






ORIGINAL

Optimized Transformer-Based Security For Vehicular Network Communication Against Denial-of-Service Attack

Seguridad optimizada basada en transformadores para comunicaciones de redes vehiculares contra ataques de denegación de servicio

Ramani Gaddam¹ , Amarendra Kothalanka¹  

¹Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation. Vaddeswaram, 522502, Andhra Pradesh, India.

Cite as: Gaddam R, Kothalanka A. Optimized Transformer- Basde Security for Vehicular Network Communication Against Denial- of - Service Attack. Salud, Ciencia y Tecnología - Serie de Conferencias. 2025; 4:1424. <https://doi.org/10.56294/sctconf20251424>


Submitted: 01-07-2024

Revised: 20-10-2024

Accepted: 11-02-2025

Published: 12-02-2025

Editor: Prof. Dr. William Castillo-González 

Corresponding Author: Amarendra Kothalanka 

ABSTRACT

Objective: a Vehicular Ad-Hoc Network (VANET) is one of the crucial elements of an Intelligent Transport System (ITS) and plays a significant role in security and communication. VANETs are susceptible to Denial of Service (DoS) attacks, which are an inherent threat to the security and performance of such networks, requiring more sophisticated detection and countermeasures.

Method: in response to this problem, the Spatial Hyena Security Transformer Model (SHSTM) is introduced to improve the security and use of Vehicular Ad-hoc Network (VANET) communication against DoS attacks. The network nodes are set up to enable Vehicle-to-Vehicle (V2V) communication; the SHSTM constantly detects each node to detect and filter out DoS attack targets. The model includes an effective Cluster Head (CH) selection approach based on traffic patterns to enhance network security.

Results: comparative performance measurements conducted based on network positions before and after the attacks show enhanced overall performance in terms of Packet Delivery Ratio (PDR), Network Throughput (NT), Energy Consumption (EC), End-to-End Delay (EED), and Attack Detection Ratio (ADR). The network attains an NT of 3,91 Mbps, minimal EC of 1,02 mJ, highest PDR of 99,04 %, minimal EED of 0,0206 seconds, and higher ADR of 98 %.

Conclusions: the design of the proposed SHSTM proved a significant improvement in security and network performance, which outperforms the existing state-of-the-art technique. Hence, it is considered a potential solution to address the DoS threat in VANET.

Keywords: VANET; Denial of Service; Security; Cluster Head; Packet Delivery Ratio; Dely; Network Throughput; Energy Consumption.

RESUMEN

Objetivo: una red ad hoc vehicular (VANET) es uno de los elementos cruciales de un sistema de transporte inteligente (ITS) y desempeña un papel importante en la seguridad y la comunicación. Las VANET son susceptibles a ataques de denegación de servicio (DoS), que son una amenaza inherente a la seguridad y el rendimiento de dichas redes, que requieren una detección y contramedidas más sofisticadas.

Método: en respuesta a este problema, se presenta el modelo de transformador de seguridad de hiena espacial (SHSTM) para mejorar la seguridad y el uso de la comunicación de la red ad hoc vehicular (VANET) contra ataques DoS. Los nodos de la red están configurados para permitir la comunicación de vehículo a vehículo (V2V); el SHSTM detecta constantemente cada nodo para detectar y filtrar los objetivos de ataques DoS. El modelo incluye un enfoque de selección de cabeza de clúster (CH) eficaz basado en patrones de tráfico para

mejorar la seguridad de la red.

Resultados: las mediciones comparativas de rendimiento realizadas en función de las posiciones de la red antes y después de los ataques muestran un rendimiento general mejorado en términos de índice de entrega de paquetes (PDR), rendimiento de red (NT), consumo de energía (EC), retraso de extremo a extremo (EED) y tasa de detección de ataques (ADR). La red alcanza un NT de 3,91 Mbps, un EC mínimo de 1,02 mJ, un PDR más alto del 99,04 %, un EED mínimo de 0,0206 segundos y un ADR más alto del 98 %.

Conclusiones: el diseño del SHSTM propuesto demostró una mejora significativa en la seguridad y el rendimiento de la red, que supera a la técnica de vanguardia existente. Por lo tanto, se considera una solución potencial para abordar la amenaza DoS en VANET.

Palabras clave: VANET; DoS; Seguridad; Jefe de Grupo; PDR; Retraso; Rendimiento de Red; Consumo de Energía.

INTRODUCTION

The Internet of Things (IoT) and Wireless Sensor Networks (WSN)⁽¹⁾ have become more and more standard in modern periods as an improved paradigm for communication with several applications,⁽²⁾ like Intelligent Transportation Systems (ITS), smart homes, and smart cities. It is anticipated that the number of IoT devices will increase, along with the problems.⁽³⁾ In cars, wireless sensors can monitor various parameters uninterruptedly,⁽⁴⁾ including engine performance, tire pressure, fuel level, and battery health. In the meantime, real-time data enables proactive maintenance and services, which helps identify possible problems before they arise. Wireless sensors are made up of spatially autonomous sensors.⁽⁵⁾

ITS includes VANET, which has enhanced road safety and communication by sharing real-time information between vehicles and nearby locations. These networks use Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication to help improve transport efficiency, decrease accidents, and increase passenger safety. By using of wireless communication renders these networks vulnerable to many cyber threats, with Denial of Service (DoS) attacks being most troublesome.⁽⁶⁾ A DoS attack sends many prohibited packets over the network, resulting in a decline in the network's performance, high response time, and the failure of safety applications to network performance.⁽⁷⁾ It is, therefore, essential to protect Vehicular Ad-hoc Networks (VANET) from DoS attacks to ensure that ITS is reliable and effective.⁽⁸⁾

Typically, anti-such attacks use conventional methods of static intrusion detection or direct cryptography systems that can hardly operate effectively in the given dynamically changing and operating in limited resources VANET.⁽⁹⁾ However, these methods may be primary to an increased number of computations in the network, which may decrease the network's efficiency and Energy Consumption (EC).⁽¹⁰⁾ To overcome these challenges, an intelligent, adaptive, and resource-effective solution is required to improve network security.⁽¹¹⁾

Bio-inspired solutions provide new paradigms for protecting VANETs⁽¹²⁾ that duplicate the behaviors and the optimization algorithms found in biological entities.⁽¹³⁾ These methods rely on features like flexibility, decentralization, and optimality, which make them similarly suitable for VANETs, which are very dynamic and have limited resources.⁽¹⁴⁾ For example, Ant Colony Optimization (ACO) and Particle Swarm Optimization (PSO), two types of swarm intelligence algorithms, have been used in providing solutions for routing, clustering, and intrusion detection in VANET.⁽¹⁵⁾

Likewise, predator-prey models and hyena or bee-inspired social animal behavior give strong approaches for identifying and responding to DoS and other cyber threats.^(16,17,18,19,20) Integrating bio-inspired solutions into VANET security architectures provides real-time scalability and low complexity while achieving high accuracy in threat identification.⁽²¹⁾ They facilitate optimal use of the available resources, optimize network capacity, and increase capability.^(22,23,24,25) Thus, by mimicking the effectiveness and robustness of the biological systems, the bio-inspired approaches present a probable direction for enhancing secure and intelligent communication in VANET.^(26,27)

In this context, the newly introduced Spatial Hyena Security Transformer Model (SHSTM) aims to propose a new approach to managing DoS attacks and their impacts on network performance. The proposed SHSTM combines a *state-of-the-art* transformer-based model with a metaheuristic inspired by nature for reliable and optimal VANET. In this case, the transformer model checks node activities and quickly recognizes the malicious nodes accurately. In parallel, a novel bio-inspired clustering algorithm that draws from hyenas works to select Cluster Heads (CH) according to traffic patterns, thereby minimizing energy cost and latency.

Real-time adaptability is proposed as one of the SHSTM's components so the network can respond to new threats efficiently. Detailed performance analysis provides the evaluation of SHSTM and proves that the proposed solution is effective with the increase of Packet Delivery Ratio (PDR), Network Throughput (NT), Energy Consumption (EC), End-to-End Delay (EED), and Attack Detection Ratio (ADR). These improvements

secure VANET and increase their EED and NT to make the SHSTM a complete ITS solution. The increasing application of VANET in ITS points to the importance of developing efficient security solutions to support continuous communication and the safety of passengers.

One of the most unsafe cyber threats is the so-called DoS attacks, which can cause accidents and jeopardize the vital workings of vehicles and ITS. Present-day detection techniques are inefficient and do not work well under dynamic networks. This led to the idea of a *state-of-the-art* solution known as SHSTM, which uses Machine Learning (ML) models and bio-inspired methods for securing VANET communication. With these limitations solved, SHSTM provides better attack detection than previous approaches, reduced utilization of system resources, and improved network performance for secure and sustainable ITS.

The significant contribution of this work is summarized as follows

1. To establish the SHSTM, which combines transformer-based models with bio-inspired optimization methods to detect and prevent DoS attacks in VANETs.
2. To maximize the CH selection by using hyena inspired clustering mechanism that dynamically considers traffic patterns to minimize EC to improve scalability and EED.
3. To assess the performance of the proposed SHST with the help of PDR, NT, EC, EED, and ADR to compare its efficiency with the existing security solutions.

The article arrangement is fundamentals as follows: section 2 reviewed the previous related methods with limitations and merits, section 3 states the common problem in the VANET communication, section 4 explains the recommended methodology in detail, the results of the model are computed and compared in section 5; finally, the conclusion is provided in section 6.

Related works

Authors⁽²⁷⁾ introduced a unique model for adapting the crypto keys in in-vehicle Wireless Sensor Networks (WSN), enhancing security and confidentiality. It suggests using the message validation code sent by the sender as a validation method for separate network subsystems. The model is intended for embedded devices, the Internet of Things (IoT), and fixed and limited-range networks. However, it is not flexible for dynamic networks or those with an Internet interface.

Authors⁽²⁸⁾ research on the ITS study suggests a blockchain-based approach for Internet of Vehicles (IoV) privacy security, enabling consensus among problematic nodes. The system uses anonymous communication technologies between vehicles and service providers, outperforming previous methods in efficiency and security. However, more efficient consensus methods and communication data structures are needed.

Authors⁽²⁹⁾ anticipated a Signal-to-Interference-Noise-Ratio (SINR)-based Signal-to-Power Optimizing Network (SOPN) to enhance system efficiency and reduce load. The algorithm identifies nodes with minimum weight, increases their methodologies for nodes with Device-to-Device communication, and considers connectivity factors for better communication. It must include sharing algorithms for the 5Generation sensor network.

Authors⁽³⁰⁾ formed the bio-inspired key-based energy-aware protocol for WSN. Using Lightweight-based Authentication and Key Management (L-AKM), DSTE for secure data transfer, and the Golden Jackal Optimization (GJO) algorithm for clustering increases security and energy efficiency. Simulations demonstrate improved performance, but there are still problems in adjusting to changing network conditions.

Author⁽³¹⁾ suggested a hybrid cryptography method for the IoV, combining a modified elliptic curve, Advanced encryption standards, and dynamic key management. This method improves data security and communication performance in WSN, reducing transmission time and preventing intrusion attempts. The hybrid approach has a success rate of over 99 % in overcoming the malware that attempts during simulated intrusion scenarios, surpassing vulnerabilities of the crypto process trusting on a traditional system. The comprehensive analysis of the literature review on VANET is given in table 1.

The current research problems in VANET are that the security mechanism is not adaptive, problems with EC, inefficient CH selection, high-traffic scalability, and little analysis of security metrics.^(54,55) The traditional security solutions are generally passive and, therefore, can be easily bypassed by advanced methods such as the DoS. Many of the models do not incorporate energy efficiency, so they are inefficient in terms of EC and EED.^(56,57,58,59,60) CH selection methods in existing models are deterministic or random, which leads to low performance and weaknesses. Another issue is scalability, and many frameworks cannot demonstrate acceptable speed when the size of the network increases, which results in delays and decreased NT.^(61,62,63,64,65)

Most of these works lack integration and evaluation based on key factors such as PDR, NT, EC, EED, and ADR.^(66,67,68,69,70) The Spatial Hyena Security Transformer Model (SHSTM), an adaptive security model that uses the behavior of hyenas and transformer models, fills these gaps. This also guarantees real-time identification and prevention of DoS attacks.^(71,72,73,74,75) In this paper, SHSTM employs traffic-aware CH optimization to achieve

better efficiency and minimize EC to increase NL. Due to its scalability, it can perform well under high traffic, effectively close these gaps, and improve VANET security and performance.^(76,77,78,79,80)

Table 1. Analysis of VANET

Proposed Technique	Purpose	Inference
Encrypted and authenticated tunnels with periodic cryptographic key exchange using Advanced Encryption Standard-Cipher Block Chaining-128 (AES-CBC 128), Hash-Based Message Authentication Code (HMAC), and HMAC-based Key Derivation Function (HKDF) ⁽³²⁾	Enhance communication security in in-vehicle WSN	Improved security and integrity using AES-CBC-128, HMAC, and HKDF. Reduced EC compared to Datagram Transport Layer Security (DTLS) and Transport Layer Security (TLS).
Blockchain-based License Plate Recognition (LPR) ⁽³³⁾	Privacy and security in IoV using decentralized LPR	Ensures secure and efficient license plate management by avoiding central gateways and employing key revocation to detect malicious users in the IoV.
SINR-based energy optimization for Device-to-Device (D2D) communication in 5G Vehicular Sensor Networks (VSN) ^(34,35,36)	Optimize EC and system capacity in VANET.	The proposed SINR-based algorithm improves battery lifetime and interference management while maintaining system load and enhancing efficiency.
Efficient Key Distribution for Secure and Energy-Optimized Communication using Bioinspired Algorithms (EKD-SOCBA) ^(37,38,39,40)	Ensure security and energy efficiency in WSN.	GJO improves clustering and CH selection. Dynamic Step-wise Tiny Encryption Algorithm (DS-TEA) ensures lightweight encryption, achieving superior performance over traditional models.
Hybrid Encryption with Dynamic Key Management (DKM) combining Improved Elliptic Curve Cryptography (IECC) and Advanced Encryption Standard (AES-256) ^(41,42,43)	Enhance security and communication performance in IoV	Achieved 99 % success in intrusion prevention and a 30 % reduction in message transmission time. Balances computational efficiency and security in resource-constrained environments.
Adaptive Cross Layered Threshold Protocol (CLTP) ^(44,45)	To improve communication reliability and minimize EC in WSN	CLTP improves energy efficiency and performance by adapting to dynamic network conditions.
Fuzzy based Cross Layer Architecture (FbCLA) ^(46,47,48)	To provide an energy-efficient cross-layer architecture by integrating fuzzy logic for network management	FbCLA optimizes EC through adaptive fuzzy decision-making, increasing the network's stability.
Sailfish K-medoid Model (SKM) ^(49,50)	To optimize CH selection in WSNs using the Sailfish optimization algorithm and K-medoids	SKM improves energy efficiency by reducing the distance between nodes and minimizing EED in CH selection.
Optimized Radial Basis Network (ORBN) ^(51,52,53)	To enhance energy efficiency in VANET communication by optimizing CH selection using a radial basis network	By optimizing CH selection, ORBN achieves lower EC, higher NT, and better network lifespan.

System Model and Problem Statement

The vehicle nodes comprise several constraints that make the entire network communicate with the neighbors. The lack of these constraints leads to malicious measures entering the network, degrading the quality of service (QoS). Considering all other malicious measures, the DoS attack is the most harmful one that marks the wireless vehicle network.^(81,82,83,84,85) Also, the occurrence of a DoS attack cannot be identified at the initial stage. The system model and the problems are described in figure 1.

In VANET^(86,87,88,89,90) nodes have several operational constraints, such as PDR, EED, EC, NT, and ADR. These constraints define the normal behavior of a node, which is mathematically represented by equation (1).

$$C_i = \{P_i \geq P_{th}, D_i \leq D_{th}, E_i \leq E_{th}, S_i \geq S_{th}\} \quad (1)$$

Where P_{th} , D_{th} , E_{th} , and S_{th} are threshold values for normal behavior. A node is considered malicious if it deviates from this normal behavior. The deviation Δ_i for each node v_i is quantified as in equation (2).

$$\Delta_i = w_1 \cdot (P_{th} - P_i) + w_2 \cdot (D_i - D_{th}) + w_3 \cdot (E_i - E_{th}) + w_4 \cdot (S_{th} - S_i) \quad (2)$$

Where $w_1, w_2, w_3,$ and w_4 are weights assigned based on the importance of each metric. A node is flagged as malicious if the deviation exceeds a threshold in equation (3).

$$\Delta_i > \Delta_{th} \tag{3}$$

A transformer-based mechanism is used to compute the probability of a DoS attack given the feature vector of the node. The prediction is given by equation (4).

$$\hat{Y}_i = f_{transformer}(F_i) \tag{4}$$

Where $(Y_i \in [0, 1])$ is the predicted probability of malicious node v_i . If $(Y_i) \geq Y_{th}$, the node is classified as malicious and rejected from the network.

CH is selected using a traffic-aware optimization method to optimize the network after removing malicious nodes, where the CH is selected in equation (5).

$$CH = \text{Arg Max}_{v_i \in V} \left(w_1 \cdot P_i + w_2 \cdot \frac{1}{D_i} + w_3 \cdot \frac{1}{E_i} \right) \tag{5}$$

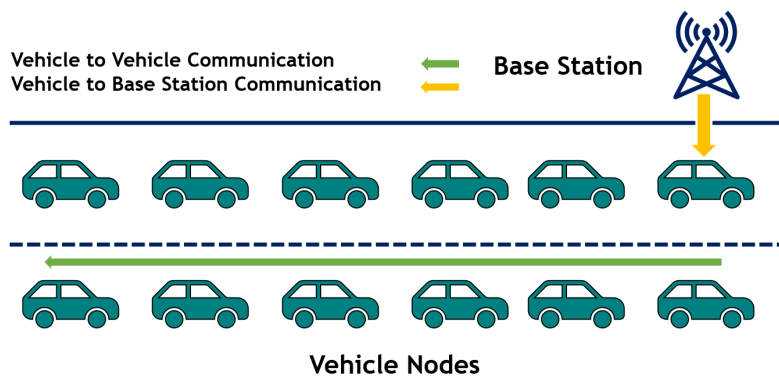


Figure 1. System Model

This model helps to prevent and deal with DoS attacks as successfully as possible while trusting the network and communication parameters at their best.

The DoS attacks frequently act like the normal node, and during data broadcasting, they fail to share the packet with the rear hub, which causes packet drop. These behaviors have attracted the researchers to do the analysis and must end the rate of the DoS result in the network channel. (91,92,93,94,95) There is a need for privacy measures to maintain the network communication. So, the present study has designed a novel optimized transformer mechanism for analyzing and predicting the DoS event. Once the DoS event is predicted, it is eliminated from the vehicular network environment.

METHOD

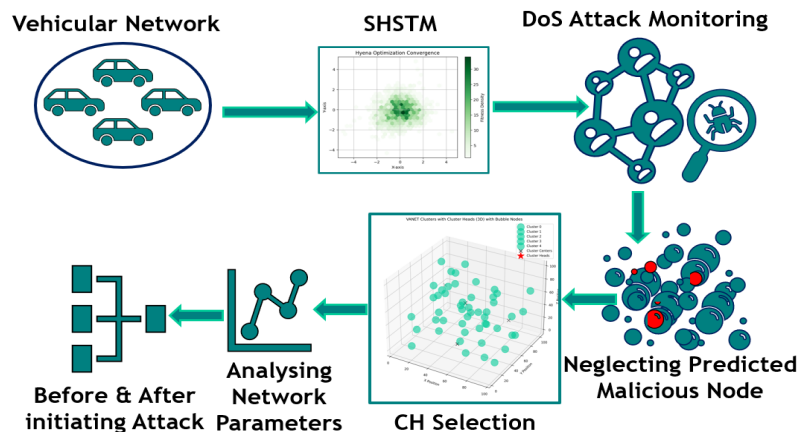


Figure 2. Proposed Methodology

The proposed SHSTM is the hybrid method that integrates the function of the Spatial Transformer Network (STN)⁽²¹⁾ and the Spotted Hyena Optimization Algorithm (SHOA).⁽²²⁾ The spotted hyena optimization is structured based on the social and hunting behavior of the spotted hyena, where individuals explore for prey independently (exploration) while also learning from the successes of others (exploitation). This balanced approach prevents the algorithm from becoming stuck in local optima and efficiently searching for the global optimum solution. It provides better prediction results for attack detection. The model provides better convergence, which results in the quick identification of optimal solutions. To execute the process of the designed SHSTM, required vehicle nodes are initialized in the NS2 environment. The nodes are initialized based on the concept of the spatial transformer. The node deploying process is detailed in equation (6).

$$N = V_x, x = 1, 2, 3 \dots n \quad (6)$$

Here, the node initialization variable is defined as N, V_x is the vehicle nodes deployed at the network n is the number of nodes. Here, the vehicle nodes are randomly deployed at different locations. Each node senses the data of the environment and sends it to the destination.

DoS Attack Detection and Elimination

In VANET communication, the attackers begin the DoS attack by overwhelming the nodes by sending fake warning messages and jamming the channel by sending extensive data. During the DoS attack, the node PDR is distributed. Therefore, in this research, the DoS attack is detected by tracking the traffic of each initialized node. Here, the designed model continuously monitors each node’s receiving and sending packets in the communication environment. The monitoring of the node traffic pattern is conducted based on the encircling behavior of the spotted hyenas, which is explained in equation (7).

$$M = V_x - \vec{v}_1 \cdot d_x (\vec{v}_2 \cdot p_x - t) \quad (7)$$

Here, the node traffic monitoring variable is denoted as V_x , d_x , and t , indicates the coefficient vectors, as well as the node’s sending and receiving data rate, P_x denotes the PDR, and t represents the data flow rate. The nodes ‘ traffic is monitored using the spotted hyena’s behavior, and the DoS attack nodes are predicted. The attack node must be removed for vehicle communication security. The node removal function is detailed in equation (8).

$$E = V_x - a^* \quad (8)$$

Here E is the attack node elimination variable, a^* which is the detected DoS attack nodes. Thus, the DoS attack events in the vehicle communication environment were predicted and prevented to enhance the security of the VANET. Thus, the designed transformer continuously monitors the DoS malicious events and eliminates them to improve the network’s security.

CH Selection

After the DoS attack event elimination, an optimal CH is selected to boost the security and efficacy of the VANET. Here, some parameters, such as EC, mobility, and distance, are considered to select the ideal CH in the created VANET environment. The group formation behavior of the spotted hyena earned the best CH. The hunting phase of the hyena is conducted by the group that moves towards the best agent and saves the ideal solution. Similar to this behavior, the optimal CH from the group is selected and explained in equation (9) for vehicle communication.

$$S_{CH} = \frac{c_m \times f(e, m, d)}{N} \quad (9)$$

Here, the CH selection variable is mentioned as C_m , denoting the cluster members, f is the fitness constant, e indicates the node’s EC, m represents the node mobility, d denotes the distance, and N is the iterations count. The variable S_{CH} saves the optimally selected cluster heads based on the considered parameters. Further, the data transmission occurs between the source and destination through the selected CH. Thus, the security and performance of the VANET can be improved. The performances of the network are measured before and after the introduction of the attack.

Algorithm 1 for Proposed SHSTM

```

Initialize vehicle nodes at random locations in the network
For Each node vi in the network:
Compute initial parameters: Pi, Di, Ei, Si (PDR, EED, EC, ADR)
For Each node vi:
If  $C_i = \{P_i \geq P_{th}, D_i \leq D_{th}, E_i \leq E_{th}, S_i \geq S_{th}\}$ :
Node is considered normal.
Else
Node is considered potentially malicious
For Each node vi:
 $\Delta_i = w_1 \cdot (P_i - P_{th}) + w_2 \cdot (D_i - D_{th}) + w_3 \cdot (E_i - E_{th}) + w_4 \cdot (S_{th} - S_i)$ 
For Each node vi:
If  $\Delta_i > \Delta_{th}$ :
Flag node vi as malicious
For Each node vi:
Fi = Feature Vector (Pi, Di, Ei, Si)
 $(Y_i) = f_{Transformer}(F_i)$ 
If  $(Y_i) >= Y_{th}$ :
Node vi is classified as malicious
For Each malicious node vi:
Remove node vi from the communication network
For Each node vi:
Compute fitness value using:
Fitness =  $w_1 \times P_i + w_2 \times (1/D_i) + w_3 \times (1/E_i)$ 
Select CH as node vi with the maximum fitness value
For selected CHs:
Transmit data between source and destination nodes
Monitor network parameters: PDR, NT, EED, EC, and ADR
Repeat the above steps periodically to ensure network security and optimal performance
End If
End
    
```

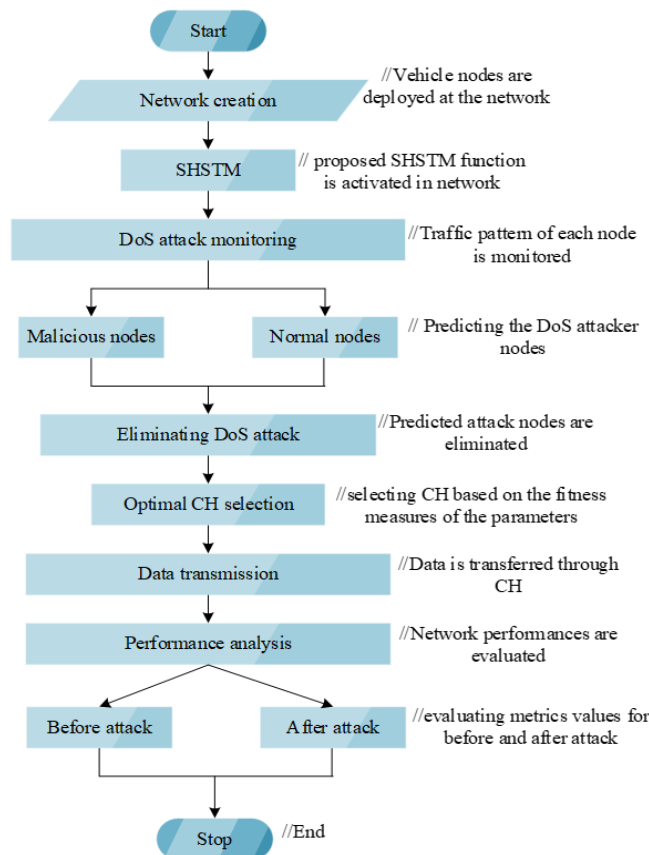


Figure 3. Flowchart SHSTM

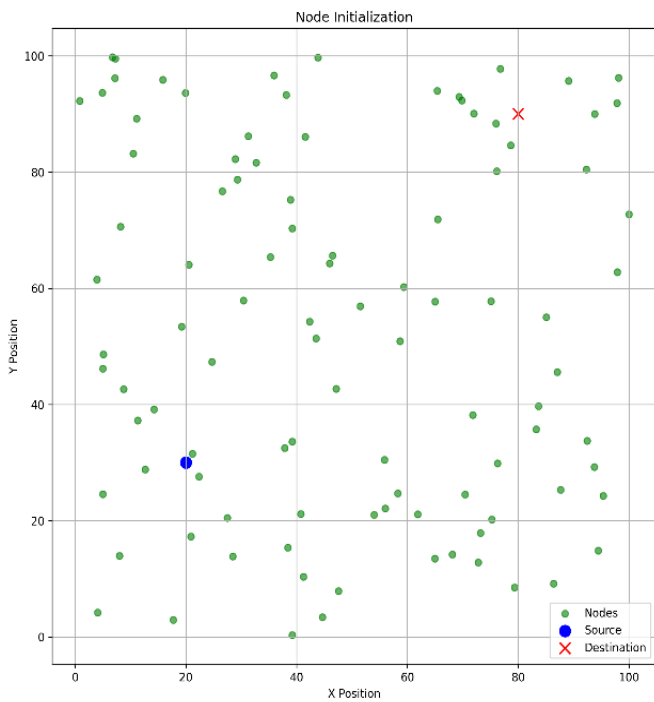
Algorithm 1 provided a complete description of the processes in the created SHSTM model. These step processes served as the basis for running the NS2 code, and the outcomes were confirmed. All of the pseudo-coded mathematical function parameters were integrated into the algorithm. These procedures are provided step-by-step in an algorithm. A comprehensive flow visualization of the proposed plan may be found in figure 2.

RESULTS AND DISCUSSION

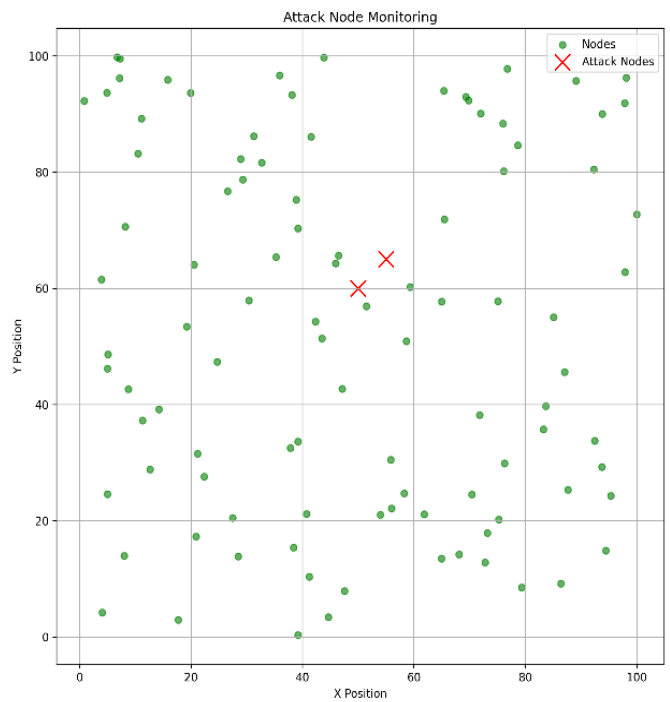
The proposed SHSTM is run on the NS2 tool. Initially, the needed communication nodes were recognized in the VANET. The SHSTM is designed with monitoring and optimal features and is activated in the created network. The designed SHSTM carried out the attack node detection, elimination, and CH selection process to improve the security and performance of the network. The parameters required for simulating the presented research are listed in table 2.

Table 2. Simulation parameters	
Parameter description	
Simulator	NS2
OS	UBUNTU
Application	Vehicle communication
Topology	2D
Network type	WSN
Network size	100×100 m ²
Nodes	100
CH	4
Node Status	Moving
Node mobility	Random
Communication medium	Wireless
Algorithm	Spotted Hyena Optimization

Network Simulation



(a). Node Initialization



(b). Attack Node Monitoring

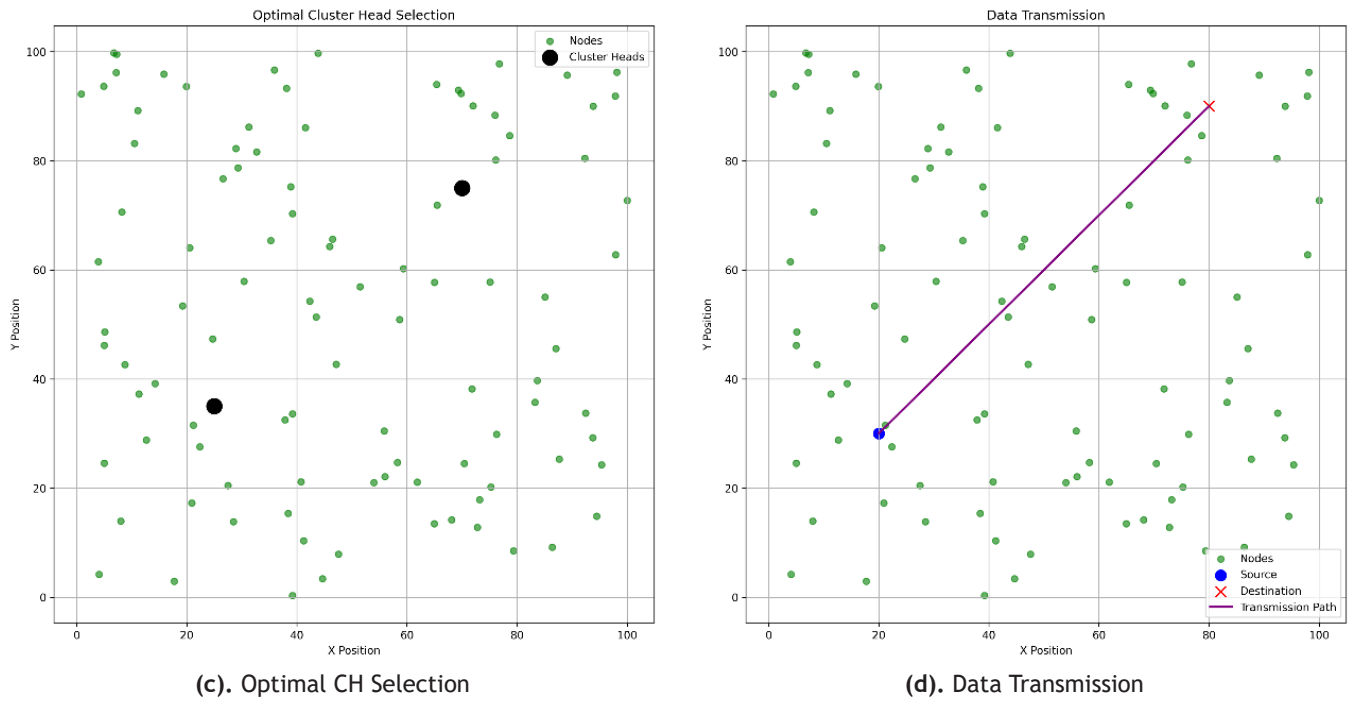


Figure 4. Simulation of VANET

Figure 4 shows different phases of the VANET simulation employing the SHSTM. The first phase, represented in figure 4 (a), shows the nodes randomly placed within the network, with the source node indicated by the blue circle and the destination node shown by the red cross. Figure 4 (b) illustrates the monitoring phase in which DoS attack nodes are shown in red, as indicated by the SHSTM. Figure 4 (c) shows the top CH selection where nodes having high energy, mobile, and distant from the base station are selected as black-colored nodes. Last, figure 4 (d) represents the data transmission phase, where the arrows indicate the transmission direction with the actual transmission path highlighted in purple. Combined, figures 4 (a) to (d) represent the operational size of the SHSTM in terms of protecting and managing the VANET.

Performance Metrics

Energy Consumption (EC)

By the formed network, the network EC transfers the data packets from the source node to the Base Station (BS) in the presence of the proposed SHSTM, measured as EC. The EC rate can be considered using the expression in equation (10).

$$E = \frac{\lambda}{\sum_{i=1} [CH (i) + S(i)]} \quad (10)$$

Here E is the complete energy monitoring variable, λ which is the total initial energy, indicating the head, S the member hubs, and the complete node counts.

Network Lifetime (NL)

The network lifetime refers to how much it can fulfill its allocated packet transmission. The network lifetime can be assessed by considering the various constraints, such as EC, communication patterns, and network topology. The formulation for measuring the total network lifetime is expressed in equation (11).

$$N = \min_k \left[\frac{\sum_{i=1} v_{ij} + t_i}{n_j} \right] \quad (11)$$

Here N, it represents the lifespan variable, v_{ij} denotes the range matrix, t_i defines each node’s span, and n_j denotes the nodes inside the transmission range. The overall network lifespan of the created network can be assessed using this equation.

Network Throughput (NT)

The ratio at which the source nodes of the created vehicular transfer its data to the destination side is measured as NT. It is typically measured in bits per second (*bps*). NT is a critical performance metric for WSNs because it directly affects the network’s ability to effectively collect and transmit sensor data. The NT of the network is measured using the expression given in equation (12).

$$Throughput = \frac{sent\ packets + packet\ size}{time} \quad (12)$$

End-to-End Delay (EED)

The time the network assumes to collect and send the information from the source to the BS through the wireless channel is assessed as EED metrics. The mathematical formulation for the EED calculation is shown in equation (13).

$$delay = packet\ depart\ time - arrived\ time \quad (13)$$

Packet Delivery Ratio (PDR)

The PDR shows the percentage of data packets successfully delivered from a source to a terminal node. It’s a key metric used to evaluate the reliability and efficiency of data transmission within a network. The formulation for PDR calculation is shown in equation (14).

$$PDR = \frac{packets\ received}{total\ packets} \quad (14)$$

Attack Detection Ratio (ADR)

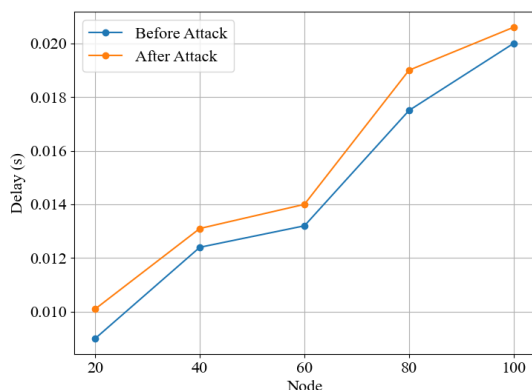
The ADR represents the effectiveness of the designed method in predicting the attack nodes. The ratio of correctly identified attack nodes among the total nodes is measured as the ARD. The total time the proposed SHSTM takes to detect the initialized nodes as normal or DoS attack nodes is defined as attack detection time. The ADR and time calculation formulas are mentioned in equation (15) and equation (16).

$$R_d = \frac{\chi_i}{m} \quad (15)$$

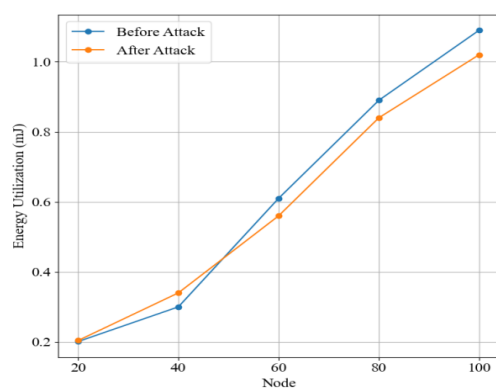
$$T_d = m * T_s \quad (16)$$

Here R_d is the ADR variable, χ_i indicates correctly predicted attack nodes, m represents the total nodes in the network, T_d expresses the attack detection time, T_s and is the time consumed for the single attack node detection. Higher the ADR, the privacy of the shared data is improved.

DISCUSSION



(a). EED



(b). EC

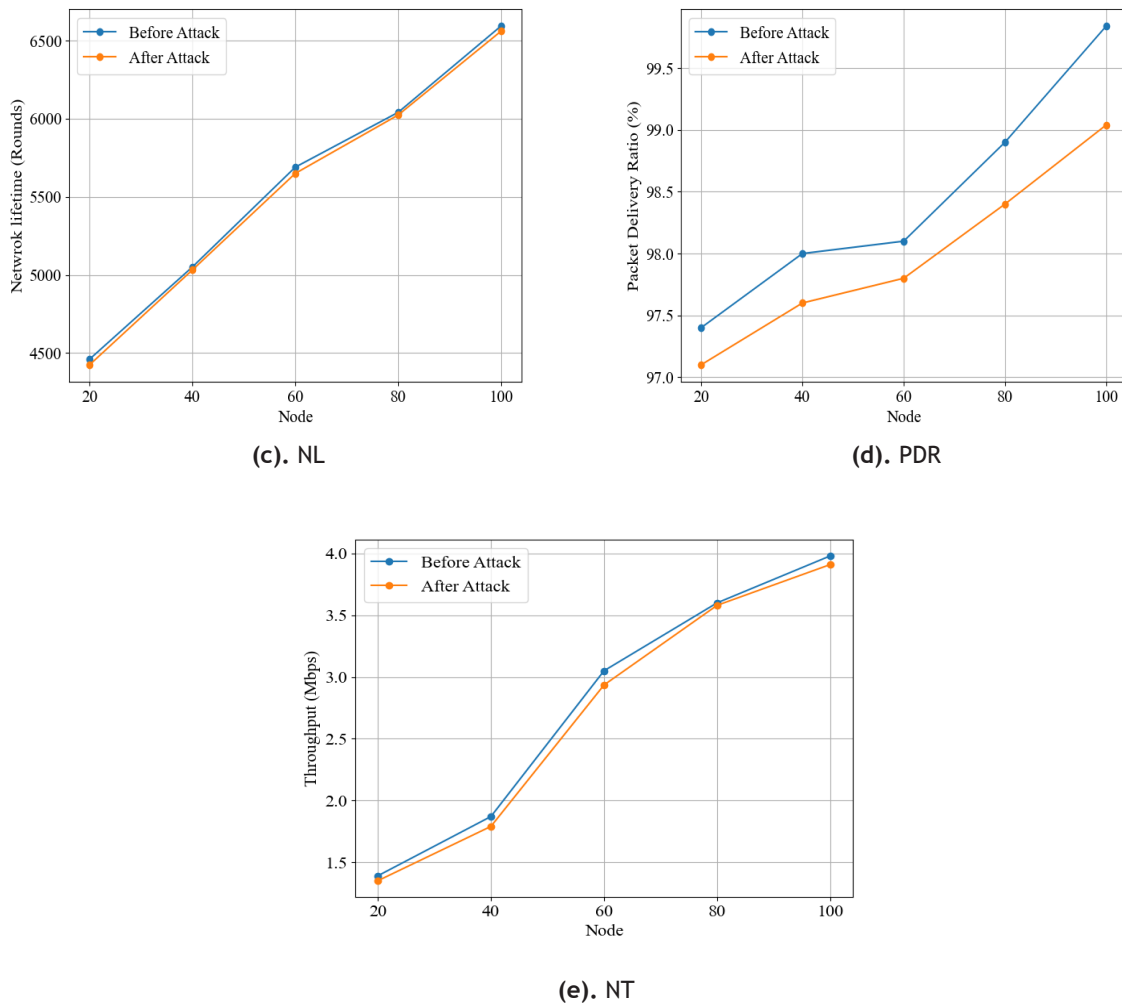


Figure 5. Network performance before attack and after attack with Proposed SHSTM

Table 3. Simulation analysis of proposed and existing techniques

Metrics	SKM	FbCLA	CLTP	ORBN	SHSTM
EC (<i>mJ</i>)	1,97	7,75	8,43	1,10	1,02
NT (<i>Mbps</i>)	0,99	0,96	0,95	3,8	3,91
EED (Sec)	0,0492	1,9617	2,9425	0,025	0,0206
ADRe (%)	83	84	81	86	98
Attack detection time (<i>ms</i>)	45	34	33	42	13
NL (<i>Rounds</i>)	5908	5395	4904	6210	6561
PDR (%)	79	82	77	85	99,4

The data from the source to the target node is transmitted through the nearby selected CHs, and the simulation is shown in figure 5. The security robustness and network efficiency of the SHSTM in the created network are validated in terms of NT, PDR, EC, NL, and EED. The results of those mentioned metrics for the variable nodes from 10 to 100 are shown in figure 8. The results are validated for two scenarios: before and after the attack.

The proposed model is explained in the NS2, and the efficiency score has been validated in terms of EED, EC, NT, NL, PDR, ADR, and time. The resulting network efficiency metrics values are compared with the Adaptive Cross Layered Threshold protocol (CLTP),⁽²³⁾ Fuzzy based Cross Layer Architecture (FbCLA),⁽²³⁾ Sailfish K-medoid Model (SKM),⁽²³⁾ and Optimized Radial Basis Network (ORBN)⁽²⁴⁾ for 100 nodes environment. The comparison of the results is detailed in table 3 and figure 6.

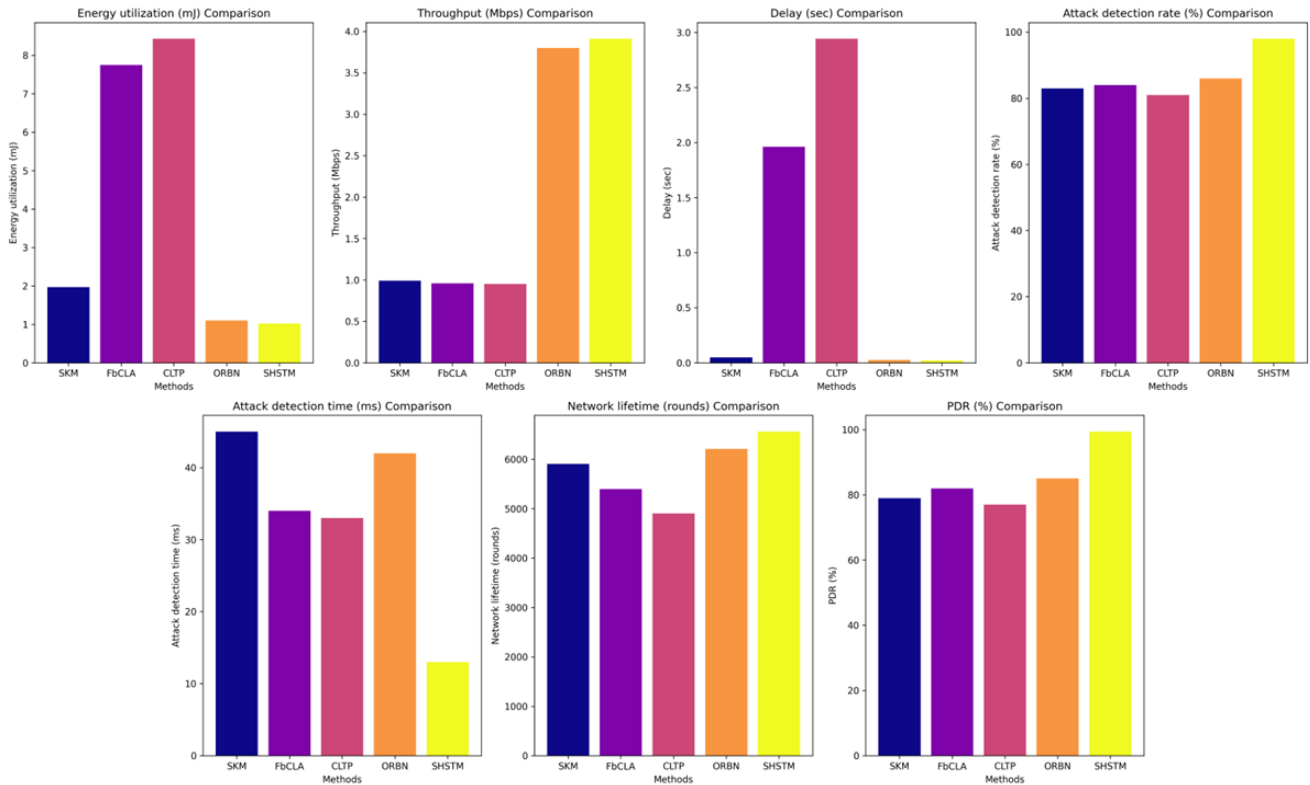


Figure 6. Simulation analysis of proposed and existing techniques

Simulation Discussion

The proposed SHSTM has been evaluated in terms of key network performance metrics, with a comparative analysis against existing models: Sailfish K-medoid Model (SKM), Fuzzy-based Cross-Layer Architecture (FbCLA), Adaptive Cross Layered Threshold Protocol (CLTP), and Optimized Radial Basis Network (ORBN) in a 100-node environment. The SHSTM demonstrates the lowest EC of 1,02 mJ, outperforming other models, including SKM (1,97 mJ) and ORBN (1,10 mJ). FbCLA and CLTP show considerably higher EC, with values of 7,75 mJ and 8,43 mJ, signifying that SHSTM's superior energy efficiency is vital for VANET with energy-constrained devices.

SHSTM achieves the highest NT at 3,91 Mbps, surpassing ORBN (3,8 Mbps), SKM (0,99 Mbps), FbCLA (0,96 Mbps), and CLTP (0,95 Mbps). This indicates that SHSTM is superior in providing efficient data transfer rates, vital for applications requiring high bandwidth. SHSTM outperforms all models in terms of EED, with a value of 0,0206 Sec., significantly lower than SKM (0,0492 Sec.), ORBN (0,025 Sec.), FbCLA (1,9617 Sec.), and CLTP (2,9425 Sec.). Lower EED translates to faster communication, enhancing the overall user experience, especially in real-time applications.

SHSTM leads in ADR by 98 %, surpassing ORBN (86 %), SKM (83 %), FbCLA (84 %), and CLTP (81 %). This highlights SHSTM's robust security mechanism, making it highly effective in detecting DoS, a critical feature for VANET susceptible to security threats. SHSTM also excels in attack detection time, with the fastest detection at 13 ms, which is significantly lower than SKM (45 ms), FbCLA (34 ms), CLTP (33 ms), and ORBN (42 ms). Faster detection enables rapid countermeasures, minimizing the impact of attacks on the network.

The proposed model enhances network longevity, reaching 6561 rounds, outperforming SKM (5908 rounds), FbCLA (5395 rounds), CLTP (4904 rounds), and ORBN (6210 rounds). A longer network lifetime is vital for maintaining continuous communication in large-scale VANET. SHSTM achieves the highest PDR of 99,4 %, demonstrating its reliability in PDR, compared to SKM (79 %), FbCLA (82 %), CLTP (77 %), and ORBN (85 %). SHSTM outperforms existing models across all evaluated metrics, demonstrating superior EC, NT, low EED, high ADR, and extended NL, making it a model solution for VANET applications.

CONCLUSIONS

This research develops a novel SHSTM to enhance network performance and secure the VANET against DoS attacks. The network nodes were set up for the vehicular communication. The specially designed SHSTM maintains tracking every node to identify DoS attack targets and remove them from the network. The system chose the top CH depending on traffic patterns to further support network security and performance. The networks' PDR, NT, EC, NL, and ADR were examined before and after the attack. The NT of the created network is 3,91 Mbps, EC is 1,02 mJ, PDR is 99,04 %, the EED is 0,0206 Sec., and the ADR is 98 %. The PDR is increased

by about 1 % compared to the existing methods, and the EED is significantly reduced. The designed model has shown significant improvement in network security and performance.

The model can be extended in the future. Future research can be directed to extend the implementation of lightweight cryptography with the SHSTM so that the security of the data packets will be maximized with minimal EC. Further studies of adaptive attack detection approaches and the proposed model's scalability for many VANETs could enhance DoS attack tolerance and overall network performance.

BIBLIOGRAPHIC REFERENCES

1. Ghamry, Walid K., and Suzan Shukry. "Multi-objective intelligent clustering routing schema for internet of things enabled wireless sensor networks using deep reinforcement learning." *Cluster Computing*, (2024):1-21.
2. Zainaddin, D. A., et al. "Recent trends and future directions of congestion management strategies for routing in IoT-based wireless sensor network: a thematic review." *Wireless Networks*, (2024): 1-45.
3. Priyadarshi, Rahul. "Exploring machine learning solutions for overcoming challenges in IoT-based wireless sensor network routing: a comprehensive review." *Wireless Networks*, (2024):1-27.
4. Tharini, V. J., & Vijayarani, S. "IoT in healthcare: Ecosystem, pillars, design challenges, applications, vulnerabilities, privacy, and security concerns." In *Incorporating the Internet of Things in healthcare applications and wearable devices*, IGI Global, (2020):1-22.
5. Hu, Xi, and Rayan H. Assaad. "BIM-enabled digital twin framework for real-time indoor environment monitoring and visualization based on autonomous LIDAR-based robotic mobile mapping, IoT sensing, and indoor positioning technology." *Journal of Building Engineering* (2024): 108901.
6. Khan, M. A. R., et al., "Optimizing hybrid metaheuristic algorithm with cluster head to improve performance metrics on the IoT." *Theoretical Computer Science*, 927, (2022): 87-97.
7. Shenbagharaman, A., and B. Paramasivan. "Trilateration method-based node localization and energy efficient routing using RSA for underwater wireless sensor network." *Sustainable Computing: Informatics and Systems*,41 (2024):100952.
8. Fadhil, Muthna J., Sadik Kamel Gharghan, and Thamir R. Saeed. "Path-Loss Model for Wireless Sensor Networks in Air Pollution Environments Leveraging of Drones." *Arabian Journal for Science and Engineering*, (2024):1-17.
9. Benyezza, Hamza, et al. "Smart platform based on IoT and WSN for monitoring and control of a greenhouse in the context of precision agriculture." *Internet of Things*, 23 (2023):100830.
10. Oladimeji, Damilola, et al. "Smart transportation: an overview of technologies and applications." *Sensors* 23, 8 (2023):3880.
11. Abro, Ghulam E. Mustafa, et al. "Comprehensive review of recent advancements in battery technology, propulsion, power interfaces, and vehicle network systems for intelligent autonomous and connected electric vehicles." *Energies* 16, 6, (2023):2925.
12. Al-Ani, Ruqayah, et al. "Privacy and safety improvement of VANET data via a safety-related privacy scheme." *International Journal of Information Security* 22, 4 (2023):763-783.
13. choudhary, Deepak, and Roop Pahuja. "Awareness routing algorithm in vehicular ad-hoc networks (VANETs)." *Journal of Big Data* 10.1 (2023): 122.
14. Karabulut, Muhammet Ali, et al. "Inspecting VANET with various critical aspects-a systematic review." *Ad Hoc Networks* (2023): 103281.
15. Ye, Zhoujing, et al. "IoT-enhanced smart road infrastructure systems for comprehensive real-time monitoring." *Internet of Things and Cyber-Physical Systems* (2024).
16. Venčkauskas, Algimantas, et al. "Enhancing Communication Security an In-Vehicle Wireless Sensor Network." *Electronics* 13.6 (2024): 1003.

17. Alharbi, Fares, et al. "Intelligent transportation using wireless sensor networks blockchain and license plate recognition." *Sensors* 23.5 (2023): 2670.
18. Sachan, Smriti, Rohit Sharma, and Amit Sehgal. "SINR based energy optimization schemes for 5G vehicular sensor networks." *Wireless Personal Communications* 127.2 (2022): 1023-1043.
19. Khadidos, Adil O et al. "Efficient key distribution for secure and energy-optimized communication in wireless sensor network using bioinspired algorithms." *Alexandria Engineering Journal* 92 (2024): 63-73.
20. Lilhore, Umesh Kumar, et al. "Secure WSN Architecture Utilizing Hybrid Encryption with DKM to Ensure Consistent IoV Communication", *Wireless Personal Communications* (2024): 1-29.
21. Finnveden L, Jansson Y, Lindeberg T. Understanding when spatial transformer networks do not support invariance, and what to do about it. 25th IEEE International Conference on Pattern Recognition (ICPR), (2021): 3427-3434.
22. Jia H, Li J, Song W, Peng X, Lang C, Li Y. "Spotted hyena optimization algorithm with simulated annealing for feature selection." *IEEE Access.*, 7, (2019): 71943-62.
23. Cherappa V et al., "Energy-Efficient Clustering and Routing Using ASFO and a Cross-Layer-Based Expedient Routing Protocol for Wireless Sensor Networks." *Sensors*. 23, 5, (2023):2788.
24. Ramani G, K A. "An optimized energy management and load balancing system based on cluster head selection for the vehicular network communication." *Multimedia Tools and Applications*. (2024): 1-22.
25. Subasini CA, Karuppiyah SP, Sheeba A, Padmakala S. "Developing an attack detection framework for wireless sensor network-based healthcare applications using hybrid convolutional neural network." *Transactions on Emerging Telecommunications Technologies*. (2021), 32(11):e4336.
26. Das R, Dwivedi M. "Cluster head selection and malicious node detection using large-scale energy-aware trust optimization algorithm for HWSN." *Journal of Reliable Intelligent Environments*. (2023), 1-7.
27. Khot PS, Naik U. "Particle-water wave optimization for secure routing in wireless sensor network using cluster head selection." *Wireless Personal Communications*. 119 (3), (2021):2405-29.
28. Sridhar Panneerselvam et al., "Federated learning-based fire detection method using local MobileNet." *Scientific Reports*, 14, 30388, (2024): 1-24.
29. Asir Chandra Shinoo, Robert Vincent, and Sudhakar Sengan. "Edge computing-based ensemble learning model for health care decision systems." *Sci Rep.*, 14(26997) (2024).
30. Asir Chandra Shinoo, Robert Vincent and Sudhakar Sengan, "Effective clinical decision support implementation using a multi-filter and wrapper optimisation model for Internet of Things based healthcare data." *Sci Rep*, 14, 21820 (2024).
31. Gulista Khan et al., "Energy-Efficient Routing Algorithm for Optimizing Network Performance in Underwater Data Transmission Using Gray Wolf Optimization Algorithm." *Journal of Sensors*, 2024(2288527), (2024):1-15.
32. Madhubala, P. et al., "Bridging the gap in biomedical information retrieval: Harnessing machine learning for enhanced search results and query semantics." *Journal of Intelligent & Fuzzy Systems*, (2024): 1-20, 2024, DOI: 10.3233/JIFS-237056.
33. Sudhakar Sengan et al., "Improved LSTM-Based Anomaly Detection Model with Cybertwin Deep Learning to Detect Cutting-Edge Cybersecurity Attacks." *Human-centric Computing and Information Sciences*, 13(55), (2023).
34. Mohammad Khalid Imam Rahmani et al., "Early Pathogen Prediction in Crops Using Nano Biosensors and Neural Network-Based Feature Extraction and Classification," *Big Data Research*, 38 (100412), (2023).

35. Sudhakar Sengan et al., “Fake News Detection Using Stance Extracted Multimodal Fusion-Based Hybrid Neural Network.” *IEEE Transactions on Computational Social Systems*, DOI:10.1109/TCSS.2023.3269087.
36. Arodh Lal Karn et al., “IoT Based Smart Framework Monitoring System for Power Station.” *Computers, Materials & Continua*, 74(3), (2023): 6019-6037.
37. Eman S. Sabry et al., “Sketch-Based Retrieval Approach Using Artificial Intelligence Algorithms for Deep Vision Feature Extraction.” *Axioms*, 11 (12), (2022): 663; DOI:10.3390/axioms11120663.
38. Prabu Selvam et al., “A Transformer-Based Framework for Scene Text Recognition.” *IEEE Access*, 10, (2022): 100895-100910, DOI:10.1109/ACCESS.2022.3207469, 2022.
39. Arodh Lal Karn et al., “ICACIA: An Intelligent Context-Aware framework for COBOT in defense industry using ontological and deep learning models, *Robotics and Autonomous Systems*.” (2022), 104234, DOI:10.1016/j.robot.2022.104234.
40. Tribhuwan Kumar et al., “Fuzzy Logic and Machine Learning-Enabled Recommendation System to Predict Suitable Academic Program for Students.” *Mathematical Problems in Engineering*, 2022 (5298468), (2022):1-7, DOI:10.1155/2022/5298468.
41. Surbhi Bhatia et al., “An efficient modular framework for automatic LIONC classification of MedIMG using unified medical language.” *Frontiers in Public Health*, (2022) DOI:10.3389/fpubh.2022.926229.
42. Mahrukh Mansoor et al., “A machine learning approach for non-invasive fall detection using Kinect, Springer-Multimedia Tools, and Applications.” 2022, DOI:10.1007/s11042-022-12113-w.
43. Thirumoorthy Palanisamy et al., “Improved Energy Based Multi-Sensor Object Detection in Wireless Sensor Networks.” *Intelligent Automation & Soft Computing*, 33(1), (2022):227-244, DOI:10.32604/iasc.2022.023692.
44. Abolfazl Mehbodniya et al., “Fetal health classification from cardiocotographic data using machine learning.” *Expert Systems Wiley*, (2021), DOI:10.1111/exsy.12899.
45. Vasanthi Raghupathy et al., “Interactive Middleware Services for Heterogeneous Systems.” *Computer Systems Science and Engineering*, 41, 3, (2022):1241-1253, DOI:10.32604/csse.2022.021997.
46. Abolfazl Mehbodniya et al., “Proportional Fairness Based Energy Efficient Routing in Wireless Sensor Network.” *Computer Systems Science and Engineering*, 41(3), (2022): 1071-1082, DOI:10.32604/csse.2022.021529.
47. D. Stalin David et al., “Cloud Security Service for Identifying Unauthorized User Behaviour.” *Computers, Materials & Continua*, 70, 2, (2022): 2581-2600, DOI:10.32604/cmc.2022.020213.
48. K. Rajakumari et al., “Fuzzy Based Ant Colony Optimization Scheduling in Cloud Computing.” *Computer Systems Science and Engineering*, 40(2), (2022): 581-592, DOI:32604/csse.2022.019175.
49. R. Nithya et al., “An Optimized Fuzzy Based Ant Colony Algorithm for 5G-MANET.” *Computers, Materials & Continua*, 70(1), (2022): 1069-1087, DOI:10.32604/cmc.2022.019221.
50. Razia Sulthana Abdul Kareem et al., “Multilabel land cover aerial image classification using convolutional neural networks.” *Springer Arabian Journal of Geosciences*, 14(2021) DOI:10.1007/s12517-021-07791-z.
51. Keerthana Nandakumar et al., “Securing data in transit using data-in-transit defender architecture for cloud communication.” *Soft Computing*, (2021), DOI:10.1007/s00500-021-05928-6.
52. Sudhakar Sengan et al., “Cost-effective and efficient 3D human model creation and re-identification application for human digital twins.” *Multimedia Tools and Applications*, (2021). DOI:10.1007/s11042-021-10842-y.
53. Roy Setiawan et al., “Encrypted Network Traffic Classification and Resource Allocation with Deep Learning in Software Defined Network.” *Wireless Personal Communication*, (2021), DOI;10.1007/s11277-021-08403-5.

54. Omnia Saidani Neffati et al., "Migrating from traditional grid to smart grid in smart cities promoted in developing country." *Sustainable Energy Technologies and Assessments*, 45 (2021), DOI:10.1016/j.seta.2021.101125.

55. Prabhakaran Narayanan et al., "Novel Collision Detection and Avoidance System for Mid-vehicle Using Offset-Based Curvilinear Motion." *Wireless Personal Communication*, (2021). DOI:10.1007/s11277-021-08333-2.

56. Balajee Alphonse et al., "Modeling and multi-class classification of vibroarthrographic signals via time domain curvilinear divergence random forest." *J Ambient Intell Human Comput*, (2021), DOI:10.1007/s12652-020-02869-0.

57. Ganesh Kumar, K, and Sudhakar Sengan, "Improved Network Traffic by Attacking Denial of Service to Protect Resource Using Z-Test Based 4-Tier Geomark Traceback (Z4TGT)." *Wireless Personal Communications*, (2020), DOI:10.1007/s11277-020-07546-1.

58. Sudhakar Sengan et al., "Enhancing cyber-physical systems with hybrid smart city cyber security architecture for secure public data-smart network." *Future Generation Computer Systems*, (2020), DOI:10.1016/j.future.2020.06.028.

59. Sudhakar Sengan and Chenthur Pandian S, "Hybrid Cluster-based Geographical Routing Protocol to Mitigate Malicious Nodes in Mobile Ad Hoc Network." *International Journal of Ad Hoc and Ubiquitous Computing*, 21,4, (2016): 224-236. DOI:10.1504/IJAHUC.2016.076358.

60. T. Gopalakrishnan et al., "Leveraging blockchain technology to combat deception, deepfake, and counterfeit system." *Journal of Discrete Mathematical Sciences and Cryptography*, 27:7, (2024), 2143-2154, DOI: 10.47974/JDMSC-2087

61. Madan Mohan Tito Ayyalasomayajula et al., "Enhanced network security through algebraic cryptanalysis of elliptic curve cryptography." *Journal of Discrete Mathematical Sciences and Cryptography*, 27, 7, (2024): 2219-2230, DOI: 10.47974/JDMSC-2093.

62. Milton Lopez-Cueva et al., "A Multi-Moving Target Localization in Agricultural Farmlands by Employing Optimized Cooperative Unmanned Aerial Vehicle Swarm." *Scalable Computing: Practice and Experience*, 25, 6, (2024): 4647-4660, DOI 10.12694/scpe.v25i6.3130.

63. Firas Tayseer Ayasrah et al., "Strategizing Low-Carbon Urban Planning through Environmental Impact Assessment by Artificial Intelligence-Driven Carbon Foot-Print Forecasting." *Journal of Machine and Computing*, 4, 4, (2024), doi: 10.53759/7669/jmc202404105.

64. Roberto E. Roque-Claros et al., "UAV Path Planning Model Leveraging Machine Learning and Swarm Intelligence for Smart Agriculture." *Scalable Computing: Practice and Experience*, 25, 5, (2024): 3752-3765, DOI 10.12694/scpe.v25i5.3131.

65. Hayder M. A. Ghanimi et al., "Smart Fertilizing Using IOT Multi-Sensor and Variable Rate Sprayer Integrated UAV." *Scalable Computing: Practice and Experience*, 25, 5, (2024): 3766-3777, DOI 10.12694/scpe.v25i5.3132.

66. Bernabe Canqui-Flores et al., "Echocardiographic cardiac views classification using whale optimization and weighted support vector machine." *Vessel Plus*. 8,29, (2024), <http://dx.doi.org/10.20517/2574-1209.2023.140>.

67. Shaymaa Hussein Nowfal et al., "Genetic Algorithms for Optimized Selection of Biodegradable Polymers in Sustainable Manufacturing Processes." *Journal of Machine and Computing*, 4, 3, (2024): 563-574, <https://doi.org/10.53759/7669/jmc202404054>.

68. V. Jeevika Tharini et al., "Business Decision-Making Using Hybrid LSTM for Enhanced Operational Efficiency." In: Vimal, V., Perikos, I., Mukherjee, A., Piuri, V. (eds) *Multi-Strategy Learning Environment. ICMSLE Algorithms for Intelligent Systems*. Springer, Singapore, (2024) https://doi.org/10.1007/978-981-97-1488-9_12.

69. A. Jermanshiyamala et al., "ACO-Optimized DRL Model for Energy-Efficient Resource Allocation in High-Performance Computing. In: Vimal, V., Perikos, I., Mukherjee, A., Piuri, V. (eds) *Multi-Strategy*

Learning Environment.” ICMSLE Algorithms for Intelligent Systems. Springer, Singapore. (2024), https://doi.org/10.1007/978-981-97-1488-9_11.

70. Hayder M. A. Ghanimi et al., “An open-source MP + CNN + BiLSTM model-based hybrid model for recognizing sign language on smartphones.” *Int. J. Syst. Assur. Eng. Manag.* (2024). <https://doi.org/10.1007/s13198-024-02376-x>.

71. Ghanimi, Hayder M. A., et al., “Chebyshev polynomial approximation in CNN for zero-knowledge encrypted data analysis.” *Journal of Discrete Mathematical Sciences and Cryptography*, 27:2-A, (2024): 203-214, DOI: 10.47974/JDMSC-1880, 2024.

72. Ghanimi, Hayder M. A., et al., “Merkle-Damg hash functions and blockchains: Securing electronic health records.” *Journal of Discrete Mathematical Sciences and Cryptography*, 27, 2-A, (2024): 237-248, DOI: 10.47974/JDMSC-1878, 2024.

73. Sagar, P. Vidya, et al., “Secure multi-party computation in deep learning: Enhancing privacy in distributed neural networks.” *Journal of Discrete Mathematical Sciences and Cryptography*, 27, 2-A, (2024):249-259, DOI: 10.47974/JDMSC-1879, 2024.

74. Rao, Ganga Rama Koteswara, et al., “Enhanced security in federated learning by integrating homomorphic encryption for privacy-protected, collaborative model training.” *Journal of Discrete Mathematical Sciences and Cryptography*, 27, 2-A, (2024), 361-370, DOI: 10.47974/JDMSC-1891, 2024.

75. Krishna, Raguru Jaya, et al., “Security and privacy concerns in social networks mathematically modified metaheuristic-based approach.” *Journal of Discrete Mathematical Sciences and Cryptography*, 27,2-A, (2024): 371-382, DOI: 10.47974/JDMSC-1892.

76. Swapna Siddamsetti et al., “Modular metric spaces: Some fixed-point theorems and application of secure dynamic routing for WSN.” *Journal of Interdisciplinary Mathematics*, 27, 2, (2024): 393-401, DOI: 10.47974/JIM-1890

77. Shaymaa Hussein Nowfal et al., “Advancing viscoelastic material modeling: Tackling time-dependent behavior with fractional calculus.” *Journal of Interdisciplinary Mathematics*, 27, 2, (2024): 307-316, DOI: 10.47974/JIM-1827.

78. P. Vidya Sagar et al., “Utilizing stochastic differential equations and random forest for precision forecasting in stock market dynamics.” *Journal of Interdisciplinary Mathematics*, 27, 2, (2024): 285-298, DOI: 10.47974/JIM-1822.

79. Ghayth Almahadin et al., “Enhancing Video Anomaly Detection Using Spatio-Temporal Autoencoders and Convolutional LSTM Networks.” *SN COMPUT. SCI.* 5,190, (2024). <https://doi.org/10.1007/s42979-023-02542-1>.

80. Senthil Kumar Nramban Kannan et al., “Analysis of COVID-19 Datasets Using Statistical Modelling and Machine Learning Techniques to Predict the Disease.” *SN COMPUT. SCI.* 5,181, (2024). <https://doi.org/10.1007/s42979-023-02464-y>.

81. Nayer Tumi-Figueroa E, et al., “Adaptive Approach To Anomaly Detection In Internet of Things Using Autoencoders And Dynamic Thresholds.” *Journal of Machine and Computing*, doi: 10.53759/7669/jmc202404001.

82. Rasheed Abdulkader et al., “Optimizing student engagement in edge-based online learning with advanced analytics.” *ARRAY*, (2023), doi: <https://doi.org/10.1016/j.array.2023.100301>.

83. Arokia Jesu Prabhu Lazar et al., “Gaussian Differential Privacy Integrated Machine Learning Model for Industrial Internet of Things.” *SN Computer Science*, 4, 454, (2023), <https://doi.org/10.1007/s42979-023-01820-2>.

84. Kalaivani Pachiappan et al., “Quality of Smart Health Service for Enhancing the Performance of Machine Learning-Based Secured Routing on MANET.” *EAI/Springer Innovations in Communication and Computing*. Springer, Cham. (2023), DOI:10.1007/978-3-031-23602-0_17.

85. Maheswari Subburaj et al., "Artificial Intelligence for Smart in Match Winning Prediction in Twenty20 Cricket League Using Machine Learning Model." EAI/Springer Innovations in Communication and Computing. Springer, Cham. (2023), DOI:10.1007/978-3-031-23602-0_3.

86. Joel Sunny Deol Gosu et al., "Comparative Analysis of Handwritten Digit Recognition Investigation Using Deep Learning Model." EAI/Springer Innovations in Communication and Computing. Springer, Cham, (2023), DOI:10.1007/978-3-031-23602-0_3.

87. M. Anto Bennet et al., "Classification and Localization of COVID-19 based on a Pneumonia Radiograph using a Deep Learning Approach." In Proceedings of the 4th International Conference on Information Management & Machine Intelligence (ICIMMI '22). Association for Computing Machinery, New York, NY, USA, 20, (2023):1-6, DOI:10.1145/3590837.3590857.

88. Abolfazl Mehbodniya et al., "Classification of Cervical Cells Using Deep Learning Feature Extraction." Innovations in Computer Science and Engineering. ICICSE 2022. Lecture Notes in Networks and Systems, Springer, Singapore, 565, (2022): 27-41, DOI:10.1007/978-981-19-7455-7_3.

89. Julian L. Webber et al., "Hybrid Power Generation Forecasting Using an Intellectual Evolutionary Energy-Preserve Rate Clustering Technique." Innovations in Computer Science and Engineering. ICICSE 2022. Lecture Notes in Networks and Systems, Springer, Singapore, 565, (2022): 27-41, DOI:10.1007/978-981-19-7455-7_10.

90. Arodh Lal Karn et al., "Evaluation and Language Training of Multinational Enterprises Employees by Deep Learning in Cloud Manufacturing Resources, Innovations in Computer Science and Engineering." ICICSE 2022. Lecture Notes in Networks and Systems, Springer, Singapore, 565, (2022): 369-380, DOI:10.1007/978-981-19-7455-7_28.

91. Arodh Lal Karn et al., "Design of Concurrent Engineering Systems for Global Product Development Using Artificial Intelligence, Innovations in Computer Science and Engineering." ICICSE 2022. Lecture Notes in Networks and Systems, Springer, Singapore, 565, (2022): 425-434, DOI:10.1007/978-981-19-7455-7_32.

92. Abolfazl Mehbodniya et al., "Certain Investigations of MEMS for Optimised Sensor Coverage, Innovations in Computer Science and Engineering." ICICSE 2022. Lecture Notes in Networks and Systems, Springer, Singapore, 565, (2022):479-489. DOI:10.1007/978-981-19-7455-7_35.

93. Abolfazl Mehbodniya et al., "Medical Images Analysis for Segmentation and Classification Using DNN." Innovations in Computer Science and Engineering. ICICSE 2022. Lecture Notes in Networks and Systems, Springer, Singapore, 565, (2022):525-534. DOI:10.1007/978-981-19-7455-7_39.

94. Gladson Maria Britto James et al., "Deep Convolutional Neural Networks-Based Market Strategy for Early-Stage Product Development." Innovations in Computer Science and Engineering. ICICSE 2022. Lecture Notes in Networks and Systems, Springer, Singapore, 565, (2022): 597-606, DOI:10.1007/978-981-19-7455-7_46.

95. Julian L. Webber et al., "Glioma Segmentation in MR Images Using 2D Double U-Net: An Empirical Investigation." Innovations in Computer Science and Engineering. ICICSE 2022. Lecture Notes in Networks and Systems, Springer, Singapore, 565, (2022), 645-654. DOI:10.1007/978-981-19-7455-7_50.

96. K. Bhavana Raj et al., "Equipment Planning for an Automated Production Line Using a Cloud System." Innovations in Computer Science and Engineering. ICICSE 2022. Lecture Notes in Networks and Systems, Springer, Singapore. 565, (2022): 707-717, DOI:10.1007/978-981-19-7455-7_57.

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Formal Analysis: G. Ramani.

Display: K. Amarendra.

Drafting - Original Draft: G. Ramani.

Writing - Proofreading and Editing: G. Ramani and K. Amarendra.