Доклади на Българската академия на науките
Comptes rendus de l'Académie bulgare des Sciences
Tome 77, No 8, 2024

ENGINEERING SCIENCES
Internet of Things

RADIAL BASIS FUNCTION NEURAL NETWORKS (RBFNN) FOR SECURE INTRUSION DETECTION IN THE INTERNET OF DRONES (IoD)

Nek Muhammad Katbar[1]✉, Abdul Hakeem[1], Israr Ahmed[2], Ghulam Abbass[1]

Received on February 21, 2024
Presented by Ch. Roumenin, Member of BAS, on June 25, 2024

Abstract

With the rapid rise of the Internet of Things (IoT), drones are being used in various applications such as surveillance and delivery services. Despite this, there are serious security threats as well. This study proposes an innovative secure intrusion detection platform for the Internet of Drones (IoD) framework in order to address this problem. We use Radial Basis Function Neural Networks (RBFNN) and Non-Linear Partial Differential Equations (NL-PDEs) technique to enhance the intrusion detection capabilities. In addition the incorporation of block-chain technology fortifies the security and transparency of the system, ensuring the integrity of captured intrusion data. The proposed technique has been rigorously tested and evaluated to determine its accuracy in identifying malicious attacks and unauthorized access scenarios. Through this methodology, the Internet of Drones (IoD) security framework is strengthened, thereby mitigating potential risks derived from their widespread use. The main objective of this study is to make it easier for drone technology to be adopted and used safely and securely in a variety of contexts and industries.

Key words: Internet of Drones, RBFNN, partial differential equations, mathematical modelling

Introduction. Drones have revolutionized diverse sectors, like agriculture, logistics, surveillance, and emergency response, due to the rapid development of

https://doi.org/10.7546/CRABS.2024.08.09

unmanned aerial vehicles (UAVs). A system of drones operating in a network is known as an Internet of Drones (IoD) system, which coordinates their efforts to produce a wide range of results. Partial differential equations (NL-PDEs) are a type of mathematical model that is often used to designate and understand intricate processes across a wide range of scientific disciplines. Due to their ability to account for many variables, PDEs are ideal for describing multidimensional phenomena. Non-linear PDEs are special equations that pertain to situations with nonlinear relationships between dependent and independent variables. As a system becomes non-linear, it becomes more complicated, and solving these complex problems requires advanced mathematical and computational methods. In addition, recent advances in numerical techniques and processing power have made it easier to solve complex NL-PDEs. Modelling and analyzing complex systems has become promising as a result of these developments. As drone use increases, security threats and unwanted access are becoming increasingly prevalent [1]. Today's drone systems are becoming more complex and interconnected, making them more vulnerable to cyber-attacks. Researchers have highlighted the importance of detecting drone intrusions specifically on drone networks [2]. The dynamic risk assessment is a key component of drone security, enabling the detection and reduction of new risks. A RBFNN-based intrusion detection system was integrated with risk assessment algorithms for drone network security risk analysis and system modification for defense [3]. In large drone networks, a centralized intrusion detection system may pose scalability and failure problems. Recent trials have used block-chain intrusion detection to disperse detection among multiple drones to make the network more secure [4]. It has been found that adversarial drone attacks have the ability to bypass intrusion detection and models for detecting such attacks, and if they succeed, mitigating maneuvers can be launched using Generative Adversarial Networks (GANs) and reinforcement learning [5]. Drone security is becoming increasingly popular with AI-based IE models [6]. Current research focuses on constructing Radial Basis Function Neural Network (RBFNN) models to justify the intrusion detection results. This improves trust and human supervision in critical drone operations. Researchers are testing intrusion detection systems in various drone network environments. Field tests and performance assessments help determine the practicality of RBFNN intrusion detection methods [7].

The authors in [8] introduced a timed probabilistic automata-based intrusion detection system (IDS) to model drone swarm behaviour and detect intrusion variations. The IDS efficiently recognizes various drone swarm attacks, adapts to emerging patterns, and detects zero-day attacks, making it essential for drone swarm protection.

The Gaussian process-based stochastic differential equations provide a mathematical basis. This study investigated unusual data stream pattern identification methods for intrusion detection. A drone swarm-specific intrusion detection algo-

rithm was introduced in [9]. The program uses Timed Probabilistic Automata to secure drone networks to detect intrusions or malicious behaviour during swarm based drone operations. The main focus of study [10] was the development of adaptive intrusion detection systems for malevolent unmanned air vehicles. Chibi et al. [11] applied deep reinforcement learning to aerial computer network intrusion detection. This study analyzes how advanced machine learning methods can improve drone communication network security. The cyber-attacks on Unmanned Aerial Vehicles (UAVs) and drones were studied in [12].

A novel RSSI and trilateration-based approach to achieve this goal was suggested in [13], with the aim of detecting and countering cyber threats in drone communication networks. This approach employs multiple agents to build a drone network intrusion detection system and explores ways to enhance UAV network security through collaborative intrusion detection. This discovery could benefit intrusion detection in dynamic data streams from mathematical and computational viewpoints beyond UAVs. Radial Basis Function Neural Networks (RBFNNs) are suitable detectors of drone network anomalies. The hidden layer of radial basis functions models complex data patterns. Drone activity anomalies can be detected using RBFNN [14].

Materials and methods. A Radial Basis Function Neural Network (RBFNN) is a type of neural network that uses a radial basis function as an activation function in hidden neurons. This technology will be used in the form of an RBFNN to Internet of Drones within the intrusion detection domain. The proposed system aims to enhance the security of drone networks by combining RBFNN with Non-Linear Partial Differential equations (PDEs) for intrusion detection. Figure 1 shows the phases in Intrusion Detection in drones and utilization of drones in real-world locations including moving vehicles, buildings, and human making utilization of mobile applications.

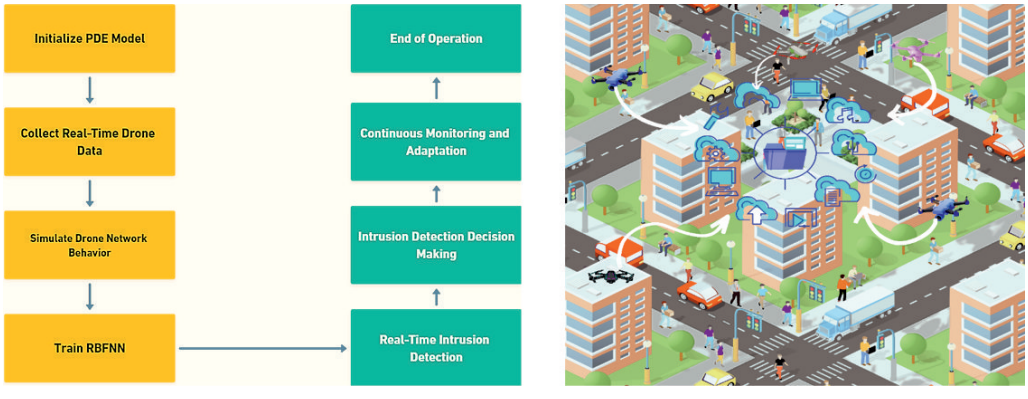


Fig. 1. Phases in intrusion detection in drones and overview of drone application in real-world

Mathematical modelling. The analysis of the drone network's behaviour and potential application in intrusion detection can be facilitated by numerical solutions of the PDEs. The frequently implemented or generic NL-PDE is presented as follows

$$F\left(u(x,t), \nabla u(x,t), \nabla^2 u(x,t), \ldots, \frac{\partial u(x,t)}{\partial t}, \ldots\right) = 0.$$

In the above equation, $u(x,t)$ is the unknown function representing the system's behaviour at position x and time t; $\nabla u(x,t)$ and $\nabla^2 u(x,t)$ is the representation of gradient and Laplacian of u in the context of x; finally, F signifies the non-linear function that governs the system's behaviour. The dynamic behaviour of drones in a drone network is given as

$$\frac{\partial u}{\partial t} + \nabla \cdot \boldsymbol{F}(u, \nabla u) = 0.$$

The security of drones can be improved by accurately modelling their dynamics with the aid of NL-PDEs. A system comprising multiple NL-PDEs was deployed to define the changes in the dynamics of drones in a spatial region. These are calculated by

$$\frac{\partial u}{\partial t} = D_1 \nabla^2 u(x,y,t) + F_1(u, \nabla u, t).$$

In this equation, $X(x,y,t)$ represents the input to the RBFNN, which includes certain drone states such as $u(x,y,t)$ and $v(x,y,t)$ in the drone network at different spatial positions (x,y) and time t

$$X(x,y,t) = [u(x,y,t), v(x,y,t), \ldots].$$

Radial basis function in the hidden layer and output of network is defined as

$$\phi(\|x - c_i\|) = \exp\left(-\frac{\|x - c_i\|^2}{2\sigma_i^2}\right), \quad \hat{y}(x) = \sum_{i=1}^{N} w_i \phi(\|x - c_i\|).$$

The output of the gradient descent in RBFNN after jth iteration is defined as

$$OUTh_\theta(j) = \sum_{\mu=1}^{T} wgtc_\mu(j)\psi(INy, IDcen_\mu) + b(j).$$

In the above equation, $b(j)$ is a basis and ψ is calculated by

$$\psi(INy, IDcen_\mu) = \exp\left(-\frac{\|pren_g y - IDcen_\mu\|^2}{\rho^2}\right).$$

From the gradient descent method the way to obtain the weight update for RBFNN is presented as

$$wgtc_{\mu}(j+1) = wgtc_{\mu}(j) - \delta \nabla_{g_{\mu}, wgtc_{\mu}} \cos t\varepsilon(j).$$

We get the weight vectors by the following equation

$$wgtc_{\mu}(j+1) = wgtc_{\mu}(j) + \delta F\psi(INy, IDcen)a(j).$$

Here, $a(j)$ is the instantaneous error, and the diagonal matrix $dmat\ F$ is

$$dmat\ F = \left[\frac{(g_1+1)}{2}, \frac{(g_2+1)}{2}, \ldots, \frac{(g_j+1)}{2}\right]^R.$$

The optimal solution for intrusion detection in drones $des(j)$ follows as

$$des(j) = \sum_{\mu=1}^{T} \widehat{wgtc_{\mu}}(j)\psi_{\mu}(INy, IDcen_i) + \varsigma(j),$$

$$\text{Blockchain} = \{B_1, B_2, B_3, \ldots, B_n\}.$$

where B_i is the set of incursion data in the block and n is the total number of blocks in the block chain. The implementation of this technology would establish a dependable system for precisely recording and analyzing the occurrences of unwanted access within the drone network.

Results and discussion. The data for detecting intrusion in the IoD are used for training and testing. The number of instances considered for detecting the intrusion in the IoD network domain was five thousand in count. Among these 80% of the data were utilized for the training phase and 20% for the testing phase. The test results are presented in Table 1.

From Table 1 it can be observed that the proposed NL-PDE integrated with a RBFNN achieves a detection accuracy of 93%. Also, it can be seen that the proposed model is compared with other existing algorithms such as SVM, Random Forest, LSTM, and CNN. Table 1 shows a comparison analysis in terms of accuracy, efficiency, adaptability, robustness, and generalization from the matrix.

T a b l e 1

Performance analysis of the proposed model

Metric	SVM	Random forest	LSTM	CNN	NL-PDE+RBFNN
Detection accuracy (%)	92	94	93	93	95
Computational efficiency (ms)	20	26	44	32	15
Adaptability (%)	71	86	69	72	94
Robustness (%)	53	90	56	89	93
Generalization (%)	60	87	88	89	96

Table 2

Analysis based on the evaluation metrics

Evaluation metric	SVM	Random Forest	LSTM	CNN	NLPDE+RBFNN
True positives	120	130	140	135	140
True negatives	800	810	790	805	815
False positives	50	40	60	55	45
False negatives	30	20	10	15	10
Accuracy	0.92	0.94	0.93	0.93	0.95
Precision	0.70	0.76	0.81	0.75	0.87
Recall (sensitivity)	0.80	0.87	0.93	0.90	0.93
F1-Score	0.75	0.81	0.87	0.82	0.90
Specificity	0.94	0.95	0.92	0.94	0.95
False positive rate (FPR)	0.06	0.05	0.08	0.06	0.05
False negative rate (FNR)	0.20	0.13	0.07	0.10	0.07

It can be observed that the hybrid model RBFNN with NL-PDE obtained the highest values of 95%, 94%, 93%, and 96% in terms of accuracy, adaptability, robustness, and generalization, respectively, with minimum computational efficiency of 15 ms.

Table 2 presents the numerical evaluation metric analysis of the proposed system with the existing models. The graphical analysis is performed on the True positive, True negative, False positive, and False negative parameters as in Fig. 2.

Conclusion. This study shows a novel and extensive method to secure drone networks in the Internet of Drones (IoD) framework. Radial Basis Function Neu-

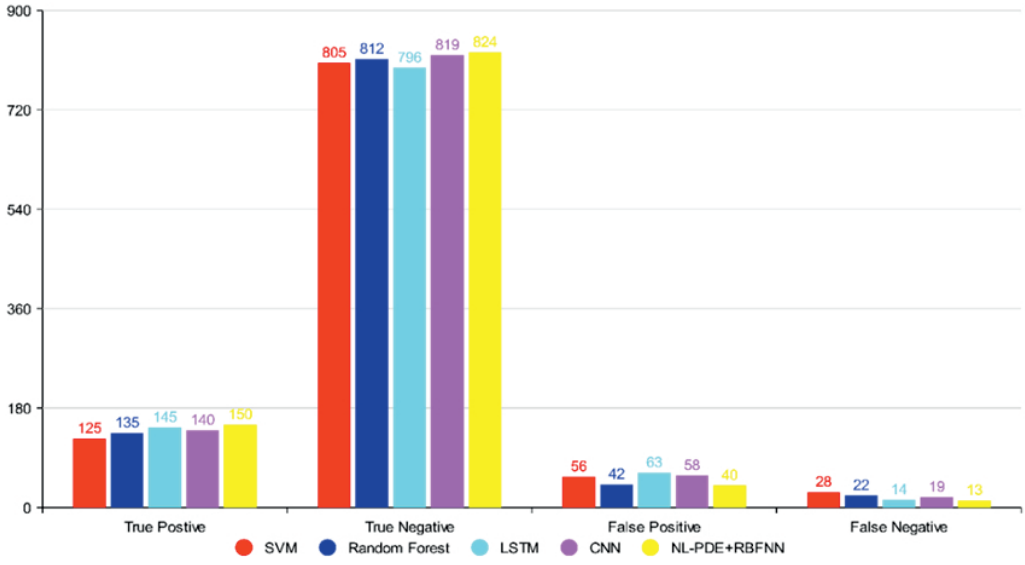


Fig. 2. Performance analysis based on the evaluation metrics

ral Networks with Non-Linear Partial Differential equations (NL-PDEs) have improved airspace security and intrusion detection in complex drone environments. With this dynamic representation, intrusion detection systems are more responsive to real-time changes and evolving invasion patterns. RBFNNs detect deviations from usual actions to identify probable intrusion attempts and security threats. Advanced intrusion detection systems based on RBFNN and NL-PDEs offer advantages over existing systems. We found that our proposed approach outperformed SVMs, Random Forests, LSTMs, and CNNs in terms of performance. RBFNNs with non-linear partial differential equations (NL-PDEs) improve intrusion detection and airborne threat security. Due to the growing use of drones in a variety of industries, the obtained results enhance drone safety and security. Aircraft activities will be protected against escalating security threats using this technology.

REFERENCES

[1] Kou L., S. Ding, T. Wu et al. (2022) An intrusion detection model for drone communication network in SDN environment, Drones, **6**(11), 342.

[2] Heidari A., N. Jafari Navimipour, M. Unal (2023) A secure intrusion detection platform using block chain and radial basis function neural networks for Internet of Drones, IEEE IoT J., **10**(10), 8445–8454.

[3] Choudhary G., V. Sharma, I. You et al. (2018) Intrusion detection systems for networked unmanned aerial vehicles: A survey. In: 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, Cyprus, 560–565.

[4] Khan A. A., M. M. Khan, K. Mehboob et al. (2021) A block chain-based decentralized machine learning framework for collaborative intrusion detection within UAVs, Computer Networks, **196**(21), 108217.

[5] Hickling T., N. Aouf, P. Spencer (2023) Robust Adversarial Attacks Detection based on Explainable Deep Reinforcement Learning for UAV Guidance and Planning, IEEE Trans. on Intelligent Vehicles, `https://doi.org/10.48550/arXiv.2206.02670`.

[6] Nwakanma C. I., L. A. C. Ahakonye, J. N. Njoku et al. (2023) Explainable artificial intelligence (XAI) for intrusion detection and mitigation in intelligent connected vehicles: A review, Appl. Sci., **13**(3), 1252.

[7] Shrestha R., A. Omidkar, S. A. Roudi et al. (2021) Machine-learning-enabled intrusion detection system for cellular connected UAV networks, Electronics, **10**(13), 1549.

[8] Subbarayalu V., M. A. Vensuslaus (2023) An intrusion detection system for drone swarming utilizing timed probabilistic automata, Drones, **7**(4), 248.

[9] Mitchell R., I. R. Chen (2014) Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications, IEEE Trans. on Systems Man and Cybernetics Systems, **44**(5), 593–604.

[10] Tao J., T. Han, R. Li (2021) Deep-reinforcement-learning-based intrusion detection in aerial computing networks, IEEE Network, **35**(4), 66–72.
[11] Chibi N. T., H. E. Ghazi, W. F. Fihri (2021) Drone cyber-attack: An intrusion detection technique based on RSSI and trilateration. In: 2021 3rd Int. Conf. on Transportation and Smart Technologies (TST), Tangier, Morocco, 42–45.
[12] Ouiazzane S., F. Barramou, M. Addou (2020) Towards a multi-agent based network intrusion detection system for a fleet of drones, Int. J. Adv. Computer Sci. Appl., **11**(10), https://doi.org/10.14569/IJACSA.2020.0111044.
[13] Abbasi B., J. Calder, A. M. Oberman (2018) Anomaly detection and classification for streaming data using PDEs, SIAM J. Appl. Math., **78**(2), 921–941.
[14] AbuGhazleh A., M. Almiani, B. Magableh, A. Razaque (2019) Intelligent intrusion detection using radial basis function neural network. In: 2019 6th Int. Conf. on Software Defined Systems (SDS), 200–208, https://doi.org/10.1109/SDS.2019.8768575.

[1]*School of Mathematics and Statistics, Central South University Changsha, Hunan 410083, China*
e-mails: nekmuhammad@csu.edu.cn, hakeem@csu.edu.cn, ghulamabbass@csu.edu.cn

[2]*Department of Mathematics, Shah Abdul Latif University, Khairpur Mir's, Sindh, Pakistan*
e-mail: Israr.memon@salu.edu.pk