Journal of Optimization in Industrial Engineering

Vol.18, Issue 2, Summer & Autumn 2025, 161-170

Research Article

A hybrid metaheuristic approach to optimize intrusion detection and malicious node identification in mobile ad hoc networks

Yahya Shahin Barsim Barsim [1], Azam Andalib [2,*], Hossein Azgomi [3,*], Seyed Ali Sharifi [4]

1. Computer Engineering Department, Urmia University, Urmia, Iran.
2. Department of Computer Engineering, Ra.C., Islamic Azad University, Rasht, Iran.
3. Department of Computer Engineering, Ra.C., Islamic Azad University, Rasht, Iran.
4. Department of Computer Engineering, Bon.C., Islamic Azad University, Bonab, Iran.

https://doi.org/10.71720/joie.2025.1217274

Received: 08 September 2025
Revised: 04 October 2025
Accepted:14 October 2025

Abstract

An Intrusion Detection System (IDS) is a vital security mechanism that monitors network or system activities to detect and mitigate malicious behaviors. By identifying threats such as unauthorized access or sabotage, the IDS responds promptly to prevent further compromise, ensuring system integrity. These vulnerabilities are especially pronounced in mobile ad hoc networks (MANETs), where the dynamic topology and lack of centralized control make robust authentication and key agreement critical components of network security. Conventional two-factor authentication schemes, while widely used, often fall short against attacks such as smart card loss, offline password guessing, identity spoofing, and replay attacks. These weaknesses expose networks to significant risks, necessitating advanced detection mechanisms. To address these challenges, this paper proposes a novel hybrid metaheuristic approach integrated with elliptic curve cryptography (ECC) for enhanced two-factor authentication in MANETs. The proposed method optimizes malicious node detection by combining metaheuristic optimization techniques with ECC's lightweight, secure key exchange. This approach significantly improves detection accuracy, increases the number of active nodes, and optimizes residual energy, thereby enhancing both security and operational efficiency. Simulation results demonstrate that the proposed system outperforms existing methods in identifying malicious nodes while maintaining energy efficiency, making it particularly suited for resource-constrained MANETs. By addressing the limitations of traditional authentication schemes, this hybrid approach offers a robust solution for securing dynamic and vulnerable network environments, paving the way for more resilient intrusion detection systems in dynamic networks.

Keywords:
Mobile Ad Hoc Networks, Intrusion Detection System, Two-Factor Authentication and Elliptic Curve Cryptography

Citation:
Shahin Barsim Barsim, Y., Andalib, A., Azgomi , H. & Sharifi, S.A. (2025). A hybrid metaheuristic approach to optimize intrusion detection and malicious node identification in mobile ad hoc networks. *Journal of Optimization in Industrial Engineering*, 18(2), 161- 170. https://doi.org/10.71720/joie.2025.1217274

* **Corresponding Author:**
Azam Andalib
Department of Computer Engineering, Ra.C., Islamic Azad University, Rasht, Iran.
E-Mail: **Azam.Andalib@iau.ac.ir**
Hossein Azgomi
Department of Computer Engineering, Ra.C., Islamic Azad University, Rasht, Iran.
E-Mail: **Hossein.Azgomi@iau.ac.ir**

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC) license (https://creativecommons.org/ licenses/by/4.0/).

1. Introduction

An Intrusion Detection System (IDS) is a vital security mechanism that monitors computer networks to detect and mitigate malicious activities, such as unauthorized access, data collection, or port scanning, which could compromise system integrity or enable sabotage (Chander et al., 2019). IDSs can be classified based on criteria like detection methods (e.g., signature-based or anomaly-based) or deployment types (e.g., host-based or network-based), as shown in Figure 1.

Anomaly-based intrusion detection systems (IDSs) identify malicious behaviors by distinguishing them from normal system activities. When network traffic exceeds a predefined threshold separating normal and abnormal behavior, the system generates an alert for a potential attack, though this approach often results in a high false alarm rate. In contrast, signature-based IDSs rely on patterns of known intrusions, transforming the detection process into a classification task that accurately identifies learned attack patterns with a low false alarm rate. Hybrid IDSs combine these approaches, first using signature-based techniques to detect known attacks and then applying anomaly-based methods to identify novel attacks absent from the database (Chander, 2020). Host-based IDSs (HIDS), installed on individual systems, monitor only the network interface card's information exchange. This method is costly, lacks compatibility with all operating systems, and often fails to detect widespread network attacks. Conversely, Network-based IDSs (NIDS) analyze both incoming packets and transmitted data, offering broader attack detection (Chander, 2020b). IDSs can also be categorized by processing structure: centralized (processing occurs on a single system) or distributed (each system processes packets independently). Additionally, they are classified by response behavior—active (e.g., redirecting attackers to a honeypot) or passive—and by data sources used for detection. Temporal aspects further divide IDSs into real-time (continuous packet examination) or periodic (snapshot-based analysis) systems (Aluvala et al., 2016).

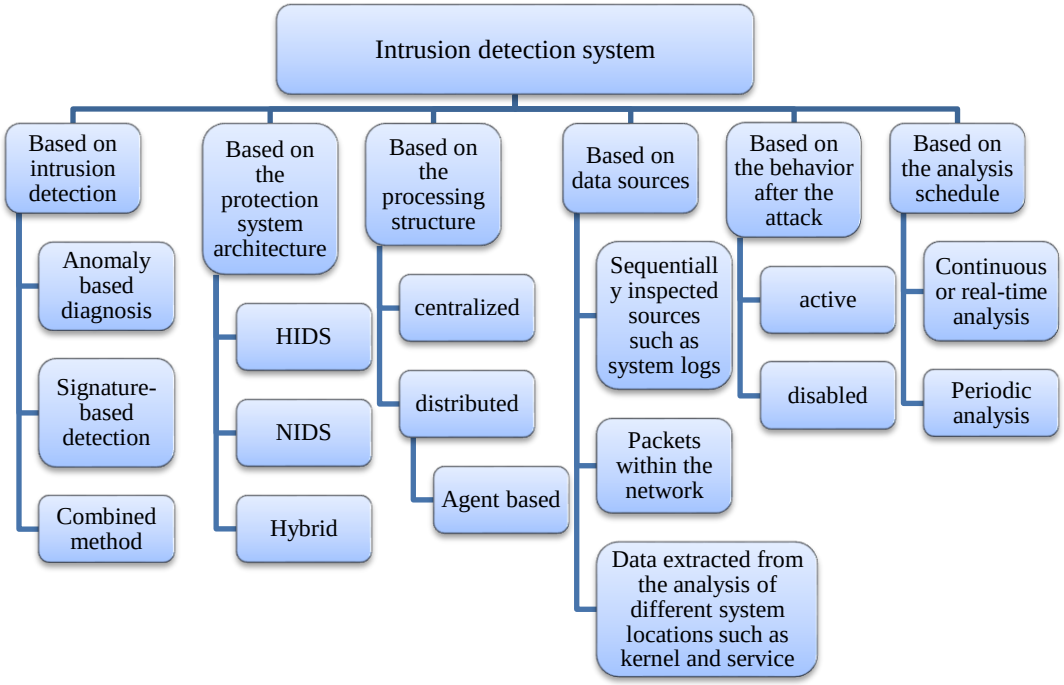

Fig. 1. Different categories of intrusion detection systems

Mobile ad hoc networks (MANETs) face significant challenges in secure service usage and information exchange due to their reliance on insecure wireless media, which are vulnerable to attacks such as eavesdropping, spoofing, data modification, and deletion. Ensuring security, data integrity, and user anonymity during transmission is paramount. Various remote authentication schemes have been proposed, including single-factor (password-based), two-factor (password and smart card), and three-factor (password, smart card, and biometrics) authentication, alongside key agreement protocols (Sadri & Asaar, 2021). Three-factor authentication is generally more secure due to biometrics' unique properties, such as resistance to spoofing and their constant association with the user, combined with a large state space that complicates unauthorized access. However, implementing authentication in insecure environments risks vulnerabilities, including:

- Accessing unauthorized stored data via stolen smart cards.
- Eavesdropping, modifying, deleting, retransmitting, or redirecting exchanged messages.
- Discovering passwords and user IDs due to limited state spaces, solvable in polynomial time.
- Leaking confidential information by legitimate users to external attackers through insider attacks.

To address these challenges, this paper proposes a hybrid metaheuristic approach for detecting malicious nodes in intrusion detection systems, leveraging two-factor authentication and key agreement based on elliptic curve cryptography (ECC) in MANETs. Users authenticate and establish keys via the Session Initiation Protocol (SIP) to access servers securely. This approach effectively establishes a robust framework for securing dynamic, resource-constrained MANETs by enhancing detection accuracy, node activity, and energy efficiency, as validated through simulations.

2. Literature Review

The rapid proliferation of emerging technologies, such as the Internet of Things (IoT), wireless sensor networks (WSNs), vehicular ad hoc networks (VANETs), and cloud-assisted systems, has driven innovation while introducing significant security and performance challenges. Research in authentication, intrusion detection, cryptography, and optimization-based solutions is critical to ensuring system integrity, reliability, and efficiency. This review synthesizes recent advancements in authentication protocols, intrusion detection frameworks, and optimization-driven approaches across IoT, VANETs, and MANETs, emphasizing lightweight cryptographic techniques, meta-heuristic optimization, and artificial intelligence (AI)-based security solutions.

Intrusion detection systems (IDS) are pivotal for securing dynamic network environments. Genetic algorithm-based feature selection, as employed by Xue et al. (2021), Jiang (2020), Wu et al. (2021b), Far et al. (2021), and Meshram et al. (2021), enhances IDS efficiency by automatically selecting relevant features and reducing dimensionality. These approaches often combine genetic algorithms with support vector machines (SVM) or other classifiers to improve real-time intrusion detection, though Far et al. (2021) noted high false positive rates requiring classifier modifications. Similarly, Kantola et al. (2020) optimized SVM parameters using genetic algorithms alongside kernel principal component analysis (KPCA) for preprocessing, achieving robust intrusion detection. Naveena and Reddy (2016) and Shrivastava et al. (2015) also utilized genetic algorithms for IDS in MANETs, leveraging linear genetic programming and evaluation theory to model and classify network intrusions effectively.

Deep learning-based IDS approaches have gained traction for their robustness. Shams et al. (2023) developed a flow-based IDS for VANETs using a Context-Aware Feature Extraction-Based Convolutional Neural Network (CAFECNN), which collects data from vehicles and Roadside Units (RSUs) with synthetic datasets generated via Network Simulator 3 (ns-3) and Simulation of Urban Mobility (SUMO). Similarly, dos Santos et al. (2025) proposed IoTSafe, a fog-based IoT security platform integrating deep learning for attack detection, achieving 99.57% accuracy and 99.66% precision. Saviour and Samiappan (2023) proposed a Chronological Anticoronavirus Optimization-based Deep Residual Network (CACVO-DRN) for intrusion detection, combining optimization and deep learning for high performance. Bagirathan et al. (2025) introduced an Ensemble Long Short-Term Memory (ELSTM) model for VANETs, evaluating trust and node parameters like data forwarding rate and link quality to detect malicious nodes with improved accuracy. Deivakani et al. (2024) applied a Precise Probability Genetic Algorithm (PPGA) and Stacked Recurrent Long Short-Term Memory (SRLSTM) to enhance attack detection in MANETs using features like Received Signal Strength Indication (RSSI) from NSL-KDD and CICIDS-2017 datasets. Sarangi et al. (2025) utilized a Residual Recurrent Neural Network (Res-RNN) with Enhanced African Rhinoceros Optimization (EARO) for trust-aware multicast routing in MANETs, outperforming baseline models like DNN and 1DCNN. Mansouri et al. (2025) proposed a federated learning and blockchain-based IDS for VANETs, enabling privacy-preserving distributed model training.

Authentication remains a cornerstone of network security. Wang et al. (2018) introduced a password-based remote user authentication scheme, highlighting vulnerabilities in single-factor authentication. Gupta et al. (2021) proposed a two-factor authentication scheme using passwords and smart cards, requiring server validation to enhance security. However, Sharma and Nidhi (2020) noted vulnerabilities in similar pass-card-based schemes to impersonation and spoofing attacks. Wazid et al. (2017) reviewed authentication schemes, identifying persistent vulnerabilities to temporary information threats and password invalidation issues. Wang et al. (2025) proposed a UAV–vehicle cooperative authentication scheme for VANETs, using Trusted Centers of Authority to mitigate single points of failure and reduce computational overhead.

Optimization algorithms enhance routing and security in dynamic networks. Nivedita et al. (2025) developed a cluster-based routing protocol for MANETs using density-based Adaptive Soft Clustering (DAS) and Elk Herd Optimization (EHO) for stable cluster head selection. Their ASGO-TSPCPTrustNet algorithm calculates multi-attribute trust values and optimizes routes using the Adaptive Snow Geese Optimization Algorithm (ASGO), integrated with a Stacked Convolutional Sequential Autoregressive Encoding Network (SCSAEN) for intrusion detection. Huang et al. (2025) introduced a lightweight wormhole detection algorithm for MANETs using the Address Resolution Protocol (ARP) with the AODV protocol, achieving high detection rates with minimal computational overhead. Prasad et al. (2023) proposed a comprehensive MANET IDS framework with a fuzzy logic-based performance reliability evaluation model, addressing trade-offs in statistical performance due to imbalanced sample ratios. Qi and Chen (2021) developed an efficient rule generator for denial-of-service attacks, though its applicability is limited to specific attack types. Table 1 summarizes some of the researches.

The reviewed studies highlight significant progress in securing dynamic network environments like IoT, VANETs, and MANETs through advanced intrusion detection, authentication protocols, and optimization-driven routing. However, critical gaps remain, particularly in MANETs, where dynamic topologies and resource constraints heighten vulnerabilities to attacks such as smart card loss, offline password guessing, identity spoofing, and replay attacks. Conventional two-factor authentication schemes often fail to provide robust protection, and existing intrusion detection systems struggle to balance high detection accuracy with energy efficiency in resource-limited settings.

To address these challenges, this study proposes a novel hybrid metaheuristic approach integrated with elliptic curve cryptography for enhanced two-factor authentication in MANETs. By combining metaheuristic optimization with lightweight, secure key exchange, the proposed method improves malicious node detection, boosts detection accuracy, increases active node counts, and optimizes residual energy. Simulation results demonstrate superior performance over existing methods, offering a robust and efficient solution for securing dynamic, resource-constrained networks and advancing resilient intrusion detection systems.

Table 1
Comparison of Different Authentication Methods and User Authenticity

Authors	Pros	Cons
Wazid et al. (2017)	Comprehensive analysis of authentication vulnerabilities	Identifies persistent threats and password invalidation issues
Islam et al. (2017)	Provides dynamic identity for enhanced user authentication	Vulnerable to offline password guessing, impersonation, denial of service; lacks session key provision
Wang et al. (2018)	Simple and lightweight authentication process	Susceptible to security pitfalls in single-factor authentication
Gope et al. (2018)	Computationally efficient due to hash function use	Susceptible to forward secrecy issues and offline password guessing
Yang et al. (2019)	Facilitates server-side validation	Vulnerable to impersonation, insider threats, and server spoofing
Sharma & Nidhi (2020)	Resistant to smart card theft threats	Vulnerable to user impersonation, server spoofing, offline password guessing, insider threats
Wang et al. (2020)	Simplifies user authentication process	Lacks impersonation resistance, user tracking, and password change verification
Gupta et al. (2021)	Enhances security through dual verification	Requires physical card reader, increasing complexity
Zou et al. (2022)	Supports smart card integration for enhanced security	Susceptible to smart card theft; does not ensure user anonymity
Wang et al. (2022)	Lightweight design for resource-constrained environments	Lacks resistance to offline password guessing attacks
Saviour & Samiappan (2023)	High performance in secure authentication	Complex implementation due to deep learning integration
dos Santos et al. (2025)	High accuracy (99.57%) and precision (99.66%) in secure authentication	Requires fog infrastructure, increasing deployment complexity
Wang et al. (2025)	Mitigates single points of failure, reduces computational overhead	Dependent on Trusted Centers of Authority for implementation

3. Methodology

In this section, a hybrid meta-heuristic approach is presented using local information collected by a Particle Swarm Optimization algorithm based on genetic algorithms for identifying malicious nodes for intrusion detection based on two-factor authentication using elliptic curve cryptography in mobile ad hoc networks. This approach not only detects intrusions but also reduces energy consumption, allowing malicious packets to be removed from the network in the shortest possible time.

In the Particle Swarm Optimization algorithm, each particle has a position, a velocity vector, and a fitness function (Daneshvar et al., 2021). The velocity vector determines the movement direction of the particle, while the fitness function specifies the new position of the particle. Over time, particles accelerate towards those with higher fitness criteria that are in the same communication group. Assuming the search space is D-dimensional, the i-th particle and its velocity are represented by D-dimensional vectors as $X_i = (x_{i1}, x_{i2}, \dots, x_{iD})^T$ and $V_i = (v_{i1}, v_{i2}, \dots, v_{iD})^T$ respectively, while the best position seen among the previous positions of the i-th particle is denoted as $P_i = (p_{i1}, p_{i2}, \dots, p_{iD})^T$. The parameter g is also used to represent the best particle in the population. Therefore, the best position seen in the entire population is represented by the vector $P_g = (p_{g1}, p_{g2}, \dots, p_{gD})^T$. The update of the velocity and position of particles at each stage of the population's movement is as equation (1):

$$\begin{aligned} v_{id}(t+1) &= w.v_{id}(t) + c_1.\mathrm{rand}\big(p_{id}(t) - x_{id}(t)\big) \\ &\quad + c_2.\mathrm{rand}\left(p_{gd}(t) - x_{id}(t)\right) \\ x_{id}(t+1) &= x_{id}(t) + v_{id}(t+1) \\ i &= 1,2,\dots,N \quad , \quad d = 1,2,\dots,D \end{aligned} \tag{1}$$

In the genetic algorithm, a population of chromosomes is initially created randomly, and their fitness is calculated (Daneshvar et al., 2020; Homayounfar et al., 2020; Salahi et al., 2020; Salahi et al., 2021). Then, through crossover and mutation operators, a new population with higher fitness values is generated (Nahavandi et al., 2021; Tavakol et al., 2023). The intrusion detection system consists of two main phases: the first phase involves rule generation using the audit data network, and the second phase involves selecting the responses with the highest fitness value and the best set of rules for identifying intruders. The reason for choosing the combined approach of particle swarm algorithms and genetic algorithms in this paper is that the particle swarm algorithm finds the best global value, which can influence the movement of other particles and lead to rapid convergence (Asgharizadeh et al., 2022), while the genetic algorithm can share information among chromosomes (Kazemi et al., 2024). Thus, this combination enhances the ability to search globally and escape local optimal solutions, contributing to better results. A parent generated during the particle swarm algorithm is used to produce another parent using crossover and mutation operators in the genetic algorithm, and ultimately, the next repeated parent is generated through elitist selection. The K-means method is used to dynamically adapt cluster centres and improve convergence. In this paper, the population size (number of particles), inertia weight (W), maximum speed (Vmax), learning factors (c1, c2), crossover rate, and mutation rate are initialized, and the fitness value of each particle for survival in the network is calculated based on variables such as location, energy, network connectivity[1] (number of neighbors), and the number of survival occurrences of each particle[2].

The two-factor authentication-based intrusion detection approach using elliptic curve cryptography in mobile ad hoc networks is designed to invoke the particle swarm optimization algorithm based on genetic algorithms for identifying malicious nodes. It includes five phases:

[1] Node Degree

[2] Head Count

1. System Initialization: including the selection of an elliptic curve equation and a base point by the server, selection of a private key and a public key by the server, selection of three one-way mixed equations by the server, and server publication.
2. Registration Phase: generating a random secret number and sending it along with the user ID (ID_u) and identity password ($H_1(PW_u\|b_u) * P$) by the user to the server over a secure communication channel, server verification of user ID and identity password, calculation $AID_u = (q_s + 1) * H_1(PW_u\|b_u) * P$ and $BID_u = H_2(H_1(ID_u)\|H_1(PW_u\|b_u) * P)$ using one-way mixed functions by the server, storing $\{AID_u, BID_u\}$ in a secure channel by the server, and receiving the smart card containing $\{AID_u, BID_u, b_u\}$ by the user.

3. Login Phase: placing the smart card in the card reader by the user, calculating $BID_u = H_2(H_1(ID_u)\|(H_1(PW_u\|b_u) * P)$ and verifying $BID_u = B\acute{I}D_u$ by the user, randomly selecting r_u and calculating $TID_u = AID_u - H_1(PW_u\|b_u) * P$, $M = r_u * Q_s$ and $CID_u = ID_u \oplus H_2(M\|TID_u), DID_u = M + H_1(PW_u\|b_u) * P$ and $EID_u = H_3(ID_u\|M\|R)$ until R=$r_u * P$ is provided, sending the login request message $M_1 = \{CID_u, DID_u, EID_u, R\}$ by the user.

4. Key Agreement and Confirmation Phase: calculating $TID_u = q_s * (PW_u\|b_u) * P$, $M = q_s * R$, $H_1(PW_u\acute{}\|b_u) * P = DID_u - \acute{M}$, verifying $ID_u = CID_u \oplus H_2(\acute{M}\|T\acute{I}D_u)$ and $H_3(ID_u\|\acute{M}\|R) = EID_u$ by the server, user authentication confirmation by the server, selecting a random secret number r_s and calculating $S = r_s * P$, $T = S + \acute{M}$, $H_s = H_2(S\|T\acute{I}D_u)$ by the server, sending confirmation message $M_2 = \{T, H_s\}$ to the user by the server, calculating $S = T - M, H_s = H_2(S\|H_1(\acute{PW}_u\|b_u) * Q_s)$, and verifying $\acute{H}_s = H_s$ by the user, issuing user login confirmation by the server, sending message $M_3 = \{H_{RS}\}$ that $H_{RS} = H_2(R\|S)$ by user, calculating $\acute{H}_{RS} = H_2(R\|S)$ and comparing it with H_{RS}, and if this equality holds, issuing entry permission by the server, calculating the key $sk = H_3(ID_u\|TID_u\|r_u * S) and\ sk = H_3(ID_u\|T\acute{I}D_u\|r_u * R)$ by the user and server.

5. Password Change Phase: entering ID_u and PW_u by the user, calculating $B\acute{I}D_u = H_2(H_1(ID_u)\|(H_1(PW_u\|b_u) * P))$ and comparing it with $BID_u$by the card reader, if equality holds, entering PW_u^{new} by the user, calculating $AID_u^{new} = H_1(PW_u\|b_u)^{-1} * AID_u * H_1(PW_u^{new}\|b_u)$ and $BID_u^{new} = H_2(H_1(ID_u)\|H_1(PW_u^{new}\|b_u) * P)$ by the card reader, and replacing AID_u and $BID_u$with AID_u^{new} and $BID_u^{new}$by the smart card. In Table 2, the notations of the proposed approach are displayed.

Table 2
Notations of the Proposed Approach

Server	S
User	U
Public and private key pairs of the server so that $Q_s = q_{s*P}$	(q_s, Q_s)
User Identity	ID_u
User Password	PW_u
The one-way complex function such as $H_1: 0,1^* \to G_p$	$H_1(.)$
The one-way complex function such as $H_2: G_p * G_p \to Z_p^*$	$H_2(.)$
The one-way complex function such as H_3: $\{0,1\}^* * G_p * G_p \to \{0,1\}^k$	$H_3(.)$
User-selected secret number	r_u
Secret number selected by the server	r_s
Defined Elliptical Chart in a Finite Range	$E_p(a,b)$

Figure 2 shows the flowchart of the proposed approach.

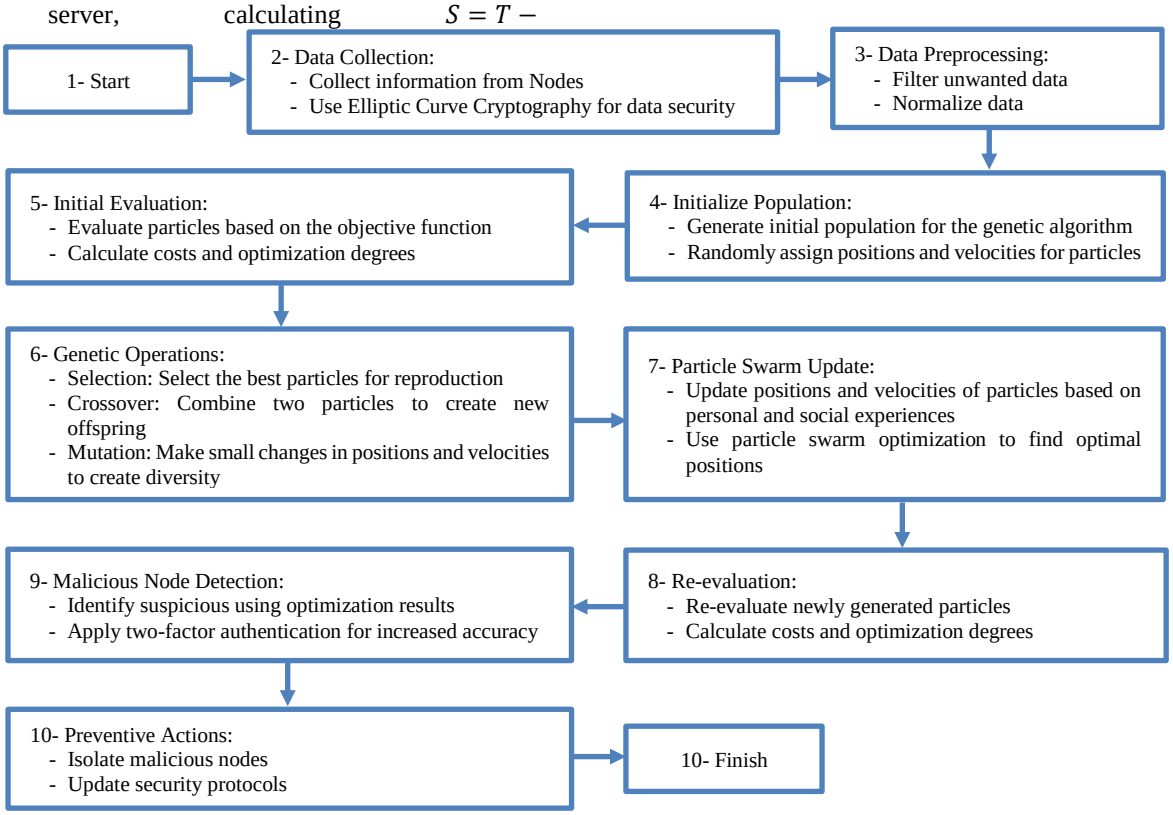

Fig. 2. Proposed Approach Flowchart

4. Results and Discussion

In this section, the simulation of the proposed approach and the evaluation of its results are discussed. The energy of each node for transmitting information is based on relationship $Etrans = \begin{cases} lEelec + l\varepsilon fsd^2 & d < dth \\ lEelec + l\varepsilon mpfd^4 & d > dth \end{cases}$, the received energy according to relationship $Erec = lEelec$, the threshold distance from relationship $dth = \sqrt{\varepsilon fs / \varepsilon mp}$, and for calculating the cluster head nodes from relationship $E(CHk) = Nk \times l \times Eelec + (Nk + 1) \times l \times EDA + l \times (Eelec + \varepsilon mpd)$ is used. Here εmp represents the amplifier energy, dth is the threshold distance and EDA is the energy required for data aggregation. The relationship $E(CHk)$ consists of three parts: the first part includes the energy spent on receiving packets, the second part relates to the energy spent on data aggregation and identifying malicious nodes, and the third part is the energy required to send packets to the main station.

In the proposed hybrid approach, malicious nodes within each cluster are identified from the existing nodes using the obtained information. Specifically, for each cluster, a node is randomly selected as an assistant, which is responsible for collecting information about location, energy, the number and degree of nodes, the best status so far, and other necessary parameters. This assistant node identifies the malicious node(s) and cuts off their communications with the other nodes in the cluster. For key agreement in the proposed approach, the user first sends a request $M_1 = \{CID_u, DID_u, EID_u, R\}$ to the server. After receiving this request, the server checks the validity of $H_3(ID_u \| M \| R) = EID_u$ and confirms the authentication by sending message $M_2 = \{T, H_s\}$ to the user, granting access. The user then compares the value of $H_2(S \| TID_u)$ with H_s to access the server, confirms its legitimacy, and shares the key $sk = H_3(ID_u \| TID_u \| r_u * S) = H_3(ID_u \| TID_u)$. In the proposed approach, forward secrecy is utilized, and even if the adversary $S = r_s * P$ و $R = r_u * P$ و $S = r_s * P$ is aware of the public channel, they still cannot access the secret key sk. The user's identity cannot be stored on the smart card and is identified by $CID_u = ID_u \oplus H_2(M \| TID_u)$, which changes with each passage. Even if the request message for passage is stolen by the adversary, without access to the server's secret key $q_s$and the user's password PW_u, the user's identity remains secure. If a malicious user wants to remotely control the server anonymously, they need to generate a valid message $M_2 = \{T, H_s\}$ such that it includes $T = S + \acute{M}, H_s = H_2(S \| T\acute{I}D_u)$. This means they must have the values of $\acute{M}$ and $T\acute{I}D_u$to compute the valid message M_2. However, without knowing the server's secret key and the user's password PW_u, they cannot compute the value of $M = \acute{q}_s * R, T\acute{I}D_u = q_s * H_1(PW_u \| b_u)$. Therefore, the proposed approach is also secure against fraud threats. Internal threats refer to the possibility that a user may register multiple servers with the same identity and password, gaining access to other servers by impersonating their identity. However, in the proposed approach, during the registration phase, the user presents their identity, password, and $H_1(PW_u \| b_u) * P$ to the server. Meanwhile, the server, facing the discrete logarithm problem, is unable to derive the password $PW_u$from $H_1(PW_u \| b_u) * P$. Additionally, in the event of the smart card being lost or stolen by a malicious user, the password cannot be guessed from AID_u and BID_u, as the true identity ID_u and password PW_u are necessary for passing through $B\acute{I}D_u = BID_u$. The proposed approach also performs well against identity impersonation. If an adversary wants to impersonate a user to gain access to the server, they would need to possess the values of q_s, ID_u, and TID_u. In the proposed approach, the periodic key consists of ID_u, TID_u, and $r_u * r_s * P$, where r_u and r_s are provided by the user and the server, respectively. This ensures that the key is pre-selected or controlled. Even if r_u and $r_s$are compromised, the adversary still cannot access the key $sk = H_3(ID_u \| TID_u \| r_u * r_s * P)$, as there is no way for them to compute ID_u and TID_u.

The initial parameter settings for particle swarm optimization algorithms, genetic algorithms, and structural network parameters are shown in Table 3.

Table 3
Initial parameter settings for PSO, GA and structural network parameters

Parameter	Value
α_3	0.3
α_2	0.4
α_1	0.2
T	200
N	100
W	0.4-1.2
C_1	2
C_2	2
Mutation Rate	0.3
Elec	50 nJ/bit
Efs	10 pJ/bit/ m
Empf	0.0013 pJ/bit/ $m4$

The criteria examined in this section include the average remaining energy, variance of remaining energy, number of alive nodes, and percentage of lost messages, which will be discussed in the following results.

- *Average Remaining Energy*

According to Figure 3, the trend of average remaining energy in the network is uniformly decreasing due to the failure phenomenon. This phenomenon occurs in the network due to the depletion of energy and the shutdown of faulty nodes, such that the faulty nodes are no longer able to communicate with other nodes. This decreasing trend is observed even under high traffic (when the traffic volume exceeds 14 messages per second) for a network with a short time period.

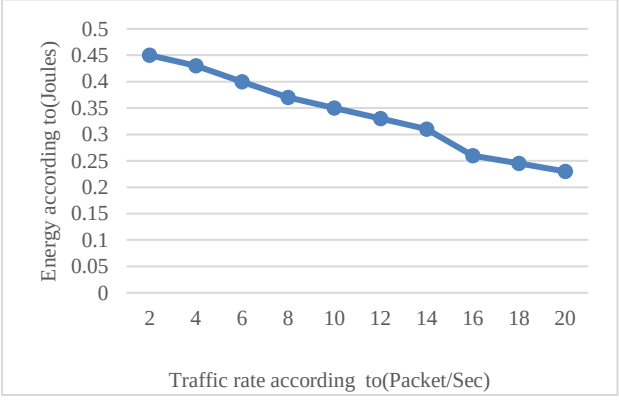

Fig. 3.Average residual energy

- *Variance of Remaining Energy*

To calculate the variance in different traffic conditions, the following relationship has been used.

$$\frac{\sum_{i-1}^{N}(E_{avg} - E_i)^2}{N} \quad (2)$$

As shown in Figure 4, with the increase in the number of faulty nodes, the variance of the remaining energy of the set increases. The lack of change in the status of the graph indicates a complete network failure, and the nodes in the network are in a state where they are not communicating with each other.

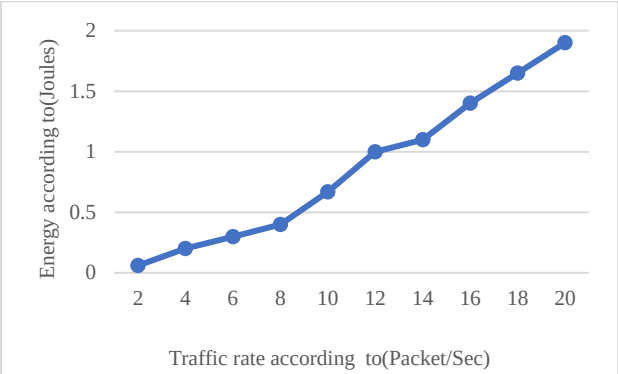

Fig. 4. Residual Energy Variance

- *Number of Alive Nodes*

A node that still has energy remaining and participates in traffic generation and information exchange is referred to as an alive node. When the energy of the nodes in the network is depleted and due to the lack of recharging, their communications are interrupted, making them no longer usable and removing them from the network. Therefore, distinguishing between faulty nodes and nodes that have exited the network due to energy depletion is one of the major challenges in this field. Thus, the number of alive nodes in the network is an important parameter. As shown in Figure 5, the rate of decline in the graph at traffic volumes of 12, 14, and 16 messages per second is faster because the network is at its highest information exchange volume, and afterward, due to network failure, these changes become less pronounced.

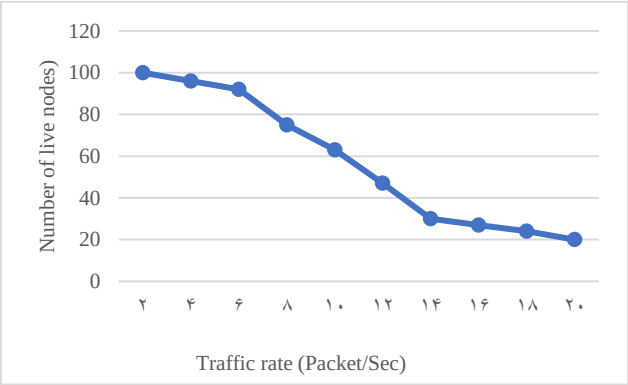

Fig. 5. Number of live nodes at different traffic rates

- *Percentage of Lost Messages*

As we know, in fixed networks, a high percentage of messages successfully reach their destination, and the percentage of lost messages is low. This percentage decreases under high traffic loads due to the reduction in the number of alive nodes and the removal of faulty nodes. However, in mobile networks, these results are unpredictable due to the lack of management of node behaviors, leading to a high percentage of messages not reaching their destination. Figure 6 shows the percentage of lost messages in the network at different traffic rates.

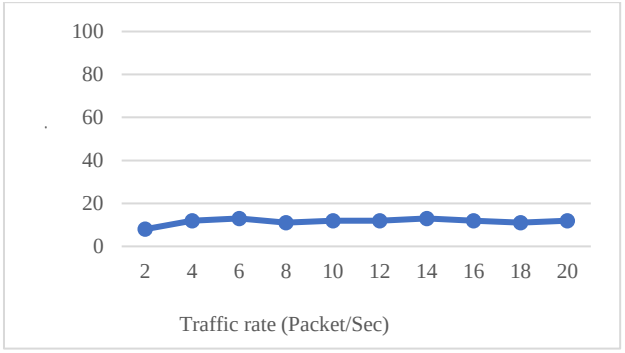

Fig. 6. Percentage of messages lost on the network

- *Comparison of the Proposed Approach with Other Methods*

In this section, the comparison of the proposed approach with the methods presented in references 16 and 18 is shown in terms of remaining energy, average number of alive nodes, and accuracy in identifying faulty nodes in each round with 100 nodes, as illustrated in Figures 7 and 8. As shown in the figures, the performance of the proposed approach is improved compared to these methods due to the use of a greater number of parameters in identifying faulty nodes and the combination of metaheuristic algorithms.

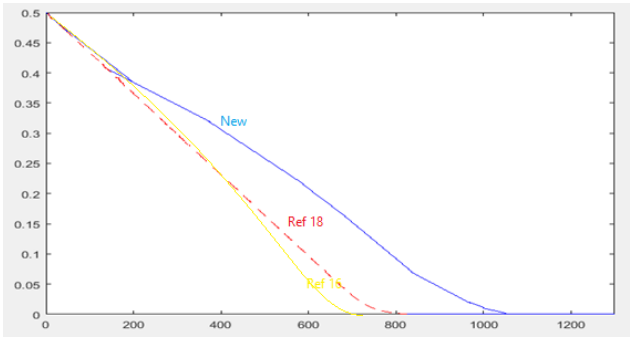

Fig. 7. Comparison of the amount of residual energy of the network in each round with 100 nodes of the proposed approach with references 16 and 18 and the protocol

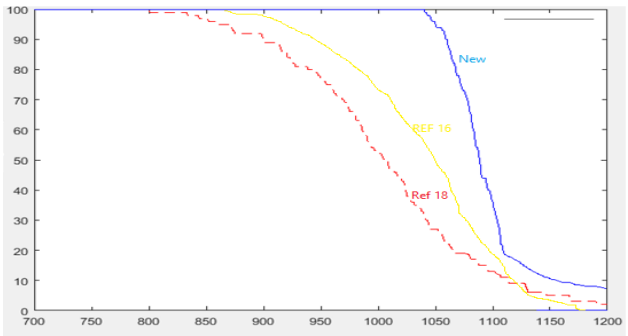

Fig. 8 Comparison of the average number of live nodes of the network in each round with 100 nodes of the proposed approach with references 16 & 18

In Table 4, the cost of the proposed approach, including the phases of registration, authentication, and the total

computation cost (multiplication, addition, and subtraction in ECC, and mixed operations), is compared with other related methods. In this table, T_m represents the time complexity of the multiplication operation in elliptic curve cryptography, T_a represents the time complexity of the addition and subtraction operations in elliptic curve cryptography, and T_h represents the time complexity of the hashing operation in elliptic curve cryptography. According to this table, the cost of the proposed approach is better compared to the other methods being compared.

Table 4
Comparison of the total cost of the proposed approach with other methods

Phases	[18]	[16]	Suggested method
Registration Stage	$1T_m+1T_h$	$1T_m+1T_h$	$2T_m+1T_a+3T_h$
Verification Stage	$8T_m+5T_a+8T_h$	$7T_m+4T_a+6T_h$	$9T_m+5T_a+13T_h$
Total Computing Cost	$9T_m+5T_a+9T_h$	$8T_m+4T_a+7T_h$	$11T_m+8T_a+14T_h$

Figure 9 Shows the comparison of the time overhead of the proposed approach with other algorithms

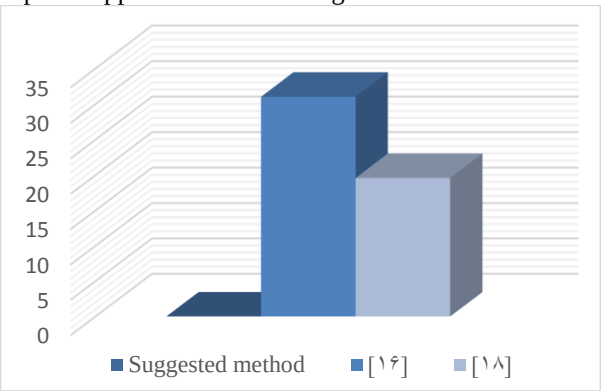

Fig. 9. Time Overhead Comparison: Proposed Approach vs. Baselines

5. Conclusion

The findings of this study demonstrate that the proposed hybrid metaheuristic approach, integrating PSO and GA with ECC-based two-factor authentication, significantly enhances the detection accuracy and energy efficiency of IDS in MANETs. By combining the global search capability of PSO with the exploration potential of GA, the proposed model efficiently identifies and isolates malicious nodes, ensuring secure and reliable data transmission even under high traffic conditions. Simulation results confirm notable improvements in key performance metrics such as average remaining energy, number of alive nodes, and detection accuracy, outperforming existing benchmark methods. These improvements collectively contribute to prolonged network lifetime, reduced computation cost, and greater robustness against a variety of attacks including impersonation, replay, and smart card loss threats.

Despite its promising results, the proposed system has certain limitations. The computational complexity associated with hybrid optimization algorithms may increase under large-scale MANET environments, and real-time adaptation to high mobility patterns or dynamic topological changes may require additional optimization. Furthermore, the approach assumes cooperative node behavior and stable communication links, which may not always hold true in heterogeneous or highly adversarial environments.

Future research should focus on addressing the computational complexity and scalability challenges associated with hybrid optimization algorithms in large-scale MANET environments. Developing lightweight or adaptive metaheuristic variants that dynamically adjust their parameters based on network conditions could significantly reduce computational overhead and improve real-time performance. Additionally, incorporating parallel or distributed processing techniques, such as edge or fog computing, may enhance the scalability and responsiveness of the proposed system under high node densities.

Another important direction is improving the adaptability of the model to handle rapid mobility and frequent topological changes. Integrating predictive mobility models or reinforcement learning mechanisms could enable the intrusion detection system to anticipate network variations and maintain stability even in highly dynamic scenarios. This would strengthen the robustness of the approach against real-time communication disruptions and minimize detection delays.

Future studies should also focus on overcoming the assumption of cooperative node behaviour by introducing trust-aware mechanisms and reputation-based learning models to detect and isolate selfish or compromised nodes. Moreover, applying blockchain technology could enable decentralized trust management and immutable recordkeeping for authentication processes. Finally, future work could also extend to multi-hop scenarios or integrate blockchain for decentralized key management, further improving system transparency and resilience in heterogeneous or adversarial environments.

References

Aluvala, S., Sekhar, K. R., & Vodnala, D. (2016). A novel technique for node authentication in mobile ad hoc networks. *Perspectives in Science*, 8, 680–682.

Asgharizadeh, E., Yadegari, E., Salahi, F., Homayounfar, M., & Daneshvar, A. (2022). Multiple criteria ABC classification: An accelerated hybrid ELECTRE-PSO method. *International Journal of Information and Decision Sciences, 14*(4), 325–344.

Bagirathan, K., Saravanan, N., Vijayabhaskar, K., & Sivasankar, C. (2025). An intelligent recurrent neural network driven secured routing protocol for vehicular ad hoc networks. *Knowledge-Based Systems*, 317, 113371.

Chander, B. (2020a). Deep learning network: Deep neural networks. In S. Sumathi & M. Janani (Eds.), Neural networks for natural language processing (pp. 1–30). IGI Global.

Chander, B. (2020b). The state-of-the-art cryptography techniques for secure data transmission. In B. B. Gupta & S. Srinivasagopalan (Eds.), Handbook of research on intrusion detection systems (pp. 284–305). IGI Global.

Chander, B., & Kumaravelan, G. (2021). Outlier detection strategies for WSNs: A survey. *Journal of King Saud University – Computer and Information Sciences*, 35, 1–24.

Daneshvar, A., Homayounfar, M., & Akhavan, E. (2021). Developing a classification method for imbalanced dataset using multi-objective evolutionary algorithms. *Journal of Industrial Management Studies*, 17(55), 161–138.

Daneshvar, A., Homayounfar, M., Nahavandi, B., & Salahi, F. (2020). A multi-objective approach to the problem of subset feature selection using meta-heuristic methods. *Industrial Management Journal*, 13(2), 278–299.

Deivakani, M., Sheela, M. S., Priyadarsini, K., & Farhaoui, Y. (2024). An intelligent security mechanism in mobile ad-hoc networks using precision probability genetic algorithms (PPGA) and deep learning technique (Stacked LSTM). *Sustainable Computing: Informatics and Systems*, 43, 101021.

dos Santos, F.C., Duarte-Figueiredo, F., De Grande, R. E., & dos Santos, A. L. (2024). Enhancing a fog-oriented IoT authentication and encryption platform through deep learning-based attack detection. *Internet of Things*, 27, 101310.

Far, H. A. N., Bayat, M., Das, A. K., Fotouhi, M., Pournaghi, S. M., & Doostari, M. A. (2021). LAPTAS: Lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT. *Wireless Networks*, 27(2), 1389–1412.

Gope, P., Lee, J., & Quek, T. Q. (2018). Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions. *IEEE Transactions on Information Forensics and Security*, 13(11), 2831–2843.

Gupta, D. S., Islam, S. H., Obaidat, M. S., Vijayakumar, P., Kumar, N., & Park, Y. (2021). A provably secure and lightweight identity-based two-party authenticated key agreement protocol for IIoT environments. *IEEE Systems Journal*, 15(2), 1732–1741.

Homayounfar, M., Daneshvar, A., & Rahmani, J. (2020). Developing meta-heuristic AntLion-Genetic and PBILDE algorithms to portfolio optimization in Tehran Stock Exchange. *Financial Engineering and Securities Management*, 9(34), 1–20.

Huang, S., Raad, R., Tubbal, F., & Odeh, N. (2025). An ARP-integrated enhancement of AODV for wormhole attack detection in mobile ad hoc networks. *Journal of Network and Computer Applications*, 243, 104283.

Islam, S. H., Vijayakumar, P., Bhuiyan, M. Z. A., Amin, R., & Balusamy, B. (2017). A provably secure three-factor session initiation protocol for multimedia big data communications. *IEEE Internet of Things Journal*, 5(5), 3408–3418.

Jain, S., Nandhini, C., & Doriya, R. (2020). ECC-based authentication scheme for cloud-based robots. *Wireless Personal Communications*, 117, 1557–1576.

Jiang, Q., Zhang, N., Ni, J., Ma, J., Ma, X., & Choo, K. K. R. (2020). Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles. *IEEE Transactions on Vehicular Technology*, 69(9), 9390–9401.

Kantola, R., Kabir, H., & Loiseau, P. (2017). Cooperation and end-to-end in the internet. *International Journal of Communication Systems*, 30(12), e3268.

Kazemi, Z., Homayounfar, M., Fadaei, M., Soufi, M., Salehzadeh, A. (2024). Multi-objective Optimization of Blood Supply Network Using the Meta-Heuristic Algorithms. *Journal of Optimization in Industrial Engineering*, 17(2), 87-104.

Mansouri, F., Tarhouni, M., Alaya, B., & Zidi, S. (2025). A distributed intrusion detection framework for vehicular ad hoc networks via federated learning and blockchain. *Ad Hoc Networks, 167*, 103677.

Meshram, C., Obaidat, M. S., Lee, C. C., & Meshram, S. G. (2021). An efficient, robust, and lightweight subtree-based three-factor authentication procedure for large-scale DWSN in random oracle. *IEEE Systems Journal*, 15(4), 4927–4938.

Nahavandi, B., Homayounfar, M., Daneshvar, A., & Shokouhifar, M. (2021). Hierarchical structure modelling in uncertain emergency location-routing problem using combined genetic algorithm and simulated annealing. *International Journal of Computer Applications in Technology*, 68(2), 150–163.

Naveena, A., & Reddy, K. R. (2016). A review: Elliptical curve cryptography in wireless ad-hoc networks. *International Journal of Advanced Research in Computer Science and Software Engineering*, 6(6), 227–230.

Nivedita, V., Shieh, C.S., & Horng, M.-F. (2025). An integrated trust-based secure routing with intrusion detection for mobile ad hoc network using adaptive snow geese optimization algorithm. *Ain Shams Engineering Journal*, 16(7), 103385.

Prasad, M., Tripathi, S., & Dahal, K. (2023). An intelligent intrusion detection and performance reliability evaluation mechanism in mobile ad-hoc networks. Engineering Applications of Artificial Intelligence, 119, 105760.

Qi, M., & Chen, J. (2021). Secure authenticated key exchange for WSNs in IoT applications. *Journal of Supercomputing*, 77, 13897–13910.

Sadri, M. J., & Asaar, M. R. (2021). An anonymous two-factor authentication protocol for IoT-based applications. *Computer Networks*, 199, 108460.

Salahi, F., Daneshvar, A., Homayounfar, M., & Pourghader Chobar, A. (2020). Presenting an integrated model for production planning and preventive maintenance scheduling considering uncertainty of parameters and disruption of facilities. *Journal of Industrial Management Perspective*, 13(1), 105–140.

Salahi, F., Daneshvar, A., Homayounfar, M., & Shokouhifar, M. (2021). A comparative study of meta-heuristic algorithms in supply chain networks. *Journal of Industrial Engineering International*, 17(1), 52.

Sarangi, S. K., Lenka, R., Mishra, J., Sahu, R., & Nanda, A. (2025). Malicious detection and trust calculation using residual recurrent neural network for trust with quality of service-aware multicast routing in mobile ad-hoc network system. *Engineering Applications of Artificial Intelligence*, 161(Part C), 112130.

Saviour, M. P. A., & Samiappan, D. (2023). IPFS based storage authentication and access control model with optimization enabled deep learning for intrusion detection. *Advances in Engineering Software*, 176, 103369.

Shams, E. A., Rizaner, A., & Ulusoy, A. H. (2023). Flow-based intrusion detection system in vehicular ad hoc network using context-aware feature extraction. *Vehicular Communications*, 41, 100585.

Sharma, S., & Nidhi. (2019, September). Vehicular ad-hoc network: An overview. In 2019 International Conference on Computing Communication and Intelligent Systems (ICCCIS) (pp. 131–134). IEEE.

Shrivastava, S., Agrawal, C., & Jain, A. (2015). An IDS scheme against black hole attack to secure AOMDV routing in MANET. arXiv preprint arXiv:1502.04801.

Tavakol, P., Nahavandi, B., & Homayounfar, M. (2023). A dynamics approach for modeling inventory fluctuations of the pharmaceutical supply chain in covid 19 pandemic. *Journal of Optimization in Industrial Engineering*, 16(1), 105–118.

Wang, D., Li, W., & Wang, P. (2018). Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. *IEEE Transactions on Industrial Informatics*, 14(9), 4081–4092.

Wang, W., Liu, Z., Xue, L., Huang, H., & Lavuri, N. R. (2025). Malicious vehicle detection scheme based on UAV and vehicle cooperative authentication in vehicular networks. Computer Networks, 258, 111037.

Wang, C., Wang, D., Tu, Y., Xu, G., & Wang, H. (2020). Understanding node capture attacks in user authentication schemes for wireless sensor networks. *IEEE Transactions on Dependable and Secure Computing*, 19(1), 507–523.

Wang, Q., & Wang, D. (2022). Understanding failures in security proofs of multi-factor authentication for mobile devices. *IEEE Transactions on Information Forensics and Security*, 18, 597–612.

Wazid, M., Das, A. K., Kumar, N., & Rodrigues, J. J. (2017). Secure three-factor user authentication scheme for renewable-energy-based smart grid environment. *IEEE Transactions on Industrial Informatics*, 13(6), 3144–3153.

Wu, F., Li, X., Xu, L., Vijayakumar, P., & Kumar, N. (2021b). A novel three-factor authentication protocol for wireless sensor networks with IoT notion. *IEEE Systems Journal*, 15(1), 1120–1129.

Wu, T. Y., Yang, L., Lee, Z., Chu, S. C., Kumari, S., & Kumar, S. (2021a). A provably secure three-factor authentication protocol for wireless sensor networks. *Wireless Communications and Mobile Computing*, 2021, 1–15.

Xie, Q., Ding, Z., & Hu, B. (2021). A secure and privacy-preserving three-factor anonymous authentication scheme for wireless sensor networks in Internet of things. *Security and Communication Networks*, 2021, 1–12.

Xue, L., Huang, Q., Zhang, S., Huang, H., & Wang, W. (2021). A lightweight three-factor authentication and key agreement scheme for multigateway WSNs in IoT. *Security and Communication Networks*, 2021, 1–15.

Yang, Z., He, J., Tian, Y., & Zhou, J. (2019). Faster authenticated key agreement with perfect forward secrecy for industrial Internet-of-Things. *IEEE Transactions on Industrial Informatics*, 16(9), 6584–6596.

Zou, S., Cao, Q., Wang, C., Huang, Z., & Xu, G. (2022). A robust two-factor user authentication scheme based on ECC for smart home in IoT. *IEEE Systems Journal*, 16(3), 4938–4949.