, S. One-way Hash Function Based on Neural Network / S. Lian, J. Sun, Z. Wang. – 2007. – arXiv:0707.4032.

15. Truong, N.D. Machine learning cryptanalysis of a quantum random number generator / N. D. Truong, J. Y. Haw, S. M. Assad, P. K. Lam, O. Kavehei // IEEE Transactions on Information Forensics and Security, 14(2). – 2018. – P. 403–414.

16. Qian, Y. Deep learning for steganalysis via convolutional neural networks / Y. Qian, J. Dong, W. Wang, T. Tan // SPIE/IS&T Electronic Imaging, P 94090J–94090J. International Society for Optics and Photonics. – 2015.

17. Pibre, L. Deep learning is a good steganalysis tool when embedding key is reused for different images, even if there is a cover source mismatch // L. Pibre, J. Pasquet, D. Ienco, M. Chaumont // Electronic Imaging, 2016 (8). – 2016. – P. 1–11.

18. Jarušek, R. Neural network approach to image steganography techniques // R. Jarušek, E. Volna, M. Kotyrba // Mendel 2015, Springer. – 2015. – P. 317–327.

19. Baluja, S. Hiding images in plain sight: Deep steganography / S. Baluja // Advances in Neural Information Processing Systems 30. Curran Associates, Inc. – 2017. – P. 2069–2079.