Artificial Immune System-Based Intrusion Detection in A Distributed Hierarchical Network Architecture of Smart Grid

DR. K. V. RUKMANI[1], LT. DR. D. ANTONY ARUL RAJ[2], MOHAMMED HISAAN N[3], ISAIYAZHINI[4], HARISH[5], SANJAY[6]

[1] Associate Professor & Head, Department of Software Systems, PSG College of Arts & Science, Coimbatore, India

[2] Associate Professor Cum ANO, Department of Software Systems, PSG College of Arts & Science, Coimbatore, India

[3, 4, 5, 6] Student, Department of Software Systems, PSG College of Arts & Science, Coimbatore, India

Abstract -The article titled "Artificial immune system based intrusion detection in a distributed hierarchical network architecture of smart grid" addresses the emerging challenges posed by cyber security threats to smart grids. With the integration of Internet-like communication networks into the traditional power grid infrastructure, smart grids become susceptible to various cyber attacks. To mitigate these risks, the authors propose a Distributed Intrusion Detection System for Smart Grids (SGDIDS) by deploying an intelligent module known as the Analyzing Module (AM) across different layers of the smart grid architecture. These layers include the home area network (HAN), neighbourhood area network (NAN), and the Wide Area Network (WAN). The AMs at each level utilize Artificial Immune System (AIS) techniques to detect and classify malicious data and potential cyber attacks. By training AMs with relevant data specific to their respective layers and enabling inter-level communication, the system enhances its capability to identify and respond to cyber threats effectively. Simulation results demonstrate the efficacy of this approach in identifying malicious network traffic, thereby bolstering the security of smart grid systems. The proposed SGDIDS presents a promising methodology for enhancing system security in smart grids, thus contributing to the realization of intelligent, efficient, and optimal power grid management. This work underscores the importance of proactive measures to safeguard critical infrastructure like smart grids against cyber threats, ensuring the reliability and resilience of the modern power grid ecosystem.

Indexed Terms-Bio inspired computing, Artificial Immune System (AIS), Wide Area Network (WAN), Analyzing Module (AM), Distributed Intrusion Detection System (DIDS), Malicious data detection.

I. MOTIVATION

The motivation behind the article is stems from the increasing integration of communication technologies into conventional power grids, transforming them into smart grids. While this transition promises significant advancements in efficiency, intelligence, and optimization, it also introduces new vulnerabilities, particularly in terms of cyber security.With the overlay of Internet-like communication networks, including wireless technologies like 802.15.4, 802.11, and Zigbee protocols, the smart grid becomes exposed to various cyber threats. These threats pose risks ranging from data breaches to potential disruptions in power distribution, emphasizing the critical need for robust intrusion detection systems tailored specifically for smart grid environments.The Distributed Intrusion Detection System for Smart Grids (SGDIDS) proposed in the article addresses this pressing need by introducing an intelligent module called the Analyzing Module (AM). By enclosing AMs tranversely different layers of the smart grid architecture - the home area network (HAN), neighbourhood area network (NAN), and the Wide Area Network (WAN) - the SGDIDS leverages Artificial Immune System (AIS) techniques to detect and classify malicious data and potential cyber attacks.The motivation for this research lies in the imperative to enhance the security posture of smart grid infrastructures, safeguarding them against evolving cyber threats. By developing and deploying effective intrusion detection mechanisms like the SGDIDS, stakeholders can mitigate risks, ensure the reliability of power distribution, and maintain the integrity of critical infrastructure.Furthermore, the simulation results presented in the article validate the effectiveness of the proposed methodology, highlighting its potential to identify malicious network traffic and bolster system security. This motivation underscores the significance of proactive measures in securing smart grid systems, ultimately contributing to the realization of intelligent, efficient, and resilient power grid management.

II. PROBLEM STATEMENT

The problem statement addressed in this article revolves around the vulnerability of smart grid infrastructures to cyber security threats resulting from the integration of Internet-like communication networks.The existing power grid infrastructure lacks adequate intrusion detection systems tailored specifically for the unique challenges posed by smart grids. Traditional intrusion detection methods may not be sufficient to address the evolving nature of cyber threats targeting smart grid environments. As a result, there is a critical need to develop a robust Distributed Intrusion Detection System for Smart Grids (SGDIDS) capable of detecting and mitigating malicious activities across multiple layers of the smart grid architecture. The proposed SGDIDS aims to address this problem by deploying intelligent Analyzing Modules (AMs) at different levels of the smart grid, including the home area network (HAN), neighborhood area network (NAN), and the Wide Area Network (WAN). These AMs utilize Artificial Immune System (AIS) techniques to detect and classify malicious data and potential cyber attacks, thereby enhancing the overall security posture of the smart grid infrastructure. However, the effectiveness of the SGDIDS relies on its ability to accurately identify and respond to various cyber threats while minimizing false positives and negatives. Additionally, the scalability and efficiency of the system must be considered to ensure practical implementation across large-scale smart grid deployments. Therefore, the problem statement encompasses the need for a comprehensive intrusion detection solution tailored specifically for smart grids, capable of addressing the unique challenges posed by the integration of communication technologies into the power grid infrastructure.

III. OBJECTIVES

The objective of this research is to propose and evaluate a Distributed Intrusion Detection System for Smart Grids (SGDIDS) using Artificial Immune System (AIS) techniques. The study aims to address the growing cyber security threats facing smart grid infrastructures due to the integration of Internet-like communication networks. By deploying intelligent Analyzing Modules (AMs) at various levels of the smart grid architecture, including the home area network (HAN), neighbourhood area network (NAN), and Wide Area Network (WAN), the SGDIDS seeks to detect and classify malicious data and potential cyber attacks. Each AM will be trained using relevant data specific to its level and will communicate with other modules to enhance detection capabilities. The research intends to demonstrate the efficacy of the proposed SGDIDS methodology through simulation results, highlighting its potential to identify malicious network traffic and enhance system security in smart grid environments.

IV. BACKGROUND AND CONTEXT

Artificial Immune Systems (AIS) have garnered attention in the field of cybersecurity for their ability to mimic the human immune system's adaptive and self-learning capabilities in detecting and responding to threats. Various studies have applied AIS to different domains within network security, such as intrusion detection, anomaly detection, and defense against cyber-physical attacks. These systems leverage the principles of immunology to develop robust and adaptive defense mechanisms, enhancing the security posture of systems and networks. With the increasing sophistication of cyber threats, AIS offers promising solutions for detecting impersonation, network intrusions, exfiltration attacks, and false data injections. By incorporating machine learning techniques and agent-based approaches, AIS-based security solutions strive to provide proactive and intelligent defense mechanisms, crucial for safeguarding critical infrastructure, smart home networks, wireless networks, and cyber-physical systems.

V. FOCUS AND SCOPE

The focus of this article is to explore the application of Artificial Immune Systems (AIS) in various domains of network security. Specifically, it investigates different approaches and techniques employing AIS for detecting and mitigating security threats such as impersonation in social network sites, intrusion detection in smart home networks, network exfiltration rootkit detection, wireless network intrusion detection, and defense against false data injection attacks in aviation cyber-physical systems. The scope encompasses research findings, methodologies, and practical implementations of AIS-based security solutions presented in conferences and workshops worldwide. By examining diverse applications of AIS, the article aims to provide insights into its effectiveness in enhancing network security posture, improving situational awareness, and mitigating cyber threats across different contexts and environments.

VI. METHODOLOGY

The methodologies employed in these articles typically involve the design and implementation of Artificial Immune Systems (AIS) for specific security tasks within various network environments. This includes:

1.Data Collection and Preprocessing: Gathering relevant data from social network sites, smart home networks, wireless networks, or cyber-physical systems to be used for training and testing the AIS.

2.Feature Extraction: Identifying key features or patterns from the collected data that are indicative of security threats such as impersonation, intrusion, exfiltration, or false data injection

3.AIS Design: Developing AIS algorithms or models tailored to the specific security task, which may involve designing detection rules, classifiers, or anomaly detection mechanisms based on the principles of immunology.

4.Training and Evaluation: Training the AIS using labeled data to learn normal behavior and detect deviations indicative of security threats. Evaluation involves testing the effectiveness of the AIS in detecting and mitigating security threats through metrics such as detection accuracy, false positive rate, and response time.

5.Integration and Deployment: Integrating the AIS into the target network environment and deploying it for real-time monitoring and defense against security threats.

Overall, the methodologies focus on leveraging AIS principles to enhance security measures and address specific challenges within diverse network contexts.

VII. LITERATURE REVIEW

1. Zhang et al. proposed a Distributed Intrusion Detection System for Smart Grids (SGDIDS) utilizing an Artificial Immune System (AIS) approach. They address the cybersecurity threats posed by the integration of wireless communication technologies into the power grid. By embedding Analyzing Modules (AMs) at multiple levels of the smart grid, they aim to detect and classify malicious data and cyber attacks. The simulation results indicate the effectiveness of this approach in identifying malicious network traffic and enhancing system security [1].

2. Yue et al. introduced a fault detection method based on Real-Value Negative Selection Algorithm (RNSA) of Artificial Immune System (AIS). Their approach utilizes self-data as the normal pattern of behavior of the monitored system and generates detector sets to detect faults. Through testing, they demonstrate the effectiveness of their method in fault diagnosis, especially with an increased number of training samples, highlighting its advantages in robustness and accuracy [2].

3. Şahin proposed DCW-RNN, a methodology integrating Clock-Work Recurrent Neural Network (RNN) with the Dendritic Cell Algorithm (DCA) for software vulnerability detection. This innovative approach aims to identify complex dependencies between object-oriented software metrics, enhancing immunity in vulnerability prediction models. Experimental findings on

different Java projects showcase the computational efficiency and effectiveness of the proposed approach [3].

4. Barani presented a hybrid approach, GAAIS, for dynamic intrusion detection in AODV-based MANETs, integrating Genetic Algorithm (GA) and Artificial Immune System (AIS). By adapting to network topology changes and utilizing spherical detectors generated by NicheMGA algorithm, GAAIS demonstrates efficiency in detecting various routing attacks, as evidenced by experimental results [4].

5. Xie and Hui proposed an Intrusion Detection Architecture for Ad Hoc Networks based on Artificial Immune System (AIS). Inspired by the vertebrate immune system, their theoretical architecture aims to protect and react against known and unknown attacks in mobile ad hoc networks. While the paper outlines the theoretical framework, it lacks empirical validation or experimental results [5].

6. Barani and Abadi introduced a hybrid approach, BeeNS, for dynamic anomaly detection in AODV-based MANETs, combining Artificial Bee Colony (ABC) and Negative Selection (NS) algorithms. By generating mature negative detectors and updating them dynamically, BeeNS achieves comparable or superior performance in terms of detection and false alarm rates, as demonstrated through simulations of routing attacks [6].

7. Hosseinpour et al. conducted a survey on Artificial Immune System (AIS) as a bio-inspired technique for Anomaly Based Intrusion Detection Systems (IDS). With the increasing connectivity of computer networks to the internet, the need for effective IDS has become crucial. AIS, being a novel bio-inspired model, has garnered attention for its application in various fields, including information security. The paper provides an overview of current AIS-based IDS, highlighting their unique features and applications [7].

8. Sandeep Kumar et al. proposed a scheme utilizing a random key distribution based Artificial Immune System (AIS) for detecting spoofing attacks in clustered wireless sensor networks. By integrating AIS into the LEACH protocol, their approach proves to be energy-efficient while providing robust security against various attacks [8].

9. Lasisi et al. focused on knowledge extraction from agricultural data using AIS algorithms, particularly the clonal selection algorithm (CLONALG) and artificial immune recognition system (AIRS). Their approach, coupled with a fuzzy-rough feature selection method, demonstrates improved detection and computational efficiency in agricultural data mining, which can enhance productivity in agriculture [9].

10. Jim and Chacko proposed a decision tree-based AIS strategy for intrusion detection in Mobile Ad hoc Networks (MANETs). Given the challenges in securing MANETs due to their dynamic nature and resource constraints, their approach aims to improve the efficiency of packet delivery by detecting cheat nodes using AIS, thereby enhancing network integrity [10].

11. Zareen and Karam explored the detection of RTL Trojans using Artificial Immune Systems (AIS) and high-level behavior classification. Leveraging AIS-based machine learning techniques, their approach aims to identify potentially unsafe or malicious behavior in hardware descriptions, providing an effective means for hardware security assurance [11].

12. Rouhani Zeidanloo et al. proposed a Botnet detection framework utilizing Artificial Immune System (AIS). Their approach defines Botnets as groups of bots exhibiting similar communication and malicious activity patterns, and employs AIS to effectively detect such malicious activities, such as spam and port scanning, in bot-infected hosts [12].

13. Hosseinpour et al. designed a distributed model for Intrusion Detection System (IDS) based on Artificial Immune System (AIS). Their distributed multi-layered framework aims to enhance IDS detection performance and efficiency by distributing detectors to each host, thereby reducing detection time for each connection [13].

14. Aljohani et al. proposed a Continuous Authentication (CA) system on PCs using Artificial Immune System (AIS). Their approach continuously checks the identity of the current user based on every user action performed, achieving high accuracy in user authentication without the need for traditional password-based authentication [14].

15. Chao and Tan proposed a Virus Detection System (VDS) based on Artificial Immune System (AIS). Their approach utilizes negative selection and clonal selection algorithms to generate a detector set and calculates affinity vectors for virus files, achieving strong detection ability and good generalization performance [15].

16. Kebande and Venter presented a cognitive approach for botnet detection using Artificial Immune System (AIS) in the cloud environment. With the proliferation of botnets in cloud computing, their approach offers an effective mechanism for detecting botnet infections, contributing to enhancing security in cloud environments [16].

17. M. Bere and H. Muyingi, "Initial investigation of Industrial Control System (ICS) security using Artificial Immune System(AIS),"2015InternationalConference on Emerging Trends in Networks and ComputerCommunications(ETNCC),Windhoek,Namibia,2015,pp.7984,doi:10.1109/ETNCC.2015.7184812. [Ref. 17] .

18. E. Abd El Raoof Abas, H. Abdelkader and A. Keshk, "Artificial immune system based intrusion detection," 2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS), Cairo, Egypt, 2015, pp. 542-546, doi: 10.1109/IntelCIS.2015.7397274. [Ref. 18]

19. E. B. Nuakoh and M. Anwar, "Detecting Impersonation in Social Network Sites (SNS) Using Artificial Immune Systems (AIS)," SoutheastCon 2018, St. Petersburg, FL, USA, 2018, pp. 1-3, doi: 10.1109/SECON.2018.8479274. [Ref. 19]

20. Yu Qiao and Jiayi Xu, "A network security situation awareness model based on cooperative artificial immune system," 2011 International Conference on Computer Science and Service System (CSSS), Nanjing, 2011, pp. 1945-1947, doi: 10.1109/CSSS.2011.5972215. [Ref. 20]

21. E. D. Alalade, "Intrusion Detection System in Smart Home Network Using Artificial Immune System and Extreme Learning Machine Hybrid Approach," 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2020, pp.12,doi:10.1109/WFIoT48130.2020.9221151. [Ref. 21]

22. M. B. S. Terra and J. J. C. Gondim, "NERD: a Network Exfiltration Rootkit Detector based on a Multi-agent Artificial Immune System," 2021 Workshop on Communication Networks and Power Systems (WCNPS), Brasilia, Brazil, 2021, pp. 1-7, doi: 10.1109/WCNPS53648.2021.9626241. [Ref. 22]

23. G. V. P. Kumar and D. K. Reddy, "An Agent Based Intrusion Detection System for Wireless Network with Artificial Immune System (AIS) and Negative Clone Selection," 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies, Nagpur, India, 2014, pp. 429-433, doi: 10.1109/ICESC.2014.73. [Ref. 23]

These studies collectively demonstrate the versatility and effectiveness of Artificial Immune System (AIS) in various domains, including intrusion detection, security in wireless sensor networks, agricultural data mining, hardware security, continuous authentication, virus detection, and botnet detection in cloud computing environments

ACKNOWLEDGMENT

We would like to express our sincere gratitude to the authors of the referenced articles for their valuable contributions to the field of cybersecurity. Their research has significantly enriched our understanding

of the application of Artificial Immune Systems (AIS) in various domains such as intrusion detection, network security, social network analysis, and smart home networks.

We extend our sincere gratitude to Lt. Dr. D. Antony Arul Raj and Dr. K. V. Rukmani for their invaluable guidance and support in the preparation of this review paper. Their expertise, encouragement, and insightful feedback have been instrumental in shaping our understanding of the subject matter and refining our analysis. We are deeply appreciative of their mentorship and dedication, which have significantly enhanced the quality and comprehensiveness of this collaborative effort.

We also extend our appreciation to the organizers of the conferences where these papers were presented, as well as to the reviewers and editors involved in the publication process. Their efforts have ensured the dissemination of important findings and advancements in the realm of computer science and cybersecurity.

Furthermore, we acknowledge the funding agencies and institutions that supported this research, enabling the exploration of innovative approaches to addressing cybersecurity challenges.

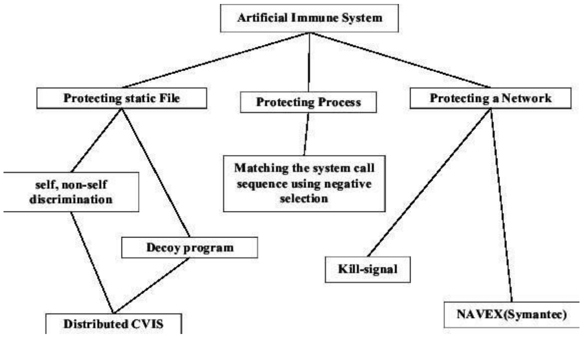
CONCLUSION

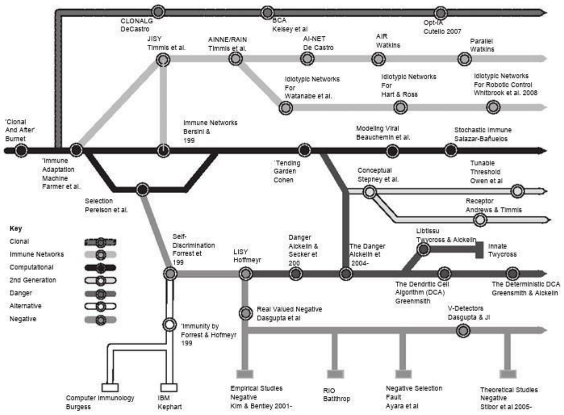
In conclusion, the surveyed literature demonstrates the widespread application and effectiveness of Artificial Immune System (AIS) in various domains, particularly in the realm of cybersecurity. AIS, inspired by biological immune systems, offers innovative solutions for anomaly-based intrusion detection systems, network security, agricultural data mining, hardware Trojan detection, continuous user authentication, virus detection, and botnet detection in cloud environments.

The surveyed studies highlight AIS's adaptability, robustness, and efficiency in addressing cybersecurity challenges, including detecting spoofing attacks, identifying malicious behavior, enhancing network security, and defending against evolving threats like botnets and viruses. Additionally, AIS-based approaches showcase promising results in terms of detection accuracy, false alarm reduction, computational efficiency, and scalability.

Overall, AIS emerges as a valuable bio-inspired technique for enhancing cybersecurity measures, offering proactive defense mechanisms, continuous monitoring, and adaptive responses to mitigate risks and protect critical systems and data assets in an increasingly interconnected and vulnerable digital landscape. Continued research and development in AIS promise further advancements in cybersecurity solutions, contributing to a safer and more resilient cyber ecosystem.

ARCHITECTURE





REFERENCES

[1] Y. Zhang, L. Wang, W. Sun, R. C. Green, and M. Alam, "Artificial immune system based intrusion detection in a distributed hierarchical network

architecture of smart grid," IEEE Power and Energy Society General Meeting, 2011. [Ref. 1]

[2] X. Yue, D. Wen, H. Ma, and J. Zhang, "Fault Detection Based on Real-Value Negative Selection Algorithm of Artificial Immune System," International Conference on Intelligent Computing and Cognitive Informatics, 2010. [Ref. 2]

[3] C. B. Şahin, "DCW-RNN: Improving Class Level Metrics for Software Vulnerability Detection Using Artificial Immune System with Clock-Work Recurrent Neural Network," International Conference on INnovations in Intelligent SysTems and Applications, 2021. [Ref. 3]

[4] F. Barani, "A hybrid approach for dynamic intrusion detection in ad hoc networks using genetic algorithm and artificial immune system," Iranian Conference on Intelligent Systems, 2014. [Ref. 4]

[5] H. Xie and Z. Hui, "Notice of Violation of IEEE Publication Principles: An Intrusion Detection Architecture for Ad Hoc Network Based on Artificial Immune System," International Conference on Parallel and Distributed Computing, Applications and Technologies, 2006. [Ref. 5]

[6] F. Barani and M. Abadi, "An ABC-AIS Hybrid Approach to Dynamic Anomaly Detection in AODV-Based MANETs," IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, 2011. [Ref. 6]

[7] F. Hosseinpour, K. A. Bakar, A. H. Hardoroudi, and N. Kazazi, "Survey on Artificial Immune System as a Bio-inspired Technique for Anomaly Based Intrusion Detection Systems," in 2010 International Conference on Intelligent Networking and Collaborative Systems, Thessaloniki, Greece, 2010, pp. 323-324. DOI: 10.1109/INCOS.2010.40. [Ref. 7]

[8] E. Sandeep Kumar, S. M. Kusuma, and B. P. Vijaya Kumar, "A random key distribution based Artificial Immune System for security in clustered wireless sensor networks," in 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science, Bhopal, India, 2014, pp.17.DOI:10.1109/SCEECS.2014.6804506. [Ref. 8]

[9] A. Lasisi, R. Ghazali, T. Herawan, F. Lasisi, and M. M. Deris, "Knowledge extraction of agricultural data using artificial immune system," in 2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Zhangjiajie, China, 2015, pp. 1653-1658. DOI: 10.1109/FSKD.2015.7382193. [Ref. 9]

[10] L. E. Jim and J. Chacko, "Decision Tree based AIS strategy for Intrusion Detection in MANET," in TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), Kochi, India, 2019, pp. 1191-1195. DOI: 10.1109/TENCON.2019.8929362. [Ref. 10]

[11] F. Zareen and R. Karam, "Detecting RTL Trojans using Artificial Immune Systems and HighLevel Behavior Classification," in 2018 Asian Hardware Oriented Security and Trust Symposium (AsianHOST), Hong Kong, China, 2018, pp. 68-73. DOI: 10.1109/AsianHOST.2018.8607172. [Ref. 11]

[12] H. Rouhani Zeidanloo, F. Hosseinpour, and P. Najafi Borazjani, "Botnet detection based on common network behaviors by utilizing Artificial Immune System(AIS)," in 2010 2nd International Conference on Software Technology and Engineering, San Juan, PR, USA, 2010, pp. V1-21-V1-25. DOI: 10.1109/ICSTE.2010.5608967. [Ref. 12]

[13] F. Hosseinpour, K. Abu Bakar, Amir Hatami Hardoroudi, and Ali Farhang Dareshur, "Design of a new distributed model for Intrusion Detection System based on Artificial Immune System," in 2010 6th International Conference on Advanced Information Management and Service (IMS), Seoul, Korea (South), 2010, pp. 378-383. [Ref. 13]

[14] O. Aljohani, N. Aljohani, P. Bours, and F. Alsolami, "Continuous Authentication on PCs using Artificial Immune System," in 2018 1st

International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2018, pp. 1-6. DOI: 10.1109/CAIS.2018.8442022. [Ref. 14]

[15] R. Chao and Y. Tan, "A Virus Detection System Based on Artificial Immune System," in 2009 International Conference on

[16] Computational Intelligence and Security, Beijing, China, 2009, pp. 6-10. DOI: 10.1109/CIS.2009.106. [Ref. 15]

[17] V. R. Kebande and H. S. Venter, "A cognitive approach for botnet detection using Artificial Immune System in the cloud," in 2014 Third International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Beirut, Lebanon, 2014, pp. 52-57. DOI: 10.1109/CyberSec.2014.6913971. [Ref. 16]

[18] M. Bere and H. Muyingi"Initial investigation of Industrial Control System (ICS) security using Artificial Immune System (AIS),"2015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), Windhoek, Namibia, 2015, pp79-84, DOI: [10.1109/ETNCC.2015.7184812](https://doi.org/10.1109/ETNCC.2015.7184812). [Ref. 17]

[19] E. Abd El Raoof Abas, H. Abdelkader, and A. Keshk "Artificial immune system based intrusion detection," 2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS), Cairo, Egypt, 2015, pp. 542DOI:[10.1109/IntelCIS.2015.7397274](https://doi.org/10.1109/IntelCIS.2015.7397274). [Ref. 18]

[20] E. B. Nuakoh and M. Anwar"Detecting Impersonation in Social Network Sites (SNS) Using Artificial Immune Systems (AIS)," SoutheastCon 2018, St. Petersburg, FL, USA, 2018, pp. 1-3, DOI:[10.1109/SECON.2018.8479274](https://doi.org/10.1109/SECON.2018.8479274). [Ref. 19]

[21] Yu Qiao and Jiayi Xu "A network security situation awareness model based on cooperative artificial immune system," 2011 International Conference on Computer Science and Service System (CSSS), Nanjing, 2011, pp. 1945-1947,DOI:[10.1109/CSSS.2011.5972215](https://doi.org/10.1109/CSSS.2011.5972215). [Ref. 20]

[22] E. D. Alalade "Intrusion Detection System in Smart Home Network Using Artificial Immune System and Extreme Learning Machine Hybrid Approach," 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2020, pp. 1-2,IoT48130.2020.9221151](https://doi.org/10.1109/WF-IoT48130.2020.9221151). [Ref. 21]

[23] M. B. S. Terra and J. J. C. Gondim "NERD: a Network Exfiltration Rootkit Detector based on a Multi-agent Artificial Immune System,"2021 Workshop on Communication Networks and Power Systems (WCNPS), Brasilia, Brazil, 2021, pp. 1-7, DOI: [10.1109/WCNPS53648.2021.9626241](https://doi.org/10.1109/WCNPS53648.2021.9626241). [Ref. 22]

[24] G. V. P. Kumar and D. K. Reddy "An Agent Based Intrusion Detection System for Wireless Network with Artificial Immune System (AIS) and Negative Clone Selection," 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies, Nagpur, India, 2014, pp. 429-433,DOI: [10.1109/ICESC.2014.73](https://doi.org/10.1109/ICESC.2014.73). [Ref. 23]

[25] Alsulami and S. Zein-Sabatto "Detection and Defense from False Data Injection Attacks In Aviation Cyber-Physical Systems Using Artificial Immune Systems," 2020 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2020, pp. 69-75,DOI: [10.1109/CSCI51800.2020.00019](https://doi.org/10.1109/CSCI51800.2020.00019). [Ref. 24]

[26] EshghiShargh "Using Artificial Immune System on Implementation of Intrusion Detection Systems," 2009 Third UKSim European Symposium on Computer Modeling and Simulation, Athens, Greece, 2009, pp. 164-168,DOI: [10.1109/EMS.2009.45](https://doi.org/10.1109/EMS.2009.45). [Ref. 25]