Enhancing Security in Mobile Ad Hoc Networks: Enhanced Particle Swarm Optimization-driven Intrusion Detection and Secure Routing Algorithm

Nikitina Vlada[1*], Raúl A. Sánchez-Ancajima[2], Miguel Ángel Torres Rubio[3], Walter Antonio Campos- Ugaz[4], Anibal Mejía Benavides[5], María Del Rocío Hende-Santolaya[6] and Jacqueline C. Ponce-Meza[7]

[1*] PhD, Professor, Peoples' Friendship University of Russia, Russia. erchenko5@rambler.ru, Orcid: https://orcid.org/0000-0003-0780-3140

[2] Doctor, Professor, Faculty of Economic Sciences, Universidad Nacional de Tumbes, Tumbes, Perú. rsanchez@untumbes.edu.pe, Orcid: https://orcid.org/0000-0003-3341-7382

[3] Doctor, Professor, Faculty of Humanities, Universidad Católica Santo Toribio de Mogrovejo, Chiclayo, Perú. miguel.torres@usat.edu.pe, Orcid: https://orcid.org/0000-0001-9901-4880

[4] Doctor, Professor, School of Engineering, Universidad Nacional Pedro Ruiz Gallo, Lambayeque, Perú. wcampos@unprg.edu.pe, Orcid: https://orcid.org/0000-0002-1186-5494

[5] Doctor, Professor, Faculty of Social Sciences, Universidad Nacional de Tumbes, Tumbes, Perú. amejiab@untumbes.edu.pe, Orcid: https://orcid.org/0000-0003-2190-2647

[6] Doctor, Professor, Faculty of Humanities Universidad Católica Santo Toribio de Mogrovejo, Chiclayo, Perú. rociohende@gmail.com, Orcid: https://orcid.org/0009-0002-5078-5582

[7] Master, Professor, Teaching Accompaniment, Universidad Privada del Norte, Lima, Perú. jaynita_22@hotmail.com, Orcid: https://orcid.org/0000-0001-9241-4902

Received: May 20, 2023; Accepted: July 04, 2023; Published: September 30, 2023

Abstract

Wireless technologies have grown in popularity and are used in many applications. Transient Mobile Ad hoc Networks (MANETs) serve specific goals without infrastructure. The dynamism of these networks makes them useful for ubiquitous computing. However, high mobility, the lack of a centralized authority, and open media make MANETs vulnerable to various security risks. Thus, an Intrusion Detection System (IDS) should be used to monitor and detect system security issues. To prevent and improve security against unauthorized access, intrusion screening is crucial. The depletion of a mobile node's power supply can impact its capacity to transmit packets, as this functionality is contingent upon the system's overall lifespan. Computational Optimization-driven solutions have been prevalent in the context of IDS and secure routing inside MANETs. This research employs the Enhanced Particle Swarm Optimization-driven Intrusion Detection and Secure Routing Algorithm (EPSO-IDSRA). Enhanced Particle Swarm Optimization technique (EPSO) has provided confidence-based, secure, and energy-efficient routing in MANETs. The EPSO technique is applied to identify optimal hops for enhancing the routing process. The initial step involves the activation of the fuzzy clustering algorithm, followed by selecting Cluster Heads (CHs) based on

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 14, number: 3 (September), pp. 77-88. DOI: *10.58346/JOWUA.2023.I3.006*

*Corresponding author: PhD, Professor, Peoples' Friendship University of Russia, Russia.

assessing their indirect, direct, and recent confidence values. Furthermore, the identification of value nodes was contingent upon assessing confidence levels. Also, the CHs are involved in multi-hop routing, and determining the optimal route depends on the anticipated protocol, which chooses the most favorable paths considering factors such as latency, throughput, and connectivity within the designated area. The EPSO method, presented for secure routing (at time 50ms), yielded an optimal energy consumption of 0.15 millijoules, a minimal delay of 0.008 milliseconds, a maximum throughput of 0.8 bits per second, and an 89% detection rate.

Keywords: MANET, Intrusion Detection, Secure Routing, Particle Swarm Optimization, Cluster Head, Confidence Values.

1 Introduction

A MANET is a network consisting of a collection of wireless nodes that are linked and capable of self-organization. In a MANET, each node operates as a router, facilitating the transmission of packets from the source node to the destination node. Remote ad hoc networks are networks of significant scale that are widely utilized. Each mobile node is a self-managed node without a central mobile network administration node. Mobile nodes are authorized to access specific locations based on their requirements. The network allows for efficient node joining and exiting (Dhindsa, K.S., 2021). There are no limitations on the communication capacity of nodes.

Data loss may occur if the nodes are located outside the network's radio range after establishing the connection. MANETs are used widely across several domains, including scientific research, emergency response operations, and military activities. The prevalence of cyberattacks has increased due to enhanced interconnectivity across networks (Ramphull, D., 2021). MANETs are vulnerable to several security vulnerabilities due to shared channel illumination, uncertain operational environment, restricted mobility, constantly changing device topology, and resource constraints (Sookhak, M., 2018).

The detection process that relies on abnormalities allows for the inclusion of interference resulting from the routine operations of a given system. Listing standard system output might be challenging due to the fluctuating nature of system activity (Mandal, B., 2020). The unconventional process is designed to identify newly occurring or inexplicable assaults but with a somewhat high risk of false positives. Signature-based intrusion detection systems are distinguished by utilizing distinctive patterns, such as byte sequences, in network traffic to identify potential attacks (Himeur, Y., 2021). The system's recognition is limited to established attack patterns and cannot detect emerging attacks that do not conform to existing trends.

Ensuring secure connectivity in MANETs poses significant challenges attributable to the absence of a permanent infrastructure and the intricate nature of network topology, among other factors. The concept of IDS is upheld by using cryptography and access control techniques, ensuring the maintenance of equilibrium. The system exhibits the ability to address and mitigate ongoing or imminent attacks through the implementation of automated detection and warning mechanisms. The concept of identification is stored in many types of IDS, including Host IDS (HIDS), application-based IDS, and Network IDS (NIDS). Being in a passive state, the IDS refrains from taking any preventive measures and focuses on detecting intrusions that activate an alert (Kenaza, T., 2021).

The intrusion prevention system safeguards the system against attacks that exploit node behavior. Intrusions are identified using data mining (DM) methodologies, with its primary categorization consisting of reinforcement learning, regression, classification, optimization, ensemble learning, rule-based decision-making, and clustering (Salo, F., 2018). Recently, there have been proposals for utilizing

both conventional machine learning methodologies and deep learning-based approaches in intrusion detection and avoidance.

Routing protocols have consistently served as the fundamental technology in both wired and wireless networks, making them a prominent area of research. This has led to their status as research hotspots (Sharma, V., 2017). In the context of MANETs, the significant mobility of nodes can result in prevalent route breaks. Consequently, this leads to periodic routing updates, causing a substantial increase in control overhead within the network. These route breaks can also pose challenges in achieving route convergence, resulting in a higher forwarding delay and packet loss rate. The routing protocol may sometimes become invalid due to these factors.

Establishing dependable and efficient networking among highly dynamic nodes necessitates the resolution of routing protocols as a crucial concern in MANETs (Vijayan, P., 2022). This study employs the Enhanced Particle Swarm Optimization (EPSO) algorithm to optimize security and routing mechanisms in MANETs. The components mentioned above encompass intrusion detection, which serves the purpose of recognizing and addressing security risks, as well as secure routing, which guarantees secure data transmission between network devices.

2 Related Works

MANETs are wireless networks where devices communicate directly without a central hub. They are flexible and diverse, but their dynamic and decentralized nature makes them vulnerable to security threats. In MANETs, data transmission and network operations security are crucial. This literature review examines MANET security research and advances, focusing on the "Optimization-driven Intrusion Detection and Secure Routing Algorithm."

Korir and Cheruiyot (2022) suggest a survey to assess MANET routing protocol security risks. Implementation involves collecting data from relevant literature and analyzing MANET routing protocols (Korir, F., 2022). MANET routing protocol security, vulnerabilities, and deficiencies are examined in the output values. A holistic analysis of security vulnerabilities helps researchers and practitioners find areas for improvement. The survey's breadth and MANET security concerns' constant evolution may limit this study's benefits.

Kaur and Kakkar (2022) propose a new routing security method for Vehicular Ad Hoc Networks. Their approach combines hybrid optimization and deep learning-based attack detection. The implementation phase includes creating a confidence-based routing algorithm, adding deep learning models to detect attacks, and evaluating the system in a VANET (Kaur, G., 2022). The output values include implementing a robust routing algorithm and assessing its security and efficiency. VANETs improve security and attack detection. VANETs have drawbacks like computational load and resource requirements.

Torky et al. (2022) propose a new drone charging system management method. The proposed method improves system scheduling and security with PSO and blockchain technology. Implementation included developing a scheduling algorithm, integrating blockchain technology for security, and deploying the system in drone charging stations (Torky, M., 2022). The values include a safe and efficient drone charging mechanism. Blockchain technology improves security and scheduling. However, blockchain integration has drawbacks like the complexity of the process and scalability issues.

In their 2022 study, Srinivas et al. proposed a novel cloud IDS solution. Their method improves IDS using virtual machine migration and deep recurrent neural networks. Implementation involves designing

and training the IDS, incorporating virtual machine migration techniques to prevent evasion, and deploying the system in the cloud. IDSs with high intrusion detection rates are included (Srinivas, B.V., 2022). This method improves intrusion detection and evasion prevention. However, moving virtual machines may increase resource overhead.

In their 2020 study, Islabudeen and Kavitha Devi propose a new method for improving MANET intrusion detection and prevention systems to prevent security attacks (Islabudeen, M., 2020). The technique involves creating and implementing a MANET-specific intrusion detection and prevention system. The results relate to a MANET-specific security system and its assessment during security attacks. MANETs enable customized security solutions. MANETs have drawbacks, particularly in scalability and flexibility.

In their 2022 study, Abdan and Seno proposed machine learning to detect MANET wormhole attacks. Implementation involves training machine learning models to identify and classify wormhole attacks and deploying the detection system in a MANET (Abdan, M., 2022). The system detects wormhole attacks and outputs values. This approach protects against wormhole attacks better. One drawback of this method is the possibility of false positives and the need for frequent model changes.

Alsarhan et al. (2021) propose a machine learning-based optimization strategy to improve VANET IDS performance using Support Vector Machines (SVM). Implementation involves creating an optimal IDS using machine learning and deploying it in a VANET (Alsarhan, A., 2021). A refined IDS and VANET performance assessment are output values. Machine learning models improve intrusion detection precision and effectiveness. However, this approach has drawbacks, particularly in terms of the resources needed to implement and maintain these models.

Srilakshmi et al. (2022) present a MANET-specific safe optimization routing method. The process includes creating and optimizing a secure routing algorithm (Srilakshmi, U., 2022). The algorithm is tested in a MANET environment during implementation. The output values include a custom safe routing method. Increased security improves routing efficiency and security. There may be overhead costs associated with implementing these security measures.

Due to their unique characteristics and vulnerabilities, MANET security is crucial. Integrating PSO into MANET intrusion detection and safe routing may improve security. Future studies should focus on pragmatic applications and comprehensive assessments to evaluate this methodology in real-world MANET contexts. As MANETs become increasingly important in many applications, researchers and practitioners prioritize their security.

3 Enhanced Particle Swarm Optimization-driven Intrusion Detection and Secure Routing Algorithm

Efficient routing in MANETs is crucial for optimizing the transportation of information from the source to the destination while minimizing information loss during the transmission phase. In addition, the EPSO algorithm has been designed to minimize power loss during transfer and improve the system's overall lifespan. The initial phase involves the execution of fuzzy clustering and CH selection, utilizing the maximum direct, indirect, and recent confidence values. Subsequently, the second step entails the detection of intruded nodes, employing a predetermined threshold value of 0.5mJ. Nodes with confidence values beyond a certain threshold are classified as normal, whereas those below this level are categorized as intruded. This method aims to protect the infiltrated node while guaranteeing the secure delivery of data from the source to the destination. The EPSO is utilized to select the optimal

paths, considering the desired target feature and the path's capacity, throughput, and communication. Fig. 1 depicts the proposed EPSO-IDSRA framework explicitly designed for MANETs. The EPSO algorithm is employed to fine-tune the optimal hops, resulting in a globally optimal solution with enhanced convergence rates.

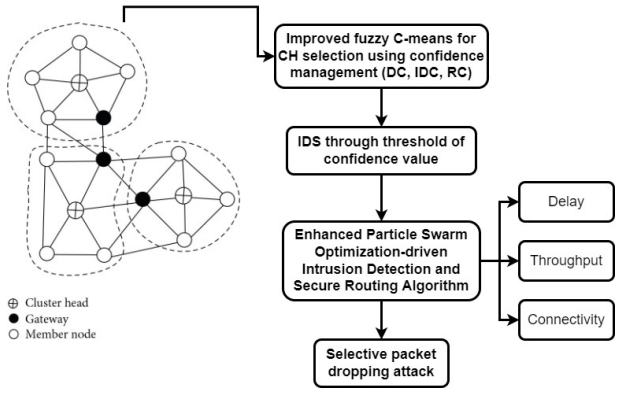

Figure 1: Proposed EPSO-IDSRA Framework Designed for MANETs

Confidence Management System for IDS

- **Direct Confidence (DC)**

The temporal extent is determined by the projected timeframe required for communication between the i^{th} node and the j^{th} destination. The measurement of DC involves calculating the discrepancy between the true and projected time intervals for the i^{th} node to verify the public key provided by the j^{th} destination. In this particular scenario, the transmission of information between the i^{th} node and the j^{th} destination has been shown as:

$$DC_i^j(\gamma) = \left(\frac{1}{3}\right)[DC_i^j(\gamma - 1) - \left[\frac{\gamma_{proj} - \gamma_{test}}{\gamma_{proj}}\right] + \varphi \quad (1)$$

The variable γ_{proj} represents the projected duration, whereas γ_{test} denotes the test duration required for the authentication of the public key. In other terms, γ_{proj} and γ_{test} represent the projected duration for the destination and the node to receive and transmit the public key. φ represents the variable of opinion for these nodes.

- **Indirect Direct Confidence (IDC)**

The opinion variable node is shown in line with the decision tree. However, the IDC scheme is employed to authenticate a node lacking an observer variable.

$$IDC_i^j(\gamma) = (\frac{1}{Nb})\sum_{i=1}^{Nb} DC_i^j(\gamma) \quad (2)$$

The variable Nb denotes the total number of neighbors of a given node.

- **Recent Confidence (RC)**

The determination of the RC is contingent upon the assessment of the DC and IDC, together with the crucial aspects of validity and acceptance of the destination or sink, which are provided throughout a specific period. The RC has been developed in the following manner:

$$RC_i^j(\gamma) = \alpha * DC_i^j(\gamma) + (1-\alpha) * IDC_i^j(\gamma) \quad (3)$$

Where $\alpha = 0.35$, $RC_i^j, DC_i^j \; and \; IDC_i^j$ denotes the RC, DC, and IDC values, respectively.

The Selection of CH Using the Fuzzy Clustering (FC) Method

Engaging in social interactions with the fuzzy clustering technique allows for the assignment of each member of a cluster to several degrees of "fuzziness." The selection of CHs in a fuzzy clustering method is determined by identifying the nodes with the highest level of node confidence. To reciprocate this shared trust, the node that receives the most optimal CH returns it to the other node. The applicability of FC is constrained by its dependence on overlapping numerical values, hence limiting its usage to a restricted set of patients' records. Consequently, assigning patient data points to a singular CH is inevitable. FC is a method employed for data reduction. The concept is articulated as:

$$F_f = \sum_{i=1}^{Nb} \sum_{k=1}^{Ch} v_{ik}^f * \|n_i - H_k\|^2 \;\; 1 \le f \le \infty \quad (4)$$

The proposed location of the i^{th} node from the MANET is denoted as n_i. In this context, H_k represents the k^{th} CH, Ch represents the total number of CHs and specifies the Euclidean distance between the i^{th} node and the k^{th} CH. The mathematical expression represents the fuzziness indicator $\{f|f \in R > 1\}$. The fuzzifier f, designated by the symbol F_f, is defined by the purpose function. CHs are assigned to nodes inside a cluster based on their proximity to the CH, as determined by the shortest Euclidean distance.

For a node to attain the status of a CH, it is necessary to satisfy the maximizing function (Mx) as defined below:

$$Mx = \left(\frac{1}{3}\right)[D + I + R] \quad (5)$$

The variables D, I, and R represent the relative direct, indirect, and recent confidence levels. The D, I, and R values may be calculated using equations (1), (2), and (3).

Comparison of Threshold Values for Recognizing Intruded Nodes

In an alternative formulation, intruders are identified by a sink node, which relies on information transmitted to it by other nodes via the CHs. This information is contingent upon network trust factors. After identifying the invading node, the network proceeds to prevent any attempts made by the node to establish communication with the other network components. The presence of intruders in the sink node may be detected by implementing a predetermined threshold value within the sink node set at 0.5mJ. The primary objective of intrusion detection is to provide a secure network connection while minimizing energy use and transmission latency.

Enhanced Particle Swarm Optimization (EPSO) Algorithm

Kennedy and Eberhart introduced the PSO algorithm as a numerical technique for efficiently solving optimization problems. This algorithm drew inspiration from the collective behavior of birds in a flock, where each bird was represented as a particle confined to a hyperdimensional search space (Fig. 2). The particle evaluates its velocity for the following instant in every iteration using its present personal best (P_{best}) and present global best (G_{best}) values, and then it changes its location.

The arrangement of components inside the search area can be modified and adjusted according to the social psychological inclinations exhibited by the participants. Two factors within information/swarm

encounters impact the mobility of components inside the swarm. The phenomenon of swarming returning to previously successful locations in the solution space can be attributed to the emergence of social behavior. Equations (6) and (7) are employed to calculate the velocity (V_{node}) and node location (L_{node}) of each element.

$$V_{i,l}(\gamma+1) = W_{i,l} + KE_1 Ar_1 \left(PbA_{i,l}(\gamma) - G_{i,l}(\gamma)\right) + KE_2 Ar_2 \left(PbB_{i,l}(\gamma) - G_{i,l}(\gamma)\right) \quad (6)$$

$$G_{i,l}(\gamma+1) = G_{i,l}(\gamma) + V_{i,l}(\gamma+1) \quad (7)$$

The notation $V_{i,l}(\gamma+1)$ denotes the velocity of element i at iteration l, whereas $G_{i,l}(\gamma+1)$ represents the location of element i at iteration l. Tot is the total number of iterations. Moreover, $W_{i,l}$ represents the inertia weight employed to mitigate the impact of the previous velocity logarithm. The first element, KE_1, represents the awareness knowledge component, while the second element, KE_2, pertains to the gregarious learning aspect. Additionally, Ar_1 and Ar_2 are numerical variables inside the solution space ranging from 0 to 1, which are utilized to regulate the capacity for storing information. In alternative terms, the objective is to monitor or eliminate excessive velocity by upholding the Velocity component (V_{node}) within the specified range of $[V_{min}, V_{max}]$. The PSO technique is utilized to determine the optimal location for each piece inside a given swarm. If the number of roles is increased at this juncture, my advancement will be impeded. Consequently, EPSO showcases its effectiveness and superiority in problem-solving.

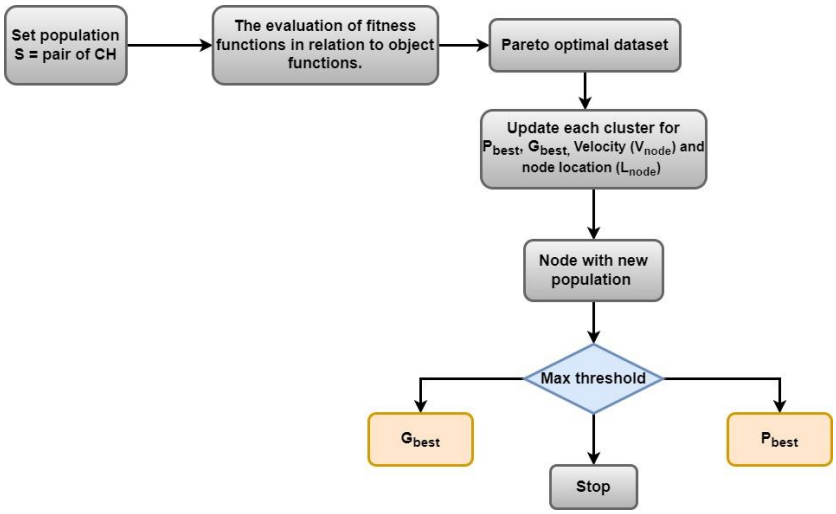

Figure 2: Flowchart of EPSO Routing in MANET

The EPSO algorithm in this study investigates the disposal solution set and efficiently generates the external archives set, therefore serving as a competitive approach. To begin the process, select one element G from the population S; ideally, opt for the initial element inside the population. Next, the objective function of Pareto dominance relations is employed to compare each population element with the objective function's value. This comparison is conducted by subtracting G from the set S. If GH, the element is removed from the population S; if $G = H$, the element persists inside the population S. Ultimately, let N be the set $NU\{g\}$ until S reaches $threshold$, at which juncture N becomes the non-dominant solution set that necessitates rectification. The approach is employed when the non-dominant solution set converges with the external archive set. The frequency of algorithmic execution lowers proportionally to eliminating additional elements, resulting in a notable reduction in method complexity and a corresponding improvement in search velocity.

4 Results and Discussion

The experimental data consists of a total of 50 nodes that are distributed throughout a geographical region of 2 kilometers. Simulation was conducted using a network where malevolent nodes constituted a percentage ranging from 10% to 50% of the total nodes. Simulation has been done using Network Simulator 2 software. Table 1 shows the parameters used for the simulation.

Table 1: Simulation Parameters

Parameter	Value
Data transfer rate	3Mbps
Transmission power	50mW
Velocity of the node	5ms
The energy threshold of the node	0.5mJ
Route timeout	5s
Interval of hello message	Uniform distributed

The current investigation methodologies, encompassing attacks in nodes, are evaluated about the suggested procedure using the following criteria: latency, energy consumption, throughput, and detection rate.

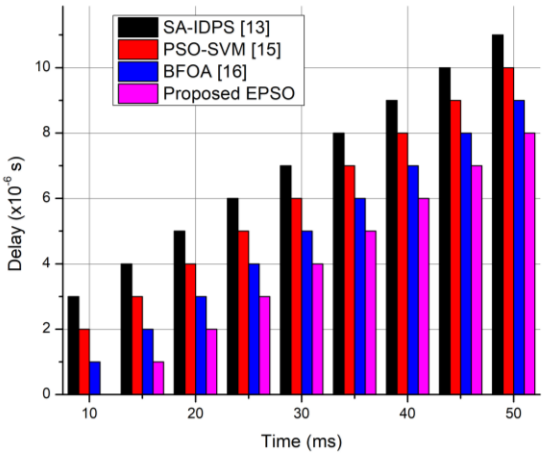

Figure 3: Comparative Evaluation of the Proposed EPSO-IDSRA in Terms of Delay

Fig. 3 presents a significant comparison of delay values, measured in microseconds, for different IDSRA throughout various time intervals, measured in milliseconds. The EPSO under consideration consistently exhibits the lowest level of delay throughout all measured time intervals, commencing at 0 microseconds and steadily rising with time. On the other hand, the currently available algorithms, specifically SA-IDPS (Islabudeen, M., 2020), PSO-SVM (Alsarhan, A., 2021), and BFOA (Srilakshmi, U., 2022), demonstrate elevated starting delay values and encounter subsequent delays that increase with time. The comparison mentioned above highlights the effectiveness of the Proposed EPSO in reducing latency, a crucial aspect in MANETs, hence enhancing the transmission of real-time data and the responsiveness of the network.

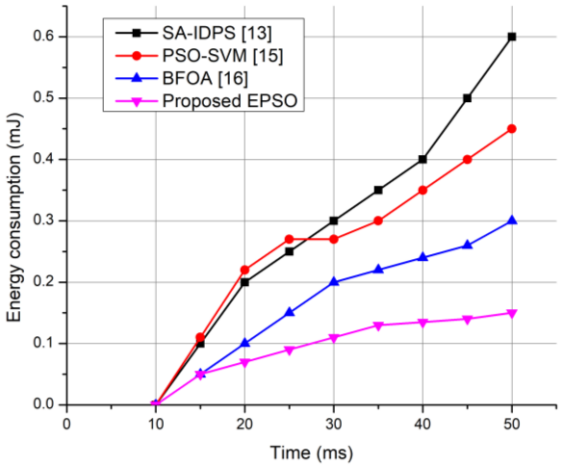

Figure 4: Comparative Evaluation of the Proposed EPSO-IDSRA in Terms of Energy Consumption

Fig. 4 provides a thorough analysis of energy consumption values, measured in millijoules, for several IDSRA over varying time, measured in milliseconds. The Proposed EPSO algorithm is particularly noteworthy for its exceptional energy efficiency, continuously demonstrating the lowest energy consumption over time. On the other hand, the SA-IDPS, PSO-SVM, and BFOA algorithms exhibit comparatively elevated levels of beginning energy consumption, with specific algorithms seeing notable increments as time progresses. The present investigation highlights the efficacy of the EPSO in mitigating energy usage, a critical aspect in extending the operational longevity of devices in MANETs and augmenting their sustainability.

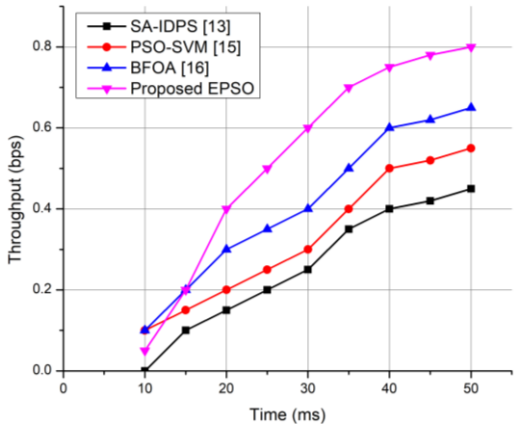

Figure 5: Comparative Evaluation of the Proposed EPSO-IDSRA in Terms of Throughput

Figure 5 presents a detailed analysis of throughput numbers, measured in bits per second (bps), for IDSRA throughout various time intervals, measured in milliseconds. The proposed EPSO algorithm's superiority in throughput is clearly apparent. Over time, the throughput of the proposed EPSO algorithm exhibits a consistent upward trend, culminating in a maximum value of 0.8 bits per second (bps) at a latency of 50 ms. This notable achievement is evidence of the algorithm's exceptional efficacy in facilitating data transmission. On the other hand, the currently available algorithms, such as SA-IDPS, PSO-SVM, and BFOA, have comparatively lower starting throughput values, with certain algorithms displaying slower rates of increase as time progresses. The comparison, as mentioned above, highlights the capacity of the proposed EPSO to enhance data throughput, which is a crucial element in enhancing the effectiveness and promptness of MANETs.

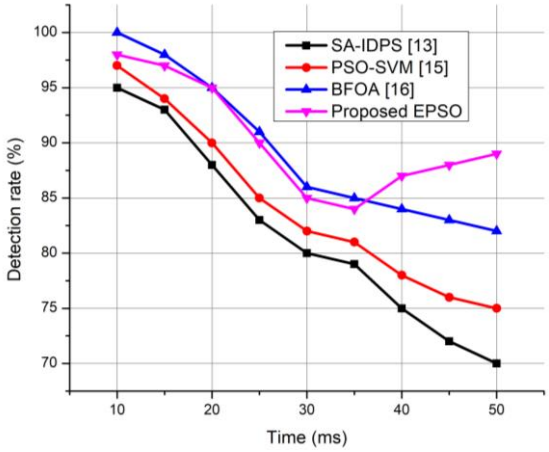

Figure 6: Comparative Evaluation of the Proposed EPSO-IDSRA in Terms of Detection Rate

Fig. 6 compares detection rates, shown as percentages, for several IDSRA over various time intervals, measured in milliseconds. The EPSO that has been proposed consistently demonstrates the highest detection rate across various times. Notably, it peaks at 98% at 10 ms and then decreases to 89% at 50 ms. On the other hand, the SA-IDPS, PSO-SVM, and BFOA algorithms exhibit marginally lower initial detection rates, accompanied by diverse rates of increase over time. As mentioned above, the comparison underscores the proposed EPSO's heightened efficacy in intrusion detection, a vital facet of security inside MANETs. This, in turn, strengthens the network's resilience and dependability.

5 Conclusion

The present study utilizes the Enhanced Particle Swarm Optimization-driven Intrusion Detection and Secure Routing Algorithm (EPSO-IDSRA). The present study proposes using an Enhanced Particle Swarm Optimization approach (EPSO) to establish confidence-based, safe, and energy-efficient routing in MANETs. The EPSO approach determines the most optimal hops for improving the routing process. The first phase is initiating the fuzzy clustering method, selecting CHs by evaluating their indirect, direct, and recent confidence values. Moreover, the determination of value nodes depended on the evaluation of degrees of confidence.

Moreover, the CHs play a crucial role in facilitating multi-hop routing. The selection of the ideal route relies on the expected protocol, which considers several aspects such as latency, throughput, and detection rates within the specified region, to identify the most advantageous pathways. The EPSO technique, which was introduced to ensure secure routing (at a time interval of 50 milliseconds), resulted in an energy consumption of 0.15 millijoules, a latency of 0.008 milliseconds, a throughput of 0.8 bits per second, and a detection rate of 89%.

References

[1] Abdan, M., & Seno, S.A.H. (2022). Machine learning methods for intrusive detection of wormhole attack in mobile ad hoc network (MANET). *Wireless Communications and Mobile Computing*, *2022*, 1-12.

[2] Alsarhan, A., Alauthman, M., Alshdaifat, E.A., Al-Ghuwairi, A.R., & Al-Dubai, A. (2021). Machine Learning-driven optimization for SVM-based intrusion detection system in vehicular ad hoc networks. *Journal of Ambient Intelligence and Humanized Computing*, 1-10.

[3] Dhindsa, K.S., & Singh, K. (2021). Entropy-based DDoS Attack Detection in Cluster-based Mobile Ad Hoc Networks. *Adhoc & Sensor Wireless Networks*, *49*.
[4] Himeur, Y., Ghanem, K., Alsalemi, A., Bensaali, F., & Amira, A. (2021). Artificial intelligence-based anomaly detection of energy consumption in buildings: A review, current trends and new perspectives. *Applied Energy*, *287*.
[5] Islabudeen, M., & Kavitha Devi, M.K. (2020). A smart approach for intrusion detection and prevention system in mobile ad hoc networks against security attacks. *Wireless Personal Communications*, *112*, 193-224.
[6] Kaur, G., & Kakkar, D. (2022). Hybrid optimization enabled trust-based secure routing with deep learning-based attack detection in VANET. *Ad Hoc Networks*, *136*.
[7] Kenaza, T. (2021). An ontology-based modelling and reasoning for alerts correlation. *International Journal of Data Mining, Modelling and Management*, *13*(1-2), 65-80.
[8] Korir, F., & Cheruiyot, W. (2022). A survey on security challenges in the current MANET routing protocols. *Global Journal of Engineering and Technology Advances*, *12*(01), 078-091.
[9] Mandal, B., Sarkar, S., Bhattacharya, S., Dasgupta, U., Ghosh, P., & Sanki, D. (2020). A review on cooperative bait based intrusion detection in MANET. *Proceedings of Industry Interactive Innovations in Science, Engineering & Technology (I3SET2K19)*.
[10] Ramphull, D., Mungur, A., Armoogum, S., & Pudaruth, S. (2021). A review of mobile ad hoc NETwork (MANET) Protocols and their Applications. *In IEEE 5th international conference on intelligent computing and control systems (ICICCS)*, 204-211.
[11] Salo, F., Injadat, M., Nassif, A.B., Shami, A., & Essex, A. (2018). Data mining techniques in intrusion detection systems: A systematic literature review. *IEEE Access*, *6*, 56046-56058.
[12] Sharma, V., & Kumar, R. (2017). G-FANET: an ambient network formation between ground and flying ad hoc networks. *Telecommunication Systems*, *65*(1), 31-54.
[13] Sookhak, M., Tang, H., He, Y., & Yu, F.R. (2018). Security and privacy of smart cities: a survey, research issues and challenges. *IEEE Communications Surveys & Tutorials*, *21*(2), 1718-1743.
[14] Srilakshmi, U., Alghamdi, S.A., Vuyyuru, V.A., Veeraiah, N., & Alotaibi, Y. (2022). A secure optimization routing algorithm for mobile ad hoc networks. *IEEE Access*, *10*, 14260-14269.
[15] Srinivas, B.V., Mandal, I., & Keshavarao, S. (2022). Virtual machine migration-based Intrusion Detection System in cloud environment using deep recurrent neural network. *Cybernetics and Systems*, 1-21.
[16] Torky, M., El-Dosuky, M., Goda, E., Snášel, V., & Hassanien, A.E. (2022). Scheduling and securing drone charging system using particle swarm optimization and blockchain technology. *Drones*, *6*(9), 1-26.
[17] Vijayan, P., Anbalagan, P., & Selvakumar, S. (2022). An Ensembled Optimization Algorithm for Secured and Energy Efficient Low Latency MANET with Intrusion Detection. *Journal of Internet Services and Information Security (JISIS), 12*(4), 156-163.

Authors Biography

Nikitina Vlada, Associate Professor, PhD in Philology. Works at the Peoples' Friendship University of Russia. Research interests include artificial intelligence, language consciousness, methodology of teaching foreigners. Author of methodological textbooks, articles on language consciousness, intellectual security, problems of teaching foreigners in Russian universities.

Raúl A. Sánchez-Ancajima, Degree in Mathematics from the Faculty of Sciences of the National University of Piura (UNP), Peru (2004). He obtained a Master's degree in Science with a major in Applied Mathematics from the National University of Piura (UNP), Peru (2011). D. in Mathematics from the National University of Trujillo (UNT), La Libertad, Peru (2021), with an internship at the University of Sao Paulo (USP) in Brazil.

Miguel Ángel Torres Rubio, Degree in secondary education, specializing in philosophy and religion. Master in education with mention in educational and administrative management of educational centers. Doctor in education. Specialization in quality management in education. Diploma: expert in curriculum management and competency-based training projects.

Walter Antonio Campos- Ugaz, Bachelor in Primary Education; Bachelor in Secondary Education, specializing in Mathematics and Computer Science; Agricultural Engineer; Bachelor in Civil Engineering; Master in University Teaching and Research; Master in Integrated Water Resources Management and Master in Quality Assurance; Doctor in Educational Sciences; Doctor in Public Management and Governance and Doctor in Environmental Sciences.

Anibal Mejía Benavides, Bachelor's Degree in Education, graduated from Universidad Nacional Pedro Ruiz Gallo, Lambayque, Br. Systems and Computer Engineering; Master's Degree in Educational Management and Teaching, Doctor in Educational Administration. Specialization in Management in Scientific Research Methodology, and Evaluation, Accreditation and Certification of Educational Quality.

María Del Rocío Hende-Santolaya, Doctor from the Universidad Particular de Chiclayo. ALTAGORA Graduate School, with extensive experience in teaching at the university level, both undergraduate and graduate. She currently serves as director of the School of Education-USAT.

Jacqueline C. Ponce-Meza, Educational Psychologist, Master's Degree in Psychology with mention in Psychoeducational Intervention in Neurodevelopmental Disorders. Master in Virtual Teaching, External Consultant in monitoring and evaluation of pedagogical teaching practices.