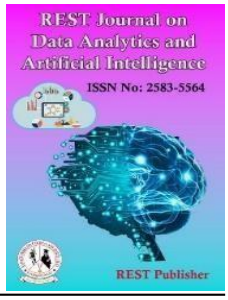
REST Journal on Data Analytics and Artificial Intelligence
Vol: 2(4), December 2023
REST Publisher; ISSN: 2583-5564
Website: http: //restpublisher.com/journals/jdaai/
DOI: https://doi.org/10.46632/jdaai/2/4/5



Analysis of Wireless Security and Networks using COPRAS Method

Madhusudhan Dasari sreeramulu
Leading financial institution USA.
Corresponding author: dsmadhu007@gmail.com

Abstract: *The wireless networks have become integral to our daily lives, powering everything from smart phones to smart home devices. However, alongside their benefits, wireless networks also bring forth significant security challenges. Wireless networks, unlike traditional wired networks, transmit data over the airwaves, making them susceptible to various forms of unauthorized access and data breaches. Ensuring the security of these networks is crucial to safeguard sensitive information, protect user privacy, and prevent cyber-attacks. The significance of research in wireless security and networks lies in the critical role that wireless technologies play in our interconnected world. As wireless networks become increasingly prevalent in various sectors, including communication, commerce, healthcare, transportation, and more, ensuring their security becomes paramount. Research in wireless security and networks contributes to the advancement of secure and reliable wireless technologies, protecting users' privacy, data, and overall well-being in an increasingly connected world. The COPRAS-G method requires identifying selection criteria, evaluating information related to these criteria, and developing methods to evaluate Meeting the participant's needs Criteria for doing in order to assess the overall performance of the surrogate. Decision analysis involves a Decision Maker (DM) Situation to do consider a particular set of alternatives and select one among several alternatives, usually with conflicting criteria. For this reason, the developed complexity proportionality assessment (COPRAS) method can be used. A genetic algorithm; Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), Differential Evolution (DE). Detection Accuracy, Resource Efficiency; Implementation Complexity; Time-to-Deployment. From the result Differential Evolution (DE) is got the first rank whereas is Ant Colony Optimization (ACO) is having the lowest rank*
Keywords: *Wireless Sensor Networks, Denial of Service, Intrusion Detection System, Decision Trees, Support Vector Machines.*

1. INTRODUCTION

In the realm of wireless networks, interference emerges when other devices transmit data within the identical frequency range, causing simultaneous disruptions in communication between a transmitting unit and a receiving unit. This disruptive phenomenon remains persistent even when utilizing (CDMA) technology, which allows multiple users to share the same frequency using distinct spreading codes. Despite the intention behind this spreading technique to decrease interference, the interference power builds up at the receiver due to the physical proximity of users. In networks featuring central controlling entities, interference can be mitigated or even exploited by implementing techniques such as scheduling and signal processing. These techniques encompass multiuser identification and interference cancellation. Nevertheless, interference remains a limiting factor in performance, especially in decentralized systems lacking specific controlling bodies to oversee access to the shared wireless medium. This limitation partly stems from the inherent unreliability of interference [1]. Because of the inherent traits of such networks, specifically their limited hardware capabilities and infrastructure-independent design, the widespread adoption of (WSNs) has led to numerous security vulnerabilities. Among the most prevalent dangers faced by these networks is the threat of denial of service attacks. Developing an intrusion detection and prevention system to mitigate the impact of such attacks proves to be challenging. This study proposes the utilization of decision trees and support vector machines, two machine learning methods, as an approach to recognize attack patterns within a specific dataset. The dataset used encompasses both normal profiles and various scenarios of Denial of Service attacks in WSNs. Based on the experimental results, the decision tree technique outperforms

Support Vector Machines, exhibiting superior true positive rates (99.86% vs. 99.62%) and more favorable false positive rates (0.05% vs. 0.09%). [2] Wireless Sensor Network (WSN) attacks aim to disrupt the intended operation of the network. WSNs are limited-resource networks deployed in unpredictable environments, making them vulnerable to unauthorized access. These attacks exploit weaknesses in specific network layers, often impacting multiple layers simultaneously. Detecting potential malicious actions involves monitoring and evaluating local sensor behavior across different network layers. This study introduces a comprehensive method for an intrusion detection system (IDS) based on anomalies, referred to as mIDS. This system employs (BLR), a statistical tool, to categorize local sensor actions as either legitimate or malicious. The effectiveness of the proposed approach is assessed through simulations involving attacks on the routing layer. The results demonstrate that the mIDS can accurately identify malicious behavior in the range of 88% to 100% [3]. Wireless networks commonly employ the OSI protocol architecture, comprised of the application, transport, network, MAC, and physical layers. To address security prerequisites like authenticity, confidentiality, integrity, and availability, each of these layers individually addresses security vulnerabilities and potential threats. For example, encryption is frequently utilized to preserve the confidentiality of transmitted data, preventing unauthorized access. Although cryptography enhances communication confidentiality, it introduces latency and necessitates additional processing power due to the time taken for data encryption and decryption. Presently, wireless networks often utilize multiple authentication methods simultaneously across different protocol layers, [4]. The aim of authorized communications is to safeguard them against harmful attempts of eavesdropping and interference. However, the emergence of mobile communication networks without traditional infrastructure brings about significant concerns for public safety, as they are difficult to regulate and can be exploited for illegal purposes (such as by terrorists or criminals). This paper suggests a fundamental shift in wireless security approach to tackle this issue. It proposes the simultaneous utilization of both authorized eavesdropping and interference, aimed at monitoring and disrupting suspicious and malicious wireless communications that occur in infrastructure-free environments. Specifically, the proposal introduces proactive eavesdropping, achieved through jamming, to intercept and decipher information from questionable communication channels. The ultimate objective is to comprehend the intentions behind these communications and decide on appropriate punitive actions. Furthermore, the concept of cognitive jamming is put forth, involving eavesdropping, to disturb, incapacitate, and potentially counterfeit targeted unfriendly wireless communications. This approach facilitates various forms of intervention activities. A wireless sensor network can encompass numerous sensor nodes, with each node being equipped with sensors, microprocessors, memory, a wireless transmitter, and a battery. Once deployed, these sensor nodes create a network using short-range wireless communication. They are responsible for collecting data related to the environment and subsequently transmitting this data to a central node known as the sink node or data processing center. One prominent application of wireless sensor networks lies in the realm of environmental data collection and surveillance. For instance, envision a scenario where researchers desire deeper insights into the progression of a specific phenomenon across a designated area. To achieve this, they can establish an extensively distributed wireless sensor network within the area, comprising multiple sensor nodes. At regular intervals, each individual sensor node compiles local measurements of pertinent variables like temperature and humidity, which are then transmitted back to the sink node. Each recorded measurement corresponds to a specific sensor location. A Wireless Intrusion Detection System (IDS) employs a Wrapper Based Feature Extraction Unit (WFEU) in conjunction with a Feed-Forward Deep Neural Network (FFDNN). The WFEU employs the Extra Trees technique to generate an optimized feature vector with reduced dimensions. The effectiveness and efficiency of the WFEU-FFDNN system are evaluated using the UNSW-NB15 and AWID intrusion detection datasets. To gauge its performance, the WFEU-FFDNN system is compared to conventional machine learning (ML) techniques like Random Forest (RF), Support Vector Machine (SVM), Naive Bayes (NB), Decision Tree (DT), and k-Nearest Neighbor (kNN). The experimental setup includes both binary and multiclass intrusion scenarios. The WFEU generates an optimized feature vector with 22 attributes, achieving an overall accuracy of 87.10% for binary classification and 77.16% for multiclass classification on the UNSW-NB15 dataset. Moreover, on the AWID dataset, the WFEU achieves remarkable overall accuracies of 99.66% and 99.77% for binary and multiclass classifications [7]. In summary, the intent behind these policies is to alleviate traffic congestion by reducing the occurrence of congested roads. The implementation of these measures, however, has given rise to challenges in managing multimedia data. Specifically, the proposed solution has led to a narrow margin for acceptable packet loss during the transmission of video data. The MPEG compression codec introduces three types of frames: I-frames, B-frames, and P-frames. Among these, I-frames and P-frames hold the most significance, as the absence of either of these frames results in a noticeable deterioration in video quality. Within Wireless Multimedia Sensor Networks (WMSNs), Cluster Heads (CHs) play a crucial role in aggregating, processing, and receiving multimedia data from participants. The level of responsibility and energy consumption of these Cluster Heads is contingent on the number of participants they serve. The forthcoming sections introduce a novel metric termed MCUR, propose an optimal selection, and present the Equal Size Clusters to Decrease Congestion (ESCC) protocol. The ESCC protocol is designed to address congestion by striving to lower the MCUR in a decentralized manner. It introduces an additional phase to the election process referred to as "balancing." This phase employs a force-join message to harmonize the cluster sizes, representing a pivotal aspect of our approach [8]. Industry 4.0 integrates information and communication technologies, with a focus on wireless communication,

to facilitate smart and interconnected manufacturing processes [1]. Wireless networks offer several benefits [2]. By removing the need for physical cables, wireless technology reduces expenses and streamlines the design, setup, and upkeep of structures. Additionally, in regions where mobile autonomous vehicles and robots, which often necessitate communication while moving around a worksite, operate, wireless connectivity is essential. These wireless connections can also operate effectively in environments with elevated temperatures and corrosive elements [9]. New data analysis methods are being developed to aid in the establishment and operation of sensor networks that monitor environmental activities, including the identification of forest fires. Instead of concentrating solely on individual environmental concerns, the objective is to uncover techniques applicable across various environmental datasets. Consequently, a substantial volume of data is necessary to ensure precise and lucid outcomes. The initial phase, which involves the preparation of sensor data for analysis, includes removing irrelevant data, addressing missing values, and potentially summarizing or amalgamating data. This procedure essentially readies the data for scrutiny. Another key step is the clustering of sensor data. This entails categorizing a collection of objects into clusters or groups, with objects within a cluster exhibiting high similarity and distinct dissimilarity from objects in other clusters [10]. This study proposes the utilization of RF fingerprinting to enhance the security of wireless networks. When a radio transmitter is activated, it emits an RF signal with temporary attributes related to its instantaneous frequency and amplitude. Various factors, including the characteristics of frequency synthesis systems, modulator components, and RF amplifiers, can impact the behavior of these transient signals. The duration of this temporary behavior can differ based on the transmitter's type and model. Even among transmitters of the same type, disparities are frequently noticeable, primarily due to manufacturing variations and device aging. This unique transient signal pattern during a radio's activation, often referred to as its RF fingerprint, can be employed for the purpose of transmitter identification [11]. This research investigates multiple actual datasets acquired through devices for short-range wireless communication. It assesses the characteristics of each dataset and categorizes the publications that utilized these datasets into different groups. The study offers valuable insights to researchers seeking appropriate datasets for analysis or practical use. It also serves as a point of reference for individuals aiming to conduct experiments that involve monitoring the latest developments in short-range wireless networks and exploring effective ways to leverage authentic data sources. [12] Wireless sensor networks (WSNs) serve as a form of fundamental infrastructure in smart cities, gathering information from the city to provide smart services. One of the main challenges with smart cities is the security of WSNs. Dynamic ongoing or unknown attacks typically avoid isolated defence components in resource-constrained WSNs. We therefore provide a hierarchical system based on chance discovery and use control (UCON) technologies to address this issue while still taking into account the low complexity and high security needs of WSNs. Using powerful persistent threat detection, UCON's continuous decision and dynamic attribute features may stop ongoing threats. In order to find undiscovered attacks, we also employ a dynamic adaptive chance discovery mechanism. A unified framework is suggested for the design and implementation of a system employing the process described above, in which sensors conduct low level attack detection using straightforward rules and sinks and base stations provide high level attack detection using intricate rules. In addition, when either low level or high level threats are discovered, attack mitigation is carried out using software-defined networking (SDN) and network function virtualization (NFV) technologies. In order to gather an attack data set for analysis, an experiment was conducted. Then, a simulation was developed to gauge resource usage and attack detection efficiency. The outcomes show that the suggested plan is workable and effective. [13] Intrusion detection has emerged as a significant approach for uncovering attacks and ensuring network security. With the exponential growth of data on the Internet each year, relying solely on a single algorithm for network security is no longer sufficient. This is due to potential issues related to statistics, computations, and representations that a single learning approach could encounter. To address these challenges, this study introduces a novel approach that combines multiple machine learning algorithms through a technique known as stacked ensemble learning. This approach enhances attack detection compared to traditional methods that rely on a single algorithm for identifying attacks. The stacked ensemble system was evaluated using the NSL-KDD benchmark dataset, and its performance was compared against other widely used machine learning algorithms including ANN, CART, random forest, SVM, and other methods proposed by researchers. The experimental findings demonstrate that stacked ensemble learning outperforms existing methods in accurately classifying attacks. Moreover, the proposed system exhibits superior accuracy when compared to other intrusion detection models [14]. Because of limited resources, transmitting complete imaging data wirelessly in networks of visual sensors (WVSNs) is not practical. Additionally, the overwhelming quantity of surveillance footage poses challenges for analysts trying to extract meaningful insights. To address the limitations of traditional WVSNs, this research introduces an energy-efficient framework for prioritizing images. In this suggested approach, only semantically relevant information is selected for transmission to a central node. The foundation of this framework is salient motion detection, which mimics human cognitive processes. To enhance salient motion detection, each camera node employs a bootstrapping technique to estimate the background. Based on the identified salient motion, each sensor node is categorized as having high or low priority. This classification is dynamic, allowing camera nodes to switch from high to low priority based on the coverage of areas of interest. To ensure efficient data transfer, high-priority camera nodes are allocated reliable radio channels. We compare the effectiveness of this framework with other advanced methods for both single-camera and multi-camera monitoring scenarios. The results demonstrate

the advantages of the proposed approach in terms of capturing important events, reducing processing and transmission expenses, and assisting analysts in identifying visually relevant semantic data [15].

2. MATERIALS AND METHOD

2.1Detection Accuracy: Accuracy of detection refers to the degree of correctness or precision in identifying or classifying something correctly. In various contexts, such as machine learning, data analysis, and quality control, detection accuracy is a measure of how accurately a system or process can identify specific elements, patterns, or anomalies within a given dataset or scenario.

2.2 Resource Efficiency: Resource efficiency refers to the concept of using available resources in a careful, economical, and sustainable manner to maximize output while minimizing waste and negative environmental impacts. It involves optimizing the use of materials, energy, and other resources to achieve desired outcomes while minimizing resource consumption and the generation of waste or pollution. This approach aims to strike a balance between meeting human needs and ensuring the long-term health of the planet by reducing resource depletion and environmental degradation.

2.3Implementation Complexity: "Implementation complexity" refers to the level of difficulty, intricacy, and challenges associated with putting a plan, idea, or concept into action. It encompasses the various factors, such as technical difficulties, resource allocation, coordination, and potential obstacles. That can make the process of executing a particular task or project more intricate and demanding. In essence, it measures the level of effort and expertise required to successfully bring a plan to fruition.

2.4Time-to-Deployment: "Time-to-Deployment" refers to the amount of time it takes to fully implement or launch a product, service, software, or project from the initial planning or development stages. It encompasses all the steps involved, including design, development, testing, quality assurance, and any other necessary processes before the final product or service is ready to be used or released to the intended audience or market. Minimizing the time-to-deployment is often a goal in various industries to ensure quicker delivery of innovations and improvements to customers or users.

2.5A genetic algorithm is a computational technique inspired by the process of natural selection and evolution. It's used for solving optimization and search problems by mimicking the way biological organisms evolve and adapt over time. In a genetic algorithm, a population of potential solutions (individuals) undergoes successive generations of selection, recombination (crossover), and mutation. The algorithm evaluates each individual's fitness based on how well it solves the problem at hand. Individuals with higher fitness values have a better chance of being selected for reproduction.

2.6Particle Swarm Optimization (PSO) is a computational optimization technique inspired by the social behavior of birds or fish swarms. It's used to solve complex optimization problems in various domains, such as engineering, finance, and artificial intelligence. In PSO, a group of potential solutions (particles) move through the solution space, adjusting their positions based on their own experiences and the experiences of their neighbors. The goal is to iteratively converge towards the optimal solution by optimizing a given objective function. PSO is particularly effective for problems that are non-linear, multi-dimensional, and lack a specific mathematical representation.

2.7 Ant Colony Optimization (ACO) refers to a nature-inspired optimization technique that is based on the foraging behavior of ants. In ACO, an algorithm simulates the way real ants discover the shortest path between their nest and a food source by leaving pheromone trails on the ground. These pheromone trails communicate information to other ants about the quality of the path, and as more ants follow a certain path, the pheromone concentration increases, making that path more attractive. In optimization problems, ACO algorithms use this concept to find optimal solutions by constructing and evaluating potential solutions iteratively. Solutions are represented as paths in a graph, and the algorithm uses pheromone levels to guide its search towards promising areas of the solution space. Over time, the algorithm converges towards optimal or near-optimal solutions by exploiting the paths with higher pheromone concentrations.

2.8 Differential Evolution (DE) denotes a computational optimization technique that belongs to the family of evolutionary algorithms. In DE, a population of candidate solutions is evolved iteratively to find the optimal or near-optimal solution for a given problem. This algorithm operates by creating new candidate solutions through the combination of existing solutions, guided by a differential mutation strategy and a selection process. DE is commonly used to solve optimization problems in various fields, such as engineering, economics, and science, where finding the best solution among a large set of possibilities is essential.

Method: COPRAS (Complex Proportionality Assessment) is one of the most used Multi-Criteria Decision Making (MCTM) methods, and the ratio of the best solution Determining the solution with the best rate in the set of possible

alternatives by Provides a better alternative Bad Solution This technique has Decision making problems Various to solve used by researchers [16]. The COPRAS-G method requires identifying selection criteria; evaluating information related to these criteria, and developing methods to evaluate Meeting the participant's needs Criteria for doing in order to assess the overall performance of the surrogate. Decision analysis involves a Decision Maker (DM) Situation to do consider a particular set of alternatives and select one among several alternatives, usually with conflicting criteria. For this reason, the developed complexity proportionality assessment (COPRAS) method can be used [17]. In 1996 in Lithuania COPRAS (Complex Proportion evaluation) method was developed. construction, economics, real estate and management. One of the articles assesses the risks involved in construction projects. The assessment is based on various multi-objective assessment methods. The risk assessment indices are selected considering the interests, objectives and factors of the countries that influence the construction efficiency and real estate price increase [18] to describe and consider the task model. Complex Proportionality Assessment (COPRAS) Method Similar to any Many other criteria will make the decision (MCDM) tool, first Proposed COBRAS method of several related criteria Basically for alternatives Used to prioritize criterion weights. This method is better and Worst-Best Solutions Best decision considering Selecting alternatives [19]. Cobras approach is used for device tool choice; Because of this the triangle Ambiguous numbers are selected their computational performance. Three area specialists are selected to assign weights and by way of combining the fuzzy cobra's method, System 1 (MC1) and device 2(MC2) similarly are ranked, with way of ma chine three and four. -based totally approach is utilized in mixture with fuzzy. COPRAS assesses the complexity of consumer dating management (CRM) performance. A combined choice matrix is obtained from a panel of 20 specialists offered 3 options with set, and 5 criteria Assessment are done [20]. COPRAS to resolve MCDM issues, wherein the weights of the criteria and Performance ratings of alternatives are absolute Based on linguistic terms are calculated. Comparison of criteria Importance calculated and Cobras method become used to assess renovation strategies [21]. This have a look at ambitions to develop the impact of latest overall performance metrics in TPM and COPRAS in an ambiguous context Primarily multi-criteria selection based on opinions Use the do method. Looseness of paper is prepared as follows [22]. Complex proportional estimation approach with gray c language Numbers (COPRAS-G) approach. Cobras- G's idea approach is based on standards values expressed in durations, actual decision-making conditions, and programs of Gray Systems Theory. Diploma [23]. COPRAS method changed into The most relevant social media platform Rank and choose is used. Proposed Applicability of the structure We proved and proved the character [24].COPRAS (Complex Proportionality Assessment) To examine Cumulative of an alternative Performance, it is essential become aware of the maximum vital criteria, examine the options and compare the facts Depending on those criteria to fulfil the wishes of the DMs to compare grades evaluation involves a situation in which a DM must pick amongst several downloaded alternatives given a selected set of commonly conflicting standards. For this motive, the developed complex proportionality evaluation (COPRAS) method can be used in real situations, alternatives The criteria for assessment are vague is related to the factor, And the values of the standards are real Cannot be expressed with numbers [25].

3. RESULTS AND DISCUSSION

TABLE 1. Wireless Security and Networks

	Detection Accuracy	**Resource Efficiency**	**Implementation Complexity**	**Time-to-Deployment**
GA-IDS	0.85	0.75	0.6	0.7
PSO-FW	0.8	0.7	0.65	0.75
ACO-NM	0.75	0.8	0.7	0.8
DE-EN	0.9	0.85	0.65	0.7
RS-NS	0.7	0.6	0.55	0.65

Table 1 shows the wireless security and networks for COPRAS Method. The highest accuracy is achieved by method DE-EN with a value of 0.9, followed closely by GA-IDS with 0.85. RS-NS has the lowest accuracy at 0.7. DE-EN again leads with the highest resource efficiency score of 0.85. ACO-NM follows closely at 0.8. RS-NS has the lowest resource efficiency at 0.6. GA-IDS has the lowest complexity with a score of 0.6. PSO-FW and DE-EN share a score of 0.65. ACO-NM has the highest complexity at 0.7. ACO-NM and DE-EN have the shortest time-to-deployment with a score of 0.7. PSO-FW follows at 0.75. RS-NS has the longest time-to-deployment at 0.65.

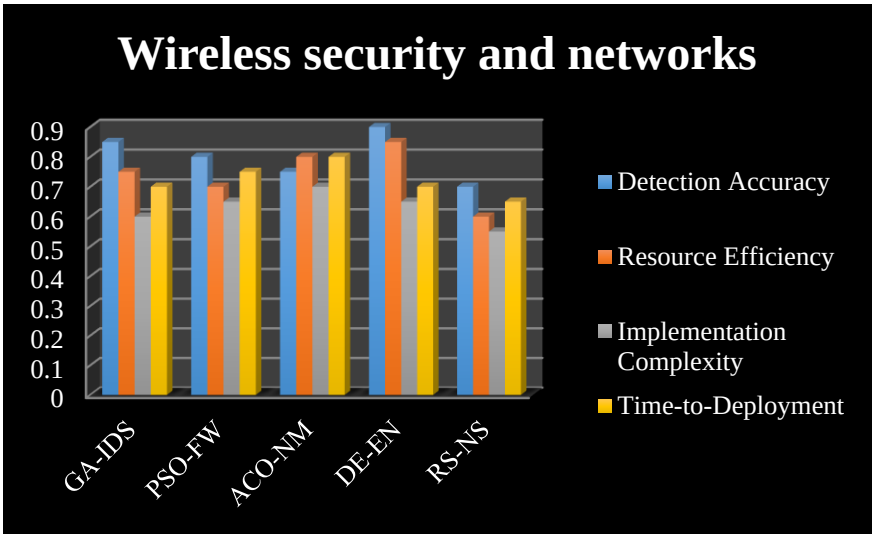


FIGURE 1. Wireless security and networks

TABLE 2. Normalized Data

Normalized Data			
Detection Accuracy	**Resource Efficiency**	**Implementation Complexity**	**Time-to-Deployment**
0.2125	0.2027	0.1905	0.1944
0.2000	0.1892	0.2063	0.2083
0.1875	0.2162	0.2222	0.2222
0.2250	0.2297	0.2063	0.1944
0.1750	0.1622	0.1746	0.1806

Table 2 shows the wireless security and networks Normalized Data for GA-IDS, PSO-FW, ACO-NM, DE-EN, RS-NS Normalized value

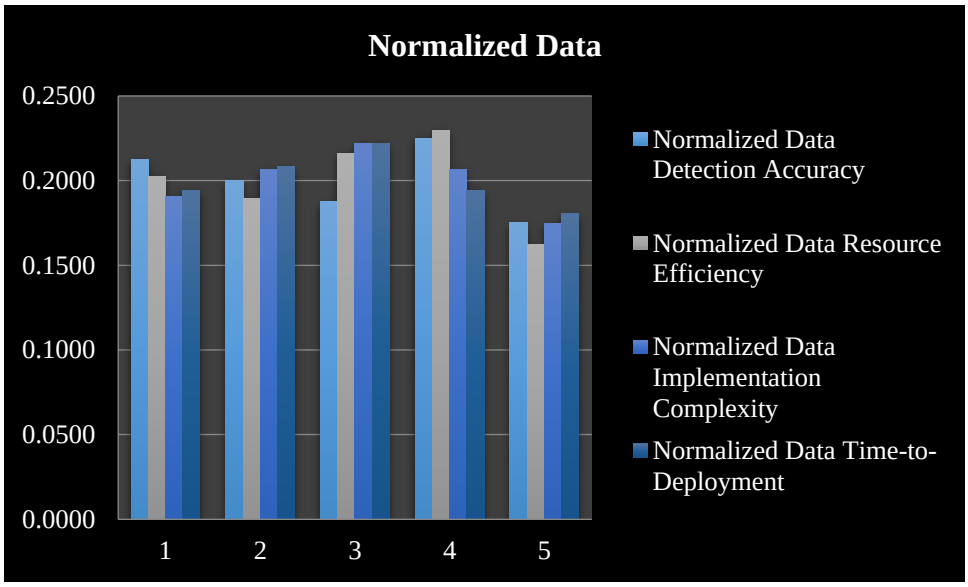


FIGURE 2. Normalized Data

Figure 2 shows the shows the wireless security and networks Normalized Data for GA-IDS, PSO-FW, ACO-NM, DE-EN, RS-NS Normalized value.

TABLE 3. Weightages

Weight			
0.25	0.25	0.25	0.25
0.25	0.25	0.25	0.25
0.25	0.25	0.25	0.25
0.25	0.25	0.25	0.25
0.25	0.25	0.25	0.25

Table 3 shows Weight ages used for the analysis. We take same weights for all the parameters

TABLE 4. Weighted normalized decision matrix

Weighted normalized decision matrix			
0.05	0.05	0.05	0.05
0.05	0.05	0.05	0.05
0.05	0.05	0.06	0.06
0.06	0.06	0.05	0.05
0.04	0.04	0.04	0.05

Table 4 shows the weighted normalized decision matrix for GA-IDS, PSO-FW, ACO-NM, DE-EN, RS-NS is also Multiple value.

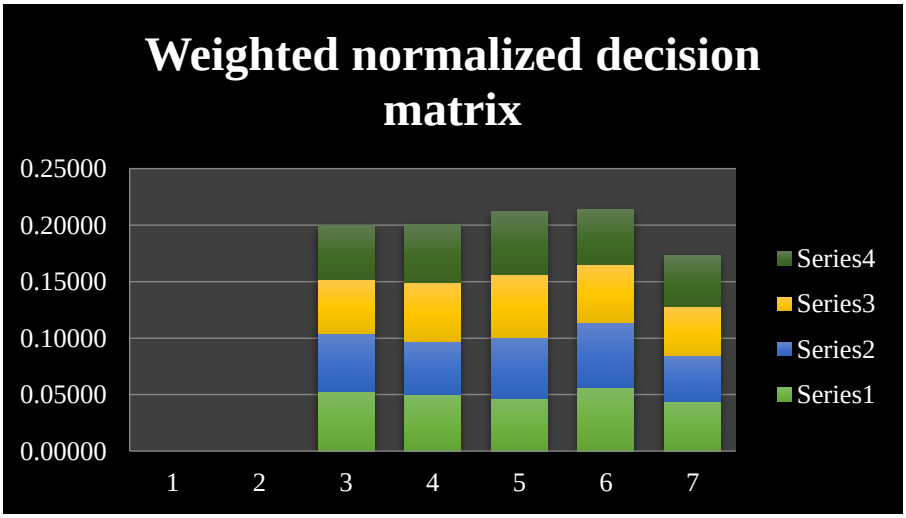


FIGURE 3. weighted normalized decision matrix

Figure 3 shows the weighted normalized decision matrix for GA-IDS, PSO-FW, ACO-NM, DE-EN, RS-NS is also multiple values.

TABLE 5. Wireless security and networks Bi, Ci, Min(Ci)/Ci

Bi	Ci	Min(Ci)/Ci
0.104	0.096	0.9227
0.097	0.104	0.8565
0.101	0.111	0.7991
0.114	0.100	0.8861
0.084	0.089	1.0000

Table 5 shows the wireless security and networks Bi, Ci, Min(Ci)/Ci GA-IDS, PSO-FW, ACO-NM, DE-EN, RS-NS it is sum of minimum value.

TABLE 6. Final Result of Wireless security and networks

Qi	Ui	Rank
0.207	97.2812	2
0.193	90.7437	4
0.190	89.4327	5
0.213	100.0000	1
0.196	92.1853	3

Table 6 shows the final result of COPRAS for wireless security and networks. Qi wireless security and networks is calculated using the DE-EN is having is Higher Value and ACO-NM is having Lower value. Ui wireless security and networks calculated using the DE-EN is having is Higher Value and ACO-NM is having Lower value.

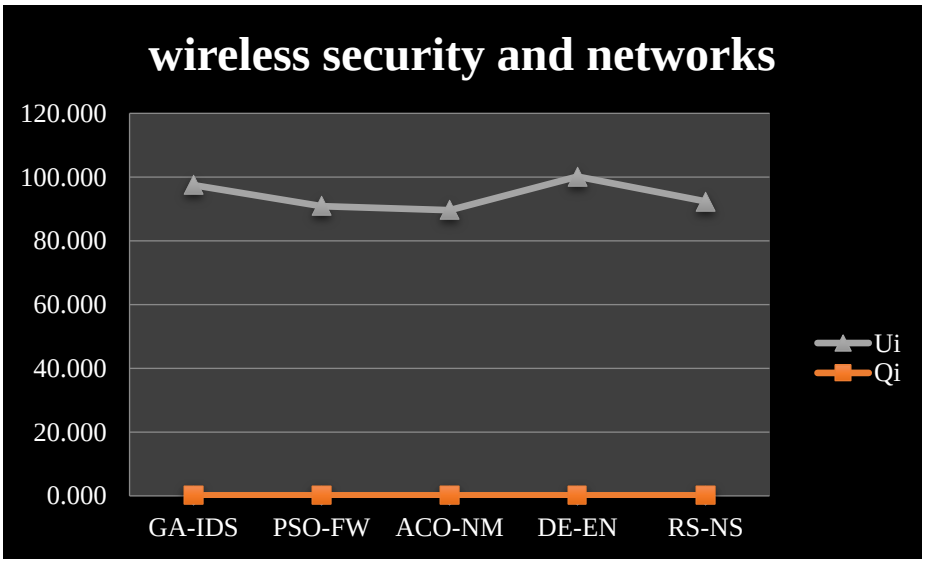


FIGURE 4. Wireless security and networks Qi, Ui

Figure 4 shows the final result of COPRAS for wireless security and networks. Qi wireless security and networks is calculated using the DE-EN is having is Higher Value and ACO-NM is having Lower value. Ui wireless security and networks calculated using the DE-EN is having is Higher Value and ACO-NM is having Lower value.

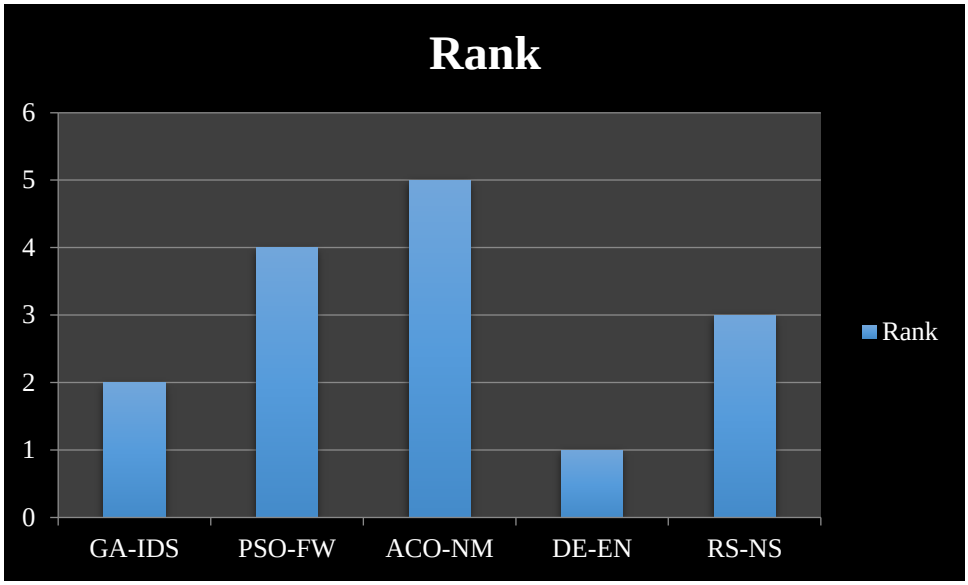


FIGURE 5. Shown the Rank

Figure 5 Shows Ranking of wireless security and networks. Differential Evolution (DE) is got the first rank whereas is Ant Colony Optimization (ACO) is having the Lowest rank.

4. CONCLUSION

Wireless security and networks is of paramount importance in today's interconnected world. As the reliance on wireless technologies grows, ensuring the confidentiality, integrity, and availability of data transmitted over these networks becomes a significant concern. This field encompasses various strategies and technologies aimed at safeguarding wireless communications from unauthorized access, data breaches, and other malicious activities. Throughout this study, we have delved into the key challenges and solutions in wireless security. From encryption protocols such as WPA3 to authentication methods like multi-factor authentication, the arsenal of tools available to protect wireless networks is diverse and ever-evolving. Additionally, the emergence of technologies like 5G brings both opportunities and new security considerations, highlighting the need for continuous research and adaptation. However, despite the progress made in wireless security, vulnerabilities persist. The evolution of hacking techniques and the increasing complexity of cyber threats necessitate a proactive approach. Regular security audits, timely software updates, and user education are essential components of a robust wireless security strategy. In the realm of wireless networks, striking a balance between usability and security is crucial. Network administrators and individuals must make informed decisions about the trade-offs involved. While convenience is vital, it should not come at the expense of leaving networks susceptible to breaches. In conclusion, the landscape of wireless security and networks is intricate and dynamic. A comprehensive understanding of the evolving threat landscape, coupled with the implementation of robust security measures, is imperative for fostering a safer wireless environment. As technology advances, collaboration among stakeholders, ongoing research, and a commitment to best practices will continue to play pivotal roles in enhancing wireless security across the borders.

REFERENCES

[1]. Cetin, Burak, Alina Lazar, Jinoh Kim, Alex Sim, and Kesheng Wu. "Federated wireless network intrusion detection." In 2019 IEEE International Conference on Big Data (Big Data), pp. 6004-6006. IEEE, 2019.

[2]. Al-issa, Abdulaziz I., Mousa Al-Akhras, Mohammed S. ALsahli, and Mohammed Alawairdhi. "Using machine learning to detect DoS attacks in wireless sensor networks." In 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), pp. 107-112. IEEE, 2019.

[3]. Onat, Ilker, and Ali Miri. "An intrusion detection system for wireless sensor networks." In WiMob'2005), IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2005., vol. 3, pp. 253-259. IEEE, 2005.

[4]. Zou, Yulong, Jia Zhu, Xianbin Wang, and Lajos Hanzo. "A survey on wireless security: Technical challenges, recent advances, and future trends." Proceedings of the IEEE 104, no. 9 (2016): 1727-1765.

[5]. Xu, Jie, Lingjie Duan, and Rui Zhang. "Surveillance and intervention of infrastructure-free mobile communications: A new wireless security paradigm." IEEE Wireless Communications 24, no. 4 (2017): 152-159.
[6]. Liu, Chong, Kui Wu, and Jian Pei. "An energy-efficient data collection framework for wireless sensor networks by exploiting spatiotemporal correlation." IEEE transactions on parallel and distributed systems 18, no. 7 (2007): 1010-1023.
[7]. Kasongo, Sydney Mambwe, and Yanxia Sun. "A deep learning method with wrapper based feature extraction for wireless intrusion detection system." Computers & Security 92 (2020): 101752.
[8]. Xu, Zheng. "The analytics and applications on supporting big data framework in wireless surveillance networks." International Journal of Social and Humanistic Computing 2, no. 3-4 (2017): 141-149.
[9]. Jiang, Xiaolin, Zhibo Pang, Michele Luvisotto, Fei Pan, Richard Candell, and Carlo Fischione. "Using a large data set to improve industrial wireless communications: Latency, reliability, and security." IEEE Industrial Electronics Magazine 13, no. 1 (2019): 6-12.
[10]. Mittal, Ruchi, and MP S. Bhatia. "Wireless sensor networks for monitoring the environmental activities." In 2010 IEEE International Conference on Computational Intelligence and Computing Research, pp. 1-5. IEEE, 2010.
[11]. Ureten, Oktay, and Nur Serinken. "Wireless security through RF fingerprinting." Canadian Journal of Electrical and Computer Engineering 32, no. 1 (2007): 27-33.
[12]. Lin, Zhiting, and Pengfei Wang. "A review of data sets of short-range wireless networks." Computer Communications 147 (2019): 138-158.
[13]. Wu, Jun, Kaoru Ota, Mianxiong Dong, and Chunxiao Li. "A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities." IEEE Access 4 (2016): 416-424.
[14]. Rajadurai, Hariharan, and Usha Devi Gandhi. "A stacked ensemble learning model for intrusion detection in wireless network." Neural computing and applications (2020): 1-9.
[15]. Mehmood, Irfan, Muhammad Sajjad, Waleed Ejaz, and Sung Wook Baik. "Saliency-directed prioritization of visual data in wireless surveillance networks." Information Fusion 24 (2015): 16-30.
[16]. Yazdani, Morteza, Ali Alidoosti, and EdmundasKazimierasZavadskas. "Risk analysis of critical infrastructures using fuzzy COPRAS." Economic research-Ekonomskaistraživanja 24, no. 4 (2011): 27-40. https://doi.org/10.1080/1331677X.2011.11517478
[17]. Aghdaie, Mohammad Hasan, Sarfaraz HashemkhaniZolfani, and EdmundasKazimierasZavadskas. "Market segment evaluation and selection based on application of fuzzy AHP and COPRAS-G methods." Journal of Business Economics and Management 14, no. 1 (2013): 213-233.https://doi.org/10.3846/16111699.2012.721392
[18]. Kildienė, Simona, Arturas Kaklauskas, and EdmundasKazimierasZavadskas. "COPRAS based comparative analysis of the European country management capabilities within the construction sector in the time of crisis." Journal of Business Economics and Management 12, no. 2 (2011): 417-434.
[19]. Das, Manik Chandra, Bijan Sarkar, and Siddhartha Ray. "A framework to measure relative performance of Indian technical institutions using integrated fuzzy AHP and COPRAS methodology." Socio-Economic Planning Sciences 46, no. 3 (2012): 230-241.https://doi.org/10.1016/j.seps.2011.12.001
[20]. Dhiman, Harsh S., and Dipankar Deb. "Fuzzy TOPSIS and fuzzy COPRAS based multi-criteria decision making for hybrid wind farms." Energy 202 (2020): 117755.https://doi.org/10.1016/j.energy.2020.117755
[21]. Fouladgar, Mohammad Majid, Abdolreza Yazdani-Chamzini, Ali Lashgari, EdmundasKazimierasZavadskas, and ZenonasTurskis. "Maintenance strategy selection using AHP and COPRAS under fuzzy environment." International journal of strategic property management 16, no. 1 (2012): 85-104.https://doi.org/10.3846/1648715X.2012.666657
[22]. TuranogluBekar, Ebru, Mehmet Cakmakci, and Cengiz Kahraman. "Fuzzy COPRAS method for performance measurement in total productive maintenance: a comparative analysis." Journal of Business Economics and Management 17, no. 5 (2016): 663-684.https://doi.org/10.3846/16111699.2016.1202314
[23]. Zolfani, Sarfaraz Hashemkhani, Nahid Rezaeiniya, Mohammad Hasan Aghdaie, and EdmundasKazimierasZavadskas. "Quality control manager selection based on AHP-COPRAS-G methods: a case in Iran." Economic research-Ekonomskaistraživanja 25, no. 1 (2012): 72-86. https://doi.org/10.1080/1331677X.2012.11517495
[24]. Tavana, Madjid, Ehsan Momeni, Nahid Rezaeiniya, Seyed Mostafa Mirhedayatian, and Hamidreza Rezaeiniya. "A novel hybrid social media platform selection model using fuzzy ANP and COPRAS-G." Expert Systems with Applications 40, no. 14 (2013): 5694-5702.https://doi.org/10.1016/j.eswa.2013.05.015
[25]. Kouchaksaraei, RamtinHaghnazar, Sarfaraz HashemkhaniZolfani, and Mahmood Golabchi. "Glasshouse locating based on SWARA-COPRAS approach." International Journal of Strategic Property Management 19, no. 2 (2015): 111-122.https://doi.org/10.3846/1648715X.2015.1004565

