Security
of Infocommunication Systems
and Internet of Things

2023 Vol 1, No 2

https://doi.org/10.31861/sisiot2023.2.02009

Received 10 November 2023; revised 26 December 2023; accepted 28 December 2023; published 30 December 2023

Information Security and Telecommunications Prospects of Machine-Learning-Based Methods in Chaotic Systems

Mykola Kushnir*, Volodymyr Toronchuk and Hryhorii Kosovan

Dept. of Radio Engineering and Information Security, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine

*Corresponding author (E-mail: myk.kushnir@chnu.edu.ua)

ABSTRACT In the dynamic landscape of information security and telecommunications, this paper delves into the multifaceted realm of machine-learning-based methods, with a particular focus on their application in chaotic systems. An informative introduction sets the way for a thorough examination of the major benefits provided by reservoir computing (RC) and machine learning (ML) in telecommunications. The first segment of this study scrutinizes the role of machine learning in fortifying information security. With the ever-evolving nature of cyber threats, understanding the nuances of ML becomes imperative. The article highlights key advancements and features in ML that contribute to bolstering data security, providing a nuanced perspective on its efficacy in addressing the intricate challenges posed by contemporary paradigms for information security. Moving forward, the discussion expands to reservoir computing and its implications in telecommunications. Reservoir computing, with its unique approach to processing information through dynamic systems, has emerged as a promising technique. The article dissects its applications in the telecommunications sector, shedding light on how reservoir computing augments information processing and transmission efficiency within complex networks. A pivotal aspect of this paper is the exploration of the double-reservoir solution — a cutting-edge approach that combines the strengths of reservoir computing for enhanced performance. This innovative solution is dissected in detail, uncovering its prospects and the challenges it presents. The incorporation of double-reservoir solutions into chaotic systems represents a paradigm shift in the optimization of system dynamics and represents a major advancement in tackling important telecommunications difficulties. Yet not just this paper offers insights into this solution, it fairly describes possible challenges with implementation of such a model. It is to be taken into consideration, hence there is no 'perfect' solution for such a complex problem. This paper provides a comprehensive view of machine-learning-based solutions for information security and telecommunications challenges. By unraveling the capabilities of both machine learning and reservoir computing, it unlocks avenues for further research and development in harnessing these technologies to fortify the foundations of secure and efficient telecommunications in the face of constantly developing threats. The insights presented herein lay the groundwork for future innovations, urging researchers and practitioners to delve deeper into the synergy of machine learning and chaotic systems for transformative advancements in these critical domains.

KEYWORDS machine learning, reservoir computing, chaotic system, telecommunications.

I. INTRODUCTION

In the rapidly evolving landscape of information security and telecommunications, the integration of cutting-edge technologies has become imperative to address the dynamic challenges presented by sophisticated cyber threats and the intricacies of chaotic systems. Keeping up with changing cyber threats in the dynamic world of telecommunications and information security requires integrating state-of-the-art solutions. The potential uses of reservoir computing and machine learning to strengthen information security and improve telecommunications systems are discussed in this article.

We utilize recent papers [1-3] that demonstrate the revolutionary power of reservoir computing and machine learning in tackling the problems presented by complex cyber threats and chaotic system intricacy in order to demonstrate the applicability of our investigation.

Our main goal is to analyze how reservoir computing and machine learning contribute to enhancing information security and transforming telecom infrastructure. We explore the importance of machine learning in the first chapter, concentrating on network monitoring, anomaly detection, and intrusion detection three crucial components of protecting sensitive data.

The emphasis moves to reservoir computing in the second chapter, which explains its elements, training strategies, and potential uses in chaotic systems. This lays the groundwork for comprehending how frameworks for telecommunications can be reshaped by reservoir computing. We dissect the components of reservoir computing systems, unravel the intricacies of their training methodologies, and explore the promising applications within chaotic systems. This section lays the foundation for understanding how reservoir computing can revolutionize telecommunications frameworks.

The second chapter shifts the focus to reservoir computing, elucidating its components, training methodologies, and promising applications within chaotic systems. This sets the foundation for understanding how reservoir computing can reshape telecommunications frameworks with this novel paradigm and present a comprehensive model description.

The narrative unfolds in the third chapter, introducing an innovative approach – the double-reservoir solution.

While confronting the challenges associated with this novel paradigm, we present a comprehensive model description, aiming to illuminate the prospects and hurdles of this dual-reservoir approach. Through this exploration, we aim to illuminate the prospects and hurdles associated with a dual-reservoir approach, offering insights into its potential as a robust solution in the intricate domains of information security and telecommunications. Join us on this journey through the intricate landscape of chaotic systems, where innovation meets the challenge, and the future of cybersecurity and telecommunications unfolds.

II. MACHINE LEARNING IN INFORMATION SECURITY

A. Anomaly Recognition. Chaotic systems can showcase intricate and uncertain behaviors. Machine learning strategies, like neural networks and clustering methodologies, may be employed to identify anomalies or unexpected variations within info-communication systems [1,6]. This could assist in pinpointing potential harmful activities or unusual network activities that suggest cyberattacks. Machine Learning-based methods and models for anomaly detection include:

1. Recurrent Neural Networks

Chaotic systems tend to generate time series data. Machine learning models, such as recurrent neural networks (RNNs) and long short-term memory networks (LSTMs), can be 'trained' to predict future values of a chaotic signal based on past observations [4]. This can be used in forecasting and understanding the system's dynamics as well as signal recovery or anomaly recognition. A typical example of an RNN is Elman Network. It is a simple recurrent network (Figure 1). Elman Network is described by:

$$\begin{cases} h_t = \sigma_h\left(W_h x_t + U_h h_{t-1} + b_h\right) \\ y_t = \sigma_y\left(W_y h_t + b_y\right) \end{cases}, \quad (1)$$

where:

x_t is input vector,

h_t is hidden layer vector,

y_t is output vector,

W and U – parameter matrices,

b – parameter vector,

σ_h and σ_y – activation functions.

2. Autoencoders

Autoencoder is a type of a neural network architecture specifically created to learn efficient representations of input data [3]. Anomaly recognition can be performed by training an autoencoder on normal data and identifying data points with high reconstruction errors as anomalies. Basic schema of an autoencoder can be sin in Fig. 2.

An autoencoder consists of two pivotal elements: an encoder and a decoder. An encoder takes input information, such as time-series data from a chaotic system, and encodes it into a lower-dimensional representation, typically called the 'latent space' or 'encoding'. The decoder then takes this encoded information and attempts to reconstruct the original data, based on its previous learning. During its training an autoencoder learns to represent data in the most close-packed and didactic way possible in the latent space. The encoder learns to capture the most important patterns, features, or structures in chaotic datasets it learns upon.

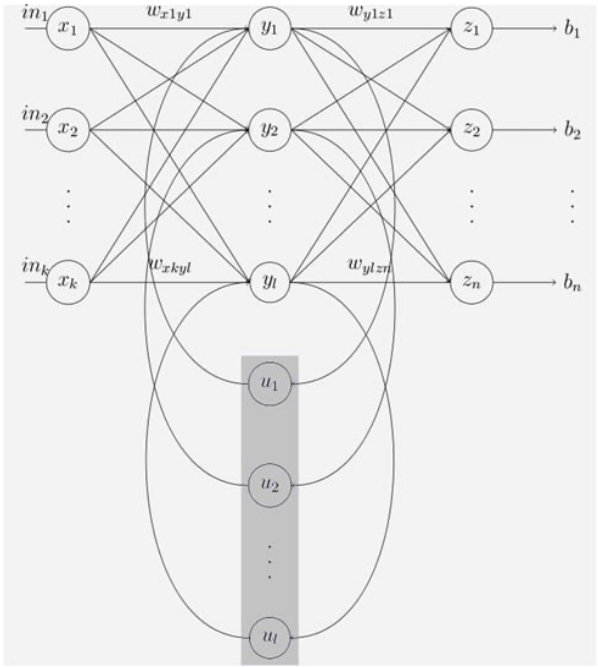

FIG. 1. Elman's RNN: (a) x is input vector; (b) y and z is output vector; (c) u is hidden layer vector.

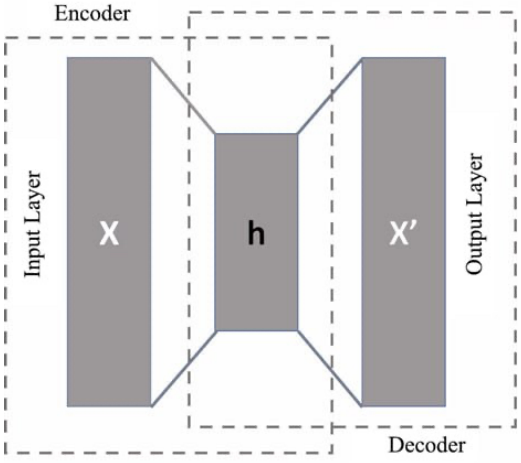

FIG. 2 An autoencoder scheme: (a) X is input vector; (b) h is hidden layer vector; (c) X' is output vector.

3. Recurrent Autoencoders

Recurrent Autoencoders (RAEs), which combine the principles of autoencoders with recurrent neural networks (RNNs), develop a compressed representation of the data while capturing sequential patterns in it. RAEs are thus particularly well suited for sequential data applications, such as information security and anomaly detection. They combine recurrent connections with the autoencoder's encoder-decoder architecture.

Both the temporal dependencies and compressed representations of sequential data are intended to be captured by them. In RAEs, the recurrent connections record temporal dependencies while the encoder encodes sequential data into a lower-dimensional form. A decoder then uses this representation to reassemble the sequential

data. RAEs are valuable for anomaly detection in time-series data, particularly information security applications, because they are good at catching complicated patterns in sequential data.

RAEs are well-suited to recognize trends in software program behavior and spot anomalies that might be signs of malware or harmful activity. They also assist in locating unexpected patterns of system events or log entries that may be a sign of security breaches or system weaknesses.

4. Invasion detection and accuracy improvement tools

Apart from RNNs, AEs, and RAEs usage in anomaly detection and invasion detection (as invasion is a subdivision of an anomaly in a chaotic telecommunication system) some assisting methods and strategies need to be considered. Namely:

- Isolation forests: tree-based group of ensemble methods which key function is to detect anomalies within telecommunication systems.

- Clustering algorithms: Algorithms such as K-Means or DBSCAN, utilized for clustering, can be applied for organizing data points of resemblance within disorderly chaotic systems. Anomalies are perceived as data points that are either not included in any cluster or belong to a diminutive cluster.

- Principal Component Analysis: PCAs are effectively used to bring down the dimensionality of chaotic system data. Anomalies can be detected by identifying data points that diverge significantly from the principal components.

B. Invasion detection. Invasion detection is a specific case of Anomaly detection. Machine learning frameworks can be programmed to detect familiar attack sequences and point out potential intrusions or cyber risks. These models can adjust and learn with the passage of time, making them better at recognizing unique attack techniques and unknown vulnerabilities.

C. Network Monitoring. Machine learning can be employed to scrutinize network traffic trends and pinpoint abnormal data streams or dubious activities. Prospects of ML use in network monitoring include among the rest:

1. Predictive Maintenance

Machine learning can assess sensor data from machinery and equipment in industrial settings to forecast when maintenance or settings change is necessary, minimizing downtime and increasing operational effectiveness. Prospects include improving predictive maintenance models and expanding their use to different industries.

2. Network Traffic Optimization

Based on current demand and traffic trends, machine learning can improve resource allocation, load balancing, and network traffic routing. ML's capabilities in this area provide raising quality of service (QoS), decreasing latency, and strengthening network efficiency.

3. Security Threat Detection

In order to detect potential security threats and cyberattacks, ML models can evaluate network records, user behavior, and system activities. Prospects include creating sophisticated threat detection systems that are flexible enough to accommodate changing attack routes.

III. RESERVOIR COMPUTING IN TELECOMMUNICATIONS

Reservoir Computing is a machine-learning-based method created for sequential data processing, notably in the context of recurrent neural networks. It is renowned for its versatility in time-series data, speech recognition, and sophisticated signal processing applications. It is also regarded for its simplicity and efficiency. The idea of reservoirs or dynamic systems served as the inspiration for reservoir computing [5,7].

A. Components of Reservoir Computing system. A reservoir for mapping inputs into a high-dimensional space and a readout for pattern analysis from the high-dimensional states in the reservoir make up a reservoir computing system [5]. Let us check out each component in detail.

B. Reservoir. The centerpiece of a reservoir computing system is the reservoir. It is often implemented as a dynamical system with randomly initialized connections or a RNN [5,7]. There are two primary aspects of a reservoir:

1. Dynamics.

As a result of input data, the reservoir's internal state changes over time. It can recognize temporal dependencies because of its recurrent connections, which preserve a short-term memory of previous inputs.

2. Fixed Structure.

Unlike conventional RNNs, the internal connections of the reservoir are randomly initialized and maintained throughout training. This quality makes training easier and lowers the chance of overfitting.

C. Input Data. Sequential or time-series data that is supplied into the reservoir computing system for processing is referred to as input data [5]. Time-stamped measurements, sensor readings, speech signals, and other sequential information can all be included in this data.

D. Readout Layer. The readout layer is a neural network layer that receives the internal state of the reservoir and produces the wanted output. It is trainable and its capabilities and efficiency will depend on precision and quality of the trainings given to it. It maps the high-dimensional internal state of the reservoir to the output space, making it compatible with the task at hand. A readout layer can consist of various types of neural networks, namely feedforward neural networks (Fig. 3), recurrent neural networks, or simple linear regression models [4]. As opposed to the reservoir, the readout

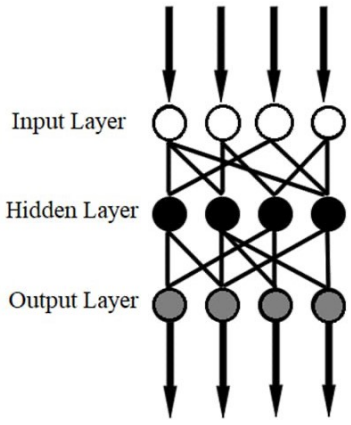

FIG. 3. A feedforward network scheme.

layer's parameters are trained during a supervised learning phase, where the system learns to produce the desired outputs for given inputs. The output of the Reservoir Computing system is typically a linear combination of the reservoir's internal state. In the simplest case, this can be described as:

$$d_{out}(t) = W_{out} r(t), \quad (2)$$

where $d_{out}(t)$ is an output data set, W_{out} is the weight matrix of the readout layer, and $r(t)$ represents the internal state of the given reservoir at time *t*.

E. Training Algorithm. Optimizing the readout layer's settings is the responsibility of the training algorithm. Techniques based on gradient descent, such as backpropagation through time (BPTT) or ridge regression, are frequently used in optimization. A training procedure uses a loss function suitable to the job at hand (e.g., mean squared error for regression or cross-entropy for classification) to reduce the discrepancy between the predicted outputs and the actual target outputs.

F. Output. Output information depends on the input data and its precision, a task that was defined, performance of a readout layer and its accuracy that depends on quality of the training provided and its suitability for the given task. Typical instances of output are predictions (like function prediction, chaotic system behavior prediction, etc.), classifications, or signal transformations (if our task is to encrypt or/and restore a signal).

G. Hyperparameters. The size of the reservoir, the weight matrix's spectral radius, the kind of activation functions being utilized, and the training parameters for the readout layer are all examples of the hyperparameters that define the design of the reservoir computing system. The system's performance can be greatly impacted by even the tiniest change in such hyperparameters.

H. Reservoir Computing Training. Principles. In reservoir computing, the reservoir's internal connections have fixed dynamics that were given a random initialization. Throughout training, they don't change. This set up makes training easier and helps avoid overfitting. Typical reservoir dynamics that represents the internal state of a RNN can be described as:

$$r(t+1) = f_a\left[w_{in} d_{in}(t) + W_{res} r(t) + b_{res}\right], \quad (3)$$

where:

$r(t)$ is the internal state of the reservoir,

$d_{in}(t)$ is the input,

W_{in} is the input-to-reservoir weight matrix,

W_{res} is the recurrent weight matrix of the given reservoir,

b_{res} is the bias vector of the reservoir,

f_a is the activation function.

Training in reservoir computing is largely an issue of supervised learning. The objective is to reduce the discrepancy between the intended outputs and forecast outputs for a given input sequence by optimizing the readout layer's settings.

I. Training Methods.

1. Linear Regression

The mapping from the internal state of the reservoir to the output is often learned using linear regression, which is a fairly trivial learning method. The mean squared error between the expected and the target outputs is minimized by this technique (Fig. 4).

2. Ridge Regression

Another regularized linear regression technique widely exploited in Reservoir Computing is Ridge Regression. It adds a regularization term to the mean squared error loss function to avert overfitting and refine generalization.

3. Echo State Networks

ESNs are a well-favored option of Reservoir Computing. They use linear regression but with specialized techniques such as the pseudoinverse method for optimizing the readout layer. ESNs frequently employ leaky integration to stabilize training.

4. Nonlinear Approaches

Sometimes, nonlinear models e.g. feedforward neural networks or support vector machines are used as the readout layer, which allows the system to capture complex relationships between the reservoir state and the target outputs.

J. Training Models.

1. Supervised Training

In supervised training, where both input sequences and their associated goal outputs are provided during training, the Reservoir Computing system learns from labeled data.

2. Online Training

The readout layer is incrementally updated during online training as fresh data is received. This method works well for applications where data is received sequentially and the model needs to be flexible.

3. Batch Training

During batch training, the readout layer's parameters are updated using the whole training dataset. When all data is accessible at once and the model can be trained in a single pass, it is frequently utilized.

4. Sequential Training

Throughout sequential training the readout layer is trained separately for each time step. It is especially useful for applications where the mapping from the reservoir state to the output changes over time.

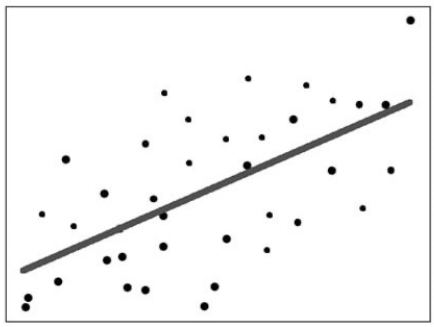

FIG. 4. An example of a linear regression within a two-dimensional plot (the line) attempting to minimize the residual sum of squares between the observed responses in the dataset as responses predicted by the linear approximation.

K. Applications of Reservoir Computing in Chaotic Systems: Prospects. Reservoir Computing is being successfully applied to a wide range of tasks, including:

1. Time-series prediction: Forecasting future values in time-series datasets.

2. Speech recognition: converting spoken language into text and viseversa, voice change, communication language change like in most recent AI developed by HeyGen Labs.

3. Robotics: sensor data handling, control over AI behavioral patterns, etc.

4. Signal processing: filtering, denoising, encrypting, and decrypting signals, extracting signals' features.

5. Natural language processing: visual- and sound-based.

However, in terms of the topic of this particular paper TSP and Signal processing ought to be specifically highlighted. It is imperative that tools and approaches in cybersecurity are in the eternal race on both sides: attackers and defenders [7]. A perspective idea that should be looked into in the future is to use a double-reservoir model that should be assisted by external devices.

IV. A DOUBLE-RESERVOIR SOLUTION: PROSPECTS AND CHALLENGES

The idea of a double reservoir system is simple. It combines two existing models and proposes use of two different reservoirs as two lines of defense [8-10]. While first reservoir uses a machine learning model to encrypt and decrypt the signal we want to transmit, the second one should adjust to signal transmission media and apply a pseudo-noise to an already encrypted signal, thus damaging the signal in a seemingly random way, while being specifically trained to restore such already encrypted signals after they are being damaged in a learned pseudo-random pattern. It is imperative that the signal should be pseudo-damaged not before, but after encryption as it adds an additional layer of protection.

A. The key challenges of the described approach.

1. Complexity

Implementing and training two separate reservoirs for signal protection and manipulation can significantly increase the complexity of the system. This complexity may impact the system's performance and efficiency.

2. Security

The security of the signal protection layer is of course a critical issue [8,9]. If an adversary gains access to the protected signal and understands the encryption/decryption process, they may themselves restore the damaged signal using their own model. This can be partially countered by damaging an already encrypted signal. Not only this will make it harder to recover such signal, but it will secure at least the second reservoir data in case if encryption process is compromised. If the signal is damaged before encryption and the encryption is hacked it will give away the fact that the pseudo-damaging is used.

3. Quality

An extra layer of signal manipulation can introduce noise or artifacts into the signal. It's important to ensure that the signal restoration process is effective in mitigating the effects of manipulation so that the signal remains usable after its full decryption and pseudo-restoration.

4. Resourcefulness

Training and optimizing two separate reservoirs can be challenging. The reservoirs may interact in complex ways, and coordinating their behavior may require extensive tuning and testing. Depending on the complexity and size of the reservoirs, as well as the training data, implementing a double-reservoir system may require significant computational resources.

B. Model description.

The aim of this entire model is of course to transmit a desired signal safely through our chose communication medium. In a perfect system we would alter our S(t) by applying encryption and pseudo-damaging it, run it through our communication medium, decrypt and restore it to receive S(t) on the end. However, in reality we shall provide a simplified description of our system described in equations 4, 5, and 6.

$$\begin{cases} E(t) = f_1\left[W_{res1}R_1(t) + W_{in1}S(t)\right] \\ D(t) = E(t) + N(t) = f_2\left[W_{res2}R_2(t) + W_{in2}E(t)\right] \end{cases}, \quad (4)$$

where:

E(t) and *D(t)* are encrypted *S(t)* and encrypted pseudo-damaged *S(t)* respectively;

$R_1(t)$ and $R_2(t)$ – internal states of reservoirs 1 (encryption layer) and 2 (pseudo-damaging layer) respectively;

f_1 and f_2 are activation functions for reservoirs 1 and 2 respectively;

N(t) – noise (or pseudo-noise) function.

Apart from the pseudo-noise applied by the second chaotic reservoir we have to acknowledge possible transmission media effects:

$$X(t) = D(t) + M(t), \quad (5)$$

where *X(t)* is the signal that the receiver shall read and *M(t)* is medium function that might have its own natural noise.

Then we should restore and decrypt the received signal to recover the transmitted information:

$$\begin{cases} D'(t) = X(t) - M'(t) \\ E'(t) = D'(t) - N(t) = f_2\left(\dfrac{D'(t) - W_{res2}R_2(t)}{W_{in2}}\right) \\ S'(t) = f_1\left(\dfrac{E'(t) - W_{res2}R_2(t)}{W_{in1}}\right) \end{cases}, \quad (6)$$

where:

$M'(t) \approx M(t)$ – estimated removed natural noise,

$D'(t) \approx D(t)$ – damaged encrypted signal on receiving end,

$E'(t) \approx E(t)$ – encrypted signal after restoration,

$S'(t) \approx S(t)$ – fully restored and decrypted signal.

Such parameters as reservoir size, reservoir dynamics, reservoir initialization, input encoding, volume and quality of the training data, validity and quality of the

training algorithm, and reservoir memory all affect the difference between $S(t)$ and $S'(t)$.

The general process of information transmission by a telecommunications system with the calculation of a double reservoir in the process of encryption and decryption is described by equations (4-6). The transfer process combined two existing models and uses two different reservoirs as two lines of defense. The first tank uses a machine learning model to encrypt and decrypt the signal we want to transmit. The second tank must adjust to the signal transmission environment and apply pseudo noise to the already encrypted signal, thus corrupting the signal. Using machine learning, seemingly random signal damage is predicted and the system learns to restore damaged signals. Being specially trained to restore such already encrypted signals, the system will increase the reliability of the transmission of encrypted signals.

V. CONCLUSION

We analyzed how redundant computing and machine learning contribute to the improvement of information security and the transformation of the telecommunications infrastructure. It is worth noting that reservoir computing and other machine learning-based tactics for data protection in chaotic telecommunications systems should become increasingly popular as computing power and software development continue to grow along with the introduction of new generations of AI. While the concept of a double-tank computing system for signal protection and manipulation is currently interesting, it poses challenges in terms of complexity, security, and signal quality. To mitigate these issues, the machine learning-based models in use today need to improve accuracy and quality. But this does not negate the prospects of using machine learning to solve the problem of information security and improve telecommunication systems.

ACKNOWLEDGMENT

We acknowledge the contributions of our colleagues and research peers who have engaged in thoughtful discussions, shared valuable perspectives, and provided constructive feedback. The diverse range of ideas has enriched the depth and breadth of our exploration. We also express our most sincere gratitude to all the colleagues, whose research papers are mentioned in References.

AUTHOR CONTRIBUTIONS

M.K. – supervision, conceptualization, methodology, formal analysis; V.T. – methodology, formal analysis, investigation, writing original draft, visualization; H.K. – writing-review, editing, visualization.

COMPETING INTERESTS

Neither of the authors have any competing interests.

REFERENCES

[1] J. Boiko, I. Pyatin, O. Eromenko and O. Barabash "Methodology for Assessing Synchronization Conditions in Telecommunication Devices". advances in Science Technology and Engineering Systems Journal, vol. 5, no. 2, pp. 320-327, March 2020.

[2] O. Semenova, A. Semenov, O. Voznyak, D. Mostoviy and I. Dudatyev, "The fuzzy-controller for WiMAX networks". in 2015 International Siberian Conference on Control and Communications (SIBCON), 2015, pp. 1-4, doi: 10.1109/SIBCON.2015.7147214.

[3] M. Sakurada, T. Yairi "Anomaly Detection Using Autoencoders with Nonlinear Dimensionality Reduction". Proceedings of the MLSDA 2014 2nd Workshop on Machine Learning for Sensory Data Analysis. Gold Coast, Australia QLD, Australia: ACM Press. pp. 4–11.

[4] C. Liou, J. Huang, W. Yang. "Modeling word perception using the Elman network". Neurocomputing, Volume 71, Issues 16–18, pp. 3150-3157, 2008.

[5] B. Schrauwen, D. Verstraeten, and J. V. Campenhout. "An overview of reservoir computing: theory, applications, and implementations". Proceedings of the European Symposium on Artificial Neural Networks, ESANN 2007, pp. 471–482.

[6] Kramer, Mark A. "Nonlinear principal component analysis using auto-associative neural networks". AIChE Journal. № 37, vol. 2, pp. 233–243, 1991.

[7] C. Gallicchio, A. Micheli, L. Pedrelli, Deep reservoir computing: A critical experimental analysis, Neurocomputing, Volume 268, pp. 87-99, 2017.

[8] F. Sabahi and A. Movaghar, "Intrusion Detection: A Survey", Third International Conference on Systems and Networks Communications, Sliema, Malta, 2008, pp. 23-26.

[9] S. Hawkins, H. He, G. Williams and R. Baxter "Outlier Detection Using Replicator Neural Networks". Data Warehousing and Knowledge Discovery. Lecture Notes in Computer Science. Vol. 2454. pp. 170–180, 2002.

[10] F. T. Liu, K. M. Ting, and Z. Zhou "Isolation Forest". Eighth IEEE International Conference on Data Mining. pp. 413–422, December 2008.

Mykola Kushnir

Associate Professor of the Department of Radio Engineering and Information Security. 19 Scopus documents, h-index -5.
Two Erasmus grants - Iasi - 2014-2015, Valencia - 2015. Two CRDF grants - 2022 and 2023. State Order "For Courage" (III degree).

ORCID ID: 0000-0001-9480-3856

Volodymyr Toronchuk

Born in 1997 in Chernivtsi, Ukraine. Entered Yurii Fedkovych Chernivtsi National University in September 2014 as a student of the Department of Radio Engineering and Information Security. Since September 2020 – a PhD student of this department.

ORCID ID: 0009-0009-0306-2083

Hryhorii Kosovan

Was born in Ukraine in 1985. Received the PhD degree in 2019. He is an assistant at the Department of Radio Engineering and Information Security of Yuri Fedkovich Chernivtsi National University. Research interests include chaos theory, secure telecommunications networks.

ORCID ID: 0000-0002-3351-3852

Перспективи методів, що базуються на машинному навчанні у хаотичних системах в галузі інформаційної безпеки та телекомунікацій

Микола Кушнір*, Володимир Торончук, Григорій Косован

[1]Кафедра радіотехніки та інформаційної безпеки, Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна

*Автор-кореспондент (Електронна адреса: myk.kushnir@chnu.edu.ua)

АНОТАЦІЯ: У динамічному ландшафті інформаційної безпеки та телекомунікацій ця стаття заглиблюється в багатогранну сферу методів, заснованих на машинному навчанні, з особливим акцентом на їх застосуванні в хаотичних системах. Інформаційний вступ відкриває шлях для ретельного вивчення основних переваг резервуарних обчислень (RC) і машинного навчання (ML) у телекомунікаціях. Перший сегмент цього дослідження детально розглядає роль машинного навчання у зміцненні інформаційної безпеки. Оскільки природа кіберзагроз постійно розвивається. Саме через це розуміння нюансів ML стає обов'язковим. У статті висвітлюються ключові досягнення та функції ML, які сприяють зміцненню безпеки даних, надаючи тонкий погляд на його ефективність у вирішенні складних проблем, пов'язаних із сучасними парадигмами інформаційної безпеки. Рухаючись вперед, обговорення розширюється до резервуарних обчислень та їх наслідків для телекомунікацій. Обчислення резервуару з його унікальним підходом до обробки інформації за допомогою динамічних систем стало багатообіцяючою технікою. Стаття розбирає його застосування в секторі телекомунікацій, проливаючи світло на те, як резервуарні обчислення підвищують ефективність обробки та передачі інформації в складних мережах. Ключовим аспектом цієї статті є дослідження рішення подвійного резервуара — передового підходу, який поєднує в собі сильні сторони обчислення пласта для підвищення продуктивності. Це інноваційне рішення детально розбирається, розкриваючи його перспективи та виклики, які воно створює. Включення рішень із подвійним резервуаром у хаотичні системи являє собою зміну парадигми в оптимізації системної динаміки та значний прогрес у вирішенні важливих телекомунікаційних труднощів. Проте ця стаття не просто пропонує розуміння цього рішення, вона чесно описує можливі проблеми з впровадженням такої моделі. Це слід взяти до уваги, тому не існує «ідеального» рішення для такої складної проблеми. Розкриваючи можливості як машинного навчання, так і резервних обчислень, він відкриває шляхи для подальших досліджень і розробок у використанні цих технологій для зміцнення основ безпечних і ефективних телекомунікацій перед обличчям загроз, що постійно розвиваються. Представлені тут ідеї закладають основу для майбутніх інновацій, спонукаючи дослідників і практиків глибше досліджувати синергію машинного навчання та хаотичних систем для трансформаційних досягнень у цих критичних областях.

КЛЮЧОВІ СЛОВА машинне навчання, резервуарні обчислення, хаотична система, телекомунікації.