IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 29 July 2023, accepted 14 August 2023, date of publication 23 August 2023, date of current version 6 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3308035

RESEARCH ARTICLE

Detecting and Preventing False Nodes and Messages in Vehicular Ad-Hoc Networking (VANET)

SADAF MASOOD[1], YOUSAF SAEED[1], ABID ALI[2,3], HARUN JAMIL[4], NAGWAN ABDEL SAMEE[5], HAYAM ALAMRO[6], MOHAMMED SALEH ALI MUTHANNA[7], AND ABDUKODIR KHAKIMOV[8]

[1]Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan
[2]Department of Computer Science, University of Engineering and Technology, Taxila, Taxila 48080, Pakistan
[3]Department of Computer Science, GANK(S) DC KTS, Haripur 22620, Pakistan
[4]Department of Electronic Engineering, Jeju National University, Jeju-si 63243, South Korea
[5]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[6]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[7]Institute of Computer Technologies and Information Security, Southern Federal University, 347922 Taganrog, Russia
[8]RUDN University, 117198 Moscow, Russia

Corresponding author: Hayam Alamro (hmamro@pnu.edu.sa)

This research was funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R361), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia, in part this paper has been supported by the RUDN University Strategic Academic Leadership Program (recipient Abdukodir Khakimov).

ABSTRACT Vehicular ad-hoc network (VANET) is an advanced mobile wireless network. The escalation of equipped vehicles on the road grabs the attention of researchers and is constantly striving to take it further. This type of wireless network infrastructure helps to establish communication between vehicles. Roadside units, sensors, and vehicular nodes are the critical components of our work to protect the vehicular network. This research is focused on detecting and preventing fake vehicular nodes and their messages by applying fake node detection and prevention algorithms and counterfeit message detection and prevention algorithms. In our proposed approach, the fake node detection and prevention algorithms check the node profile after establishing the mesh structure. If the profile attribute named ‘‘Pen/Rew’’ satisfies the condition that should be less than or equal to a threshold value (zero), the fake message detection and prevention process starts. The message will be accepted once the situation is satisfied; otherwise, it is declared fake. We utilized ONE (opportunistic network environment) simulator to generate node movement models, route messages between nodes, and visualize mobility and messaging passing in real time. The results indicated that our proposed work perfectly detects and prevents fake nodes and messages.

INDEX TERMS VANET, roadside unit, fake nodes, fake messages, ONE simulator.

I. INTRODUCTION

VANET is an advanced and particular type of mobile wireless network. The escalation of equipped vehicles on the road grabs researchers' attention, and they are constantly striving to take it further. This type of wireless network infrastructure helps to establish communication between vehicles. Roadside units, sensors, and vehicular nodes are the key components in vehicular ad-hoc networks to make communication possible. In such a network, the vehicle communicates with each other called vehicle-to-vehicle (V2V) or with a roadside unit called vehicle-to-infrastructure (V2I). The vehicular ad-hoc network aims to achieve road efficiency, reduce traffic problems, and improve VANET security. The intelligent transport system addresses network reliability, as vehicles can send information about their location across vehicular networks.

The associate editor coordinating the review of this manuscript and approving it for publication was Baoping Cai.

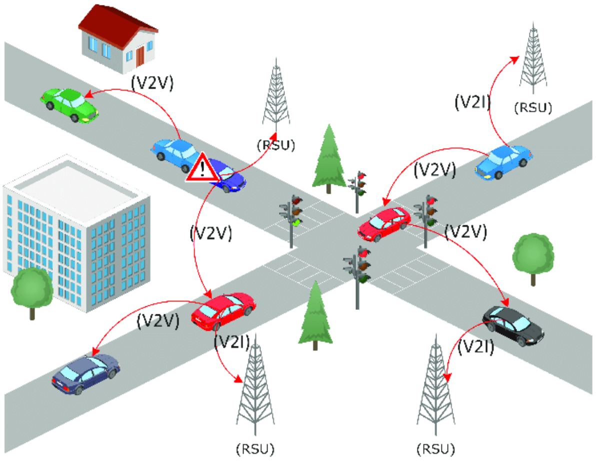


FIGURE 1. VANET architecture [1].

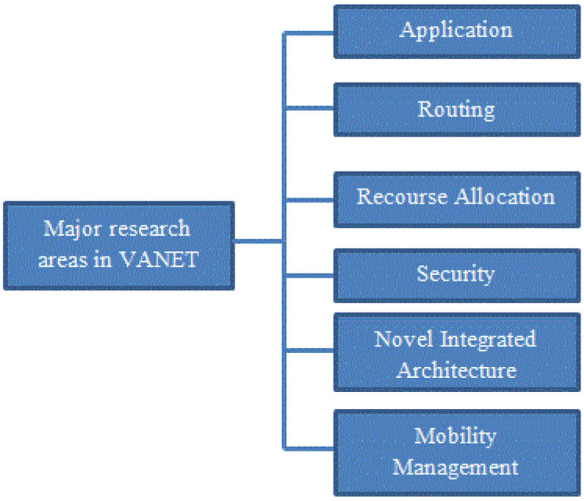


FIGURE 2. Major research areas in VANET.

Information could be about accidents, road blockage due to land sliding, weather information, or security threats. VANET applications are utilized for this purpose and are divided into two categories: comfort and safety applications. Some vehicular ad-hoc network applications can help improve safety, collision warning, accident alerts, vehicle-to-vehicle communication, traffic congestion notification, weather information, danger zone alerts, malicious entity information, etc.

Moreover, the vehicular ad-hoc network has to handle more tasks along with communication, like overcoming the delay that helps the vehicle to make the right decision at the right time, reducing network disconnectivity that allows the vehicle to stay connected with the network and can get the information from the other nodes, network security that protects the network from the malicious node, reliability check that arriving message is from reliable node or not, and sending updates to the connected nodes (V2V or V2I). These are the tasks VANET needs to perform along with sending messages. These tasks are performed with the help of components including infrastructure (roadside unit or cellular network), vehicular nodes (cars, trucks, bikes) equipped with an onboard unit that helps to send and receive information, and a central unit or base station that stores the information in real-time and sends it to the roadside unit (RSU) if requested. RSU further sends the information to the vehicle upon request. These components and their working are depicted in the architecture of VANET and shown in Figure 1.

In vehicular ad-hoc networks, the data collection process is frequent. This data is used for hazardous situations, road accidents, traffic velocity, density, etc. In VANET, updated information should be approachable by authentic nodes. According to the provided information, decision-making should be easy, pathfinding is essential in the vehicular network, network security is the primary concern, data should be protected, and efficient route selection can save time. These significant research areas in VANET are shown in Figure 2.

Considering the security of vehicular ad-hoc networks, node authentication is key to saving the network from fake entities and bogus messages [2]. Network security protects your network from threats and manufactured vehicles that send malicious messages that can corrupt the network or it can misguide a vehicular node by sending fake messages. An artificial node somehow enters the network and hides its identity, or a registered node can be a fake node [3]. The fake node sends messages to the vehicle to mislead it. Messages can be about inefficient routes that can cause a waste of time, send false accident reports, or false weather information. These can be in the form of messages from fake nodes. Fake messages can be received from fake nodes, but not in all cases. The fake node can be among authentic and reliable nodes, too, and in such a case, detecting fake messages is challenging [4].

A message-sending node may be an authentic node that forwards messages containing malicious data that can damage the entire network. The fake node can be an unauthorized node or a third-party hacker that uses a fake identity and pretends itself an authorized entity. These types of nodes misguide the vehicle. Some nodes in the network attack in two different manners. The node attacks either actively or passively. An active attack is when the third-party attacker changes the content or message information and tries to misguide the vehicle [5]. Different active attacks are carried out in a vehicular network. The VANET faces multiple attacks, such as masquerade attacks, when the vehicle is unprotected from authorized attacks [6]. Another attack is the DoS attack, which hijacks the network, pauses network operations, or shuts down network activities [7]. Modification of messages attacks, attacks on the confidentiality and integrity of data under vehicular environment [8]. Reply attack occurs when the network security is not so good, and in this attack type, the attacker fetches the real message and saves it for later use [9]. If we have an encrypted message in the network, the attacker will observe the length and frequency of the message, and afterward, a traffic analysis attack occurs [10]. In this discussion, the last attack is the release of message content attack. Voice messages, emails, or any sensitive information needs to be protected. The release of message content can be harmful to the entire network. We want to keep the information of these transmissions hidden from the attackers. As shown in Figure 7, an attacker will monitor an unprotected communication medium, such as an unencrypted email or phone call, and capture sensitive information [11].

Vehicular Ad-Hoc Networks are becoming more essential to improve passenger safety, vehicle safety, and comfort in modern urban traffic. Detecting fake messages in the form of bogus emergency messages and preventing them may help to ensure safety. Vehicular ad-hoc network uses different algorithms to protect the vehicle and entire network from physical damage or data loss. Physical damage may include accidents because of traffic or weather conditions, while data can be lost because of unauthorized access to the network or due to different attacks. Various mechanisms exist for fake node detection and counterfeit message detection approaches in vehicular ad-hoc networks. Also the same goes for prevention mechanisms. There is a need to devise a technique that can detect fake nodes and messages inside the vehicular ad-hoc network [12].

Fake nodes can be detected by devising an algorithm that can detect malicious nodes from the network efficiently, that otherwise might cause a serious accident. After identifying fake nodes, the algorithm should be able to prevent that node, so the node will not be able to misguide other nodes in the network. Fake messages can be detected by optimizing an algorithm to see bogus messages that may cause serious issues. The algorithm must be able to remove fake messages from the network after identifying them.

Our research significantly contributes to the VANET field by introducing a comprehensive approach that addresses fake node and message detection. Unlike existing methods focusing only on one aspect, our proposed approach considers the entire system's integrity. Utilizing the vehicle profile method, which includes attributes such as vehicle id, vehicle brand, model, location, and message reward/penalty, we have effectively proposed a robust system that ensures the authenticity of nodes and messages within the network.

The advantage of our research lies in its ability to increase the security and reliability of VANETs. The proposed approach can significantly reduce the risks associated with malicious attacks and information manipulation by detecting and preventing fake nodes and messages. This promotes a safer and more trusted automotive communication system, ultimately benefiting the community and society. Our research can positively impact various sectors, including transport, emergency services, and smart city initiatives. A safer VANET facilitates efficient traffic management, enables reliable emergency communications during critical situations, and supports the widespread adoption of connected vehicles. In addition, by preventing the spread of fake communication over the network, our approach protects user privacy and ensures the accuracy and reliability of information transmitted.

Our research offers a novel and valuable contribution to VANET security and solves the problems posed by fake nodes and messages. Its positive impact on the community and society makes it a promising step towards building a safer and more trusted vehicle communication environment.

Moreover, the paper is structured into different sections where Section II discusses the existing literature highlighting the related work that provides the basis for our proposed work. Section III elaborates on our proposed framework, the proposed algorithms, and a comparison with the literature. Section III presents the research simulation and results, and section IV discusses the conclusion of our work and the scope of future work for possible extended application of the project.

II. LITERATURE REVIEW

VANETs have been under research for many years. However, with the advancement of communication technology, there is a need to improve the information exchange process and provide more secure and comprehensive solutions to the threats that fit today's needs. Network security ensures integrity, confidentiality, and authentication. Network security is an important concern in network communication. Attackers have a greater edge in wireless networks than in wired networks. In this section, we will discuss related work of VANET and security systems, where the research community has done much work in the last decade. We critically examined different proposed systems in the literature review we found some limitations of the proposed methods by various authors.

The frequently changing network topology must be maintained on different levels using hardware, onboard units, roadside infrastructure, or base station. On level one, onboard units are used to send messages to the vehicular nodes in the network. On level two, the network node communicates with roadside infrastructure. Roadside infrastructure ensures the authenticity of the vehicle. On level three, the roadside infrastructure communicates with the base station. In [10] author indicates that when the number of nodes connected to the router is reduced, a sub-group of computers can interact with each other without interfering with computers outside their group. But this scenario could happen if the number of vehicular nodes in the area is small.

Suppose the number of vehicular nodes in the area is small. This scenario may not be feasible if there are many vehicles. We have to connect all the possible vehicles in the area. We cannot skip some of them and select a few vehicles. Reference [11] introduces a routing protocol that solves the scalability issue. Scalability means increasing the number of vehicular nodes without decreasing their performance and network ability. For this purpose, a hybrid location-based ad-hoc routing protocol is introduced that uses geographical location. As the location information deteriorates, the protocol is designed to transition easily to reactive routing. The reactive protocols are built on on-demand route discoveries, which only update routing tables for destinations with traffic. On the other hand, the proactive protocols are based on periodic exchanges that update the routing tables to all conceivable destinations, even if no traffic passes through.

Our way of life has already been altered by artificial intelligence. A technology that humans can see in nature and act on boosts its chances of achieving its objectives. In this context, [13] analyzes the transparency of Google smart assistant, AI-powered smartphone software, regarding risk disclosure to users and execution. Many risk evaluation algorithms utilize the same variables when computing app threat scores. Android users rely on the transparency of an application's descriptions and permission requirements for its risk evaluation. Furthermore, multiple risk evaluation models and malware detection approaches for Android apps evaluate an application's behavior based on its permissions and API usage.

Due to their nefarious behavior or selfishness, fake nodes might spread false safety alerts throughout a network. False signals in ad-hoc vehicle networks can alter driver behavior and result in a network disaster. In [14], this article suggests and analyzes a fake message detection technique. To begin, traffic flow theory examines vehicle behavior in the context of a traffic accident. It demonstrates that a ''bottle-neck'' phenomenon occurs when road capacity is restricted due to blocked lanes at an accident scene. Unlike an accident-free situation, traffic characteristics such as vehicular density show a distinct statistical property. Based on this, a false message detection system is presented, in which traveling vehicles are used as witnesses to collect traffic characteristics. Their observation data is used as evidence to feed a traffic flow model. The likelihood for each traffic scenario is calculated using a Bayesian theorem–based method, and the actual traffic 28 condition is estimated to determine whether the reported accident occurred. The proposed algorithm's detection rate (DR) and false positive rate (FPR) are calculated and compared with the previously proposed scheme. The proposed approach appears to have worked well, as a tiny percentage of attackers successfully caught all false communications. When the attacker proportion exceeded 0.2, the DR began to plummet. This is primarily due to the attackers taking advantage of their numbers and providing false evidence to deceive honest vehicles into receiving incorrect results.

In [15], an efficient algorithm is proposed to ensure the security and privacy of VCC. Using Pseudo-ID instead of real vehicle ID to ensure driver privacy, an Identifier-Based Signature mechanism to guarantee vehicle authentication, and Attribute-Based Encryption (CP-ABE) algorithm for key distribution, the problem is with the public key distribution. The public key is known to everyone, and the private key is known only to the owner and the PKG. Thus, the private keys of all users are stored in the PKG [16].

Consequently, with users, the PKG private key can impersonate another user. This is known as the key Escrow problem. Reference [17] presented a new method to increase security in the VANET environment and to assess the effectiveness of the proposed On Demand Multi-Cast Routing Protocol (ODMRP). The proposed system has implemented encryption key management systems for VANET based on RSA and AES. According to packet delivery ratio and throughput, the performance evaluation revealed that the proposed OD-MRP using the RSA and AES algorithm has a greater capacity for adaptability on VANET. It supports message authentication but does nothing about fake node detection. It also creates an escrow problem by using a key distribution algorithm.

Reference [18] Presents a security algorithm for opportunistic networks that provides node authentication to protect and prevent Sybil attacks and malicious and unauthorized nodes. This algorithm helps and improves authentication for expanding opportunistic networks from heterogeneous nodes. When a new node needs to connect, it has to contact the initial nodes, 29, and it checks the node if it has an ID, then compares it with a public list that holds all node's IDs. If it is found, the node becomes authorized; if the ID is not, the default nodes generate a new ID and broadcast it to update the public list periodically so the node can connect after authorization. This algorithm only deals with nodes and does not concern with messages.

In [19], the study provides a thorough architecture for socially conscious vehicle edge computing. It includes a DRL-based optimization technique, a traffic-aware content recommendation system, and a graph-pruning search tool. By using vehicles as edge servers and taking social context into account during the process, these components work together to improve information delivery. Even though all interactions between content consumers and content providers are encrypted, statistical attacks can still be used to predict the consumers' future pathways.

In [20], a novel system called an intrusion detection system (IDS) is proposed for spotting unauthorized access in computer networks. This strategy makes use of deep learning and time series classification. Time series data of traffic parameters closely related to traffic incidents have been acquired since different traffic metrics are influenced by time. Feature vectors are used to represent these data. Using a deep learning model known as Long Short-Term Memory (LSTM), a traffic incident classifier has been created to increase the precision of recognizing patterns in the changing traffic parameters over time.

In [21], The NTRU cryptosystem was patented by NTRU Cryptosystems. In the proposed system, NTRU has been used for node authentication and to prevent the network from fake nodes. Still, it does not support message authentication-related checks about differentiates, which makes our proposed work more advanced.

In [22], a new privacy-preserving message delivery and authenticity protocol is proposed. The protocol used an efficient combination of symmetric and asymmetric cryptographic algorithms. An efficient RSA protocol, CRT-RSA, has been used for the asymmetric key. AES-128 was used for the symmetric key. The proposed protocol effectively reduced the time required for the decryption process. The symmetric key was generated and distributed without using the DH protocol, resulting in high computational time overhead. The asymmetric key of the shared group was changed to a symmetric one in our proposed protocol to achieve the required level of security with minimum computation time. But it ensures message authenticity and does not support fake node detection and prevention.

Reference [23] proposes an Evolutionary Public Goods Game (EPGG) model to detect fake messages and stimulate nodes to implement data verification. When a node detects a rumor, it immediately broadcasts an anti-rumor. A sensitive, immune, and neutral (SIN) rumor model is introduced to characterize the spread of dishes and anti-rumors. They propose a dynamic, hierarchical public goods game (DHPGG) model to analyze the symbiosis and confrontation of rumors and anti-rumors. The simulation results show that these models could effectively detect and suppress rumors in VANETs.

A vehicle is considered malicious if it shares false or inaccurate news. Such a rule is fuzzy and not consistently accurate due to the dynamic uncertainty of the vehicle context, leading to a low detection rate. To this end, this study [24] proposed a fuzzy-based context detection model to improve the overall detection performance. A fuzzy inference system is constructed to evaluate vehicles based on their generated information. The output of the proposed fuzzy inference system is used to create a dynamic context reference based on the proposed fuzzy inference system. Vehicles are classified into honest or dishonest nodes based on the deviation of their evaluation scores calculated by the proposed fuzzy inference system from the context reference.

Current studies of intelligent transportation systems (ITS) use vehicle and communication traffic simulations due to the ethical and practical impracticability of experiments on real transportation networks. Various simulators have been developed to model vehicle mobility and vehicle-to-vehicle communication in real time under different traffic and road conditions. NetSim is a simulator covering a wide range of wired, wireless, cellular, and sensor networks. NetSim interfaces with SUMO to simulate VANETs. The first handles the WAVE standard for wireless communication between vehicles, while the second model's road traffic conditions. NetSim provides a set of network performance metrics and link and application throughput graphs. Metrics will vary depending on the type of network being simulated. Using packet tracing and event tracing, users can log details about each packet as it flows through the web [25]. The vein is an open-source framework for running vehicle network simulations. It is based on OMNeT++ and SUMO. Overall, the simulator instantiates an OMNeT++ node for each vehicle present in the simulation and then matches the node movements to the vehicle movements in the road traffic simulator (i.e., SUMO). In this case, both network and mobility simulations can run in parallel. This is possible to the two-way coupling of the standardized Traffic Control Interface (TraCI) connection protocol. Traci allows OMNeT++ and SUMO to exchange messages (e.g., containing mobility traces) while the simulation runs as part of a TCP connection. [26].

In [27] dynamic complex environments, the degradation of structural systems is a multifaceted process influenced by various factors, and uncertainty plays a significant role. Existing research has mainly focused on degradation models based on a single factor, which leaves a gap in understanding the combined effects of multiple causes on residual life (RUL) estimation. To address this gap, the proposed research introduces a hybrid physical model-data approach using Dynamic Bayesian Networks (DBN) to estimate RUL while considering the influence of multiple factors. By incorporating theoretical or empirical physical models into DBN, the authors solve the problem of limited data availability.

The RUL estimation model is built by integrating the degradation process models, and the RUL value is determined by calculating the time difference between the detection point and the predicted failure point based on the performance failure threshold. This new approach allows updating the RUL value using sensor data and expertise when needed. To demonstrate the methodology's effectiveness, the research focuses on subsea pipelines in subsea offshore oil and gas production systems. Specifically, degradation processes due to fatigue, corrosion, sand erosion, and internal waves are modeled using DBN, and RUL is estimated using a DBN-based RUL methodology.

This research [28] highlights the importance of reliability estimation in increasingly complex systems. Random effects degradation models, such as the Wiener process, have been widely used to estimate the remaining useful life (RUL). However, conventional models based on the Wiener process only consider current monitoring data, leading to inaccurate RUL predictions due to the exclusion of historical degradation data. Additionally, missing data in engineering scenarios further complicates accurate predictions by proposing an RUL re-prediction method that combines the current monitoring status and historical degradation data using a Wiener process. The initial prediction process involves the estimation of drift and diffusion coefficients using the Expectation Maximization algorithm and creating a Dynamic Bayesian Networks (DBN) model to deal with missing data uncertainties. In the re-prediction process, data from multiple stages are combined to calculate the baseline degradation at each step of the Wiener process, further increasing the accuracy of the RUL estimate.

By integrating historical data and addressing missing data, the research advances the field of RUL estimation. It provides a more robust and reliable method for predicting the remaining service life of complex systems. This approach has the potential for practical applications in various engineering fields where accurate RUL prediction is essential to ensure system reliability and performance.

In [29], RUL prediction for control systems faces challenges due to increasing uncertainty in the operational process, limited availability of real-time observational data, and noise during signal acquisition. Current research on RUL prediction techniques highlights the need for innovative approaches to address these difficulties. The proposed hybrid multistage methodology using unscented Kalman filter (UKF) and dynamic Bayesian networks (DBN) is a novel solution for RUL analysis in nonlinear degenerate systems. The integration of UKF and DBN enables uncertainty analysis during the prediction process, improving accuracy and robustness.

In the initial prediction stage, dynamic models of unscented Kalman filters are used to calculate random disturbances and process noise distributions, adjust the degree of system degradation, and obtain operational data. A circular iteration is then used to optimize the degradation process, leading to the covariance and optimal estimate calculations. In addition, the methodology simulates the actual degradation process to compensate for the lack of accurate measured data.

Their proposed approach shows promising potential for increasing the accuracy of RUL prediction for control systems in complex environments.

Eclipse MOSAIC, formerly V2X Simulation Runtime Infrastructure (VSimRTI), is an open-source, multi-scale, multi-domain simulation framework for evaluating new solutions for connected and automated mobility. The main goal of Eclipse MOSAIC is to give users the flexibility to perform various V2X simulations with their own choice of simulators. To guarantee this, Eclipse MOSAIC combines different simulators for a more realistic presentation of vehicle operation, emissions, and wireless communication [30]. One is a simulation program that was specially created for DTN. It offers a simulation environment for wireless networks like VANET, MANET, and others. ONE offers many movement models and routing architectures. Their simple functions can simulate a theme according to the user's specifications. It can quickly develop additional movement models and routing schemes.

Additionally, it can create and simulate various security attacks and their countermeasures. Eclipse is a Java-based tool that is also used for programming. Configuring 32 one simulator with Eclipse facilitates the writing of multiple routing schemes and movement models because Eclipse has some built-in Java programming methods. ONE simulator is based on Java, intended for research on delay-tolerant networks (DTNs). The ONE simulator has been developed in the SINDTN and CATDTN projects supported by Nokia Research Center (Finland). Users have the option to create information from their simulations using ONE. This simulation environment, implemented in Java, may fully customize and replicate every aspect of node activity, including node movement, connections between nodes, and routing information for every node. The ONE may accept input traces from real-time dimensions to simulate node movement. High modularity is one feature of the ONE architecture. Every movement model and routing protocol has its independent component that gets loaded at runtime on the simulator's parameter settings. New movement models and routing protocols are simple to build in the ONE simulator.

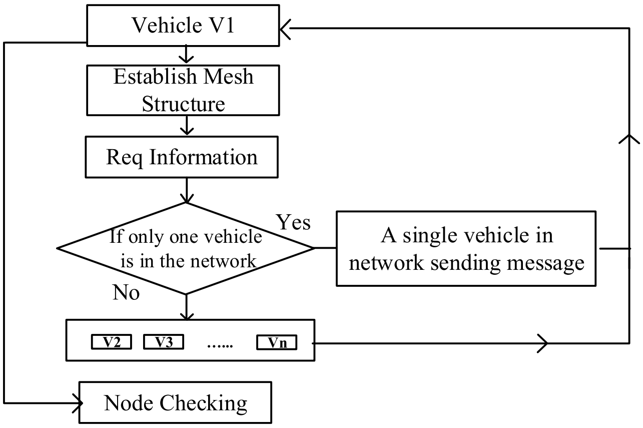

Vehicle V1
Establish Mesh Structure
Req Information
If only one vehicle is in the network
Yes
No
A single vehicle in network sending message
V2
V3
......
Vn
Node Checking

FIGURE 3. Establishing mesh structure.

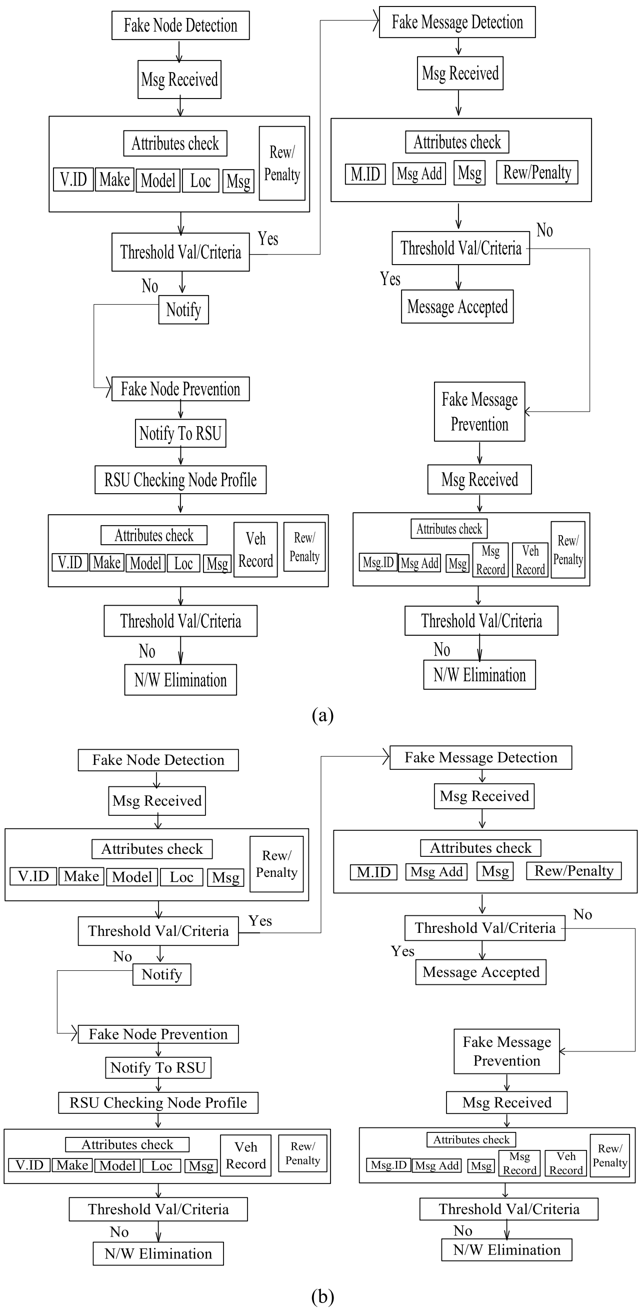
Finally, based on the existing literature, it is worth mentioning the main contribution of our research, which is the development of an approach both for the detection and prevention of fake vehicular nodes and for the detection and prevention of fake messages in VANET. While existing methods usually focus on either fake message detection or fake node detection, this research uniquely addresses both aspects to increase the overall security and reliability of VANET.

The main issues addressed in this area are the growing vulnerabilities of VANETs to malicious activities such as disinformation and unauthorized access. Fake nodes and messages can significantly compromise the safety and efficiency of vehicle communication systems, leading to potential accidents and disrupting traffic flow. Existing solutions often lack a holistic approach to address node and message authenticity simultaneously.

The research motivation stems from the critical need to protect VANETs from security threats. With the rapid development of vehicle communication technologies, VANETs have become a vital part of enabling intelligent transportation systems. However, the open nature of VANETs makes them vulnerable to attack, compromising their potential benefits. By introducing an integrated approach to detect and prevent fake nodes and messages, this research aims to increase the trustworthiness and reliability of in-vehicle communication, making VANETs safer and more efficient for real-world deployments.

III. MATERIAL AND METHODS

The relationship between base stations and sensors is of utmost importance. Base stations act as central hubs that collect and process data from various sensors in the network. Data transmission and processing efficiency depend mainly on the correct deployment and management of base stations. We recognize the importance of understanding the interplay between base stations, sensors, efficiency, and cost in the context of VANET nodes. As we focus on detecting and preventing fake nodes and messages, the effectiveness of these components becomes critical. Efficient data transmission and processing through base stations and sensors is essential for



(a)

(b)

FIGURE 4. (a) . Proposed framework for detection and prevention of fake nodes. (b). Proposed framework for detection and prevention of fake messages.

detecting anomalies and ensuring network security. However, optimizing this relationship is necessary to balance system performance and integrity, which is the primary objective of our study. By comprehensively investigating these aspects, we try to contribute valuable knowledge to increase the safety and reliability of VANET.

A. DETECTING AND PREVENTING FALSE NODES AND MESSAGES

This research also examines the possibilities of solving security and authentication problems of vehicular nodes and messages. The proposed system will help increase the efficiency of the existing system. In the proposed method, we tried to solve the network's frequent disconnection problem while ensuring the reliability of the vehicular node by checking it at different levels. A suitable checking method ensures that only authentic nodes and messages travel across the network. This may help save time and life and save the driver from another mishap.

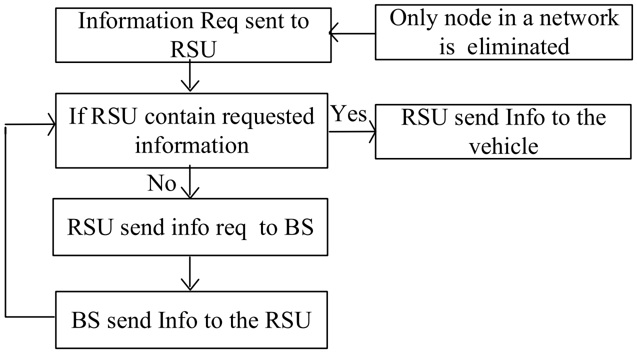

Information Req sent to RSU
Only node in a network is eliminated
If RSU contain requested information
Yes
RSU send Info to the vehicle
No
RSU send info req to BS
BS send Info to the RSU

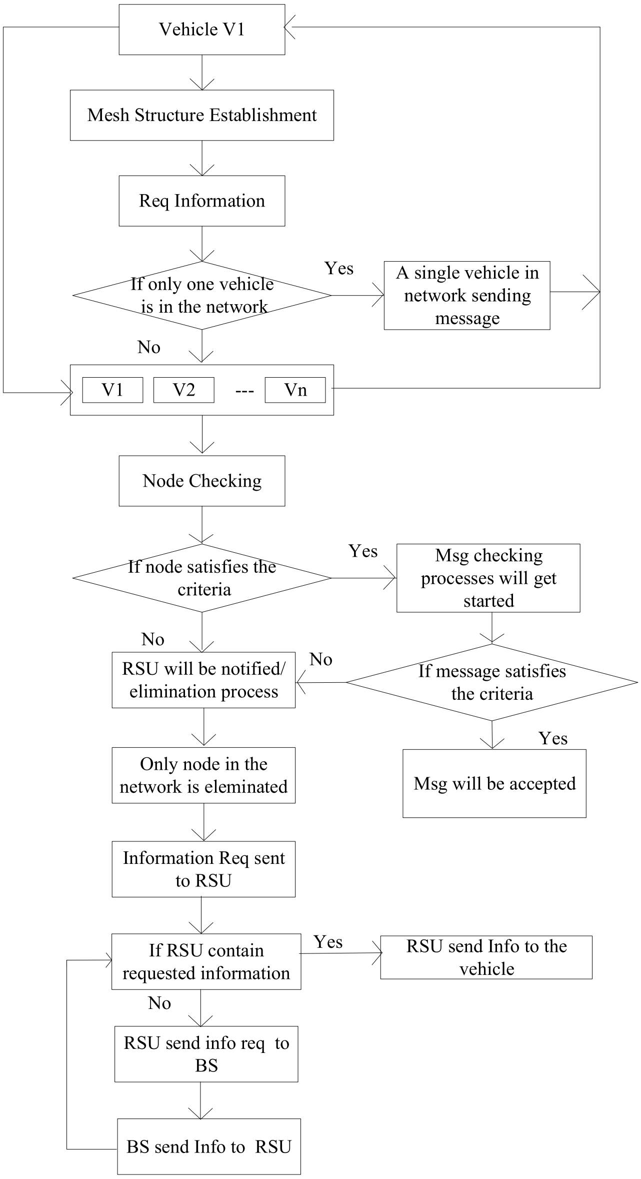
FIGURE 5. Communication structure of roadside unit (RSU) and base station (BS).

Also, a mesh structure is established in our proposed work to avoid frequent link disconnection problems. There is a condition after requesting for message request. It is possible that there is only one vehicle in the network, and another requirement is the number of vehicles in the network that have to respond. In both conditions, node-checking and the message-checking process will be performed. Figure 3 represents establishing the mesh structure, which refers to Algorithm 1.

The research introduced the detection and prevention of fake vehicular nodes and messages. For this, we use the vehicular profile method. The vehicular node's profile attributes are defined, such as vehicle id, vehicle make, vehicle model, vehicle Location, and message reward/penalty. Vehicle id identifies the vehicle that has sent the message to the requested vehicle, and the vehicle makes and model help to recognize the vehicle. Vehicle location informs about the location where the message-sending vehicle is. Message rewards/penalties are the markings assigned for their previous performance. If the vehicle sends a message discovered as fake, it will assign (-1).

On the other hand, if it sends a genuine message, it will be rewarded (+1). After receiving more penalties, the vehicle will not be able to meet the criteria after reaching the threshold value. In this case, the vehicle will be declared as a fake node. The graphical representation of the entire process is shown in Figure 4(a) and is related to Algorithm 2.

The message-checking process starts after the vehicle detection, as shown in Figure 4(b). Message attributes like message id, address, message, and reward/penalty are checked for message checking. Message-id helps to identify the message. Message address helps in finding the route of the message. Due to the mesh structure, forwarding the message to the requested vehicle received from a different vehicle is


Vehicle V1
Mesh Structure Establishment
Req Information
If only one vehicle is in the network
Yes
A single vehicle in network sending message
No
V1
V2

Vn
Node Checking
If node satisfies the criteria
Yes
Msg checking processes will get started
No
RSU will be notified/ elimination process
No
If message satisfies the criteria
Yes
Only node in the network is eleminated
Msg will be accepted
Information Req sent to RSU
If RSU contain requested information
Yes
RSU send Info to the vehicle
No
RSU send info req to BS
BS send Info to RSU

FIGURE 6. **Proposed flowchart for detection and prevention of fake nodes and messages.**

possible. The message attribute contains a message itself, and the reward/penalty will be the accountability of the message. Grading is done according to the accuracy of a message. Message profile containing rewards and penalty attributes detects and eliminates fake messages. The message profile checks if the message is received from a node. According to the proposed approach, if the reward and penalty (Rew/Pen) attribute of the profile satisfies the condition, the attribute value must be greater than or equal to a threshold value that is defined as 0, the message will be accepted, if not the message will be eliminated.

Fake node detection refers to algorithm 2, and fake message detection controls algorithm 3. In the node detection process, RSU is notified for the elimination process if the node is detected. Otherwise, the message detection process starts. Figure 4(b) provides a graphical representation of the entire procedure and is associated with Algorithm 2.

On the other hand, if the only node in the network is eliminated, then the information request is sent to RSU. If RSU contains requested information, it sends it to the vehicle. Otherwise, RSU notifies the Base Station. Base Station sends the info to RSU, and RSU forwards it to the vehicle, as shown in Figure 5.

Figure 6 shows the overall proposed flowchart for detecting and preventing fake nodes and messages.

Algorithm 1 Establishment of Mesh Structure

```
Input: I, V= {V1, V2, V3,.….,Vn}, MEsh.
Output: MeshStructure
Steps
    1. RSU registers all vehicles in the network.
    2. 5 numbers will be assigned to each Vehicle
    3. A head node will be selected (Randomly).
    4. RSU shares the node's previous record with the
    5. A new vehicle came into network.
    6. RSU sends the information to new head node
           about all the vehicles in the network.
```

B. PROPOSED ALGORITHMS

Our proposed algorithms will help to explain our proposed work. We have divided these algorithms into three parts. The first part, Algorithm 1, shows establishing a mesh structure in the network after initializing and connecting the nodes. Algorithm 2 explains the fake node's detection and prevention process. After executing Algorithm 2, if the system cannot find the fake node, it calls Algorithm 3 to detect and prevent the fake message.

1) PROPOSED ALGORITHM 1: ESTABLISHMENT OF MESH STRUCTURE

Proposed Algorithm 1 starts its work by establishing a mesh structure. All the nodes in the network connect directly or indirectly to all other nodes. After process initialization, indicated as I, vehicles in the network are defined, and thus mesh structure is established. The mesh structure helps overcome the frequent network disconnection problem that may cause delay and waste of time and useful information. It also maintains full-time connections between the vehicles.

In the first iteration of Algorithm 1, all the vehicles in the network are registered, and the RSU performs this registration process. Numbers are assigned to each vehicle in the network, i.e., 5. This increase and decreases (+1 and -1) according to a vehicle's performance. Penalties and rewards are assigned accordingly. A head node is selected randomly, and later, head node selection is based on node performance. The node with the highest Rew/Pen value is selected as the head node. The head node contains all the previous records of the vehicles and is directly connected to the RSU.

Algorithm 2 Resource Matching on MCC Server

```
1.  $V_1 \leftarrow req$
2.  If
      $V == 1$
      Go to line # 14
3.  $V_1 = \{V_1, V_2, V\ 3 \ldots..V_n\}$
4.  $M_R$
5.  Node Checking
6.  $A_t$={V.Id, Make, Model, Loc, Msg,
      Rew/Penalty}
7.  If $Rew/Pen => T_v$
        Go to Algo #3
8.  Else
      $RSU \leftarrow notify$
9.  $P_c \leftarrow RSU$
10.  $A_t \leftarrow RSU$
11.  $P_R \leftarrow RSU$
12.  If $Rew/Pen < T_v$
13.  If the only node in the network is eliminated.
14.  $RSU \leftarrow Info\ req$
15.  If RSU hase the requested information.
16.  Then
        $V_1 \leftarrow RSU$
17.  Else
        $BS \leftarrow RSU\ info\ req$
18.  $RSU \leftarrow BS$
19.  $RSU \leftarrow BS$
```

2) PROPOSED ALGORITHM 2: FAKE NODES DETECTION AND PREVENTION

Proposed Algorithm 2 shows the detection and prevention process of fake nodes in the network. Profile and previous record distinguish between fake node and genuine node. If the Rew/Pen attribute cannot satisfy the criteria and is declared as a fake node, then the alert notification is sent to RSU. The RSU checks the vehicle's previous record and behavior. In case of dissatisfaction, the node will be eliminated. On the other hand, if the node checking process online, number 7 satisfies the condition, then the control goes to algorithm number 3 for message detection and prevention. We assume the node may not be fake, but the message can be.

The main steps inside Algorithm 2 are:

1. Message request broadcasted by V1
2. If there is only one vehicle in the network
3. V1 is responded to by other vehicles in the network
4. Message received
5. Fake Node detection process
6. Node attributes check
7. If the reward/penalty is more significant than a threshold value
8. RSU will be notified
9. RSU will check the node profile
10. (Pc = profile check)
11. Attribute Check
12. Previous Record Check
13. The node will be Eliminated
14. Information request sent to RS
15. RSU will send the requested information to the vehicle.
16. RSU will send an information request to the base station (BS)
17. BS will send the requested information to RSU
18. BS will send the requested information to RSU

Algorithm 3 Fake Message Detection and Prevention

```
1.  Msg received ()
2.  $M.A_t = \{M.Id, M.add, Msg, Rew/Penalty\}$
3.  If $Rew/Penalty \Rightarrow T_v$
4.  Message Accepted
5.  Else
6.      $RSU \leftarrow notify$
7.  $M_p \longleftarrow RSU\ check$
8.  $M.A_t \leftarrow RSU\ check$
9.  $P_R \leftarrow RSU\ check$
10.  If $Rew/Pen < T_v$
11.  Msgeliminated ()
```

3) PROPOSED ALGORITHM 3: FAKE MESSAGE DETECTION AND PREVENTION

Proposed Algorithm 3 shows the detection and prevention process of fake messages in the network. Profile and previous records distinguish between fake messages and genuine messages. If the Rew/Pen attribute cannot satisfy the criteria and is declared a fake message, then the alert notification is sent to RSU. The RSU checks the message's previous record and behavior. In case of dissatisfaction, the message is eliminated.

The main steps of Algorithm 3 are.

1. Message Received refers to when the intended recipient or receiver successfully receives a message. It implies that the message has been transmitted from the sender to the receiver and has reached its destination.
2. Message Attribute Check: After receiving a message, the recipient performs a message attribute check. This involves examining the various attributes or characteristics associated with the message. These attributes can include the message type, source, destination, timestamp, priority, or other relevant metadata. The purpose of this check is to assess the nature and context of the message.
3. If Rew/Pen is greater than the threshold value: Upon conducting the attribute check, the recipient evaluates a specific attribute called "Rew/Pen" (Reward/Penalty). If this attribute's value exceeds a predetermined threshold value, it signifies that the message carries a high reward or penalty. The exact meaning and implication of the reward or penalty would depend on the specific context or system in which this process occurs.
4. RSU will be notified: If the value of the Rew/Pen attribute exceeds the threshold, the recipient, often

referred to as RSU (Roadside Unit), will be notified. This means that the RSU, typically a device or unit stationed alongside a road or in a vehicular communication network, will be informed or alerted about the message with a significant reward or penalty.

5. Message Profile Check by RSU: Upon receiving the notification, the RSU performs a message profile check. This involves examining the overall profile or characteristics of the message. It includes analyzing factors such as message content, the sender's reputation, historical data, or any other relevant information to understand the message's context and significance better.
6. Message Attribute Check by RSU: In addition to the profile check, the RSU also conducts a message attribute check similar to the one mentioned earlier. This step helps the RSU further assess the characteristics associated with the message, such as its type, source, destination, priority, or other metadata, to make more informed decisions.
7. Previous Record Check by RSU: As part of the evaluation process, the RSU examines the previous records or historical data related to the message or the sender. This check involves reviewing relevant information stored in a database or memory that could provide insights into the sender's behavior, past interactions, or other relevant patterns or trends.
8. If Rew/Pen is smaller than the threshold value, the RSU evaluates the Rew/Pen attribute value following the attribute checks and record examination. If the value is smaller than the predefined threshold value, it suggests that the message carries a relatively low reward or penalty. Again, the exact interpretation and consequences of the reward or penalty depend on the specific system or context.
9. Message Elimination: If the Rew/Pen attribute value is below the threshold, the RSU eliminates or discards the message. This means that the message is considered less significant or does not meet the criteria for further processing. Therefore, it is not acted upon or forwarded to subsequent stages in the system. The elimination of the message implies that it is disregarded or ignored for further action.

C. COMPARISON

Comparison of the existing models helps us to differentiate our work from others. The model proposed in [16] supports the node authentication process. It helps to detect fake node detection and eliminate it. But it does not support message authentication. The model [17] uses an Identifier-Based Signature mechanism to guarantee vehicle authentication. One of the main problems in a cryptosystem is distributing the secret key over a dangerous network. An ID-based signature is used to authenticate the user. In [17], it has a trusted third party (PKG) that generates a key pair (Public/Private) for each user once when the users join the network. The public key is publicly known to everyone, and the private key is known only to the owner and the PKG. Thus, the private keys of all users are stored in the PKG. Consequently, with users, the PKG private key can impersonate another user. This is known as the key Escrow problem. Creating an ID-based key exchange scheme without key escrow issues is an open problem. In [18], a way to increase security in the VANET environment and to assess the effectiveness of the proposed On Demand Multi-Cast Routing Protocol (ODMRP) was presented. The proposed system has implemented encryption key management systems for VANET based on RSA and AES. It supports message authentication, but it creates an escrow problem. In [19], the NTRU cryptosystem was patented by NTRU Cryptosystems. In their proposed system, NTRU has been used for node authentication and to prevent the network from fake nodes, but it does not support message authentication-related checks. That differentiates and makes our proposed work more advanced. Reference [20] proposed a new privacy-preserving message delivery and authenticity protocol. The protocol used a combination of symmetric and asymmetric cryptographic algorithms. A compelling version of the RSA protocol called CRT-RSA was used for the asymmetric key. AES-128 was used for the symmetric key. This protocol only supports message delivery and authentication. This protocol does not support node authentication. Additionally, the proposed protocol uses symmetric and asymmetric cryptography algorithms. The main disadvantage of symmetric key cryptography is the inherent problem related to the transmission of the key used for encryption and decryption. If these keys are exchanged over an insecure connection, they can be intercepted by malicious third parties, and the Escrow Problem happens again. Table 1 shows the comparison of our proposed approach with the existing literature.

IV. PERFORMANCE EVALUATION

A. SIMULATION

A simulation environment is set up to generate node motion using various motion models [31]. Message routing between nodes with different delay tolerant network (DTN) routing algorithms and types of senders and receivers that visualize mobility and real-time messaging in its graphical user interface.

According to the simulated scenario, we established a network in a particular area. A unique name represents 125 nodes, and each node performs in the network. In this area, fake vehicles and messages will be detected and prevented according to our defined procedure. At the initial stage, all the vehicles in the network are assigned an equal value of five (5). This value increases and decreases according to the performance of a vehicular node and its reliability and is compared to the threshold value. If the node or the message is declared fake, the value will be decreased to (-1). Otherwise, one (1) will be added. The vehicle will broadcast the information request in the network. Vehicles that have the requested information in the network will respond to the request.

TABLE 1. Comparison of the proposed approach with existing literature.

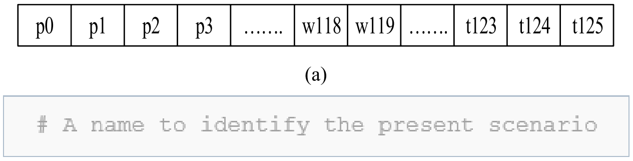
Year	Paper	Description	Approach	Msg Detection	Msg Prevention	Node Detection	Node Prevention
2022	[16]	This research suggests a blockchain-based decentralized authentication system by grouping IoT devices according to their location, computational capacity, and energy reserve. A network of connected blockchains that are organized hierarchically authenticates the devices in each cluster.	Blockchain structure	No	No	Yes	Yes
2021	[17]	This suggested approach adds a new road unit message to the base station, allowing the RSU in charge of authenticating and notifying vehicles of the results of encrypted messages received from them to do so.	ODMRP, RSA, AES	Yes	Yes	No	No
2021	[18]	The Pseudo-ID is used instead of the real vehicle ID. The Identifier-Based Signature (CP-ABE) mechanism for guaranteeing the authentication of vehicles is used for key distribution.	Identifier-Based Signature (CP-ABE) algorithm	No	No	Yes	Yes
2019	[19]	The NTRU algorithm is used for node authentication in opportunistic networks.	NTRU	No	No	Yes	Yes
2021	[20]	The proposed protocol consists of three main phases: the group registration phase, the message sending/receiving phase, and the leaving/joining phase.	CRT-RSA. combined symmetric & asymmetri c key algorithms	Yes	Yes	No	No
2023	Proposed Approach	Proposed fake node and message detection as well as prevention algorithms. After generating a profile for nodes and messages, this algorithm helps detect fake nodes and messages simultaneously.	Fake Nodes and messages detection and prevention algorithm.	Yes	Yes	Yes	Yes

1) SIMULATOR

We are using ONE simulator for this scenario. It is a simulation tool designed for DTN [34], [35], [36], [37]. ONE provides a simulation environment for complete wireless networks such as VANET, MANET, etc. ONE provides various routing schemes and motion models. We used it for fake node and message detection and prevention. We specified 125 nodes in the network, and ONE simulator shows the report of these nodes. The report shows the established connections, ups, and downs of the connections, started message relay, delivered and dropped message report. During simulation, the playfield area can be controlled accordingly.

B. IMPLEMENTATION

We implemented our proposed work on ONE simulator. It is capable of visualizing mobility as well as real-time messaging in its graphical user interface. We used 126 nodes, Helsinki city map world size, with total simulation



p0	pl	p2	p3	....	w118	w119	....	t123	t124	t125

(a)

```
# A name to identify the present scenario
```

(b)

FIGURE 7. **(a) . Created nodes. (b). Created nodes.**

TABLE 2. **Terms and their description in ONE simulator.**

S.No.	Terms	Description
1	Connection Up	The connection has been established between the nodes (Like c68 and p39)
2	Message relay started	Message sending (response to request) between the nodes (c63 and p29) started.
3	Connection down	Connection is terminated between the nodes(like p13 and c45)
4	Message dropped	Message sending from a node is established because it does not satisfy the criteria on the backend.

time 432000 seconds = 5 days, at interface transmission speed 250KBps, covering interface transmission range of 100 meters, message size 250KBs, in the network.

In the experiments performed in this work, DTN routing protocols are analyzed and evaluated using the following terminologies and performance metrics:

- Created messages (CM): the total number of messages created by all nodes during the simulation.
- Relayed messages (RM): the number of messages successfully replayed between nodes.
- Delivered messages (DM): the total number of unique messages successfully received by collection nodes.

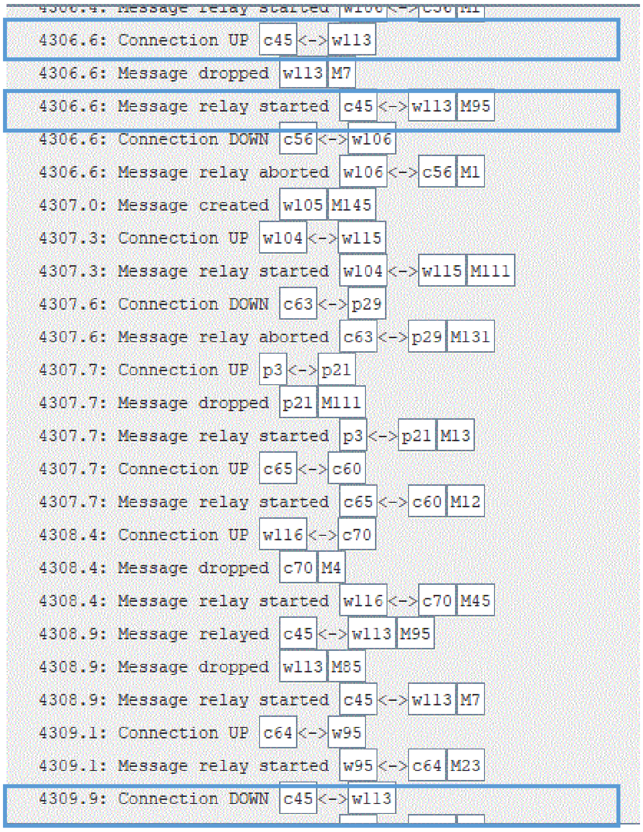
1) NODE CREATION

In the very first stage, the node has been defined. We created 126 nodes to transfer data in the network. Figure 7(a) shows created nodes in the network.

This piece of code in Figure 7(b) defines the number of nodes in the network. Sets are p0 to p39, c40 to c79, w80 to w119, t120 to t125. Node movement speed is 7 m/s, and the transmission speed is 250 KBs. Nodes send information to another node upon request. All nodes with information on a requested location send the information to the requesting node. The message is selected based on their previous record. Message from the node having a high reward value that will satisfy the defined criteria is selected.

2) EVENT LOG CONTROL

The event log control module is used to control the events that need to be performed in the final report. Using this control, we will be able to control all connections that are established in the network during processing. The connection down report will be shown, the message creation and relay starting phase will be reported and delivered, and removed nodes and dropped messages will be listed in the final report.



```
4306.4: Message relay started w106<->c56 M1
4306.6: Connection UP c45<->w113
4306.6: Message dropped w113 M7
4306.6: Message relay started c45<->w113 M95
4306.6: Connection DOWN c56<->w106
4306.6: Message relay aborted w106<->c56 M1
4307.0: Message created w105 M145
4307.3: Connection UP w104<->w115
4307.3: Message relay started w104<->w115 M111
4307.6: Connection DOWN c63<->p29
4307.6: Message relay aborted c63<->p29 M131
4307.7: Connection UP p3<->p21
4307.7: Message dropped p21 M111
4307.7: Message relay started p3<->p21 M13
4307.7: Connection UP c65<->c60
4307.7: Message relay started c65<->c60 M12
4308.4: Connection UP w116<->c70
4308.4: Message dropped c70 M4
4308.4: Message relay started w116<->c70 M45
4308.9: Message relayed c45<->w113 M95
4308.9: Message dropped w113 M85
4308.9: Message relay started c45<->w113 M7
4309.1: Connection UP c64<->w95
4309.1: Message relay started w95<->c64 M23
4309.9: Connection DOWN c45<->w113
```

FIGURE 8. **Fake node detection and prevention.**

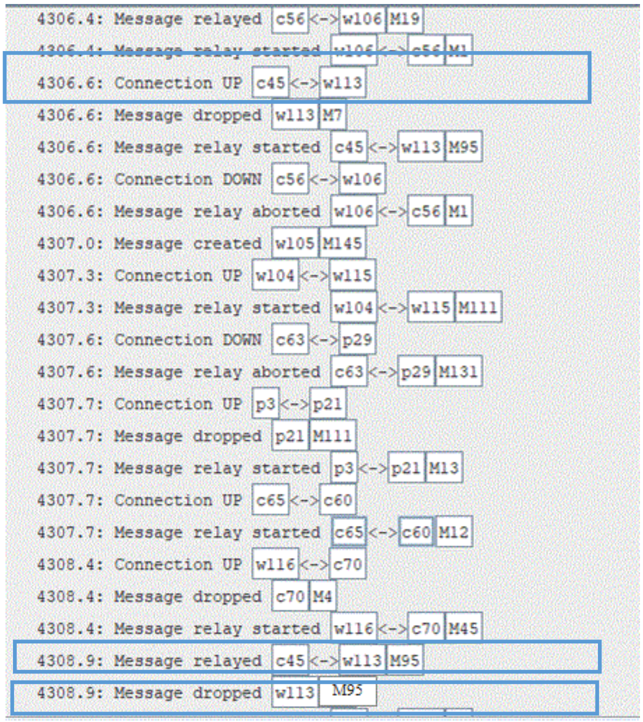
3) EVENT LOG GENERATIONS

After controlling events that need to be executed, the event log generator generates a report after the simulation stops. Eliminated node, message received and sent, dropped message, connection down, and connection established between the nodes are generated in the event log report. Table 2 explains the terms and their description used in ONE simulator.

4) FAKE NODE DETECTION AND PREVENTION

The node detection process identifies the fake node in the network. This may cause damage to human life or to waste time. In the prevention process, the detected node is eliminated from the web. In our proposed protocol, fake nodes are seen by their penalty and reward values assigned by other nodes in the network according to their performance.

We get Figure 8 from algorithm 2, captured from the simulation after the process stopped. It shows the detection and prevention process of a node in the network. The connection has been established between the nodes c45 and w113. The message relay started between node c45 and w113 containing



```
4306.4: Message relayed c56<->w106 M19
4306.4: Message relay started w106<->c56 M1
4306.6: Connection UP c45<->w113
4306.6: Message dropped w113 M7
4306.6: Message relay started c45<->w113 M95
4306.6: Connection DOWN c56<->w106
4306.6: Message relay aborted w106<->c56 M1
4307.0: Message created w105 M145
4307.3: Connection UP w104<->w115
4307.3: Message relay started w104<->w115 M111
4307.6: Connection DOWN c63<->p29
4307.6: Message relay aborted c63<->p29 M131
4307.7: Connection UP p3<->p21
4307.7: Message dropped p21 M111
4307.7: Message relay started p3<->p21 M13
4307.7: Connection UP c65<->c60
4307.7: Message relay started c65<->c60 M12
4308.4: Connection UP w116<->c70
4308.4: Message dropped c70 M4
4308.4: Message relay started w116<->c70 M45
4308.9: Message relayed c45<->w113 M95
4308.9: Message dropped w113 M95
```

FIGURE 9. Fake message detection and prevention.

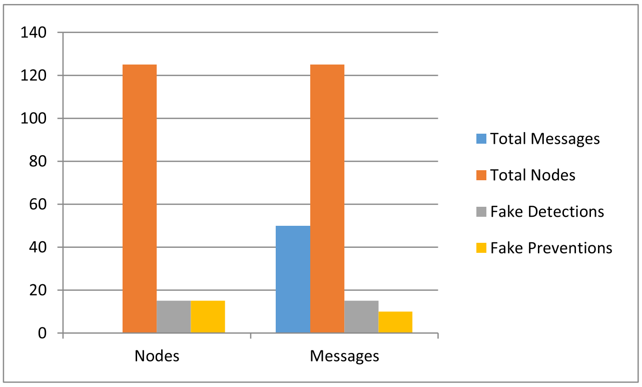


FIGURE 10. The ratio of fake node and message detection and prevention.

message M95. As we set the algorithm, in the node detection process, if the node satisfies the criteria, it is accepted; otherwise, it sends to the elimination process, named the prevention process in our proposed idea. In Figure 8, the connection is down because it did not satisfy the condition, and, therefore, the network between the nodes has been disconnected.

5) FAKE MESSAGE DETECTION AND PREVENTION

A vehicular network, where all the nodes are connected, transfers messages from one node to another. It is possible that the node may not be a fake one, but a message forwarded from the other node can be fake. Our proposed work can detect the fake message from the genuine node. Message profile that contains rewards and penalty attribute helps to detect and eliminate the fake message. The message profile checks if the message is received from a node. According to the proposed approach, if the profile's reward and penalty (Rew/Pen) attribute satisfies the condition, the attribute value must be greater than or equal to the threshold value defined as 0. The message will be accepted. If not, the message will be eliminated.

Figure 9 captures the message detection and prevention process from the simulation by following algorithm 3. Communication between c45 and w113 has been established. After establishing a connection between these two nodes, the message-transferring process is started. At the point where the message M95 relayed started, the fake message detection process also started. According to our proposed algorithm, if the notification satisfies the defined criteria, it will be accepted by the node.

On the other hand, if this message cannot satisfy the criteria, it will be eliminated from the network and called a fake node in the prevention process. After considering the proposed method, in Figure 9, the message M95 with node w113 has been detected, and at 4308sec, the message has been dropped. We can say the prevention process for message M95 has been done.

In Figure 10, the bars represent the ratio of detection and prevention of fake nodes and messages in the network. 125 nodes exist in the network, where 15 are detected as fake nodes and 15 are prevented. 50 messages are communicated in the network, of which 15 are detected as fake and 10 are prevented. It reveals that not all the nodes detected as fake contain fake messages, and not all the nodes detected as genuine contain genuine messages. Genuine nodes may have fake messages forwarded from other nodes in the network.

V. CONCLUSION AND FUTURE WORK

Our research shows progress in detecting and preventing fake nodes and messages in vehicular ad hoc networks, contributing to network trustworthiness and security assessment VANET. We identified the shortcomings of existing solutions and addressed a scenario where a real node may unknowingly forward a fake or malicious message. By implementing a two-step process that checks both the node and the message profile, we achieved positive results in distinguishing between genuine and fake elements within the network. The involvement of the Roadside Unit (RSU) further strengthened the system's ability to respond promptly to potential threats. By using the RSU confirmation process, the network can effectively identify and remove fake nodes and messages, thereby increasing the overall security and trustworthiness of the automotive ad-hoc network. Finally, results obtained from ONE simulator validated our proposed work in detecting and preventing fake nodes and messages in vehicular ad hoc networks.

ACKNOWLEDGMENT

The authors would like to express their grateful to Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R361), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia, in part to the RUDN University Strategic Academic Leadership Program (recipient Abdukodir Khakimov) *(Sadaf Masood and Harun Jamil contributed equally to this work.)*

REFERENCES

[1] S. S. Shah, A. W. Malik, A. U. Rahman, S. Iqbal, and S. U. Khan, ‘‘Time barrier-based emergency message dissemination in vehicular ad-hoc networks,’’ *IEEE Access*, vol. 7, pp. 16494–16503, 2019.

[2] A. Attkan and V. Ranga, ‘‘Cyber-physical security for IoT networks: A comprehensive review on traditional, blockchain and artificial intelligence based key-security,’’ *Complex Intell. Syst.*, vol. 8, no. 4, pp. 3559–3591, Aug. 2022.

[3] H. Sohail, M. U. Hassan, M. A. Elmagzoub, A. Rajab, K. Rajab, A. Ahmed, A. Shaikh, A. Ali, and H. Jamil, ‘‘BBSF: Blockchain-based secure weather forecasting information through routing protocol in VANET,’’ *Sensors*, vol. 23, no. 11, p. 5259, Jun. 2023.

[4] M. U. Hassan, A. A. Al-Awady, A. Ali, M. M. Iqbal, M. Akram, J. Khan, and A. A. AbuOdeh, ‘‘An efficient dynamic decision-based task optimization and scheduling approach for microservice-based cost management in mobile cloud computing applications,’’ *Pervas. Mobile Comput.*, vol. 92, May 2023, Art. no. 101785.

[5] R. Sedar, C. Kalalas, F. Vázquez-Gallego, L. Alonso, and J. Alonso-Zarate, ‘‘A comprehensive survey of V2X cybersecurity mechanisms and future research paths,’’ *IEEE Open J. Commun. Soc.*, vol. 4, pp. 325–391, 2023.

[6] H. Zhai, Y. Wang, X. Zou, Y. Wu, S. Chen, H. Wu, and Y. Zheng, ‘‘Masquerade detection based on temporal convolutional network,’’ in *Proc. IEEE 25th Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, May 2022, pp. 305–310.

[7] O. Ayeni, O. Owolafe, and O. Ogunjobi, ‘‘A security system for detecting denial of service (DDoS) and masquerade attacks on social networks,’’ *J. Inf. Secur. Cybercrimes Res.*, vol. 5, no. 1, pp. 84–90, 2022.

[8] A. Maria, A. S. Rajasekaran, F. Al-Turjman, C. Altrjman, and L. Mostarda, ‘‘BAIV: An efficient blockchain-based anonymous authentication and integrity preservation scheme for secure communication in VANETs,’’ *Electronics*, vol. 11, no. 3, p. 488, Feb. 2022.

[9] T. Li, Z. Wang, L. Zou, B. Chen, and L. Yu, ‘‘A dynamic encryption–decryption scheme for replay attack detection in cyber–physical systems,’’ *Automatica*, vol. 151, May 2023, Art. no. 110926.

[10] R. Sohail, Y. Saeed, A. Ali, R. Alkanhel, H. Jamil, A. Muthanna, and H. Akbar, ‘‘A machine learning-based intelligent vehicular system (IVS) for driver’s diabetes monitoring in vehicular ad-hoc networks (VANETs),’’ *Appl. Sci.*, vol. 13, no. 5, p. 3326, Mar. 2023.

[11] K. Rashid, Y. Saeed, A. Ali, F. Jamil, R. Alkanhel, and A. Muthanna, ‘‘An adaptive real-time malicious node detection framework using machine learning in vehicular ad-hoc networks (VANETs),’’ *Sensors*, vol. 23, no. 5, p. 2594, Feb. 2023.

[12] D. Hasselquist, M. Lindblom, and N. Carlsson, ‘‘Lightweight fingerprint attack and encrypted traffic analysis on news articles,’’ in *Proc. IFIP Netw. Conf. (IFIP Networking)*, Jun. 2022, pp. 1–9.

[13] G. Sharma, A. Kumar, and S. S. Gill, ‘‘Applications of blockchain in automated heavy vehicles: Yesterday, today, and tomorrow,’’ in *Autonomous and Connected Heavy Vehicle Technology*. Amsterdam, The Netherlands: Elsevier, 2022, pp. 81–93.

[14] M. Lee and T. Atkison, ‘‘VANET applications: Past, present, and future,’’ *Veh. Commun.*, vol. 28, Apr. 2021, Art. no. 100310.

[15] S. Kudva, S. Badsha, S. Sengupta, H. La, I. Khalil, and M. Atiquzzaman, ‘‘A scalable blockchain based trust management in VANET routing protocol,’’ *J. Parallel Distrib. Comput.*, vol. 152, pp. 144–156, Jun. 2021.

[16] K. Nazar, Y. Saeed, A. Ali, A. D. Algarni, N. F. Soliman, A. A. Ateya, M. S. A. Muthanna, and F. Jamil, ‘‘Towards intelligent zone-based content pre-caching approach in VANET for congestion control,’’ *Sensors*, vol. 22, no. 23, p. 9157, Nov. 2022.

[17] H. Isyanto, A. S. Arifin, and M. Suryanegara, ‘‘Performance of smart personal assistant applications based on speech recognition technology using IoT-based voice commands,’’ in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2020, pp. 640–645.

[18] J. Liu, W. Yang, J. Zhang, and C. Yang, ‘‘Detecting false messages in vehicular ad hoc networks based on a traffic flow model,’’ *Int. J. Distrib. Sensor Netw.*, vol. 16, no. 2, Feb. 2020, Art. no. 155014772090639.

[19] M. T. Al Ahmed, F. Hashim, S. Jahari Hashim, and A. Abdullah, ‘‘Hierarchical blockchain structure for node authentication in IoT networks,’’ *Egyptian Informat. J.*, vol. 23, no. 2, pp. 345–361, Jul. 2022.

[20] A. Ali, M. M. Iqbal, S. Jabbar, M. N. Asghar, U. Raza, and F. Al-Turjman, ‘‘VABLOCK: A blockchain-based secure communication in V2V network using ICN network support technology,’’ *Microprocessors Microsyst.*, vol. 93, Sep. 2022, Art. no. 104569.

[21] H. Goumidi, S. Harous, Z. Aliouat, and A. M. Gueroui, ‘‘Lightweight secure authentication and key distribution scheme for vehicular cloud computing,’’ *Symmetry*, vol. 13, no. 3, p. 484, Mar. 2021.

[22] S. Ahmad, S. Khan, F. Jamil, F. Qayyum, A. Ali, and D. Kim, ‘‘Design of a general complex problem-solving architecture based on task management and predictive optimization,’’ *Int. J. Distrib. Sensor Netw.*, vol. 18, no. 6, Jun. 2022, Art. no. 155013292211078.

[23] O. Cheikhrouhou, K. Mershad, F. Jamil, R. Mahmud, A. Koubaa, and S. R. Moosavi, ‘‘A lightweight blockchain and fog-enabled secure remote patient monitoring system,’’ *Internet Things*, vol. 22, Jul. 2023, Art. no. 100691.

[24] F. Jamil and I. A. Hameed, ‘‘Toward intelligent open-ended questions evaluation based on predictive optimization,’’ *Expert Syst. Appl.*, vol. 231, Nov. 2023, Art. no. 120640.

[25] P. Sharma, S. Pandey, and S. Jain, ‘‘Implementation of efficient security algorithm and performance improvement through ODMRP protocol in VANET environment,’’ *Wireless Pers. Commun.*, vol. 123, no. 3, pp. 2555–2579, Apr. 2022.

[26] N. Aung, S. Dhelim, L. Chen, A. Lakas, W. Zhang, H. Ning, S. Chaib, and M. T. Kechadi, ‘‘VeSoNet: Traffic-aware content caching for vehicular social networks using deep reinforcement learning,’’ *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 8, pp. 8638–8649, Aug. 2023.

[27] B. Cai, X. Shao, Y. Liu, X. Kong, H. Wang, H. Xu, and W. Ge, ‘‘Remaining useful life estimation of structure systems under the influence of multiple causes: Subsea pipelines as a case study,’’ *IEEE Trans. Ind. Electron.*, vol. 67, no. 7, pp. 5737–5747, Jul. 2020.

[28] B. Cai, H. Fan, X. Shao, Y. Liu, G. Liu, Z. Liu, and R. Ji, ‘‘Remaining useful life re-prediction methodology based on Wiener process: Subsea Christmas tree system as a case study,’’ *Comput. Ind. Eng.*, vol. 151, Jan. 2021, Art. no. 106983.

[29] X. Liu, B. Cai, X. Yuan, X. Shao, Y. Liu, J. A. Khan, H. Fan, Y. Liu, Z. Liu, and G. Liu, ‘‘A hybrid multi-stage methodology for remaining useful life prediction of control system: Subsea Christmas tree as a case study,’’ *Expert Syst. Appl.*, vol. 215, Apr. 2023, Art. no. 119335.

[30] Y. Yu, X. Zeng, X. Xue, and J. Ma, ‘‘LSTM-based intrusion detection system for VANETs: A time series classification approach to false message detection,’’ *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 12, pp. 23906–23918, Dec. 2022.

[31] M. Abouaroek and K. Ahmad, ‘‘Node authentication using NTRU algorithm in opportunistic network,’’ *Scalable Comput., Pract. Exper.*, vol. 20, no. 1, pp. 83–92, Mar. 2019.

[32] T. M. Mohamed, I. Z. Ahmed, and R. A. Sadek, ‘‘Efficient VANET safety message delivery and authenticity with privacy preservation,’’ *PeerJ Comput. Sci.*, vol. 7, p. e519, May 2021.

[33] Q. Ding, J. Wang, X. Zhang, and D. K. Sung, ‘‘Modeling and characterization of the detection and suppression of bogus messages in vehicular ad hoc networks,’’ *IEEE Trans. Mobile Comput.*, early access, Jun. 13, 2022, doi: 10.1109/TMC.2022.3182005.

[34] F. A. Ghaleb, F. Saeed, E. H. Alkhammash, N. S. Alghamdi, and B. A. S. Al-Rimy, ‘‘A fuzzy-based context-aware misbehavior detecting scheme for detecting rogue nodes in vehicular ad hoc network,’’ *Sensors*, vol. 22, no. 7, p. 2810, Apr. 2022.

[35] J. S. Weber, M. Neves, and T. Ferreto, ‘‘VANET simulators: An updated review,’’ *J. Brazilian Comput. Soc.*, vol. 27, no. 1, pp. 1–31, Dec. 2021.

[36] S. Babu and A. Raj Kumar P, ‘‘A comprehensive survey on simulators, emulators, and testbeds for VANETs,’’ *Int. J. Commun. Syst.*, vol. 35, no. 8, May 2022.

[37] E. A. A. Alaoui, S. C. K. Tekouabou, Y. Maleh, and A. Nayyar, ‘‘Towards to intelligent routing for DTN protocols using machine learning techniques,’’ *Simul. Model. Pract. Theory*, vol. 117, May 2022, Art. no. 102475.

SADAF MASOOD received the M.Sc. degree in information technology from the University of the Punjab, Punjab, Pakistan, in 2019. She is currently with The University of Haripur, Haripur, Pakistan. Her research interests include vehicle security planning, intelligent transportation systems, and autonomous vehicle.

YOUSAF SAEED received the Ph.D. degree (Hons.) in cognitive VANETs from NCBA&E, Lahore, Pakistan, and the M.S. degree (Hons.) in broadband and high-speed communication networks from the University of Westminster, London, U.K. His M.S. research thesis on IPv6. He is currently an Assistant Professor with the Department of Information Technology, The University of Haripur, Pakistan. His achievements include the publications of journal articles and conference papers. Moreover, he also has a patent in progress regarding emergency vehicles-based traffic lights control systems. His research interests include vehicular ad-hoc networks, cognitive cars, artificial intelligence, bioinspired algorithms, bioinformatics, and fuzzy modeling. He received the International Students Award from the College of North West London, U.K. He acquired Project of the Prime Minister Scheme of Kamyab Jawan Program from NAVTTC in the domain of artificial intelligence and seven research projects from HEC National Grassroots ICT Research Initiative (NGIRI) Program.

ABID ALI received the M.S. degree in computer science (CS) from the University of Engineering and Technology, Taxila, Pakistan, in 2018, and the Ph.D. degree in CS from the Department of Computer Science, University of Engineering and Technology, Taxila. He is currently serving as a Lecturer with the Department of Computer Science, GANK(S) DC KTS, Haripur. He has eight years of teaching and five years of research experience. His current research interests include the IoT, distributed computing, big data, task scheduling, data mining, cloud and mobile cloud computing, machine learning, AI, and ICN, vehicular ad-hoc networks, and false node detection.

HARUN JAMIL received the B.Sc. degree in electronic engineering from the Capital University of Science and Technology, Islamabad, Pakistan, and the M.S.E.E. degree in electrical engineering from Air University, Islamabad, in 2019. He is currently pursuing the Ph.D. degree with the Department of Electronic Engineering, Jeju National University, Jeju-si, South Korea. His research interests include indoor localization, data fusion techniques, nanogrids, energy optimization, and prediction.

NAGWAN ABDEL SAMEE received the B.S. degree in computer engineering from Ein Shams University, Egypt, in 2000, the M.S. degree in computer engineering and the Ph.D. degree in systems and biomedical engineering from Cairo University, Egypt, in 2008 and 2012, respectively. Since 2013, she has been an Assistant Professor with the Information Technology Department, CCIS, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia. Her research interests include data science, machine learning, bioinformatics, and parallel computing. Her awards and honors include the Takafull Prize (Innovation Project Track), Princess Nourah Award in Innovation, Mastery Award in Predictive Analytics (IBM), Mastery Award in Big Data (IBM), and Mastery Award in Cloud Computing (IBM).

HAYAM ALAMRO received the B.Sc. (Hons.) and M.Sc. degrees in computer science and information systems from King Saud University, Saudi Arabia, and the Ph.D. degree in computer science of information security from King's College London, in 2021. During her time in Kings, she has received two awards for research excellence by the Saudi Arabian Cultural Bureau. Since 2021, She has been working as an Assistant Professor in computer science and information security at the College of Computer Science and Information Systems in Princess Nourah bint Abdulrahman University, Riyadh, Kingdom of Saudi Arabia. Her research interests focuses on analysis and advanced design of string algorithms, approximate pattern matching, bioinformatics, information security, cybersecurity, and data privacy.

MOHAMMED SALEH ALI MUTHANNA received the M.S. degree from the Computer Science Department, Saint Petersburg Electrotechnical University "LETI," Russia, in 2016, and the Ph.D. degree from the Chongqing University of Posts and Telecommunications, Chongqing, China, in 2021. Currently, he is a Postdoctoral Fellow with the Institute of Computer Technologies and Information Security, Southern Federal University, Russia. His research interests include mobile edge computing, software-defined networks (SDN), the IoT, industrial wireless, and sensor networks.

ABDUKODIR KHAKIMOV received the Ph.D. degree from the St. Petersburg University of Telecommunications, in 2022, where he is currently pursuing the Graduate degree. Since 2019, he has been a Junior Researcher with the Institute of Applied Mathematics and Telecommunications, RUDN University. He is engaged in research on access and core technologies for 5G and 5G + networks. In particular, the integration of MEC technology into distributed computing networks.