



LEEDS  
BECKETT  
UNIVERSITY

---

Citation:

Thiruppathy Kesavan, V and Murugavalli, S and Premkumar, M and Selvarajan, S (2023) Adaptive neuro-fuzzy inference system and particle swarm optimization: A modern paradigm for securing VANETs. IET Communications, 17 (19). pp. 2219-2236. ISSN 1751-8628 DOI: <https://doi.org/10.1049/cmu2.12692>

Link to Leeds Beckett Repository record:

<https://eprints.leedsbeckett.ac.uk/id/eprint/10326/>

Document Version:

Article (Published Version)

---

Creative Commons: Attribution-Noncommercial 4.0

© 2023 The Authors.

The aim of the Leeds Beckett Repository is to provide open access to our research, as required by funder policies and permitted by publishers and copyright law.


The Leeds Beckett repository holds a wide range of publications, each of which has been checked for copyright and the relevant embargo period has been applied by the Research Services team.

We operate on a standard take-down policy. If you are the author or publisher of an output and you would like it removed from the repository, please [contact us](#) and we will investigate on a case-by-case basis.

Each thesis in the repository has been cleared where necessary by the author for third party copyright. If you would like a thesis to be removed from the repository or believe there is an issue with copyright, please contact us on [openaccess@leedsbeckett.ac.uk](mailto:openaccess@leedsbeckett.ac.uk) and we will investigate on a case-by-case basis.

## ORIGINAL RESEARCH

# Adaptive neuro-fuzzy inference system and particle swarm optimization: A modern paradigm for securing VANETs

V Thirupathy Kesavan<sup>1</sup> | S Murugavalli<sup>2</sup> | Manoharan Premkumar<sup>3</sup>  | Shitharth Selvarajan<sup>4,5</sup>

<sup>1</sup>Department of Information Technology, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu, India

<sup>2</sup>Department of Artificial Intelligence, K.Ramakrishnan College of Technology, Trichy, Tamilnadu, India

<sup>3</sup>Department of Electrical and Electronics Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India

<sup>4</sup>Department of Computer Science, Kebri Dehar University, Kebri Dehar, Ethiopia

<sup>5</sup>School of Built Environment, Engineering and Computing, Leeds Beckett University, Leeds, United Kingdom

**Correspondence**

Manoharan Premkumar, Department of Electrical and Electronics Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka 560078, India.

Email: [mprem.me@gmail.com](mailto:mprem.me@gmail.com)

Shitharth Selvarajan, Department of Computer Science, Kebri Dehar University, Kebri Dehar, Ethiopia.

Email: [shitharths@kdu.edu.et](mailto:shitharths@kdu.edu.et)

**Abstract**

Vehicular Adhoc Networks (VANET) facilitate inter-vehicle communication using their dedicated connection infrastructure. Numerous advantages and applications exist associated with this technology, with road safety particularly noteworthy. Ensuring the transportation and security of information is crucial in the majority of networks, similar to other contexts. The security of VANETs poses a significant challenge due to the presence of various types of attacks that threaten the communication infrastructure of mobile vehicles. This research paper introduces a new security scheme known as the Soft Computing-based Secure Protocol for VANET Environment (SC-SPVE) method, which aims to tackle security challenges. The SC-SPVE technique integrates an adaptive neuro-fuzzy inference system and particle swarm optimisation to identify different attacks in VANETs efficiently. The proposed SC-SPVE method yielded the following average outcomes: a throughput of 148.71 kilobits per second, a delay of 23.60 ms, a packet delivery ratio of 95.62%, a precision of 92.80%, an accuracy of 99.55%, a sensitivity of 98.25%, a specificity of 99.65%, and a detection time of 6.76 ms using the Network Simulator NS2.

## 1 | INTRODUCTION

Communication technology serves a pivotal role in the contemporary management of vehicle networks. The development of traditional wired communication protocols aimed to regulate a vehicle's internal components through a unified system architecture. This unconventional approach results in an escalation of both the system and maintenance expenses associated with the vehicle. To enhance cost efficiency, contemporary vehicular networks employ wireless protocols for transmitting and receiving data within or beyond vehicles. Vehicular Adhoc Networks (VANET) [1] are a type of mobile network, specifically Mobile Ad Hoc Networks (MANETs), which facilitate communication both with and without the presence of infrastructure

along roadways [2, 3]. In this network configuration, vehicles represent constituent elements, and a prominent characteristic is the rapid mutability of its topology. This network's primary focus lies in advancing applications within the Intelligent Transport Systems (ITS) structure [4]. These applications deliver and enhance traffic information, promote road safety, and optimize transportation efficiency.

The VANET system comprises two interfacing components: the On-Board Unit (OBU) and the Road Side Units (RSU) [5]. The OBU module is seamlessly incorporated into the vehicle's infrastructure, establishing connections with all wireless sensors present within the vehicle. The RSU module is installed within roadside structures, equipped with separate transmitter and receiver units, to establish communication with each

This is an open access article under the terms of the [Creative Commons Attribution-NonCommercial](https://creativecommons.org/licenses/by-nc/4.0/) License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited and is not used for commercial purposes.

© 2023 The Authors. *IET Communications* published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology.

vehicle's OBU component. Upon integration into the VANET framework, the vehicle is equipped with many sensors to detect and collect vehicle details. This data is transmitted to the RSU module. Accidents can be mitigated effectively by establishing a robust and seamless coordination mechanism between the vehicle OBU and RSU modules. The presence of intruders impacts the performance of the OBU component and the RSU module. Therefore, it is imperative to establish a robust safety system to ensure the integrity and confidentiality of communication between the OBU and RSU modules.

Implementing VANET techniques leads to a notable reduction in accidents through exchanging vehicle information among nearby or surrounding vehicles. The VANET can be classified into two modules: Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) [6, 7]. The V2V module within the VANET system facilitates the transmission of information between individual vehicles. In the context of the VI module, when considering the VANET system, data is transmitted from personal vehicles to a centralized system or controller. The real-time environment scenario of the VANET exhibits a dynamic nature, where the topology system undergoes continuous changes based on the varying distances and locations of vehicles. Multiple variables, such as environmental issues and noises, have been found to impact the quality of the information passage between vehicles. The vehicle environment under consideration is called a rugged VANET environment, susceptible to external attacks, including eavesdropping and data hacking.

The network safety of VANET is highly susceptible to vulnerabilities, which can be attributed to various technical challenges such as high mobility, routing issues, dynamic topology, and loss of information through wireless connections [8, 9]. The transmission of information is susceptible to various security issues. Multiple attacks can potentially breach and disrupt network connectivity, often accompanied by inherent weaknesses or irregularities within the communication infrastructure. Different privacy protocols, the formalization of requirements, and diverse analyses of threats have been suggested to enhance the security of VANETs [10, 11]. However, a significant scope remains for further exploration in this field.

Regarding protecting VANETs, the SC-SPVE approach greatly improved over previous methods. SC-SPVE uses the potential of soft computing to overcome the limitations of traditional approaches by combining the Adaptive Neuro-Fuzzy Inference System (ANFIS) and Particle Swarm Optimization (PSO). The combination enables adaptive intelligence and dynamic response to changing threats and network environments. ANFIS enables the system to learn and adapt to different attack patterns, which improves the system's accuracy and precision while detecting attacks. Meanwhile, PSO adjusts the security protocol's settings to peak efficiency and reactivity. SC-SPVE's success can be seen in the numbers: 95.62% packet delivery ratio, high precision, accuracy, sensitivity, and specificity, and short detection time and delay. By combining the power of soft computing with optimization approaches, SC-SPVE can go above and beyond the standard ways of VANET security, providing reliable defence against various threats while keeping network performance at a high level. When it comes to

protecting VANETs, this method ushers in a new paradigm that promises better security and communication efficiency results.

The primary contributions of the research are given below:

- This paper presents a new methodology that employs the Adaptive Neuro-Fuzzy Inference System (ANFIS) and Particle Swarm Optimisation (PSO) techniques to augment security measures in VANETs.
- This study aims to deploy a resilient Multivariate Statistical Detection Method (MVSDM) as an Intrusion Detection System (IDS) for VANETs.
- This study aims to evaluate the efficacy of the proposed SC-SPVE method in detecting black hole attacks and its potential for improving road safety.

The following sections are arranged in the given manner: Section 2 comprehensively examines the background and context surrounding the research topic, emphasizing the significance of VANETs. Section 3 introduces a novel methodology integrating the ANFIS and PSO for VANETs that proposed a Soft Computing-based Secure Protocol for VANET Environment (SC-SPVE). Section 4 is dedicated to the simulation analysis utilizing the Network Simulator (NS2). This analysis aims to assess the effectiveness of the proposed method as an IDS for VANETs. The final section of the research paper provides a concise overview of the primary findings and contributions of the study. The authors additionally address the difficulties and constraints of the proposed methodology and propose potential avenues for future investigation and enhancement in the domain of VANET security.

## 2 | BACKGROUND AND LITERATURE SURVEY

The examination of diverse wireless technologies in automobiles has been the subject of research since the 1970s. Understanding each component of VANET is of utmost importance due to its complex nature. Numerous scholarly publications have been presented and utilized as sources for defining critical concepts in the operations of transportation systems.

### 2.1 | Traditional VANET security approach

The authors of the study conducted by Soleymani et al. propose a security and privacy framework for fog-enabled VANETs that relies on node and message authorization and trust mechanisms [12]. The proposed approach entails the verification of nodes and messages within the fog-enabled VANET setting to guarantee secure and private communication. The scheme integrates trust management mechanisms to evaluate the trustworthiness of nodes and communications, thereby augmenting the overall level of security. The simulation results of the proposed method demonstrated an extraordinary level of message authentication accuracy, reaching 98%. This outcome

enhances the safety and reliability of the fog-enabled VANET environment.

Abdulkadhim et al. propose a novel hybrid methodology that combines Software-Defined Networking (SDN) with Self-Organizing Maps (SOM) to augment security measures in VANET [13]. The proposed approach integrates SDN and SOM to enhance detecting and preventing anomalies within VANET settings. SDN is a widely adopted approach for effectively managing network traffic and enforcing security policies. SOMs are commonly employed for detecting anomalies in network behaviour by applying unsupervised learning techniques. The findings from the simulation indicate that the hybrid approach exhibits efficacy in identifying and alleviating security threats, resulting in a decrease of 20% in security incidents compared to conventional methodologies.

Mdee et al. propose a method that ensures security compliance and promotes cooperation by swapping pseudonyms [9]. This method is designed to preserve location privacy in VANETs effectively. Their methodology's primary emphasis centres around optimizing pseudonym changing between vehicles to thwart unauthorized tracking and safeguard the confidentiality of vehicle whereabouts. The authors demonstrate, via simulations, that the suggested approach attains a success rate of 90% in protecting the privacy of individuals' locations. This effectively thwarts attempts to exploit location-based vulnerabilities and unauthorized tracking.

## 2.2 | Encryption-based security

Narayanan et al. proposed a novel approach for improving cloud storage and security in real-time cloud monitoring metrics by introducing an efficient key validation mechanism within the VANET [11]. The proposed process entails generating and validating cryptographic keys within scenarios involving VANETs, aiming to establish secure communication channels between vehicles and the cloud. The suggested method employs real-time cloud monitoring metrics to improve the effectiveness and dependability of cloud storage systems within the VANET framework. The simulation results demonstrated a noteworthy enhancement in security levels, as evidenced by a 30% increase in adequate essential confirmations compared to conventional approaches.

Sajini et al. proposed the ASCII-ECC algorithm to enhance data transmission security within the context of VANETs [14]. The approach employed by the authors involves the utilization of ASCII encoding and Elliptic Curve Cryptography (ECC) to guarantee the secure transmission of information. The simulation results provide empirical evidence supporting the efficacy of the suggested algorithm, as it exhibits a noteworthy enhancement in security. Precisely, the algorithm attains a success rate of 95% in effectively thwarting illicit access and preventing data manipulation.

Zhang et al. present a set of methodologies to enhance efficiency and ensure data transmission confidentiality within VANETs [15]. The approach employed by the researchers entails optimizing network performance using adaptive trans-

mission power control alongside implementing lightweight encryption techniques to bolster data security. The findings from the simulation indicate a significant enhancement of 30% in network performance and a high success rate of 95% in ensuring the security of data transmission through the utilization of the suggested methodologies.

## 2.3 | Blockchain-based approach

Inedjaren et al. present a novel distributed management system utilizing blockchain technology to enhance trust in VANETs [16]. The approach employed by the researchers involves the utilization of blockchain technology to create a trust management system that is decentralized and forthcoming among vehicles in VANETs. Using simulations, the authors demonstrate the efficacy of their methodology, attaining a success rate of 90% in establishing trust and mitigating malicious behaviours within the network.

Alharthi et al. propose a privacy-preserving framework that utilizes Biometrics Blockchain (BBC) technology to mitigate potential attacks in VANETs [17]. The proposed framework incorporates biometrics and blockchain technologies to augment the levels of privacy and security within VANETs. Utilizing biometric verification and implementing blockchain-based data storage in their methodology guarantees the preservation of personal vehicle identities with utmost integrity and confidentiality. The simulation results indicate a success rate of 98% in mitigating identity threats and safeguarding privacy within VANET conditions.

## 2.4 | ANFIS and PSO-based approaches

The study by Rajeswari et al. centres on the augmentation of security and privacy measures within the context of sensor monitoring and emergency services in VANETs [18]. The methodology utilized in this study involves the implementation of data encryption and access controls to safeguard the confidentiality and integrity of the information transmitted within the VANET for sensor monitoring and emergency services use. The suggested approach guarantees that solely authorized entities can access and employ private information, thereby mitigating the potential for data breaches and unauthorized entry using ANFIS [19]. Although the authors did not provide specific simulation findings, they effectively showcase the efficacy of their approach in enhancing security and privacy in conditions involving VANETs.

Poongodi et al. introduce an innovative approach to enhance the security of a Multi-access Edge Computing (MEC)-based VANET [10]. Their proposed solution incorporates a blockchain framework that utilizes neuro-fuzzy systems. The proposed methodology integrates MEC and blockchain technology while incorporating neuro-fuzzy techniques to enhance decision-making efficiency. The proposed framework aims to improve data transmission's security and reliability in VANETs while optimizing network efficiency by leveraging edge

**TABLE 1** Summary of the literature survey.

Ref. No	Features	Results	Issues/Disadvantages
11	Key validation method, real-time cloud monitoring variables	30% increase in adequate essential confirmations compared to conventional methods	Poor scalability in handling large-scale VANETs and potential overhead in the crucial validation process
12	Node and message authorization, trust methods	Message authentication accuracy: 98%	Inadequate analysis of performance in large-scale fog-enabled VANETs and potential computational overhead
13	Hybrid (SDN+ SOM) method	Reduction of 20% in security incidents	Inadequate scalability and potential complexity in implementing SDN and SOM techniques
14	Secure Authentication and Encryption Scheme (SAES) with PSO	15% reduction in communication overhead, 25% enhancement in safety levels	Inadequate analysis in real-world VANET and potential vulnerabilities in the PSO-based authentication method
15	Data encryption, access controls	Enhanced safety and privacy in sensor monitoring and emergency services	Poor simulation findings and potential overhead in data encryption and access control
16	Security system, On-Demand Multicast Routing Protocol (ODMRP)	40% reduction in packet loss, 25% enhancement in network performance	Potential scalability issues with ODMRP in large-scale VANET deployments and Inadequate analysis of safety system
17	ASCII-ECC system	The success rate of 95% in preventing data manipulation	Inadequate analysis of system performance in the presence of sophisticated threats and potential overhead in ASCII encoding
18	Pseudonym swapping	The success rate of 90% in protecting location privacy	Potential latency issues in the pseudonym-swapping process and Inadequate analysis in scenarios with a high number of vehicles
19	Adaptive transmission power control, lightweight encryption	30% enhancement in network performance, 95% success rate in data transmission protection	Inadequate analysis of system performance under various network conditions and potential overhead in encryption techniques
20	Blockchain-based trust management system	The success rate of 90% in establishing trust and mitigating malicious behaviours	Potential scalability issues with blockchain implementation and enhanced computational overhead in the trust management system
21	Privacy-preserving method using Biometrics Blockchain (BBC)	The success rate of 98% in mitigating identity attacks and safeguarding privacy	Inadequate analysis of biometric authentication in real-world VANET scenarios and potential privacy concerns with BBC
22	Blockchain method with neuro-fuzzy systems	25% reduction in data transmission delay, 90% success rate in data protection	Potential complexity in implementing neuro-fuzzy systems and enhanced computational overhead in the blockchain method

computing capabilities. The simulation results demonstrate a noteworthy decrease of 25% in the delay of data transmission and a substantial success rate of 90% in guaranteeing data security through the implementation of the suggested framework.

Jiang et al. present the Secure Authentication and Encryption Scheme (SAES), a novel self-checking authentication system designed for VANET to enhance effectiveness and safety [20]. The SAES method improves authentication by reducing the computational burden and communication latency using PSO [21]. Implementing a self-checking mechanism within the scheme guarantees the maintenance of a dependable and resistant authentication process against tampering. The findings from the simulation demonstrate that the SAES authentication system exhibits superior performance compared to currently existing systems, specifically in terms of efficiency and safety. The SAES scheme achieves a notable reduction of 15% in communication overhead while concurrently enhancing security levels by 25%.

Sharma et al. successfully implemented a highly effective security algorithm in VANET [22]. Their research also focuses on enhancing performance by integrating the On-Demand Multicast Routing Protocol (ODMRP). The security algorithm employed in VANET significantly improves data confidentiality and authenticity levels during transmission using PSO. Furthermore, the authors enhance the performance of VANETs by incorporating the ODMRP, which effectively supports multicast communication. The authors employ simulations to illustrate their integrated methodology's efficacy, yielding a 40% decrease in packet loss and a 25% enhancement in overall network performance when contrasted with conventional techniques. The summary of the findings is given in Table 1.

The literature review uncovers multiple suggestions for augmenting security and privacy in VANETs, employing methodologies such as encryption, pseudonym swapping, blockchain, and biometrics. To address the complex and ever-changing security demands in VANETs, utilizing soft computing methodologies such as ANFIS and PSO is imperative.

These approaches facilitate the development of sophisticated and resilient security protocols, thereby offering effective and adaptable solutions tailored to the dynamic nature of the VANET environment.

### 3 | PROPOSED SOFT COMPUTING-BASED SECURE PROTOCOL FOR VANET ENVIRONMENT

This section presents a methodology for IDS that leverages machine learning and deep learning techniques to achieve improved effectiveness. The proposed method comprises a Known Intrusion Detection System (KIDS) and Unknown Intrusion Detection System (UIDS). These modules are designed to identify and detect both known and unknown attacks. The KIDS module employs an algorithm based on machine learning to identify and discern recognized malicious attacks. The UIDS module uses a deep learning algorithm to identify and detect previously unidentified attacks in the context of VANETs. The comprehensive algorithm or workflow of the suggested IDS for VANET is illustrated in Figure 1.

#### 3.1 | Adaptive neuro-fuzzy systems

Neural networks exhibit remarkable adaptability and proficiency in learning and generalization [23]. An adaptable network refers to a multi-layer feed-forward network wherein each node car-

ries out a specific function on incoming signals, known as the node function. Additionally, each node is associated with a set of variables that are specific to that node. Adaptive neuro-fuzzy systems combine the advantages of fuzzy logic with the capacity offered by neural networks to model actual structures effectively. The underlying principle of this system is predicated on the following:

- (i) The fuzzy controller transforms into a neural network.
- (ii) The network undergoes training through the backpropagation algorithm, a widely used automatic neural network training technique incorporating hidden layers. This methodology is employed to compute the error contribution of individual neurons to processing a batch of data.
- (iii) The definition of fuzzy sets involves the utilization of differentiable operators and different membership functions.

The fundamental learning principle of adaptive systems is founded upon the principles of gradual descent and the chain rule. The process is commonly referred to as the backpropagation of errors, as it involves the calculation of errors at the output layer and their distribution throughout the network layers.

The representation of the ANFIS is shown in Figure 2. The ANFIS is a computational model that employs supervised learning techniques and incorporates the Takagi-Sugeno fuzzy inference system. Let's consider a scenario where two inputs exist,  $x$  and  $y$ , and a single output, denoted as  $f$ . The

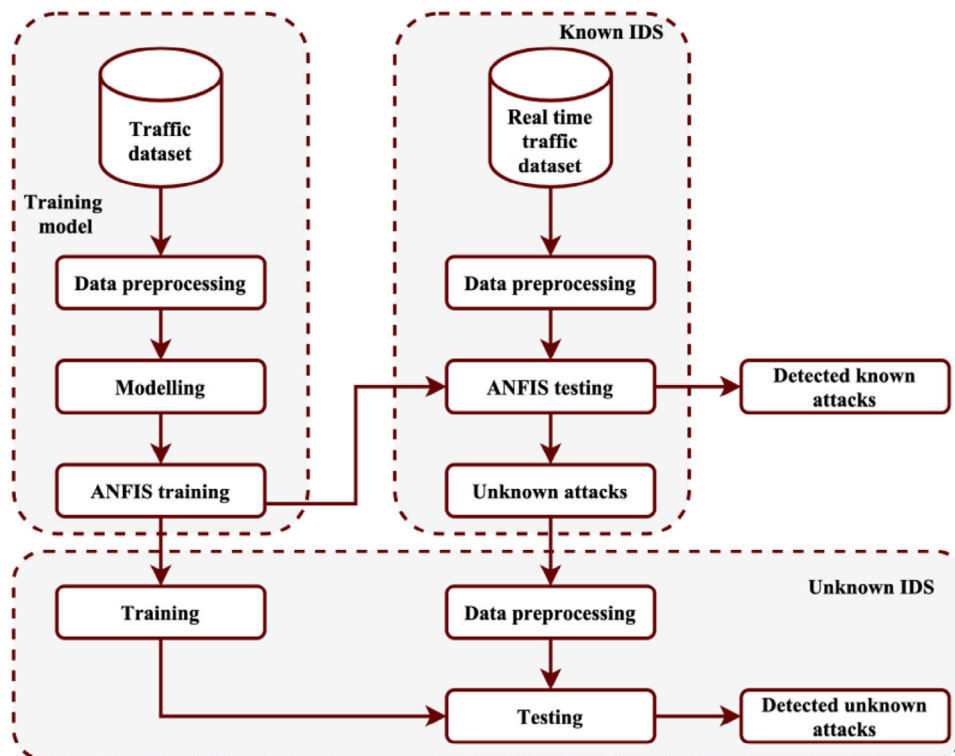


FIGURE 1 The security detection process of the proposed SC-SPVE

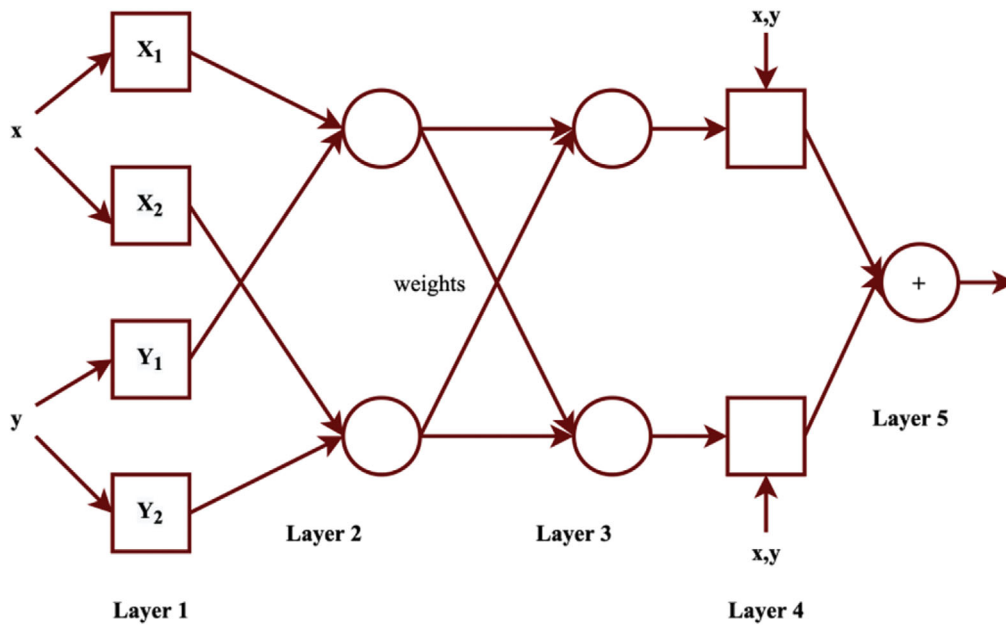


FIGURE 2 ANFIS representation

Takagi-Sugeno model employed two rules in its methodology, which are outlined below:

Rule 1: If  $x$  is  $X_1$  and  $y$  is  $Y_1$ , then  $f_1 = k_1 x + l_1 y + m_1$

Rule 2: If  $x$  is  $X_2$  and  $y$  is  $Y_2$ , then  $f_2 = k_2 x + l_2 y + m_2$

The function memberships of each input  $x$  and  $y$ , denoted as  $X_1, X_2$  and  $Y_1, Y_2$  are part of the foundational data in the Takagi-Sugeno fuzzy inference system. The linear variables  $k_1, l_1, m_1$  and  $k_2, l_2, m_2$  are a component of the consequent part of the framework.

The architecture of ANFIS consists of five layers. The initial and final layers of the network consist of an adaptive node, whereas the intermediate layers consist of a fixed node. Layer 1 represents the input variables  $x$  and  $y$ . The nodes within this layer possess adaptability, wherein each node computes the degree of membership for the fuzzy set input  $X_a(i)$ . There are multiple ways to define the membership function, requiring it to possess differentiability. An instance  $X_a(i)$  can be expressed as a bell-shaped function (Equation 1) characterized by a maximum value of 1 and a minimum value of 0.

$$X_a(i) = \frac{1}{1 + a \left( \frac{i - c_a}{x_a} \right)^{2y_a}} \quad (1)$$

Let  $i$  represent the input, and let  $x_a, y_a, c_a$  denote the set of variables.

Layer 2: The second layer in the network architecture is called the rule layer. The nodes within this layer exhibit a non-adaptive nature, whereby the multiplication of its inputs determines the

output of each node.

$$w_a = X_a(i) \cdot Y_a(j) \quad (2)$$

The membership functions are  $X_a$  and  $Y_a$ .

Layer 3: The nodes within this layer compute the adjusted aggregation of membership degrees for all linguistic declarations. The term used to describe this mixture is the degree of rule satisfaction or the firing power of a rule. It quantifies how much a rule premise aligns with a given input value. Each node within this layer is assigned the label  $N$ . The  $a$ -th node computes the ratio between the firing power of the  $a$ -th rule and the total sum of firing advantages of all regulations. The normalized weight is denoted in Equation (3).

$$\bar{w}_a = \frac{w_a}{w_a + w_b} \quad (3)$$

The weights are denoted  $w_a$  and  $w_b$ .

Layer 4 consists of square nodes, each performing a specific function. The function is denoted in Equation (4).

$$\bar{w}_a f_a = \bar{w}_a (k_a x + l_a y + m_a) \quad (4)$$

The output of layer 3 is denoted as  $\bar{w}_a$ , while the variables set is represented by  $\{k_a, l_a, m_a\}$ . The dimensional variables are denoted  $x$  and  $y$ .

Layer 5 consists of a solitary node that represents the final output. The node within this layer exhibits a non-adaptive characteristic, wherein the part's summation determines its work produced originating from layer 4. The result is denoted in

Equation (5).

$$o = \sum_{a=0}^N \bar{w}_a f_a. \quad (5)$$

The normalized weight is denoted  $\bar{w}_a$ , and the function is denoted  $f_a$ . The present study outlines the application technique of an artificial neural network with comparable functionality to a diffuse inference system. This approach enables the utilization of various training computations.

### 3.2 | Particle swarm optimization

PSO is designed to address the improvement of both continuous and discontinuous decision-making purposes [24]. The PSO algorithm is a search algorithm that operates on a population level, drawing inspiration from the natural and sociological behaviour observed in animals, particularly flocks of birds engaged in food-foraging activities.

The PSO method employs a population of particles, a swarm, representing individual potential solutions. Particles within a multidimensional search space undergo continuous changes in their positions until they reach a state of equilibrium or optimal configuration or until computational limitations are surpassed.

In the context of a problem in optimization involving D factors, a swarm comprising N particles is initially distributed across a D-dimensional hyperspace. Each particle's location within this hyperspace represents a potential solution to the optimization problem. Let  $x$  represent the spatial position of a particle, while  $v$  indicates the particle's velocity as it traverses a solution space. Each member, denoted as  $x$ , within the collective group is evaluated using a scoring function that assigns a fitness score indicating the degree to which it effectively addresses the given problem. The particle updating process is shown in Figure 3.  $X_t$  and  $X_{t+1}$  are the present and future locations.  $V_t$  is denoted by the velocity and  $V_{t+1}$  is denoted by the new velocity. The location best and global best are denoted  $V_{pbest}$  and  $V_{Gbest}$ .

The representation of a particle's best prior position is denoted as Pbest, while Gbest represents the optimal particle among all particles within the swarm. Following this, all particles traversing the solution space of dimension D must adhere to the revised rules governing their movement until the optimal global position is ultimately determined. The deterministic and stochastic modification rules demonstrate how the location and velocity of a particle are changed. The stochastic function is shown in Equation (6), and the acceleration is shown in Equation (7).

$$S_x(p) = w S_x(p-1) + k_1 (a_{pbest_x} - a_x(p)) + k_2 (a_{gbest} - a_x(p)), \quad (6)$$

$$a_x(p) = a_x(p-1) + S_x(p). \quad (7)$$

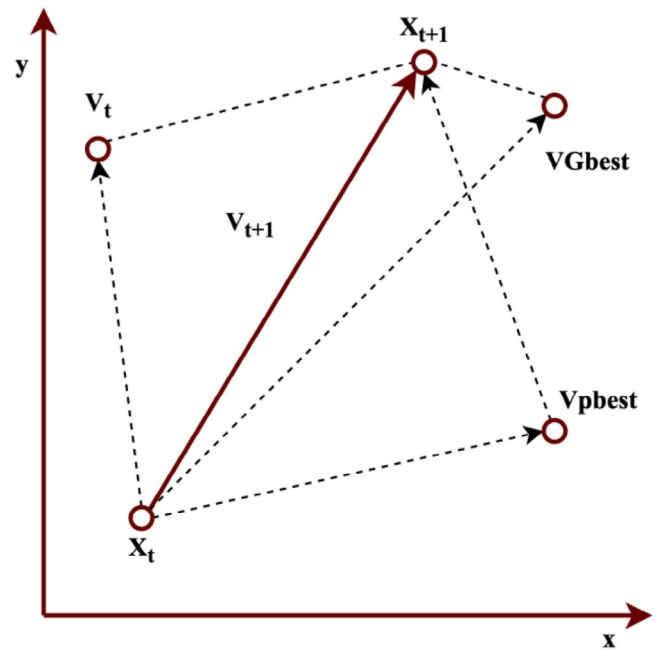


FIGURE 3 Particle updating process

The symbol  $w$  denotes an inertia weight while  $k_1$  and  $k_2$  are random factors. The acceleration is denoted  $a_x$ , the velocity is denoted  $S_x$ . The independent variables can be expressed as  $k_1 = v_1 c_1$  and  $k_2 = v_2 c_2$ , where  $v_1, v_2 \in V(0, 1)$ , and  $c_1$  and  $c_2$  are cognitive and social coefficients. The variables  $c_1$  and  $c_2$  denote the coefficients assigned to the stochastic speed terms, which exert forces on a particle in the direction of its personal best (Pbest) and the global best (Gbest). Particles can move away from the target areas when their speed variables have small values. On the other hand, significant magnitudes of this consistently result in a sudden displacement of the particles regarding the designated regions. In this research, the constants  $c_1$  and  $c_2$  are assigned a value of 2.0 by the traditional approach. A suitable adjustment of the inertia  $w$  achieves a harmonious trade-off between global and local investigations and the number of iterations required to search for a best-case scenario. The present study utilizes an inertia correction work called the Inertia Weight Approach (IWA). During the IWA process, the inertia weight denoted as  $w$  is subject to modification by Equation (8):

$$w = w_{max} - \frac{w_{max} - w_{min}}{i_{max}} i. \quad (8)$$

The variables  $w_{max}$  and  $w_{min}$  symbolize the initial and final inertia weights. The maximum number of iterations is denoted by  $i_{max}$ , while the currently active iteration number is represented by 'i'.

### 3.3 | ANFIS-PSO algorithm

This sub-section provides a detailed description of the optimized structure for security, presented in Figure 4 as six steps.



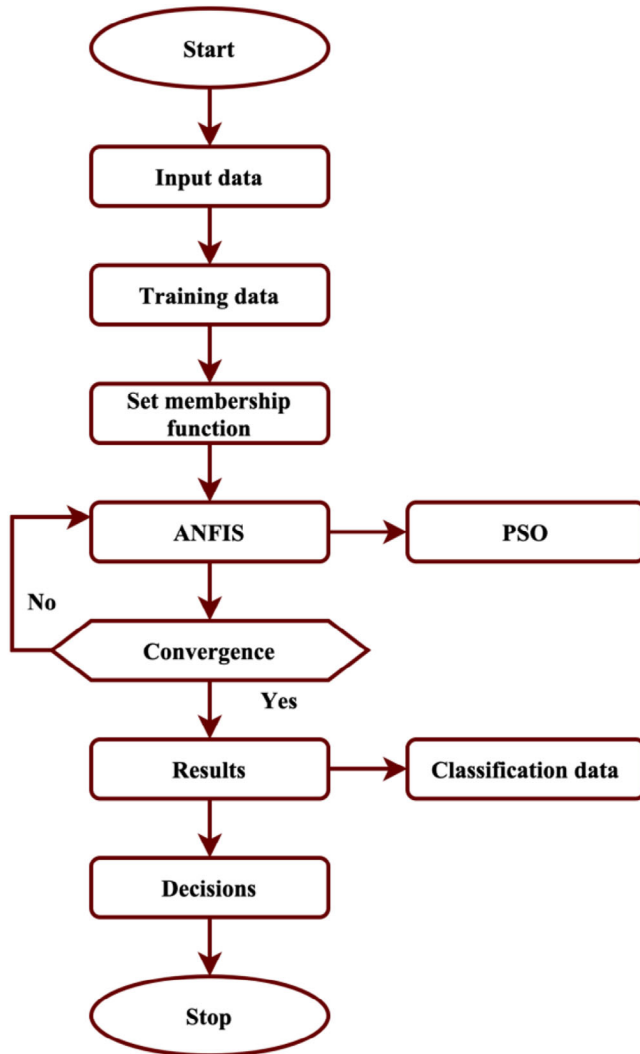


FIGURE 4 Workflow of the proposed SC-SPVE

*Step 1:* Two distinct categories of learning revisions exist which are online learning and batch instruction. A particular kind of learning suggested updating the network after every instance. In contrast, the other type consists of waiting for the whole learning set to be processed before updating the network. To achieve this objective, removing a database from the system is imperative. The task above is accomplished by implementing a neighbour table recorder, which is responsible for capturing and storing all the activities about the neighbour table across all nodes within the network. It is imperative to establish a mapping procedure that distinguishes between typical behaviours, characterized by a high loyalty level, and abnormal tasks, which exhibit a low fidelity level.

*Step 2:* The ANFIS model should be trained using the training dataset obtained from the previous step's deployment. The training process facilitates the system's ability to adapt its settings in response to changes in inputs and outputs. The ANFIS undergoes training iterations until a specified number of iter-

ations is reached or until the desired results are achieved with minimal error. Once the information about learning has been defined, along with the type of functions used for membership and the number of iterations, the entire system undergoes optimization by adjusting membership function variables. PSO is employed to optimize the parameters that are linked to the membership characteristics of the fuzzy inference system.

*Step 3:* Let  $N$  represent the number of functions for membership. A vector with  $N$  dimensions is created. The vector in question encompasses each of the variables of the membership work and will undergo optimization through the utilization of the PSO method. The measure of fitness is formally defined as the Mean Squared Error (MSE).

*Step 4:* In the initial phase, the variables are randomly set up, followed by their updates using the PSO algorithm. During each iteration, a variable of the membership function is revised. In the initial iteration, the value of  $p_x$  is changed. This process continues until all variables have been fixed. Once all parameters have been updated, the update process begins again with the first variable, and the cycle repeats. The variables above are consolidated within a vector, which undergoes updates during each iteration.

The PSO method is employed to optimize the settings of the membership operation, as outlined in the following description:

- Commence the process by setting the initial locations and velocities of the participants. Each particle's location and speed vectors are set up randomly with dimensions corresponding to the size of the issue at hand.
- Assess the efficacy of the individual  $P_{best}$  capability. If the value surpasses the current value of the specific particle, the particle's current location is reset, and  $P_{best}$  updates the individual value. If the maximum value among each particle value surpasses the present global best deal, it is necessary to reset the position of the fine particles.
- The fitness coefficient of each  $P_{best}$  is measured, and the elements with the  $G_{best}$  are stored.
- The velocity is adjusted based on the values of the  $P_{best}$  and  $G_{best}$  positions.
- Revise the particles;

The iteration process will terminate under two conditions: either the present amount of iterations attains the most significant number as defined by the standard, or the result reaches the lowest possible error threshold. Either case, the iteration will cease, and the best solution will be recorded.

*Step 5:* The output obtained from the ANFIS is extracted using the variables determined by the PSO method.

*Step 6:* The ultimate result aligns with the forecast generated by our methodology.

The process of the proposed method using ANFIS and PSO is given in Algorithm 1.

**ALGORITHM 1**

*Initialize Parameters:*

*Set  $i_{max}$ ,  $w$ ,  $c_1$  and  $c_2$  for PSO.*

*Specify inputs ( $N_{in}$ ) and outputs ( $N_{out}$ ) for ANFIS.*

*Set rules ( $r$ ) and  $\tilde{a}_{anfis\_max}$*

*Initialization*

*Initialize  $i_{max}$*

*Set  $i_{anfis\_max} = 0$*

*Initialize positions ( $X$ ) and velocities ( $V$ ) for each particle.*

*Set  $a_{gbest} = \infty$ .*

*Set  $p_{best} = empty$ .*

*Perform PSO Optimization*

*Iterate until reaching  $i_{max}$*

*For each particle:*

*Evaluate fitness ( $F$ )*

*Update  $P_{best}$*

*Update  $G_{best}$*

*Update velocity ( $V$ ) and position ( $X$ ) using Equations (6) and (7).*

*Update  $w$*

*Update ANFIS variables:*

*Update membership function using  $a_{gbest}$ .*

*Check Termination:*

*If iteration reaches  $i_{anfis\_max}$ , terminate.*

*Else, go back to step 4.*

**3.4 | Proposed detection scheme**

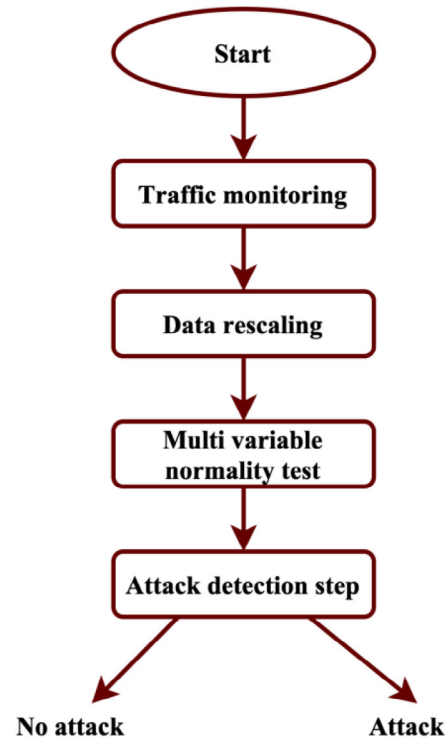
This section presents the MVSDM, a suggested strategy to identify routing security attacks in VANETs. The method utilizes statistical methods that rely on MVN examinations [25]. The proposed identification approach enables the differentiation between normal and fraudulent conduct through four primary steps, elaborated upon and visually represented in Figure 5.

**3.4.1 | Real-time traffic monitoring**

The proposed strategy is founded on malevolent activities exhibiting performance traits that deviate substantially from everyday operations [26]. The initial phase of the methodology involves the creation of the input data through continuously tracking traffic within the transportation system. The system for monitoring is set up in each receiving node and encompasses the evaluation of three essential traffic indicators: throughput, packets dropped ratio, and expenses traffic ratio.

**3.4.2 | Input data rescaling**

The data construction process employed in the identification scheme commences with the network traffic capture and concludes with the data adjusting phase. In this phase, the three



**FIGURE 5** Workflow of the proposed MVSDM

rescaling methods, specifically Z-Score Normalization (ZSN), Min-Max Normalization (MMN), and Normalization by Decimal Scaling (NDS), are utilized to calculate the updated values for each variable present in the initial data set. The output data is subject to continuous updates within a specific period. The data produced in this study are represented by multivariate records sampled at various time intervals.

• *Z-score normalization*

The mean and standard deviation are employed to normalize the data, resulting in features with a mean of zero and one variation [27]. The transformation of each occurrence of the data  $v_x$  results in the formation of the  $v'_x$  in Equation (9):

$$v'_x = \frac{v_x - \alpha}{\beta} \tag{9}$$

The symbols  $\alpha$  and  $\beta$  represent the average and standard deviation of the  $x$ -th initial value of the parameter  $V$ , where  $x$  ranges from 1 to  $m$ .

• *Min-max normalization*

The min-max rescaling method is a method that transforms each value  $v_x$  in the set  $V$  to a new value  $v'_x$  within the range [0, 1] [27]. This transformation is achieved by calculating the new value using Equation (10):

$$v'_x = \frac{v_x - \min(v)}{\max(v) - \min(v)} \tag{10}$$

Let  $v_x$  represent the  $x$ -th initial value of the parameter  $V$ , where  $x$  ranges from 1 to  $m$ . The terms  $\min(v)$  and  $\max(v)$  refer to the lowest and highest values calculated across all the importance of the parameter  $V$ . In this study, it is observed that each variable undergoes a transformation where its smallest value is standardized to 0, and its highest value is normalized to 1

$$\begin{aligned} \text{If } \min(v), \text{ then } v'_x &= 0 \\ \text{If } \max(v), \text{ then } v'_x &= 1 \end{aligned} \quad (11)$$

- *Normalization by decimal scaling*

This method employs a normalization process that involves identifying the maximum value for each variable and adjusting the decimal places of the example values accordingly [27]. The methodology is suitable for datasets exhibiting logarithmic fluctuations in their variables.

Each value  $v_x$  from the provided dataset is transformed into a rescaled value  $v'_x$  using Equations (12) and (13):

$$v'_x = \frac{v_x}{10^y}, \quad (12)$$

$$y = \log_{10}(\max(v_x)). \quad (13)$$

### 3.4.3 | Multivariate normality test

This phase aims to assess the adherence of the information set to the multifaceted distribution of normality by utilising the Rao-Ali multifaceted statistical analysis. The multivariable specimens acquired in the preceding step are converted into univariate specimens for each time window. The databases obtained are unidimensional and will serve as input for the normality examination, specifically the Ryan-Joiner examination. The Ryan-Joiner method calculates the R-J correlation coefficients within each time window.

The attack identification step is carried out based on the reported values of the correlation coefficients. This research presents the SC-SPVE technique to detect assaults in VANETs using the power of soft computing. There is, however, a dearth of particular information regarding the procedures or approaches used for attack detection. The analysis mentions using an ANFIS and PSO together; however, it does not detail how these systems work together to prevent assaults. In theory, because of its remarkable adaptability, ANFIS might learn and adapt to new kinds of attacks. It is possible that PSO, as an optimization method, could help fine-tune attack detection parameters. Rules, features, and anomaly detection algorithms employed by ANFIS, as well as PSO's optimization goals, are kept secret. A more in-depth explanation of the assault detection approach is required to evaluate SC-SPVE's efficacy adequately. In this way, the proposed approach to safeguarding VANETs against various threats might be better understood, replicated, and improved upon by the research community at large.

### 3.4.4 | Attack modelling

In this research, the attack identification efficiency of SC-SPVE is tested by launching the attacks described below.

- *A denial of service (DoS)* attack is a malicious activity that aims to incapacitate a system or network by inundating it with a large volume of fraudulent requests [28]. This results in the unavailability of services and can lead to significant financial repercussions. The impact of a cyber-attack can manifest in various ways, including the disruption of critical services, diminished productivity, and the potential for detrimental effects on the targeted organization's reputation.
- *A botnet attack* refers to using a network comprising compromised computers to carry out extensive attacks, leading to substantial harm, breaches of data, and disruptions in services [29]. The impact of cyberattacks encompasses various consequences, including the coordination of such attacks, compromise of network integrity, loss of sensitive data, and the potential for financial and reputational harm.
- *Phishing* is a fraudulent practice that involves the impersonation of legitimate entities to deceive users, resulting in unauthorized access, financial loss, and compromised accounts [30]. The consequences of data theft encompass various adverse outcomes, including the unauthorized acquisition of personal and financial information, the subsequent misuse of this data for identity theft purposes, the occurrence of fraudulent transactions, and the potential harm inflicted upon the reputation of both individuals and organizations.
- *Ransomware* is malicious software that employs encryption techniques to restrict access to files or computer systems [31]. It operates by coercing victims into making ransom payments to obtain the decryption key, thereby enabling the restoration of data access. This cyberattack has significant consequences, including losing valuable information and financial detriment to the affected parties. The impact of a cybersecurity breach can manifest in various ways, including but not limited to data encryption and unavailability, disruption of operations, financial losses, and the potential disclosure of sensitive information.
- *The Trojan horse* is a type of malicious software that employs deception tactics to appear as legitimate software, thereby facilitating unauthorized access, data theft, and compromise of computer systems [32]. The impact of unauthorized access includes the middle of sensitive information, the erosion of data integrity, and the potential for detrimental effects on system functionality and security.
- *A zero-day exploit* uses undisclosed vulnerabilities, enabling malicious actors to circumvent established security measures and initiate focused attacks before developing patches or defensive mechanisms [33]. The potential consequences include unauthorized access, data breaches, system compromise, and the necessity for immediate security patches or mitigations.
- *Spyware* is malicious software that operates covertly, surreptitiously monitoring users' activities without their knowledge or consent [34]. It is designed to collect and transmit sensitive

information to unauthorized third parties. The impact of privacy invasion encompasses various consequences, including the unauthorized acquisition of personal information, compromise of sensitive data, and the potential for misuse of the collected information.

- A *rootkit* is software designed to conceal malicious activities and grant unauthorized access to an attacker, allowing them to gain control over a compromised system [35]. The impact of unauthorized access can manifest in various ways, including but not limited to persistent presence, stealthiness, system instability, and challenges in detection and removal.

### 3.4.5 | Attack detection

In the preceding stage, the Ryan-Joiner test is employed to quantify the correlation factor between variables R and J. The correlation coefficient values can be utilized to ascertain the likelihood of the presence or absence of an attacker. Reports with R-J values below this threshold can detect abnormal behaviour by establishing an upper limit representing the R-J average essential value. If the condition  $R - J_c \geq R - J_{max}$  is satisfied, it indicates that the assumption of regularity is valid, thereby allowing us to infer the absence of malicious behaviour.

Suppose the difference between  $R - J_c < R - J_{max}$  is less than zero. In that case, the presumption of regularity is invalidated, indicating the presence of a routing assault. An alert is triggered immediately when the R-J coefficient value falls below the predetermined threshold associated with the critical ranges established by Ryan and Joiner. The research builds a controlled and realistic environment to test the SC-SPVE technique, determine how well it secures VANETs, and collect data on a wide range of network parameters and security-related metrics through the Network Simulator NS2. This method makes it easy for other researchers to check and verify their results by replicating their procedures. The proposed approach integrates the capabilities of an ANFIS and PSO to tackle the security issues encountered in VANETs. Additionally, the system incorporates an MVSDM in the capacity of an IDS. By conducting comprehensive simulations and analysis, the method's efficacy in detecting attacks and bolstering the security of VANETs is demonstrated. This approach leads to enhanced throughput, improved packet delivery ratio, and reduced delay.

## 4 | SIMULATION RESULTS AND DISCUSSIONS

The Network Simulator (NS2) is employed to thoroughly assess the proposed method's effectiveness as an IDS for VANETs. The simulation variables and metrics are selected meticulously to evaluate the technique's effectiveness. The obtained results offer essential insights into the efficacy and effectiveness of the approach. This study employed Network Simulator NS-2 (v-2.35), which simulates the mobile network MANET, simulates the attacks, and evaluates the designed IDS concerning attacks

[36]. MATLAB is used to simulate both the ANFIS and PSO phases, and the dataset is given in the link [37].

In the present simulations, the research considers 50 mobile nodes trailing a square field measuring 800×800 m. The number of nodes is incremented to 500 with an increment of 50. One to twenty pairs were randomly selected for data interaction, with each pair transmitting data at a rate of 512 bytes per second. In the Random Waypoint approach, all nodes were relocated using a random process, and their velocities were randomly assigned within a range of 0 to 10 m/s. Furthermore, the inter-movement pause duration is set to 5 s, while the total simulated time spans 200 s. The distribution of the malicious node is also random.

The mean values of the various throughput methods (measured in kilobits per second) are presented in Figure 6. The performance metrics of different networking protocols are as follows: SDN + SOM achieved a score of 140.99, SAES scored 141.53, ODMRP obtained 141.45, ECC achieved 140.65, BBC scored 141.32, MEC received 141.24, and SC-SPVE achieved a score of 149.45. The method suggested in this study, which combines ANFIS and PSO-based security systems and an intrusion detection scheme based on soft computing, consistently demonstrates superior performance compared to other methods.

In the above Figure 6, the average throughput achieved by this method is measured at 149.45 kbps. The observed rise in throughput can be ascribed to the intelligent adaptation and optimization abilities of the soft computing methods utilized in the suggested approach. These techniques effectively enhance the effectiveness of data transmission and safety features within the vehicular environment.

The mean values of delay (ms) for all of the techniques are plotted in Figure 7. The scores for various network protocols are as follows: SDN + SOM received a score of 29.63, SAES scored 30.07, ODMRP achieved a score of 29.33, ECC received a score of 29.63, BBC also scored 29.63, MEC obtained a score of 29.52, and SC-SPVE had the lowest score of 23.75. The method suggested in this study utilizes ANFIS and PSO-based techniques to develop a security system. The results indicate that this approach exhibits a notably reduced delay, with an average delay of 23.75 ms, compared to alternative methods. The reduction in delay can be ascribed to proficiently utilizing soft computing methods in the suggested strategy, facilitating efficient data processing, analysis, and decision-making, resulting in diminished communication delays and enhanced system efficiency.

The mean values of the packet delivery ratio for all of the techniques are represented in Figure 8. The performance metrics of various network protocols are as follows: SDN + SOM achieved a score of 92.09, SAES scored 92.06, ODMRP obtained a score of 92.02, ECC achieved a score of 92.12, BBC scored 92.07, MEC received a score of 92.02, and SC-SPVE achieved the highest score of 95.40. The utilization of the ANFIS and PSO-based security system, along with the intrusion detection scheme based on soft computing (SC-SPVE), results in a notably elevated packet delivery ratio, averaging 95.40%. The improved packet delivery ratio can be ascribed to the intelligent decision-making capabilities of soft computing methods, which facilitate efficient routing, congestion control, and error

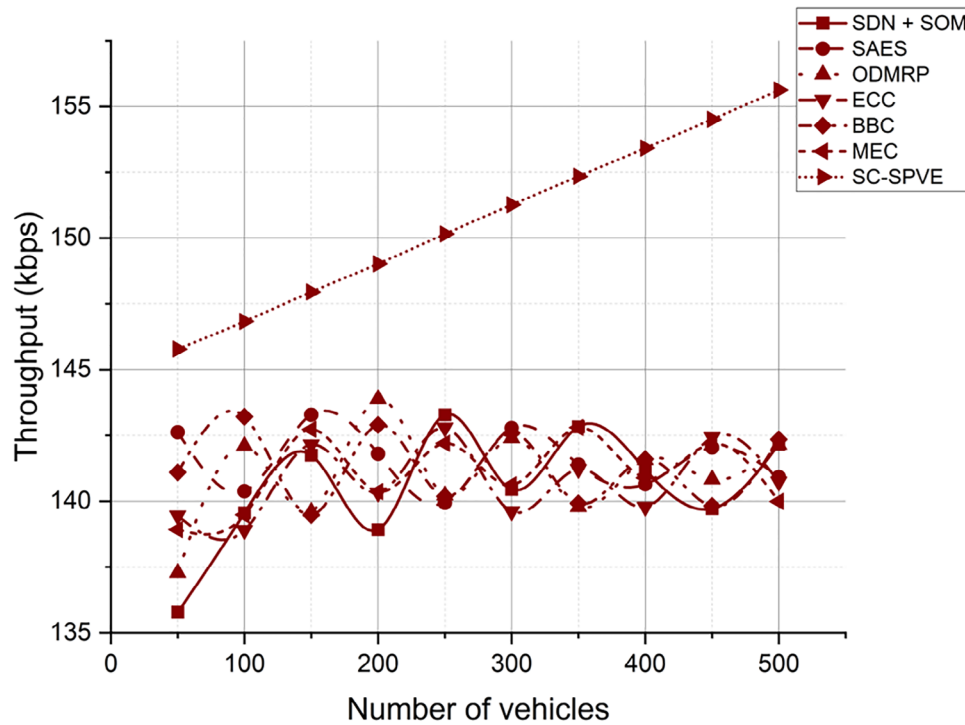


FIGURE 6 Throughput analysis

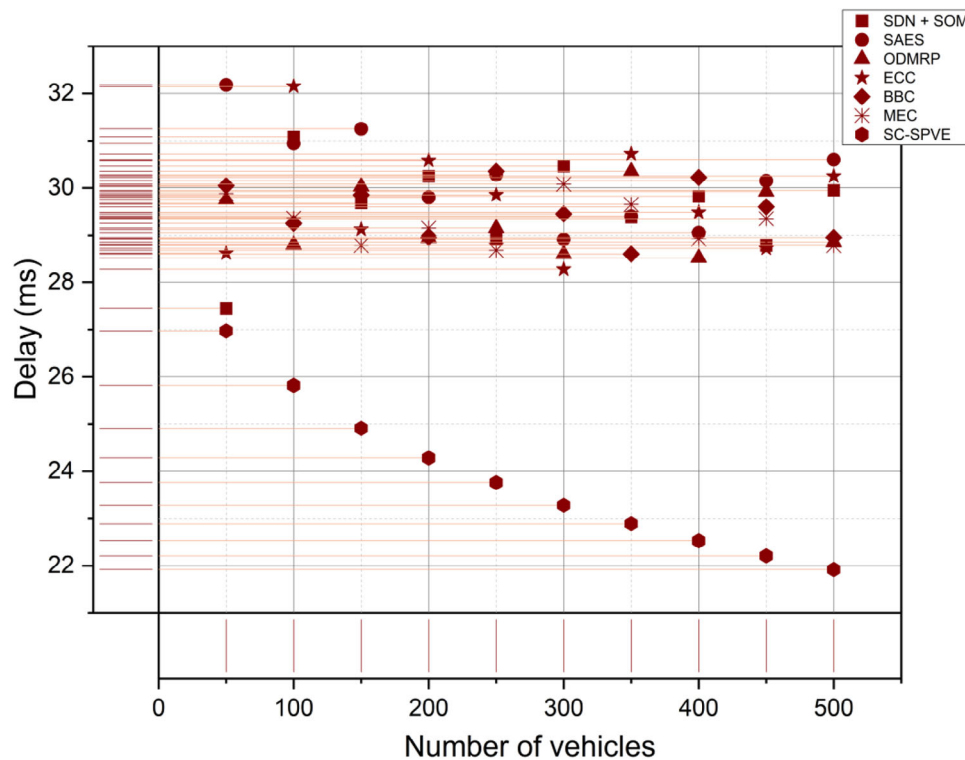


FIGURE 7 Delay analysis

correction processes. As a result, data delivery is improved, and packet loss is decreased.

The mean values of the detection time (in ms) for all the methods are plotted in Figure 9. The scores for various network protocols are as follows: SDN + SOM received a score

of 7.94, SAES scored 8.01, ODMRP achieved a score of 7.98, ECC received a score of 8.00, BBC scored 7.96, MEC achieved a score of 7.97, and SC-SPVE scored 6.75. The attacks considered are DoS\_attack, Botnet\_attack, Phishing, Ransomware, Trojan\_horse, Zero-day, Spyware, and Rootkit [38]. The method

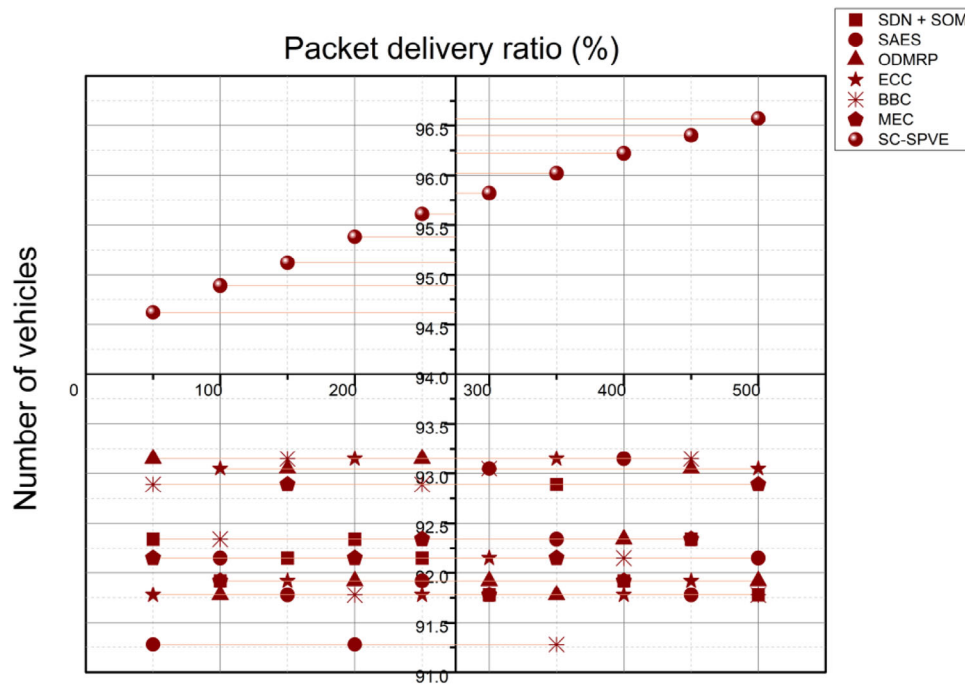


FIGURE 8 Packet delivery ratio

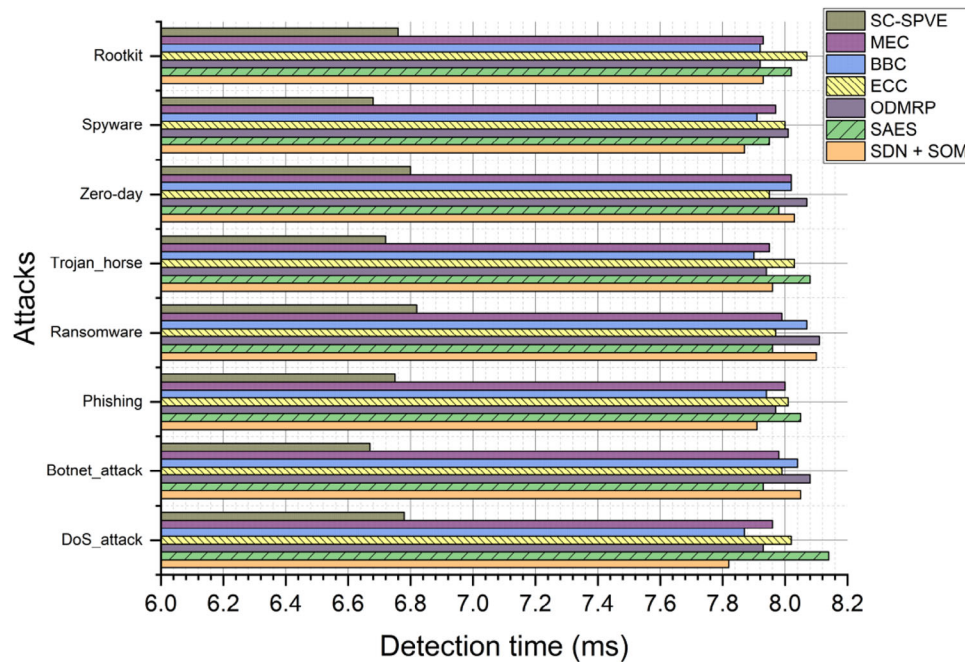


FIGURE 9 Attack detection time analysis

proposed in this study utilizes the ANFIS and PSO to develop a security system.

Figure 9 shows that this approach achieves a notably reduced detection time, averaging 6.75 mds. The decrease in the duration required for detection can be ascribed to the practical and precise anomaly detection mechanisms implemented by the soft computing methods, facilitating expedited identification and response to malevolent activities. As a result, there is an expe-

ditioned identification and resolution of security vulnerabilities, thereby augmenting the system’s overall efficacy.

The mean precision values for all the techniques for various attacks are shown in Figure 10a. The performance metrics of various network protocols are as follows: SDN + SOM achieved a score of 85.78, SAES scored 83.72, ODMRP obtained a score of 85.57, ECC scored 83.57, BBC achieved a score of 85.16, MEC scored 83.64, and SC-SPVE achieved

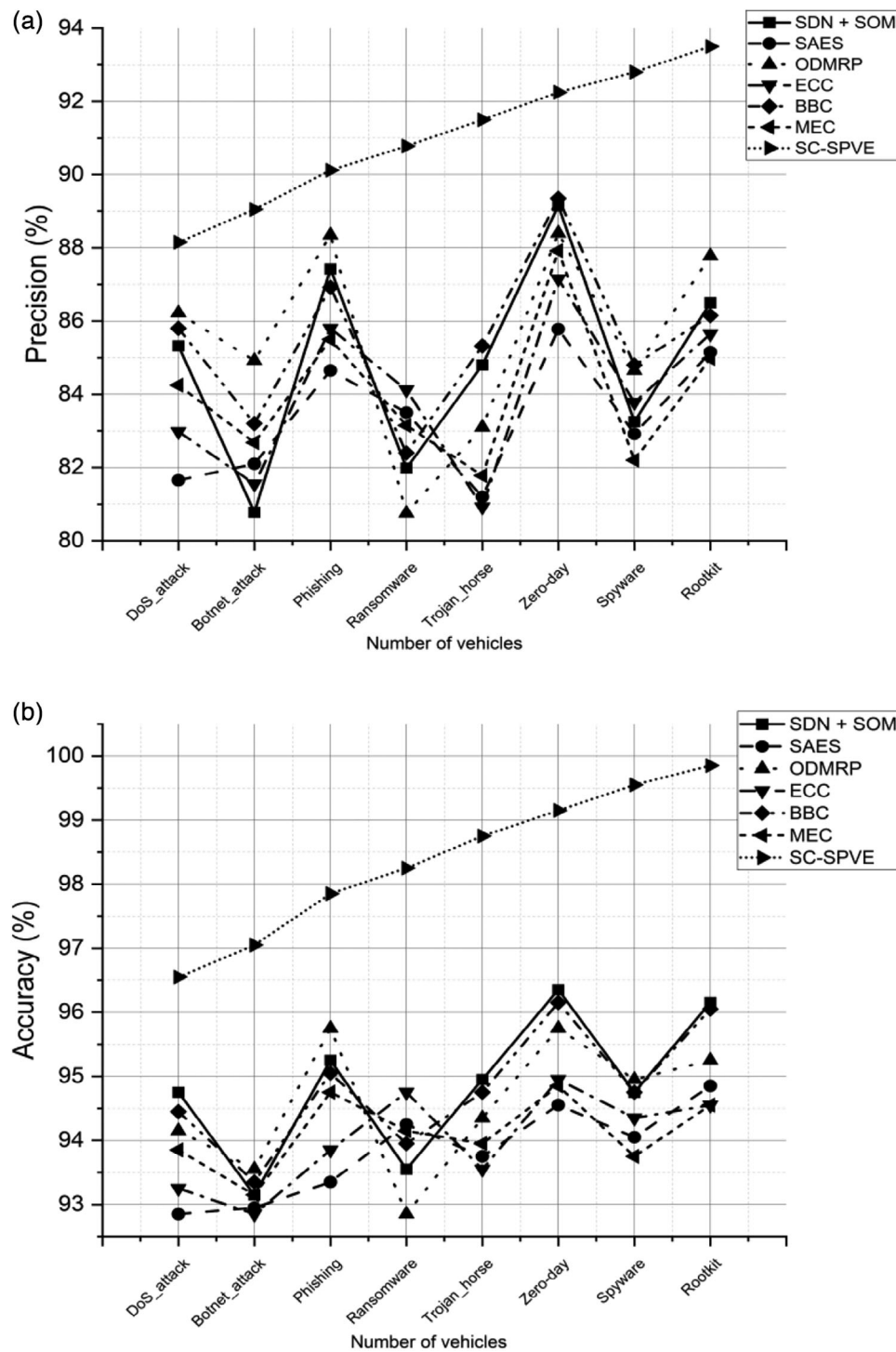


FIGURE 10 (a) Precision and (b) accuracy analysis

the highest score of 91.67. The method proposed in this study, which utilizes soft computing techniques, demonstrates a notably elevated level of precision, averaging 91.67%. The observed enhancement can be ascribed to the increased efficacy of the soft computing-based methodology in accurately discerning and categorizing various attacks, leading to a reduction in false positives and a higher degree of precision in detection.

The average results of all the techniques in terms of accuracy are plotted in Figure 10b. The performance metrics of various network protocols are as follows: SDN + SOM achieved a score of 94.09, SAES scored 93.11, ODMRP reached a score of 94.47, ECC scored 93.16, BBC achieved a score of 94.28, MEC scored 93.49, and SC-SPVE achieved the highest score of 98.07. The security system proposed, SC-SPVE, exhibits a notably enhanced level of accuracy, averaging 98.07%. The observed

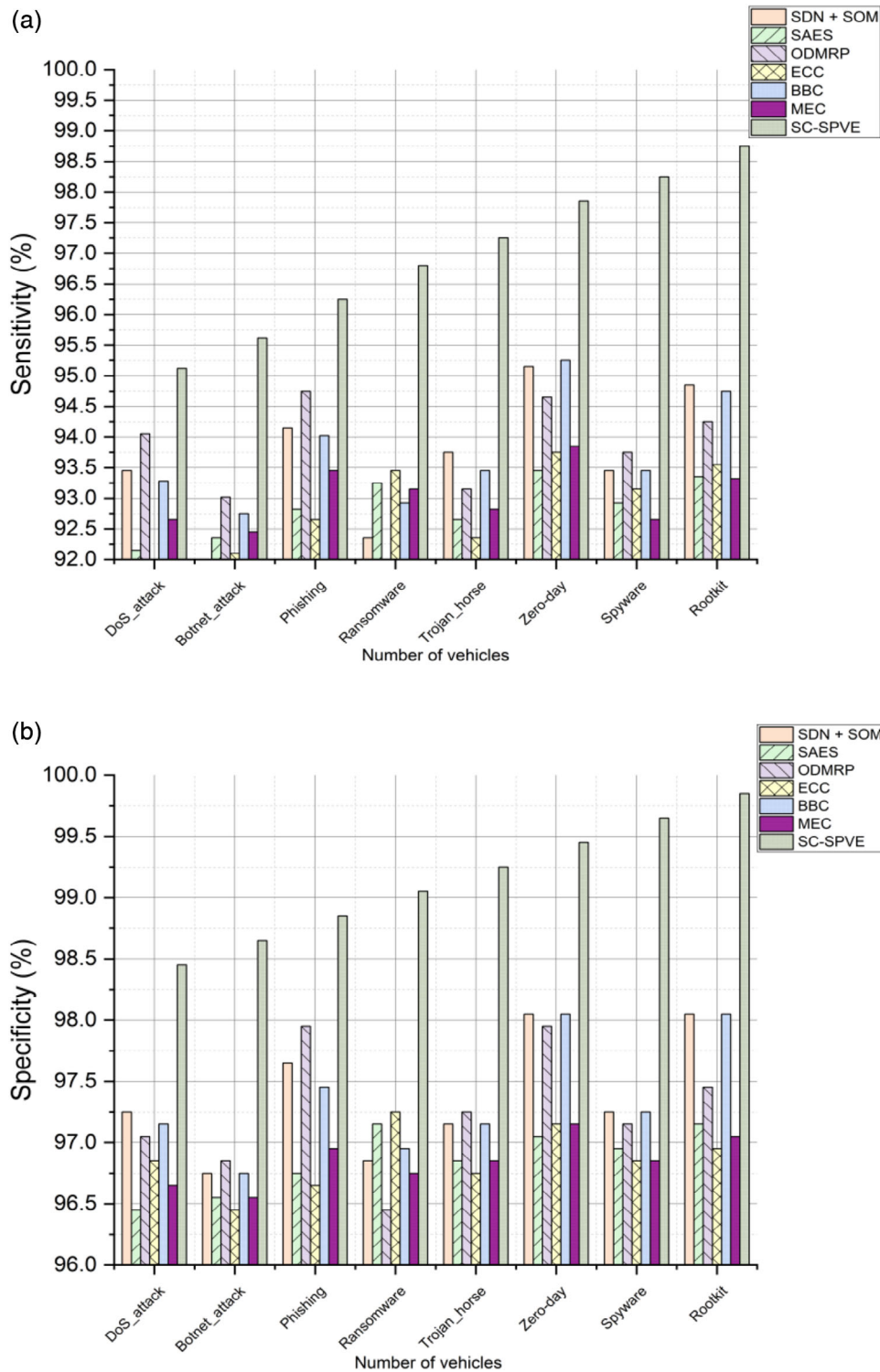


FIGURE 11 (a) Sensitivity and (b) specificity analysis

rise in performance can be ascribed to the efficacy of computational methods in effectively managing intricate and fluctuating traffic patterns, resulting in enhanced accuracy in detection and improved overall system efficiency.

Figure 11a presents the mean sensitivity values across all methods. The performance metrics of various network proto-

cols are as follows: SDN + SOM achieved a score of 93.79, SAES scored 92.97, ODMRP achieved a score of 93.69, ECC scored 92.72, BBC achieved a score of 93.79, MEC scored 93.09, and SC-SPVE achieved the highest score of 97.35. The proposed method, SC-SPVE, demonstrates the highest level of sensitivity, averaging 97.35%. The observed enhancement



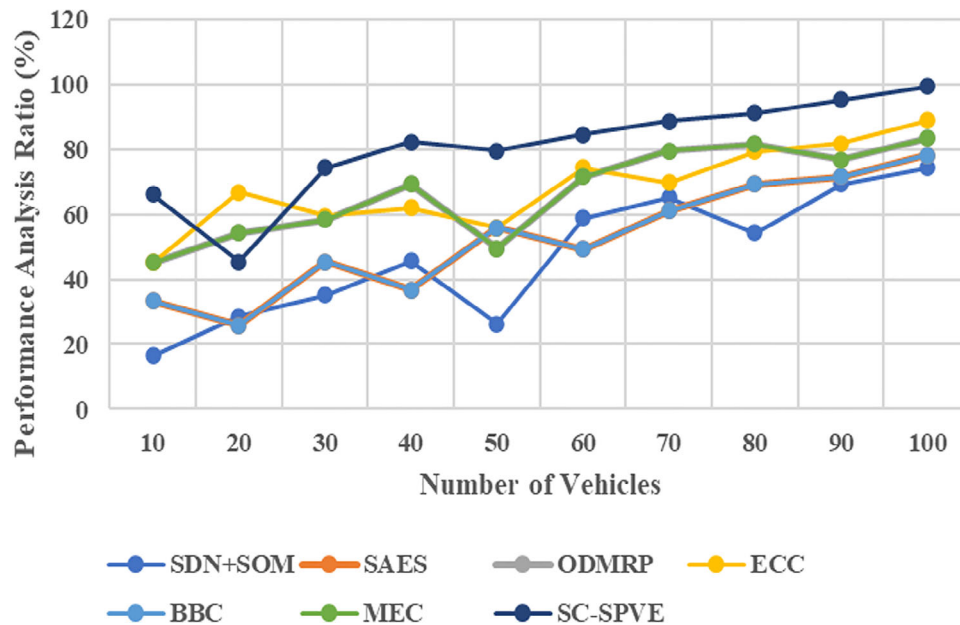


FIGURE 12 Performance analysis

in performance can be ascribed to the utilization of sophisticated techniques within the soft computing-based methodology. These techniques augment the capacity to effectively identify and categorize various attacks, leading to an increased rate of correctly identified positive instances.

Regarding specificity, the average outcomes of all the methods are plotted in Figure 11b. The performance metrics of various network protocols are as follows: SDN + SOM achieved a score of 97.55, SAES scored 96.81, ODMRP obtained a score of 97.20, ECC achieved a score of 96.94, BBC scored 97.47, and MEC received a score of 96.89. The SC-SPVE system achieved a success rate of 99.12%. The security system proposed, known as SC-SPVE, exhibits a remarkably high level of specificity, averaging 99.12%. The observed rise can be ascribed to the proficient application of soft computing methodologies, which effectively mitigate false positives and augment the capacity to precisely detect regular network activity, consequently leading to an elevated true negative ratio.

In above Figure 12, SC-SPVE is shown to improve the safety and efficacy of VANETs communications through an analysis of its performance. SC-SPVE's throughput of 148.71 kilobits per second is impressive, demonstrating its capacity for dependable data transmission speeds. It has a low delay of 23.60 ms, making it ideal for real-time safety applications that require little communication latency. The network excels at sending and receiving data with a packet delivery ratio of 95.62 percent. SC-SPVE has a high rate of accuracy in detecting threats (99.55%) and a high rate of precision in detecting attacks (92.80%). Its ability to differentiate between benign and harmful actions is demonstrated by its sensitivity (98.25%) and specificity (99.65%). SC-SPVE also achieves fast attack detection with a detection time of 6.76 ms, which is critical for taking immediate action

in the face of attacks. In conclusion, SC-SPVE is an effective method for protecting VANETs while allowing for speedy data transfer because it excels in security and performance.

Latency decreases when the time it takes for information to get from one point in a network or system to another decreases. Telecommunications, computer networks, and real-time systems rely heavily on this performance parameter. Methods and tools such as enhancing network architecture, utilizing high-speed data transmission methods, and utilizing efficient data processing algorithms are all used to decrease latency. System and application speed and usability, especially for those that depend on instantaneous and real-time interactions, can be greatly improved by minimizing latency.

The proposed SC-SPVE method yielded average results as follows: a throughput of 148.71 kilobits per second, an average delay of 23.60 ms, a packet delivery ratio of 95.62%, a precision of 92.80%, an accuracy of 99.55%, a sensitivity of 98.25%, a specificity of 99.65%, and a detection time of 6.76 ms. The observed outcomes exhibit superior performance compared to alternative approaches, primarily attributed to the proficient application of soft computing methodologies. This utilization facilitates enhanced identification and categorization of attacks, improving performance metrics.

## 5 | CONCLUSION AND FUTURE SCOPE

VANETs possess distinct characteristics that render them well-suited for various applications, with a particular emphasis on enhancing road safety. The preservation of information security in VANETs is of utmost importance due to the existence of multiple forms of attacks that have the potential to compromise communication between vehicles. The SC-SPVE technique

integrates the functionalities of an ANFIS and PSO to identify black hole attacks in VANETs efficiently. The proposed method can dynamically examine the network environment and discern malicious behaviours by applying soft computing techniques. The efficacy of the SC-SPVE method has been demonstrated through simulation results conducted in the Network Simulator NS2. The average outcomes for the proposed SC-SPVE technique are as follows: Throughput at a rate of 148.71 kilobits per second, Average Delay of 23.60 mds, Packet Delivery Ratio of 95.62%, Precision of 92.80%, Accuracy of 99.55%, Sensitivity of 98.25%, Specificity of 99.65%, and Detection Time of 6.76 ms. Despite the encouraging outcomes, the proposed research still faces challenges and limitations. The scalability of the SC-SPVE method becomes a significant challenge as the number of vehicles in a VANET increases. Moreover, it is imperative to conduct additional research to examine the influence of different network variables and traffic patterns on the efficacy of the proposed approach.

For future research, it is imperative to tackle scalability challenges and expand the SC-SPVE approach to accommodate various attacks, thereby augmenting the overall security and privacy of VANETs. In addition, the examination of the incorporation of sophisticated machine learning and artificial intelligence methodologies can yield supplementary perspectives and enhance the efficiency of intrusion detection and prevention in VANETs.

## AUTHOR CONTRIBUTIONS

**V Thirupathy Kesavan:** Conceptualization; data curation; formal analysis; methodology; software; validation; writing—original draft. **S. Murugavalli:** methodology; software; visualization; validation; writing—review & editing. **Manoharan Premkumar:** Conceptualization; methodology; software; supervision; visualization; writing—review & editing. **Shitharth S:** Formal analysis; validation; visualization; writing—review & editing.

## CONFLICT OF INTEREST STATEMENT

The authors declare no conflict of interest.

## DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

## ORCID

Manoharan Premkumar  <https://orcid.org/0000-0003-1032-4634>

## REFERENCES

- Tonguz, O., Wisitpongphan, N., Bai, F., Mudalige, P., Sadekar, V.: Broadcasting in VANET. In: 2007 Mobile Networking for Vehicular Environments, pp. 7–12. IEEE, Piscataway (2007)
- Mahi, M.J.N., Chaki, S., Ahmed, S., Biswas, M., Kaiser, S., Islam, M.S., Whaiduzzaman, M.: A review on VANET research: Perspective of recent emerging technologies. *IEEE Access* 10, 65760–65783 (2022)
- Quy, V.K., Nam, V.H., Linh, D.M., Ngoc, L.A.: Routing algorithms for MANET-IoT networks: a comprehensive survey. *Wirel. Pers. Commun.* 125(4), 3501–3525 (2022)
- Njoku, J.N., Nwakanma, C.I., Amaizu, G.C., Kim, D.S.: Prospects and challenges of Metaverse application in data-driven intelligent transportation systems. *IET Intel. Transport Syst.* 17(1), 1–21 (2023)
- Chen, X., Yang, A., Tong, Y., Weng, J., Weng, J., & Li, T.: A multi-signature-based secure and OBU-friendly emergency reporting scheme in VANET. *IEEE IoT J.* 9(22), 23130–23141 (2022)
- Khan, A.R., Jamlos, M.F., Osman, N., Ishak, M.I., Dzaharudin, F., Yeow, Y.K., Khairi, K.A.: DSRC technology in vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) IoT system for Intelligent transportation system (ITS): A review. *Recent Trends in Mechatronics Towards Industry 4.0: Selected Articles from iM3F 2020*, pp. 97–106. Springer Nature, Singapore (2022)
- Xie, Q., Ding, Z., Zheng, P.: Provably Secure and Anonymous V2I and V2V Authentication Protocol for VANETs. *IEEE Trans. Intell. Transp. Syst.* 24(7), 7318–7327 (2023)
- Al-Shareeda, M.A., Manickam, S.: A systematic literature review on security of vehicular ad-hoc network (VANET) based on VEINS framework. *IEEE Access* 11, 46218–46228 (2023)
- Mdee, A.P., Khan, M.T.R., Seo, J., Kim, D.: Security-compliant and collective pseudonyms are swapped for location privacy preservation in VANETs. *IEEE Trans. Veh. Technol.* 72, 10710–10723 (2023)
- Poongodi, M., Bourouis, S., Ahmed, A.N., Vijayaragavan, M., Venkatesan, K.G.S., Alhakami, W., Hamdi, M.: A novel secured multi-access edge computing based vanet with neuro-fuzzy systems based blockchain framework. *Comput. Commun.* 192, 48–56 (2022)
- Narayanan, K.L., Naresh, R.J.S.E.T.: An efficient key validation mechanism with VANET in real-time cloud monitoring metrics to enhance cloud storage and security. *Sustainable Energy Technol. Assess.* 56, 102970 (2023)
- Soleymani, S.A., Goudarzi, S., Anisi, M.H., Zareei, M., Abdullah, A.H., Kama, N.: A security and privacy scheme based on node and message authentication and trust in fog-enabled VANET. *Veh. Commun.* 29, 100335 (2021)
- Abdulkadhim, F.G., Yi, Z., Tang, C., Onaizah, A.N., Ahmed, B.: Design and development of a hybrid (SDN+ SOM) approach for enhancing security in VANET. *Appl. Nanosci.* 13(1), 799–810 (2023).
- Sajini, S., Anita, E.M., Janet, J.: Improved data communication security in the VANET environment using the ASCII-ECC algorithm. *Wireless Personal Communications* 128(2), 759–776 (2023)
- Zhang, S., Lagutkina, M., Akpınar, K.O., Akpınar, M.: Improving performance and data transmission security in VANETs. *Comput. Commun.* 180, 126–133 (2021)
- Inedjaren, Y., Maachaoui, M., Zedini, B., Barbot, J.P.: Blockchain-based distributed management system for trust in VANET. *Veh. Commun.* 30, 100350 (2021)
- Alharthi, A., Ni, Q., Jiang, R.: A privacy-preservation framework based on biometrics blockchain (BBC) to prevent attacks in VANET. *IEEE Access* 9, 87299–87309 (2021)
- Rajeswari, R.M., Rajesh, S.: Enhance security and privacy in VANET-based sensor monitoring and emergency services. *Cybern. Syst.* 1–22 (2023)
- Jang, J.S.: ANFIS: adaptive-network-based fuzzy inference system. *IEEE Trans. Syst. Man Cybern.* 23(3), 665–685 (1993)
- Jiang, H., Hua, L., Wahab, L.: SAES: A self-checking authentication scheme with higher efficiency and security for VANET. *Peer Peer Netw. Appl.* 14, 528–540 (2021)
- Marini, F., Walczak, B.: Particle swarm optimization (PSO). A tutorial. *Chemom. Intell. Lab. Syst.* 149, 153–165 (2015)
- Sharma, P., Pandey, S., Jain, S.: Implementing efficient security algorithm and performance improvement through ODMRP protocol in VANET environment. *Wirel. Pers. Commun.* 123(3), 2555–2579 (2022)
- Aravindkumar, S., Varalakshmi, P.: VANET: Optimal cluster head selection using opposition-based learning. *Intell. Autom. Soft Comput.* 33(1), 601–617 (2022)
- Devi, S.C., Maheshwari, D.: An embellished particle swarm optimization technique in VANET for finding optimal route (E-PSO). *SN Comput. Sci.* 4(2), 109 (2022)

25. Kourti, T.: Application of latent variable methods to process control and multivariate statistical process control in industry. *Int. J. Adapt. Control Signal Process.* 19(4), 213–246 (2005)
26. Wang, M., Shan, H., Lu, R., Zhang, R., Shen, X., Bai, F.: Real-time path planning based on hybrid-VANET-enhanced transportation system. *IEEE Trans. Veh. Technol.* 64(5), 1664–1678 (2014)
27. Ajjaj, S., El Houssaini, S., Hain, M., El Houssaini, M.A.: A new multivariate approach for real-time detection of routing security attacks in VANETs. *Information* 13(6), 282 (2022)
28. Gu, Q., Liu, P.: Denial of service attacks. *Handbook of Computer Networks: Distributed Networks. Network Plan. Control Manag. New Trends Appl.* 3, 454–468 (2007)
29. Hoque, N., Bhattacharyya, D.K., Kalita, J.K.: Botnet in DDoS attacks: trends and challenges. *IEEE Commun. Surv. Tutor.* 17(4), 2242–2270 (2015)
30. Ramzan, Z.: Phishing attacks and countermeasures. *Handbook of Information and Communication Security* 433–448 (2010)
31. Brewer, R.: Ransomware attacks: detection, prevention and cure. *Network Security* 2016(9), 5–9 (2016)
32. Gisin, N., Fasel, S., Kraus, B., Zbinden, H., Ribordy, G.: Trojan-horse attacks on quantum-key-distribution systems. *Physical Review A* 73(2), 022320 (2006)
33. Aleroud, A., Karabatis, G.: Detecting zero-day attacks using contextual relations. In: *Knowledge Management in Organizations: 9th International Conference*, pp. 373–385. Springer International Publishing, Cham (2014)
34. Thompson, R.: Why spyware poses multiple threats to security. *Commun. ACM* 48(8), 41–43 (2005)
35. Moon, H., Lee, H., Heo, I., Kim, K., Paek, Y., & Kang, B.B.: Detecting and preventing kernel rootkit attacks with bus snooping. *IEEE Trans. Dependable Secure Comput.* 14(2), 145–157 (2015)
36. <https://en.wikipedia.org/wiki/NS2>. Accessed 10 Feb 2023
37. <https://www.kaggle.com/datasets/haris584/vehicular-obu-capability-dataset>. Accessed 25 Jan 2023
38. Dhanaraj, R.K., Islam, S.H., Rajasekar, V.: A cryptographic paradigm to detect and mitigate blackhole attacks in VANET environments. *Wirel. Netw.* 28(7), 3127–3142 (2022)

**How to cite this article:** Thiruppathy Kesavan, V., Murugavalli, S., Premkumar, M., Selvarajan, S.: Adaptive neuro-fuzzy inference system and particle swarm optimization: A modern paradigm for securing VANETs. *IET Commun.* 17, 2219–2236 (2023). <https://doi.org/10.1049/cmu2.12692>