ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
Received: 6 January 2025; Accepted: 9 June 2025

https://doi.org/10.17559/TV-20250106002236
Original scientific paper

EMAO-MTRUST: A Robust Trust-Based Routing Protocol with Emergency Handling for Secure and Efficient VANETs

Parimala GARNEPUDI*, M. VANITHA

Abstract: Vehicular Ad hoc Networks (VANETs) play a vital role in Intelligent Transportation Systems (ITS), a key application of Cyber-Physical Systems (CPS). However, the functionality of these networks can be compromised by environmental challenges and malicious attacks, such as black hole and flooding attacks, which degrade network performance. To address these challenges, this paper introduces the Emergency Module with Ant Colony Optimization-based Multi-hop Trusted Routing Protocol (EMAO-MTRUST) for VANETs. The proposed protocol enhances network security and efficiency by integrating trust-based mechanisms and intelligent routing strategies. EMAO-MTRUST employs direct and indirect trust models to identify and isolate malicious nodes, ensuring reliable packet transmission. Trust computations are used to select a border node with the highest trust value for forwarding data packets. An Emergency Module is incorporated to handle critical situations, leveraging a hybrid approach that combines Time Division Multiple Access (TDMA) and Carrier Sense Multiple Access (CSMA) models. The Ant Colony Optimization (ACO) algorithm is utilized to determine the most efficient routing path between nodes, optimizing the network's performance. The protocol's effectiveness is evaluated through simulations, comparing it to existing methods in the presence of black hole and flooding attacks. Key performance metrics, including packet delivery ratio, end-to-end latency, network throughput, and energy efficiency, are assessed. Results demonstrate that EMAO-MTRUST significantly outperforms existing approaches, delivering higher packet delivery ratios, reduced latency, improved throughput, and enhanced energy efficiency. This study highlights the potential of the EMAO-MTRUST protocol to secure VANETs against malicious activities while maintaining high-quality performance, making it a promising solution for the challenges in ITS applications.

Keywords: ant colony optimization (ACO); cyber-physical systems (CPS); intelligent transportation systems (ITS); multi-hop routing protocol; vehicular ad hoc networks (VANETs)

1 INTRODUCTION

Every year, millions of people all around the globe die from traffic accidents. Some individuals are fatally injured during the road collision between various kinds of vehicles, such as trucks, buses, automobiles, etc. Because of this, there is a need to reduce the road accidents and reduce the traffic on roads. Researchers in computer networks have introduced a technology called Vehicle Ad hoc Network (VANET) [1], which is a subset of mobile ad hoc networks (MANETs) [2]. Vehicle Ad Hoc Networks provide a safer and well-organized route via rapid communication of information to drivers and relevent authorities involved. VANET plays a significant role in traffic control and provide cars on highways with emergency information. Diverse additional vehicular applications, such as safety apps, road guide applications, etc., utilize traffic information [3]. VANETs will decrease road harm to a greater degree by supplying drivers with vital information [4].

VANET is an example of MANET, where vehicles are on-board units (OBUs) [5]. These vehicles may connect directly or through routers called "roadside units" (RSUs) which is termed "vehicle to vehicle communication (V2V)", and the other is "vehicle to infrastructure (V2I)". Trusted Authorities (TA) [6] govern the complete network in both situations. The key application of VANETs is to enhance traffic safety and efficiency (such as alarms, traffic services, and warning messages). In this scenario, a security issue may have a disastrous impact since an attacker may be able to transmit misleading warnings and/or signals for his own advantage. Trust may be utilized to encourage healthy cooperation via the development of trustworthy connections between cooperating vehicles to combat uncertainty and suspects. Due to the significance of the security issue, the trust management (TM) model is utilized at the initial stage of the proposed method [7].

The VANET node moves fast and more unpredictable than the static or low speed moving vehicles seen in standard wireless networks, resulting in frequent network design changes. The routing difficulties of the VANET protocol architecture are further extended due to the VANET's unique characteristics, such as complexity and dynamic behavior. On the other hand, a Routing protocol for VANET is vulnerable due to the presence of attack in self-organized and infrastructure in the VANET network. VANET attacks are performed by Malicious cars by transmitting wrong data or even erroneously deleting packets or divert packets to incorrect nodes to prevent data from reaching their destination nodes. If the data's trust cannot be appropriately assessed, the driver may misjudge misbehaved vehicles on the basis of false information, resulting in substantial traffic congestion [8]. VANET routing protocol is to address the safe & secure multipath routing [9].

The proposed model aimed to develop an appropriate routing protocol for the VANET environment. The specific contribution of the proposed model is stated as follows:

1. Initially, to perform effective data transmission routing, trust management (TM) is employed with computation of the direct and indirect trust values of the nodes [10].
2. To perform emergency module formulation, TDMA and CSMA model is implemented for the computation of data transmission in VANET environment.
3. Upon the estimation of data, optimal path for data transmission is computed through Optimization model for computation of the path.
4. The proposed scheme uses Ant colony optimization (ACO) with transmission of Hello messages between the nodes for formulation of secure multi-hop routing.

The rest of this paper is arranged as follows. Section 2 deals with literature, proposed EMAO-MTURST is explained in section 3. Section 4 shows the ACO optimal path findings and secton 5 shows discussions. Finallay section 6 provides conclusion.

2 RELATED WORKS

VANET security is a major concern, and trust is a critical component of it. As a result, because VANETs are reliant on the interchange of data between vehicles, the reliability of data is critical [11-13]. Data exchange between trustworthy vehicles also has a direct impact on security. Furthermore, the quality for both safety and non-safety scenarios in VANETs is highly dependent on the trustworthiness of data, and trust plays a critical role in the security and quality of a vehicular network. As a result, extensive research on trust and an examination of current trust models are required.

One study addresses the challenge of Trust Manipulation Attacks (TMAs) in VANETs by proposing an adaptive trust threshold mechanism [14, 15]. This approach dynamically adjusts trust levels to more effectively identify and mitigate malicious nodes attempting to alter their behavior to evade detection. An advanced trust evaluation algorithm for VANETs has been proposed, leveraging Bayesian inference to counter trust-based attacks. This approach systematically assesses and updates trust values based on probabilistic reasoning, enhancing the system's resilience against malicious nodes manipulating trust scores.

Another work explores the concept of a trust-field in VANETs as a novel paradigm to enhance secure communication and decision-making among vehicles. It investigates how trust propagates dynamically in a networked vehicular environment, influencing interactions and cooperative behaviors. A trust-based enhancement to the AODV routing protocol, known as T-AODV [4], has been introduced to mitigate black-hole attacks in VANETs. By integrating trust metrics into route selection, this method prevents malicious nodes from intercepting and discarding data packets.

A comprehensive study evaluates various mechanisms for detecting misbehaving nodes in VANETs. It compares trust-based, anomaly-based, and cryptographic approaches to assess their effectiveness in identifying malicious behavior. An in-depth analysis of trust management in VANETs explores existing trust models and their role in establishing secure and reliable communication between vehicles. Different trust evaluation mechanisms, such as entity-based, data-centric, and hybrid models, are discussed in the context of mitigating threats like false data injection and Sybil attacks.

A trust-based mechanism has been proposed to identify malicious Roadside Units (RSUs) in Edge-Enabled VANETs. The focus is on mitigating security threats posed by compromised RSUs that manipulate data, disrupt communication, and degrade network performance [16, 17]. An efficient dynamic solution has been presented to detect and prevent Black Hole attacks [18] in VANETs. The approach enhances network integrity by identifying malicious nodes through real-time analysis and adaptive strategies, thereby safeguarding data transmission. A novel security approach integrates the AODV routing protocol with clustering [19, 20] and trust management mechanisms to detect and isolate malicious nodes.

Trust scores are assigned based on nodes' past interactions to enhance network security [21] specifies another approach in the context of Wireless Sensor Networks (WSNs) introduces a trust calculation algorithm that evaluates nodes based on behavior, communication history, and data integrity. Trust scores help in identifying and isolating untrustworthy nodes to improve network reliability. A comprehensive review of trust management mechanisms in VANETs explores existing models, security challenges [22], and emerging threats that affect vehicular communication systems. A novel trust management framework evaluates the trustworthiness of VANET nodes based on historical interactions and cooperative behavior, aiming to ensure secure and reliable network operations.

To enhance VANET security, a Trust Score Evaluation Scheme has been proposed. This mechanism assigns trust values to nodes based on their behavior and past interactions to facilitate reliable and secure data transmission. A novel detection and mitigation approach addresses blackhole and gray hole attacks using Dynamic Time Warping (DTW), a technique commonly applied in pattern recognition and time-series analysis. Lastly, a trust-based model evaluates the behavior of network nodes using direct and indirect trust metrics. This mechanism helps identify and isolate untrustworthy nodes while promoting secure data exchange among vehicles.

Despite extensive research on trust management mechanisms in VANETs, significant gaps remain in effectively countering sophisticated and evolving trust manipulation attacks [23]. Existing models often rely on static thresholds or predefined metrics, which lack adaptability to dynamic network conditions and attacker behavior. Furthermore, most approaches focus on either node behavior or data integrity in isolation, overlooking the potential benefits of hybrid models that combine entity-based and data-centric trust evaluations. Limited attention has been given to real-time trust propagation, integration with machine learning, and resilience against insider threats, indicating a need for more adaptive, context-aware, and comprehensive trust frameworks for secure VANET communication.

3 PROPOSED METHOD

The proposed Emergency module with Ant Optimization based Multi-hop Trusted (EMAO-MTRUST) architecture is illustrated in Fig. 1. The proposed model begins by constructing a trust management (TM). Trust management can be obtained by calculating the direct trust and indirect trust values of the nodes in the VANET.

Direct trust depends on the trustworthiness of nodes' threshold value, and indirect trust is based on abnormal departure, abnormal joining, normal connection, and multi-channel group power of the nodes in VANET. The calculated trust values identify the harmful nodes in the network. More trustworthy value nodes are selected as forwarding nodes, and packets are routed via trusted nodes. Emergency Module concept is initiated to carry over the emergency. Both TDMA and CSMA models are combined in the Emergency model. To find the optimum path between the nodes, the proposed model uses the Ant Colony Optimization Algorithm (ACO), and the control hello messages are transmitted between nodes to determine the optimum route. The proposed method is used to create

a secure multi-network routing to deal with different threats from aggressive vehicle nodes. The performance of the recommended approach is examined by considering the black hole and flood assaults.

3.1 Trust Model

The direct trust of node *B* by node *A* is also influenced by the duration of contact and the total number of sent packets. Therefore, two metrics may be used to characterize the direct trust, i.e., based on consideration of number of packets transmitted and the attenuation time factor. The direct trust value is calculated based on the Eq. (1) as follows:

$$dt_{AB} = \frac{\sum_{i=1}^{t} \rho^{t-i} M_{AB}^{i}}{M} \cdot t_d \tag{1}$$

where $M = \sum_{i=1}^{t} \rho^{t-i}$, ρ^{t-i} $(0 < \rho < 1)$, refers to time attenuation function which aggregates all previous interaction experiences between vehicles *A* and *B*, M_{AB}^{i} refers to the quantity of the data packets transmitted between the nodes *B* to *A* for the period of T_i. M_{AB}^{i} is used for identifying the behaviour of *B*. If M_{AB}^{i} is high, it means vehicle *B* is trustworthy otherwise vehicle *B* has been engaged in misbehaviour. The higher number of packets transmitted, the higher the trust value gained. If node *A* and *B* do not communicate directly, the value of dt_{AB} is set to 0.5.

In calculating node trust, the indirect trust factor is essential. Indirect trust of nodes *A* and *B* is determined by the history of abnormal leaving, abnormal joining, and multi-distribution between nodes. The indirect trust is the opinion about a node, which is identified on DT-based basis. But a node that does not have a witness variable is authenticated by the IDT. The direct trust value is calculated based on the Eq. (2) as follows:

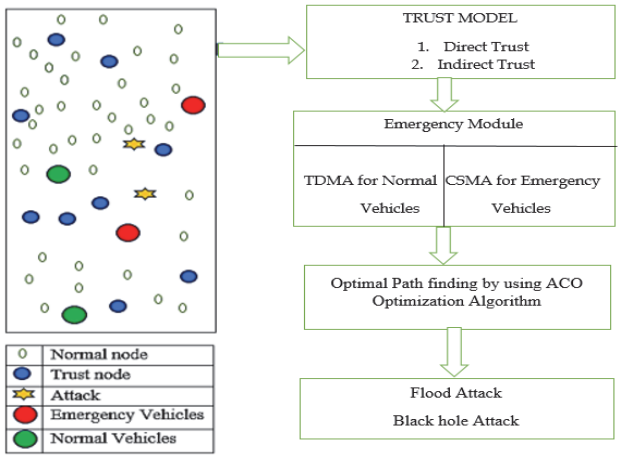

Figure 1 Schematic diagram of proposed method

$$IDT_i^d(\tau) = \frac{1}{r} \sum_{i\text{-}1}^{r} DT_i^d \ (d) \tag{2}$$

where, *r* - specifies this node's overall neighbors "*i*"; $IDT_i^d(\tau)$ - indirect trust value of vehicle ddd based on recommendations from other vehicles at time *τ*; DT_i^d (d) - direct trust values provided by *r* recommending vehicles about vehicle *d*.

3.2 Multicast Routing Scheme with Trust Management Scheme

This section is for trust improvement to the conventional ad hoc multicast distance vector routing protocol on demand (MBH-TBF). This novel trust-based protocol is named as multi-trust ad hoc protocol for vector routing on demand (i.e., MTBH-TBF). All nodes compute the trust value of its neighbor and choose the highest trust node to establish a reliable route for data transmission.

Three additional fields, including reverse journey trust, road trust, and malicious node addresses are provided in the MBH-TBF RREQ messages. The reverse route's initial trust value is 1 when all nodes in the network try to join a multicast group but do not have a valid route, a J_flag RREQ will be removed. When the RREQ message receives node reply, then reverse path is created. The messaging node may compute node's trust value and it is used to compare the value of trajectory trust to alter the opposing trajectory trust value is minimal. In case the node trust value is below the computed trust value then it will not be considered.

Table 1 Enhanced RREQ and RREP messages

Enhanced RREQ message	Enhanced RREP message
Dest_Addr	Original IP address
Dest_Seq	Dst_addr
J_flag	Dest_Seq#
R_flag	R_flag
Original IP address	Mgroup_hop
Originator Sequence Number	Lifetime
Lifetime	Hop_Cnt
Reverse path trust	Average Trust Value
Required path Trust	
Malicious Node Address	

In a new field, the original MBH-TBF RREP message is shown in Tab. 1. If the selected route has *n* nodes, you can calculate the average trust value based on the Eq. (3):

$$ATV = \frac{\sum_{i\text{-}1}^{n} trust_i}{n} \tag{3}$$

where *trust* is defined as the route node trust value. With the multi-cast group J_flag is transmitted with the RREQ message for the data transmission between the source to destination with RREP packet. The route forwarding is based on the constructed data path between source and receiver node. If more than one destination node route is identified the source node need to be activated for the data transmission. In the conventional MBH-TBF protocol, the route path with the shortest distance is provided with higher priority.

In the conventional MBH-TBF the higher priority is provided to the VANET route with the shortest path. The developed MBH-TBF model exhibits higher advantage

over the estimation of the path through transmission of the MACT messages. The established route performs the transmission of the message. If any node fails to receive the message, then it will be eliminated from the cache.

Maintenance of Trust-Based Routes

Each member of the multicast group has been undated through the multicast routing scheme. The proposed method updates the address of malicious node in the routing table, and the array is put into an improved multi-cast routing table as shown in Tab. 2. After setting up the multi-cast group and transmitting information, the upstream node may watch the upstream node's forward behavior.

In estimation of the malicious node id upstream is considered then the unicast transmits the RREQ message to the cluster head along with the address of malicious node. Upon the reception of the RREP message cluster head responds with the message and transmits the HELLO message throughout the network. The message comprises the address of the malicious node and is updated in the multi-cast routing table database. All Multi- Cast group members connect to this node and rediscover another way from the Multi-Cast Group. The node those identified as malicious and updated in the routing table will not be considered in the group until it recovers. The trust value is set as 0.5 for the routing performance in the network.

Table 2 Enhanced multicast route and hello messages

Extended multicast routing table	Enhanced hello message
Multicast Group IP address	Group Leader IP address
Multicast Group Leader IP address	Multicast Group IP address
Multicast Group Sequence Number	Multicast Group Sequence Number
Hop count to Multicast Group leader	U_flag
Hop count to next Multicast Group Member	O_flag
Next Hops: Next Hop IP Address Next Hop Interface: Link Direction Activated Flag	Hop Count
Malicious Node Address	Malicious Node address

3.3 Trusted Border-Node Based Most Forward within Radius Routing Protocol (TBMFR)

TBMFR is identical to B-MFR since the next node is the border node. The distinction consists of solving the ambiguity issue when two equidistant boundary nodes appear. In this instance, the trust value of uncertain border nodes is checked, and a node with the highest trust value is selected as forwarding node. To calculate the trust level, the total packets sent, received, and discarded by the node are taken into consideration. For a particular transfer, it decides which node should be routed based on the trust values calculated according to the total packages handled by each node. Based on this rating, two nodes of equidistance choose a node. Algorithm 1 represents the border node selection process.

Algorithm 1: Border node selection process

Step 1: Calculating the distance from the sender node to other nodes which are within the transmission range.
Step 2: Trust Evaluation: The trust value of a border node is computed using direct trust, indirect trust.

$$T_i = \left(\frac{t_{rs} - t_{rf}}{t_{rs} + t_{rf}} \right) \quad (4)$$

Step 3: Stability and Libnk reliability - Nodes with stable connections (low mobility-induced disconnections) and higher signal strength are preferred.
Step 4: Border Node Confirmation - A node is confirmed as a trusted border node if it lies near the transmission boundary and with high trust score.

In Eq. (4) Ti is the trust-value of node *i* value, t_{rs} is the node *i* packets from the following nodes received successfully, and trf is the fault rate calculated by the drop-by-node i number of packets received from its surrounding nodes.

The design of the TB-MFR technique is based on the following assumptions: Transmission of packets via border nodes. Every node assigns a trust value and selects a boundary depending on its trust value. Hello messages are communicated based on the neighbors next-hotdmap values in the VANET. Nodes in the VANET network are provided with the digital map, sensors, and GPS receivers.

3.4 Emergency Module Design

The Emergency Module employs a hybrid TDMA/CSMA approach to ensure efficient and reliable communication during normal and emergency scenarios. The CSMA/CA mechanism facilitates initial network setup and topology discovery, while TDMA scheduling provides deterministic and prioritized transmission during emergency events. Emergency Module initially interacts with random-access mechanism and utilizes CSMA/CA. During setup phase data collection and TDMA schedules are established.

Topology Discovery

The base station (BS) uses basic flood mechanism to build data transmission tree and is comparable to the PEQ routing protocol's hop tree configuration. The objective of topology discovery in our environment is not only to just construct a routing table but also to identify neighbors and monitor any changes to the tree. The BS produces a message to discover topology, consisting of the hop_count, new_parent_id and old_parent_id. This message is sent via a node to locate future offspring, as well as a reply to his parent and to notify its predecessor node, allowing it to change its parent if desired. During this phase every node reports their hop count, parent ID, list of children and list of one hop neighbors to its base station.

Assignment of TDMA Slot

At this level, the nodes are rearranged and distributed so that, if there is no space for two nodes within a 2-hop distance, our TDMA assigns a slot in a downward manner through a node without any children (leaf node). One of the aims of our proposal is to develop a communication method to facilitates message transmission from the base station to initiate the slot assessment process for nodes in the VANET network. An unloaded node (except base station) will wait until all its children report their schedules before assigning a single unicast slot, multiple unicast slots and diffusion slots for its own data to its children. The base station estimates the assigned slots in the network when it

receives messages from all of its descendants. The base station transmits the first SCHEDULE_NOTIFICATION message using TDMA. Once a child receives the message it moves to TDMA and synchronizes its kids with respective slots.

Regional Time Synchronization

Emergency Module for local time synchronization is through Flooding time synchronization protocol (FTSP). This process involves synchronization of root neighbor through parent-synchronization and children's transmission. In this approach each child must have a clock identical to their parent node which collects information from the other nodes in the network. A SYNCHRONISATION message consists of current _slot and sender_ID to synchronize new nodes. The highest _slot parameter is used to find TDMA frame length, and hop_count to assist a new node in selecting its prospective parent. The Fig. 2 shows the frame construction of Emergency Module.

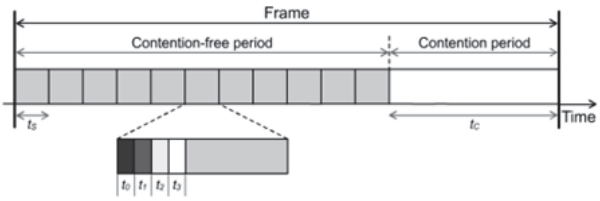

Figure 2 Frame structure of emergency module

Urgency Queue

Multiple queues are included in the emergency module to differentiate between packet with high and low priorities. The data packets lie in the slack queue until the expiry of the deadline for the data transmission from packets towards the header. The slack values are computed and updated based on the consideration of each hop count, transmission, and minimization of the delay. The fundamental concept lies in the transmission is high-priority queues are implemented in the packet for information transmission. In case the queue is filled then the packet slack is refused to connect which leads to missed deadlines. The queue is adjusted based on the fair value of the source towards the information in the base station between the nodes. Increase in the frequency leads to increase in data on its own. If packets are transmitted continuously in the queue then it is involved in the transmission of more data to the offspring.

Prioritization of Emergency Module

The Emergency Module -frame consists of two time slots such as tS-duration of content free time slot and t_C - duration of contention time slot, which is illustrated in Fig. 2. With the exception of synchronization slot, sub slots t0 , t_1, t_2 and t_3 become individual in each contest-free slot of emergency module. The $t_S - (t_0 + t_1 + t_2 + t_3)$ is used for emergency mode sub-slot and is include in MAC header along with other parameters such as source, destination and flag. From the start of the slot the packet is transmitted, the transmitter uses the normal mode, and then it goes to sleep. Insertion of extra nodes is allowed to include during the contention time at the end of each frame. Regular monitoring involves communication according to the nodes' schedules. If there is no data to broadcast and no packets are received by the transmitter, a timeout is triggered, forcing the recipient to go back to sleep in order to save more energy. When certain node sensors detect fire, only fire-impacted nodes switch to emergency mode on their MAC. A packet with an emergency flag is sent to the ancestors, one-hop neighbors of the fired nodes receive messages, and the nodes themselves emit FIRE signals, all while the others continue operating normally

Rules Followed by a Node Change the MAC

Data transmission within the slot comprises its own start and end time process. The packet which has high priority is considered in the data transmission and it is involved in the transmission of the packet, it enables the one-hop neighbors for the slot to compete.

At start of each slot, with the reception of the packets all non-owners have no potential contention. If the owner of the packet comprises the high-priority data for detection and estimation of the channel activity, it is denoted as t_0 with the time slot value of t_1 for transmission of a message from the senders as SLOT_REQUEST towards the slot. The sender involved in the estimation of the message is defined as SLOT_ ACKNOWLEDGEMENT.

The own slots are utilized by the low-precedence packets if SLOT_REQUEST is not received from the neighbors between the time period of $t_0 + t_1$. The low priority slots are obtained for no actions perceived between the period of $t_0 + t_1 + t$. The content in t_3 focused on the transmission of the SLOT_REQUEST. The sender replies with the SLOT_ACKNOWLEDGEMENT.

To stop a node from sending an emergency packet to a sleeping parent, the original emergency packet is sent during a prearranged window of time. It also allows node ancestors to switch to MAC on receipt of the packet. The initial delay in emergency module is the same as normal module. In event of a false alarm, a fire node transmits the message of FALSE_ALARM involved in enabling data transmission between one-hop neighbors for MAC to restore in the normal process. The receiver of a node in the base station is considered as an emergency process involved in the conversion of MAC in regular model for the collection of emergency packets.

Hybrid TDMA / CSMA implementation in Emergency module:

Step 1: Network initialization and topology discovery with CSMA/CA

- Base station initiates the topology discovery using flood mechanism by sending TOPOLOGY_DISCOVERY including hop_count, new_parent_id, and old_parent_id.
- Nodes reply to the BS with their hop_count, parent ID, children list, and one-hop neighbors.

Step 2: Slot Assignment for Scheduled Communication is using TDMA

1. Slot assignment strategy - leaf nodes are assigned slots first and then slot allocation moves upwards in the network tree.
2. TDMA scheduling message - Base station sends a SCHEDULE_NOTIFICATION message via TDMA to inform nodes of their slots. A node waits for its children to report before allocating its own slots.
3. Slot type - single unicast slot is used for individual node communication, multiple unicast slots are used

for multi-child nodes, and diffusion slots are assigned for broadcasting critical information.

4. Once all nodes receive their slot schedules, they switch to TDMA mode and begin their transmission.

3.5 ACO FOR OPTIMAL PATH FINDING

Ant colonies are metaheuristic and probabilistic optimization techniques. It is a bio-inspired algorithm not followed by a central problem-solving method based on the actual structure and mobility operations of an ant colony. A meta-heuristic algorithm implies that, with minimal modifications to any problem, a particular user optimization technique or solution may be obtained. The flowchart for ACO algorithm is shown in Fig. 3a. Fig. 3b specifies the complete workflow of the proposeed method. The ants in the system or colony migrate from one "*x*" node to another "*y*" node at random.

$$P_{x,y} = \frac{\left(t_{x,y}^{a}\right).\left(c_{x,y}^{b}\right)}{\sum\left(t_{x,y}^{a}\right).\left(c_{x,y}^{b}\right)} \tag{5}$$

where '$t_{x,y}$' is the concentration of pheromones deposited on edge *x*, *y*. '$c_{x,y}$' is a user- defined parameter defining the effective attractiveness of the *x*, *y* route. '*a*' and '*b*' are the parameters provided by the user to adjust the $t_{x,y}$ and $c_{x,y}$ proportional values in real-time. Thus, after each iteration, pheromone trials may be updated when the ants have successfully completed a correct solution or a tour around the formula,

$$t_{xy}(t) = \left[e.t_{xy}(t-1)\right] + \Delta t_{xy} \tag{6}$$

where Δt_{xy} is a total of movements or fake ants' input to the construction of the complete solution. "*e*" is the coefficient of pheromone evaporation and is specified by the user, whose values range between 0 and 1. Thus, from this equation, it is obvious that a portion of the pheromone trail may be vaporized after the iteration and the process is iterated again. The global routing is therefore better in the ACO since it prevents the delay by concentrating the neighborhood search for the optimal path to track. The artificial ants of ACO thus follow the proportional rule, where the likelihood of an ant travelling from node *x* to node *y* relies on any random "*z*" variable that is spread uniformly across [0, 1].

Parameters used in ACO for Emergency Module:

Pheromone Influence (*α*) - monitor pheromone concentration ($t_{x,y}$) in the decision-making process. Higher α results in ants being more biased. Lower α increases randomness, and Moderate values ensure a balance between exploration and exploitation.

Heuristic Factor (*β*) - Determines the influence of the heuristic information ($C_{x,y}$), which represents the attractiveness of a path.

Pheromone Evaporation Rate (*e*) - Represents the rate at which pheromone trails evaporate over time (values range between 0 and 1).

Pherimonce deposit Amount (Δt_{xy}) - Represents the amount of pheromone deposited by ants after completing a solution.

Number of Ants (*m*) - The total number of ants used in each iteration.

The intrinsic parallelism of ACO thus makes it suitable for quicker feedback and, therefore, chooses the optimum route not just for VANETs but also for other issues. The final step of evaporation consists of upgrading the pheromone from the first phase of creation. Whenever the ants travel from one route to the next, the pheromone of that path certainly changes. The update process should be observed to avoid the dangerous and undesired standstill condition. This happens when the update is stopped due to certain problems, and the ants build the same solutions again without looking for any alternative routes.

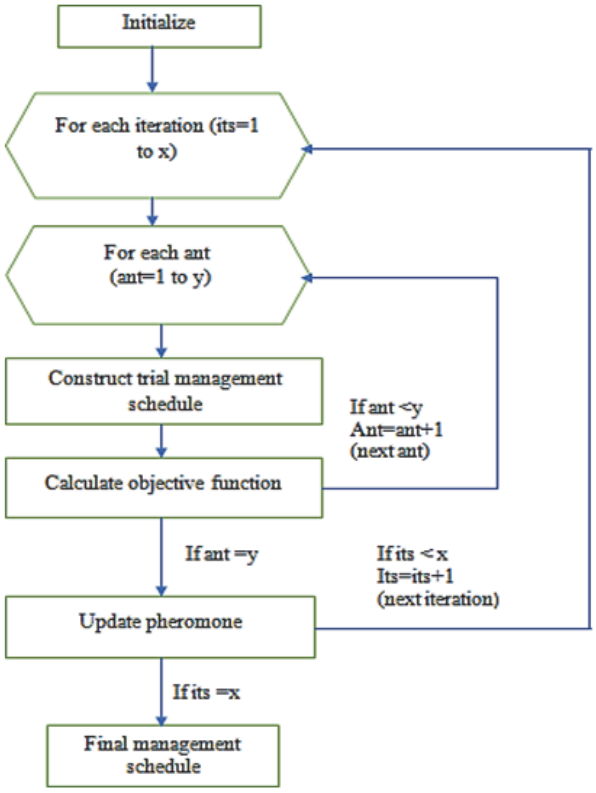

Figure 3 Flowchart for ACO

The ACO algorithm may thus be used in vehicle routing problems where the aim would be to discover optimum ways to reduce the overall latency of the network system and other limitations that should be addressed for the advantage of VANET systems using this method. The availability of many protocols for vehicle networks makes it difficult to choose just one protocol. The previous suggestions focused on boosting the system's output or conserving energy concentrated here on receiving information from the destination vehicle. The usual drawbacks to the above were either excessive latency or that the data could not reach the destination owing to the high mobility level of the VANET system. The proposed biological inspired ACO technique used fake ants and artificial neighbors. Evaporation and re-deposition of the pheromones were given high priority in order not to affect the system with the circular loop dependency and thus to avoid the same path. This improves the search for new routes in the ACO algorithm.

4 RESULTS AND EVACUATION

The simulation results of the proposed EMAO-MTRUST are shown below, along with a comparative analysis to determine the effectiveness of the proposed approach. The simulation environment is designed using NS-2.34 (Network Simulator 2.34) to analyze the behavior of a wireless ad hoc network with various network parameters, including node configurations, traffic types, energy models, and routing protocols.

The simulation's parameters are shown in Tab. 3. The simulation is conducted over 1000 × 1000 m (1 KM2). The simulation environment randomly deployed 100 nodes, with a simulation duration of 100 milliseconds. Nodes operate in an ad hoc wireless network where there is no fixed infrastructure. Each node can function as a source, destination, or intermediate router, enabling multi-hop communication. The BH-TBF protocol is utilized for routing, at an initial power of 100 J. The simulation's details are listed in Tab. 3.

In Blackhole attack, malicious nodes absorb all network traffic by falsely the shortest route to the destination but then drop the packets instead of forwarding them. Flood attack involves malicious nodes sending excessive packets into the network, causing congestion, increased energy consumption, and network overhead. Both blackhole attack and flood attacks are evaluated based on the following parameters such as Energy consumption, Packet delivery ratio, Packet loss, Overhead, End-to-end delay and throughput. Both attack models were tested and compared with EMAO-MTRUST against **THMM** and **TBF** in terms of efficiency, reliability, and network performance.

Table 3 Simulation parameters details for EMAO-MTRUST protocol

Parameters	Values
Simulator	NS-2.34
Simulation Period	100 ms
Coverage Area	1000 × 1000
No. of Nodes	100
Standard	IEEE 802.11
Propagation Model	Two Ray Propagation Model
Antenna	Omni-directional Antenna
Traffic Type	FTP
Traffic Rate	0.01 sec to 0.50 sec
Agent Type	TCP
Routing Protocol	AODV
Initial Power	100 J
Idle Power	0.1 J
Queue Type	Drop-Tail

Fig. 5 shows the network analysis in the context of a black hole attack with 100 nodes. The energy consumption of the techniques in the presence of a black hole assaults at a time 100 ms is 2.952%, 16.187%, and 29.164% for the proposed EMAO-MTRUST, BH-THMM, and BH-TBF, correspondingly. The network overhead for the proposed EMAO-MTRUST, BH-THMM, and BH-TBF is 100 ms, and the network overhead is 3828 packets, 1768 packets, and 1586 packets.

The packet delivery ratio of the proposed EMAO-MTRUST, BH-THMM, and BH-TBF is 100 ms, respectively, 96.04%, 82.24%, and 76.52%. When the time is 100 m, the throughput from the proposed EMAO-MTRUST, BH-THMM, and BH-TBF is respectively 421.17 kbps, 336.34 kbps, and 283.87 kbps.

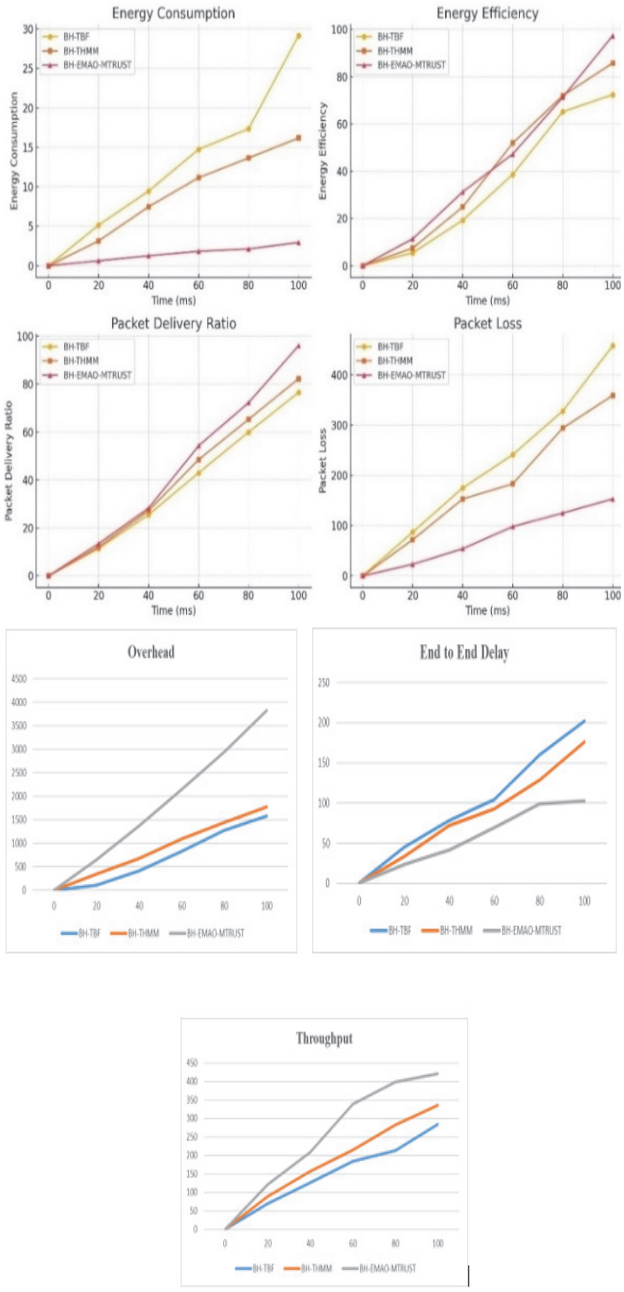

Figure 5 Analysis using the black hole attack

If the time is 100 ms, the energy efficiency of the proposed EMAO-MTRUST, BH-THMM, and BH-TBF is 97.36%, 85.72%, and 72.36%. In the case of a black hole assault. When the time is 100 ms, the delay is 102.26 ms, 176.32 ms, and 202.185 ms, correspondingly for the proposed EMAO-MTRUST, BH-THMM, and BH-TBF. The packet loss of the proposed EMAO-MTRUST, BH-THMM, and BH-TBF is 153 packets, 359 packets, and 458 packets when the time is 100 ms. It is evident from the above results that the proposed EMAO-MTRUST shows a higher throughput ratio of 421.17 Kbps, with low energy consumption, high efficiency of 97%, less end-to-end delay and minimum packet loss. Tab. 4 shows the comparative analysis of black hole attack.

Table 4 Comparative analysis with Black hole attack of proposed EMAO-MTRUST protocol

Time / ms	BH-TBF	BH-THMM	BH-EMAO-MTRUST
Energy Consumption			
0	0	0	0
20	5.148	3.145	0.632
40	9.465	7.478	1.263
60	14.751	11.154	1.832
80	17.358	13.654	2.127
100	29.164	16.187	2.952
Energy Efficiency			
0	0	0	0
20	5.4735	7.479	11.3854
40	19.2712	24.8843	31.2574
60	38.6474	51.8734	47.2568
80	65.1254	71.9353	71.2522
100	72.3647	85.7226	97.3630
Packet Delivery Ratio			
0	0	0	0
20	11.42	12.023	13.3854
40	25.53	27.221	28.2574
60	42.98	48.486	54.2568
80	59.983	65.296	72.2522
100	76.522	82.248	96.0474
Packet Loss			
0	0	0	0
20	87	72	23
40	175	153	54
60	241	183	98
80	328	294	125
100	458	359	153
Overhead			
0	0	0	0
20	103	341	657
40	412	678	1375
60	834	1091	2154
80	1274	1438	2943
100	1586	1768	3828
End to End Delay			
0	0	0	0
20	44.893	33.172	23.343
40	78.284	71.782	41.769
60	104.362	93.022	69.227
80	159.549	128.562	99.338
100	202.185	176.322	102.268
Throughput			
0	0	0	0
20	68.78	89.28	121.32
40	125.82	157.33	208.77
60	184.25	215.16	339.47
80	212.35	281.94	398.22
100	283.87	336.34	421.17

Fig. 6 shows the network analysis in the context of the flood attack with 100 nodes. If the time is 100 ms, the energy consumption is 26.22%, 26.18%, and 39.12% for the proposed EMAO-MTRUST, FL-THMM, and FL-TBF. At 100 ms time, network overhead is 2711 packets, 2568 packets, and 2414 packets correspondingly for the proposed EMAO-MTRUST, FL-THMM, and FL-TBF respectively. When the time comes to 100 ms, the packet delivery ratio is 98.21%, 81.24%, and 54.38% for the proposed EMAO-MTRUST, FL-THMM, and FL-TBF, respectively.

The throughput of the proposed EMAO-MTRUST, FL-THMM, and FL-TBF is 590.24 kbps, 426.34 kbps, and 321.58 kbps. The energy efficiency of the proposed EMAO-MTRUST, FL-THMM, and FL-TBF is 87.88%, 75.72%, and 61.54%, respectively, when time is 100 ms. When time is 100 ms, it is 68.69 ms, 128.32 ms, and 179.98 ms, correspondingly for the proposed EMAO-MTRUST, FL-THMM, and FL-TBF. The packet loss of the proposed EMAO-MTRUST, FL-THMM, and FL-TBF is 119 packets, 435 packets, and 650 packets. It is evident from the above results that, the proposed EMAO-MTRUST shows a higher throughput of 590.24 kbps and packet delivery. Similarly, energy consumption is low, efficiency is 87.88%, and the delay and losses of packages are lower compared to the current technique. Tab. 5 shows the comparative analysis with flooding attack of the proposed method.

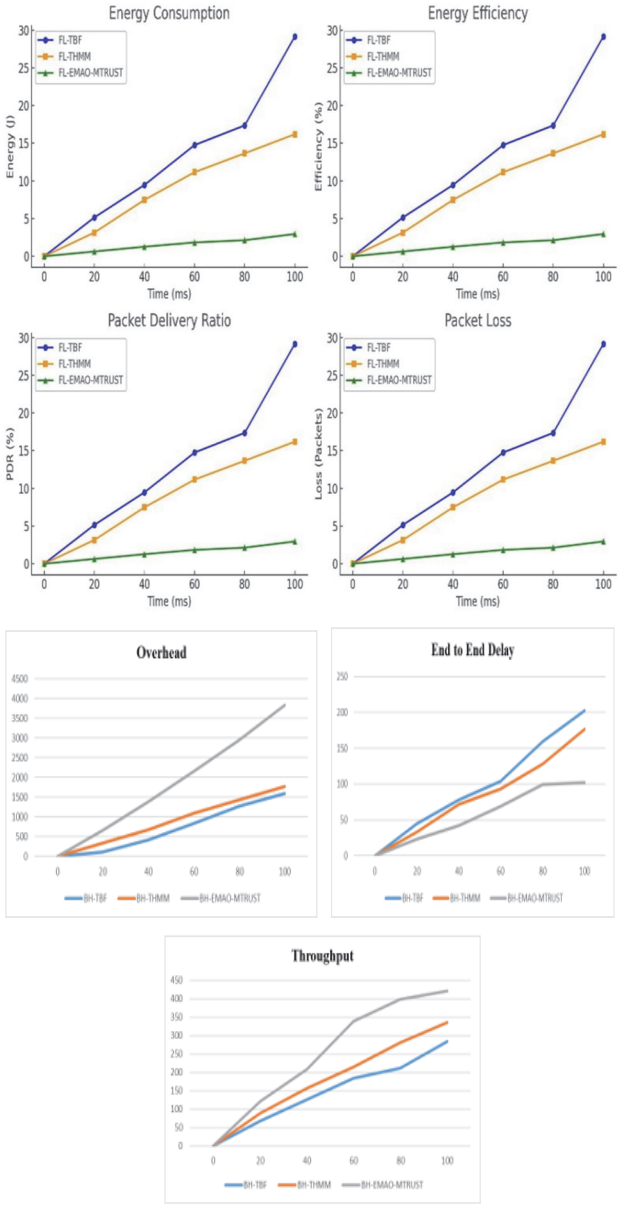

Figure 6 Analysis using the flooding

Table 5 Comparative analysis with Flooding attack of proposed EMAO-MTRUST protocol

Time / ms	BH-TBF	BH-THMM	BH-EMAO-MTRUST
Energy Consumption			
0	0	0	0
20	5.148	3.145	0.632
40	9.465	7.478	1.263
60	14.751	11.154	1.832
80	17.358	13.654	2.127
100	29.164	16.187	2.952
Energy Efficiency			
0	0	0	0

Table 5 Comparative analysis with Flooding attack of proposed EMAO-MTRUST protocol (continuation)

Time / ms	BH-TBF	BH-THMM	BH-EMAO-MTRUST
Energy Efficiency			
20	5.4735	7.479	11.3854
40	19.2712	24.8843	31.2574
60	38.6474	51.8734	47.2568
80	65.1254	71.9353	71.2522
100	72.3647	85.7226	97.3630
Packet Delivery Ratio			
0	0	0	0
20	11.42	12.023	13.3854
40	25.53	27.221	28.2574
60	42.98	48.486	54.2568
80	59.983	65.296	72.2522
100	76.522	82.248	96.0474
Packet Loss			
0	0	0	0
20	87	72	23
40	175	153	54
60	241	183	98
80	328	294	125
100	458	359	153
Overhead			
0	0	0	0
20	103	341	657
40	412	678	1375
60	834	1091	2154
80	1274	1438	2943
100	1586	1768	3828
End to End Delay			
0	0	0	0
20	44.893	33.172	23.343
40	78.284	71.782	41.769
60	104.362	93.022	69.227
80	159.549	128.562	99.338
100	202.185	176.322	102.268
Throughput			
0	0	0	0
20	68.78	89.28	121.32
40	125.82	157.33	208.77
60	184.25	215.16	339.47
80	212.35	281.94	398.22
100	283.87	336.34	421.17

5 CONCLUSION

A new Emergency Module with ant optimization based multi-hop routing protocol (EMAO- MTRUST) for VANETs was proposed, and it calculates direct and indirect trust models which are used to identify hazardous acts. More trusted nodes are selected as border nodes, and border nodes transmit the packets. The Ant Colony Optimization Algorithm (ACO) for optimum route selection. Emergency Module is added to transmit the data in priority basis which leads to reduce the delay and energy consumption in the network. The performance of the proposed EMAO- MTRUST Routing Protocol is compared with the Trust hidden markov model (THMM) and Trust-Based Finding (TBF) methods. The proposed EMAO-MTRUST Routing Protocol method gives maximum packet delivery ratio, energy efficiency and throughput, minimum energy consumption, packet loss, delay, and overhead information when compared to the existing methods. Finally, the simulation results demonstrate that the proposed approach gives better results when compared with existing methods for blackhole and flooding attacks.

6 REFERENCES

[1] Mohcine, B. & Driss, B. (2024). New Detection Approach Against Trust Manipulation Attack in VANET. *Lecture Notes in Networks and Systems*, *887*. https://doi.org/10.1007/978-3-031-74491-4_45

[2] Vinoth Kumar, K. & Duraisamy, B. (2022). Efficient Privacy-Preserving Red Deer Optimization Algorithm with Blockchain Technology for Clustered VANET. *Tehnički Vjesnik*, *29*(3), 813-817. https://doi.org/10.17559/TV-20211216115635

[3] Abd El-Latif, A., Abd-El-Atty, B., Venegas-Andraca, S., Elwahsh, H., Piran, M., Bashir, A., Song, O.-Y. & Mazurczyk, W. (2020). Providing End-to-End Security Using Quantum Walks in IoT Networks. *IEEE Access*, 1-1. https://doi.org/10.1109/ACCESS.2020.2992820

[4] Wei, S., Li, X., Ji, H., & Zhang, H. (2024). Anti-attack Trust Evaluation Algorithm Based on Bayesian Inference in VANET. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, *590*. https://doi.org/10.1007/978-3-031-67162-3_10

[5] Che, H., Duan, Y., Li, C., & Yu, L. (2022). On trust management in vehicular ad hoc networks: A comprehensive review. *Frontiers in the Internet of Things*, *1*, 995233. https://doi.org/10.3389/friot.2022.995233

[6] Siddiqua, F. & Jahan, M. (2022). A Trust-Based Malicious RSU Detec- tion Mechanism in Edge-Enabled Vehicular Ad Hoc Networks. arXiv preprint. https://doi.org/10.48550/arXiv.2208.05680

[7] Malik, A., & Khan, M. Z., Faisal, M., Khan, F., & Seo, J.-T. (2022). An Efficient Dynamic Solution for the Detection and Prevention of Black Hole Attack in VANETs. *Sensors*, *22*, 1897. https://doi.org/10.3390/s22051897

[8] Akanksha, V. & Sachin, P. (2024). Reactive & Multipath Routing with Adaptive Urban Area Vehicular Traffic (AUAVT) in VANET Environment. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(21s), 802-810.

[9] Okeke, U. & Mbarushimana, C. (2023). Enhancing Security in VANET Against Blackhole Attacks using AODV, K-Means Clustering, and PSO. *IEEE*, 1-6. https://doi.org/10.1109/ICECCE61019.2023.10441860

[10] Yeferny, T. & Hamad, S. (2021). Vehicular Ad-hoc Networks: Architecture, Applications and Challenges. https://doi.org/10.48550/arXiv.2101.04539

[11] Jeong, J., Shen, Y., Oh, T., Céspedes, S., Benamar, N., Wetterwald, M., & Härri, J. (2021). A comprehensive survey on vehicular networks for smart roads: A focus on IP-based approaches. *Vehicular Communications*, *29*, 100334. https://doi.org/10.1016/j.vehcom.2021.100334

[12] Balakrishnan, S. & Vinoth Kumar, K. (2023). Hybrid sine-cosine black widow spider optimization based route selection protocol for multihop communication in IoT assisted WSN. *Technical Gazette*, *30*(4), 1159-1165. https://doi.org/10.17559/TV-20230201000306

[13] Liu, H., Han, D., & Li, D. (2021). Behavior Analysis and Blockchain-Based Trust Management in VANETs. *Journal of Parallel and Distributed Computing*, *151*, 61-69. https://doi.org/10.1016/j.jpdc.2021.01.011

[14] Nobahari, A., Bakhshayeshi, A. D., Akhbari, A., & Nobahary, S. (2023). Investigation of Different Mechanisms to Detect Misbehaving Nodes in Vehicle Ad-Hoc Networks (VANETs). *Security and Communication Networks*, 1-40. https://doi.org/10.1155/2023/4020275

[15] Krishnan, R. & Kumar, P. (2022). Detection and Mitigation of Smart Blackhole and Gray Hole Attacks in VANET Using Dynamic Time Warping. *Wireless Personal Communications*, 124. https://doi.org/10.1007/s11277-021-09390-3

[16] Akanksha, V. & Sachin, P. (2024). Reactive & Multipath Routing with Adaptive Urban Area Vehicular Traffic (AUAVT) in VANET Environment. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(21s), 802-810.
[17] Gao, H., Liu, C., Yin, Y., Xu, Y., & Li, Y. (2022). A Hybrid Approach to Trust Node Assessment and Management for VANETs Cooperative Data Communication: Historical Interaction Perspective. *IEEE Transactions on Intelligent Transportation Systems*, *23*(9),16504-16513. https://doi.org/10.1109/TITS.2021.3129458
[18] Soni, S. (2020). Reliable Trust Computation model in Vehicular ad-hoc Network. *American Journal of Advanced Computing*, *1*, 1-5. https://doi.org/10.15864/ajac.1304
[19] Vinoth Kumar, K. & Balakrishnan, S. (2023). Multiobjective sand piper optimization based clustering with multihop routing technique for IoT assisted WSN. *Brazilian Archives of Biology and Technology*, *66*, e23220866. https://doi.org/10.1590/1678-4324-2023220866
[20] Chiluveru, R., Gupta, N., & Teles, A. (2021). Distribution of Safety Messages Using Mobility-Aware Multi-Hop Clustering in Vehicular Ad Hoc Network. *Future Internet*, *13*, 169. https://doi.org/10.3390/fi13070169
[21] Jeelani, M., Singh, K., & Zafar, A. (2021). A Trust Calculation Algorithm for Communicating Nodes in Wireless Sensor Networks. *International Research Journal on Advanced Science Hub*, *3*, 145-152. https://doi.org/10.47392/irjash.2021.083
[22] Pruthvi, C. N., Vimala, H. S., & Shreyas, J. (2023). A Systematic Survey on Content Caching in ICN and ICN-IoT: Challenges, Approaches, and Strategies. *Computer Networks*, *233*. https://doi.org/10.1016/j.comnet.2023.109896
[23] Gong, J., Shen, Y., Oh, T., Cespedes, S., Benamar, N., Wetterwald, M., & Harri, J. (2021). A Comparative Survey on Vehicular Networks for Smart Roads: A Focus on IP-Based Approaches. *Vehicular Communications*, *29*. https://doi.org/10.1016/j.vehcom.2021.100334

Contact information:

Parimala GARNEPUDI, Research Scholar
(Corresponding author)
Department of Information and Communication Engineering,
Saveetha Engineering College,
Chennai, Tamilnadu - 602105, India
E-mail: garnepudi.parimala@protonmaill.com

M. VANITHA, Professor
Department of Electronics and Communication Engineering,
Saveetha Engineering College,
Chennai, Tamilnadu - 602105, India