2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) | 979-8-3503-7024-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICCCNT61001.2024.10725800

A Reliable and Secure Multicast Transport Protocol for Space-ground Integrated Networks using RBAC

1st Madhukrishna Priyadarsini
Department of CSE
NIT Raipur
Raipur, India
mpriyadarsini.cse@nitrr.ac.in

2nd Abdullah Al Noman
Department of CSE
NIT Tiruchirappalli
Tiruchirappalli, India
106120003@nitt.edu

3rd Vipul Patel
Department of CSE
NIT Tiruchirappalli
Tiruchirappalli, India
106120142@nitt.edu

4th Subham Prakash
Department of CSE
NIT Tiruchirappalli
Tiruchirappalli, India
106120117@nitt.edu

***Abstract*—A space-ground integrated network combines space-based and ground-based components to facilitate communication, data transmission, and other functions related to space missions or satellite operations. The requirement of the space-ground integrated network in satellite communication, remote sensing, navigation, earth observation, and space exploration is essential. These networks often involve complex infrastructure and protocols to ensure reliable and efficient communication across vast distances and varying environmental conditions. They play a crucial role in modern space operations, enabling everything from telecommunications to scientific research to national security activities. Multi-cast transport protocols possess reliability and security loopholes during data transmission among the space and ground networks. This research proposes a reliable and secure multicast transport protocol for the space-ground integrated network using the role-based access mechanism (RBAC). The space and ground networks are communicating with each other through an intermediary. The role of each device in both networks is defined, and any deviation in the role creates an alarm to detect the anomaly in the network, thus making the existing protocol secure. In addition, during the intermediary's failure between both networks, one backup intermediary is activated to make the protocol reliable. The experimental results provide sufficient evidence for our claim in terms of network performance parameters: throughput (13.5 Mbps), PDR (0.004%), transmission delay (0.003%), and execution time of the protocol (30s). The results also show that the proposed method provides a higher anomaly detection rate with a lower error rate.**

***Index Terms*—RBAC, Clustering, Leader Election, Reliability, Security, Multicast Protocol.**

I. Introduction

Space-ground integrated networks are dynamic networks that consist of satellites for communication and navigation; vehicular ad-hoc networks (VANETs), and ground-based wired and wireless networks. Integrating vehicular ad-hoc networks (VANETs) into space-ground integrated networks presents a unique convergence of terrestrial and extraterrestrial communication technologies, promising transformative advancements in transportation and remote sensing applications. However, this integration poses challenges in effectively managing communication flows between ground vehicles and satellites, leading to fatal accidents. Thus, it is essential to create secure and reliable communication between the vehicles, the satellites, and the roadside units (RSUs). Multicast routing protocols play a vital role in creating secure and reliable communications. In the literature, many technologies are proposed for the same; however, every technology lacks integration of both the security and reliability parts, considering the constraints of the space-ground integrated network. Research work in [1], [2], [3], [4], and [10] introduced reliability technologies, and research works in [6], [7], and [8] proposed security mechanisms for the space-ground integrated networks. Other research works in [11], [12], and [13] analyzed the existing methods of multicast technologies in space-ground networks and presented their findings regarding those. After analyzing the shortcomings of the literature, we realized that it is necessary to integrate both security and reliability for the multicast protocol for the space-ground integrated network, which in turn will reduce fatal accidents.

We present a safe and reliable multicast transport protocol designed for managing devices (vehicles and RSUs) in satellite networks. This protocol is meant to solve these problems by adapting automatically to changing network conditions, making the best use of resources, and ensuring that data is sent reliably. Through rigorous analysis and simulation-based evaluation, this research endeavors to enhance the efficiency and scalability of integrated communication systems, paving the way for innovative solutions in the digital age. We have introduced a role-based access (RBAC) mechanism which provides dynamic security to the devices. To ensure the reliability of the protocol, we have proposed a cluster creation mechanism for the vehicles, followed by cluster head election to interact with the RSUs and the satellites, and intermediary cluster head activation in case of failure of the original cluster head. The experimental section shows the attack detection, performance evaluation results, and comparison with methodologies. The major contributions of our proposed protocol are highlighted as follows:

1) We create clusters of vehicles considering their speed, size, and direction of movement using the K-Means clustering approach.
2) We introduce a dynamic cluster head election process that provides a weighted score to each vehicle, and the highest weighted score is elected as the new cluster head. This procedure repeats over a particular interval of time.
3) In case of failure of the cluster head, another intermediary cluster head is immediately assigned with the

second-highest weighted score. This, in turn, provides reliability for the protocol.

4) For security, we propose a role-based access (RBAC) mechanism for role calculation and finding the deviation in each role. If the deviated role value is greater than the predefined threshold, then it is termed a potential attack on the space-ground integrated network.
5) The experimental analysis section claims the increase in network performance enhancement in terms of throughput (13.5 Mbps), PDR (0.004%), transmission delay (0.003%), and execution time of the protocol (30s). It also provides proof of the highest attack detection rate as compared to the existing methods.

The rest of the paper is organized as follows: Section II discusses the comprehensive review of the related works in multicast routing protocols for the space-ground integrated network. Section III describes the motivation and objective of our proposed methodology. The proposed reliable and secure multicast protocol is presented in Section IV. Section V describes the (I) experimental setup, (II) evaluation metrics in terms of detection, performance, accuracy verification, and (III) comparison with existing solutions. Finally, in Section VI, we summarize our contributions and potential future research directions.

II. Related Work

Various reliability and security mechanisms were proposed in the literature separately for space-ground integrated networks. The crucial contributions are emphasized in this section.

Lv et al. (2018) [1] designed a reliable multicast transport protocol for device management that contains 2 key ideas, including acknowledgment aggregation and local error recovery. Future efforts will concentrate on proxy node election and optimization in the localized state to improve universality. Junejo et al. (2023) [2] talked about a two-part high-reliability grouping-based communications trust model for VANETs. The dynamic group head selection (DGHS) scheme improves the group head's (GH) stability, and a hybrid dynamic trust model (DTM) scheme enhances trustworthiness. In modeling VANETs with attacks, the research can be extended to take into account dynamic group creation, group members leaving a group, and other variables. To evaluate the dataset, other machine learning techniques might be trained on it. Kalinin et al. (2018) [3] discussed the work of designing a hierarchy of objects and roles for role-based access control on VANET to improve access control and enhance data confidentiality. The RBAC traffic isolation mechanism needs to be added, which groups various data flows with multiple properties into a single logical network.

Han et al. (2015) [4] concentrated on enhancing the BGP routing transport's dependability and lowering the number of retransmissions brought on by packet loss. It is suggested that NCSR (Network Coding for Satellite Network BGP Routing Transport) be used to add network coding to the Hub-Spoke and LRMTP mechanisms used for multicast BGP transport in the GEO satellite network. KMRP is a new routing protocol for VANET that was created by Kandali et al. (2021) [5]. It combines the K-Means clustering method with the continuous hopfield network's solution to the maximum stable set problem. This protocol uses a clustering-based topology to determine the best path for data transmission between vehicles. The effectiveness of the proposed method is evaluated with special attention to how dependent it is on dynamic cluster size adjustments and the choice of a suitable number of cluster heads (CH). Sohail et al. (2023) [6] looked at the routing protocols for VANETs and put them into groups based on their functions, features, uses, and network structure. It offers a systematic classification and taxonomy of these protocols based on a range of performance metrics. New approaches should be needed to address emerging challenges while being more efficient and robust. Phillips et al. (2019) [7] proposed an in-depth access control system that draws inspiration from the dual-level key management (DLKM) plan. The proposed approach combines several approaches to enhance an RBAC model with encryption and privacy-preservation features. The time complexity of the proposed model is high. Niu et al. (2020) [8] proposed a SAGiven to enable automated, networked, and intelligent transportation systems in the future. An SFC-based network function virtualization and network resource reconfiguration technology has been presented to smoothly combine multidimensional and multiscale context information with network resources. Additionally, a bi-directional offloading (BDO) scheme has been suggested to make the best use of network resources in space and the air. Lu et al. (2023) [9] analyzed the most recent UAV network communication architecture under SAGINs as well as the relevant FANET routing protocols. Furthermore, a study of the most recent FANET routing algorithms has been carried out, along with an evaluation of the drawbacks of the current routing algorithms and a discussion and analysis of the optimization strategies for each approach. It is important to have a routing algorithm that works well with space-based networks and can handle the changing nature, limited resources, and safety concerns of flying ad-hoc networks (FANETs) in space-air-ground integrated networks (SAGINs).

Kumar et al. (2022) [10] suggested choosing a cluster head and an alternate cluster head to keep the cluster head from failing. They also suggested finding the best path between the cluster head and a member node based on the node's energy and reliability pair factor, as well as setting up a path based on the nodes' maximum energy and minimum number of hops. All of this was done using optimal route selection (ORS). This protocol could be tested in a variety of network topologies and conditions. This would allow for an evaluation of cluster-based protocol performance taking into account things like node mobility, traffic patterns, and transmission ranges. Raj et al. (2022) [11] looked at different non-metaheuristic and metaheuristic strategies for cluster head selection and cluster formation that are used in networks in a range of environmental conditions to get a better idea of how these problems are solved. A brief performance review of the approaches is also provided, along with information on

TABLE I
COMPARISON OF PROPOSED MULTICAST PROTOCOL WITH STATE-OF-THE-ART SOLUTIONS

Author(s)	**Methodology**	**Drawbacks**
Lv et al. [1]	looked at the newest UAV network communication architecture in the context of SAGINs, focusing on combining Flying Ad-Hoc Networks (FANETs) and the right routing protocols. Also investigated recent advancements in FANET routing algorithms, assessing their efficacy and identifying limitations. Conducted a thorough evaluation of existing routing algorithms and discussed optimization strategies tailored to each approach.	future efforts will concentrate on proxy node election and optimization in the localized state.
Junejo et al. [2]	developed a high-reliability grouping-based communications trust model for vehicular ad-hoc networks (VANET), dynamic group head selection (DGHS) scheme enhances group head (GH) stability, and dynamic trust model (DTM) scheme augments trustworthiness.	the current research on VANETs that are being attacked does not pay enough attention to dynamic group construction and group member dynamics, which could make the results less useful in real life. Machine learning techniques can be used to evaluate datasets, but relying too much on one method could make it hard to see subtleties in VANET behavior or attack patterns, which could lead to judgments that are not complete or are biased.
Kalinin et al. [3]	designed a hierarchy of objects and roles for role-based access control on VANET to improve access control and enhance data confidentiality.	Designing and implementing a hierarchical structure for role-based access control (RBAC) on VANETs can introduce significant complexity, especially when considering the diverse range of vehicles and roles involved.
Han et al. [4]	improved the reliability of BGP routing transport by reducing the retransmission count by using NCSR.	When analyzing network coding, ignoring cross-layer interaction reduces its practical effectiveness by not taking into consideration implementation difficulties and real-world complexity.
Kandali et al. [5]	developed a new routing protocol (KMRP) for VANET by combining the continuous hopfield network's solution of the maximum stable set problem with the K-means clustering technique.	the potential for frequent dynamic cluster size adjustments and the crucial selection of an appropriate number of cluster heads (CH) to significantly affect the proposed method's effectiveness.
Sohail et al. [6]	classified the routing protocols for VANETs according to their features, areas of application, operating tenets, and network architecture to study them.	the current approaches lack adaptability to emerging challenges, hindering efficiency and robustness.
Phillips et al. [7]	the proposed method make an access control system that is more advanced by combining RBAC with encryption and privacy-protecting methods based on dual-level key management (DLKM).	the algorithm exhibits higher time complexity compared to the alternative.
Niu et al. [8]	proposed SFC-based network function virtualization with network resource reconfiguration, alongside a bi-directional offloading (BDO) scheme, to enable automated, networked, and intelligent transportation systems.	V2X routing in the SAGiven architecture is susceptible to malicious attacks due to its open wireless channel and dynamic network topology, posing a vulnerability to hostile interference.
Lu et al. [9]	analyzed a comprehensive review of literature on UAV network communication architecture within SAGINs and FANET routing protocols. This included analyzing recent routing algorithms, assessing their limitations, and discussing optimization strategies.	designing a routing algorithm for Space-Air-Ground Integrated Networks (SAGINs) must grapple with the intricate balance of managing dynamic environments, resource limitations, and security challenges inherent in Flying Ad-Hoc Networks (FANETs).
Kumar et al. [10]	the proposed methodology involves proposing cluster head and alternate selection mechanisms to prevent failure, followed by generating optimal paths based on node energy-reliability pairs and establishing paths maximizing energy and minimizing hops via optimal route selection (ORS).	testing this protocol across various network setups may expose limitations in cluster-based performance, impacted by factors like node movement, traffic behaviors, and transmission distances.
Raj et al. [11]	presented a comprehensive review of non-metaheuristic and metaheuristic strategies for cluster head (CH) selection and cluster formation in diverse environmental network scenarios. This includes examining the performance of these approaches, analyzing their parameter settings, and assessing their benefits and drawbacks.	the analysis overlooks key performance metrics like delay, latency, and throughput, critical for optimizing application performance.
Stefanovic et al. [12]	categorized multicast routing protocols for V2X networking based on their techniques and strategies, encompassing approaches like source-based, group-based, and hybrid multicast routing.	current VANET multicast routing protocols lack standardized classification, comparative analysis, and evaluation metrics, with a gap in extending research to encompass FANET networks, notably unmanned aerial vehicles (UAVs).
Zhao et al. [13]	proposed that LEACH-M enhances LEACH-based cluster-head selection by optimizing the threshold equation to consider residual energy and network address, ensuring stability and energy efficiency. It dynamically adjusts the cluster-head selection probability based on these factors, leading to a more balanced and resilient cluster structure.	Improving LEACH-M entails optimizing cluster head-to-base station distance, cluster member proximity to heads, and considering previous round energy consumption for enhanced reliability.
proposed model [This Paper]	proposed a reliable and secure multicast protocol using RBAC mechanism and a standby cluster head. It provides high throughput (13.5Mbps), less delay (0.03%), and less PDR (0.04%)	coordinated attacks are not tested.

the method parameter settings, benefits, drawbacks, and future directions. The research lacks focus on addressing the critical aspects of delay, latency, and throughput and the importance of data for application performance. Stefanovic et al. (2023) [12] provided a brief overview and categorization of multicast routing protocols that use various techniques and strategies to accomplish vehicle-to-everything (V2X) networking. AI-based VANET multicast routing protocols do not have enough classification, comparative analysis, or established evaluation metrics. FANET networks also need to be added because unmanned aerial vehicles are becoming more important. Zhao et al. (2018) [13] presented an altered version of the LEACH-based cluster-head selection technique (LEACH-M). LEACH-M may optimize the cluster-head threshold equation by accounting for residual energy and network address, ensuring a generally stable and energy-efficient cluster structure. To optimize LEACH-M and enhance its reliability, consider factors such as the distance between cluster head and base station, proximity of cluster members to their respective cluster heads, and energy consumption in the previous round. Table I summarizes state-of-the-art solution methodology and research gaps. It also highlights our proposed reliable and secure multicast protocol in this paper.

III. Motivation and Objective

Strong and reliable communication protocols are more important than ever in an era where space exploration is developing and ground-based networks are being integrated with space technologies. Traditional multicast transport protocols face significant challenges in meeting the stringent reliability requirements of space-ground integrated networks. These challenges include managing varying link conditions, ensuring message delivery within stringent time constraints, and mitigating security threats. Integrating ground-based networks with space systems adds layers of intricacy and demands dependability. The researchers in the literature designed multiple reliable multicast transport protocols for device management, but there were no traditional security measurements. Figure 1 shows one scenario that shows vehicle communication in three clusters: clusters 1, 2, and 3, as well as with the satellite. The vehicles communicate with the satellite and other vehicles through the cluster heads. In this scenario, the attackers can attack the cluster heads and communication protocols to manipulate the complete communication mechanism, and accidents can happen. On the other hand, failure of the cluster heads can create another major issue in the vehicular ad hoc network. Recognizing these obstacles, our research endeavors to pioneer a novel solution: a reliable multicast transport protocol for space-ground integrated networks using role-based access control (RBAC). By harnessing RBAC's power and addressing existing protocol shortcomings, we aim to establish a new standard of reliability and security in communication protocols for space-ground integration.

We aim to design and implement a reliable multicast transport protocol tailored specifically to the unique demands of space-ground integrated networks. We also aim to validate its efficacy through comprehensive performance evaluations and comparisons with existing protocols. We aim to achieve this objective through the following specific goals:

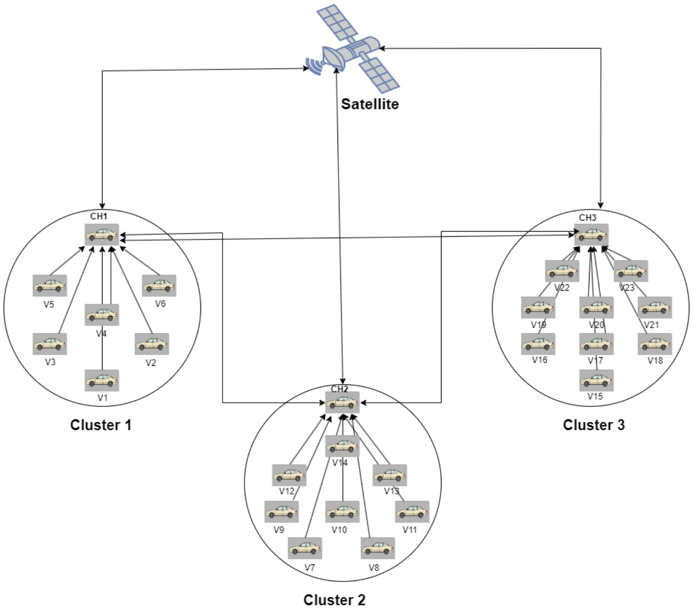

Fig. 1. Real-life scenario describing the importance of security and reliability in space-ground integrated network

- Design an adaptive multicast transport protocol for device management in a space-ground integrated network.
- Address challenges related to control message transmission in satellite networks.
- Facilitate dynamic multicast group formation within the network.
- Improve communication reliability in the space-ground integrated network.
- Enhance efficiency and security in managing devices within the network environment by integrating role-based access control (RBAC) into our protocol design.

IV. Proposed Methodology

This section proposes a reliable and secure multicast transport protocol using the RBAC mechanism for the space-ground integrated network. Here, we present the detailed implementation mechanism of the proposed multicast transport protocol.

A. Cluster formulation using modified K-Means clustering

We used the modified K-Means clustering algorithm for vehicle arrangement according to their speed, size, and direction. A modified K-Means algorithm is employed for dynamic cluster creation and maintenance. This ensures adaptability to changing network conditions. After the cluster is formulated, the cluster head selection is done out of all the vehicles present in the same cluster, and the cluster head selection is dynamic. The complete procedure for cluster head selection is mentioned in the next subsection. The satellites, cluster heads, and vehicles can be presented in a fast-multicast tree structure, which is shown in Figure 2. In this tree, node 1 represents the satellite, nodes 2, 3, and 4 represent the cluster heads, and nodes 5, 6, 7, 8, 9, 10, 11, 12, and 13 represent vehicles of multiple clusters. This tree structure is easy to represent and store, which could fit the frequently changed destinations in device management and evenly save the time used in transmission.

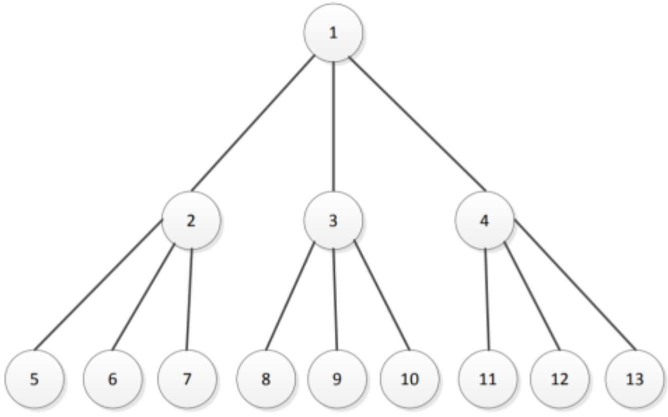

Fig. 2. Fast-multicast tree structure with K=3: Representation of K-Means clustering

B. Dynamic Cluster Head Selection

The cluster head selection process begins by evaluating key attributes such as stability, consistent speed, the direction of movement, time to link, connectivity to neighbors, and distance from the centroid, which are crucial for effective communication within vehicular networks. These attributes are weighted according to their importance, and a composite score is calculated for each vehicle within the cluster. The vehicle with the highest composite score is designated as the cluster head, ensuring it meets predefined thresholds for each attribute. Dynamic updates continuously monitor attribute changes, allowing for reevaluation and potential updates of cluster heads based on real-time conditions.

A fitness value is computed by assessing five critical factors to determine the cluster head. These factors encompass stability, consistency in speed, the direction of movement, the time required for linking, and connectivity with neighboring vehicles.

In this scheme, the fitness value is a weighted sum of the vehicles' (V_i) average speed variation (ASV_i), distance from the centroid (CD_i), time to link the vehicle V_i with the centroid (TTL), the direction of vehicle movement concerning the centroid ($DirV_i$) and the total number of neighbors in a particular range (NV_i). The scheme also calculates the vehicle's average speed variation with other network vehicles to ensure a stable cluster head. ASV_i and TTL are calculated as follows:

$$ASV_i = \frac{1}{n}\sum_{j=0}^{n-1} Vv_i - Vv_j \tag{1}$$

$$TTL = \frac{F(V_i) \ \times \sqrt{(CD_x - V_i x)^2 + (CD_y - V_i y)^2}}{V_i} \tag{2}$$

Here V_i is the speed of vehicle i, CD_x, and CD_y are the x and y coordinates of the centroid, respectively. Vi_x and Vi_y are the coordinate locations of the vehicle i, respectively. $F(V_i)$ is the direction of movement of the vehicle, given by:

$$F(V_i) = \begin{cases} 1; & \text{if } d1 \geq d2 \\ -1; & \text{if } d1 < d2 \end{cases}$$

Where $d1$ is the distance between the centroid and vehicle V_i at a beacon interval t, and $d2$ is the distance between the centroid and vehicle V_i at the next interval $t + 0.1$, $F(V_i)$ is a function whose value is 1 when the vehicle approaches the centroid and -1 when it moves away from the centroid. A vehicle moving away from the centroid has a lower chance of winning the election as it may exit the trust zone. The fitness value $F_(v)$ is determined as follows:

$$F_v = \frac{w_1}{ASV_i} + \frac{w_2}{CD_i} + \frac{w_3}{TL_i} + w_4 \times NV_i + w5 \times DirV_i \tag{3}$$

Here, w_1, w_2, w_3, w_4, and w_5 are weighting factors. In the clustering process, the node with the highest fitness value within a cluster is designated as the cluster head. In addition, the node with the second highest fitness value is assigned as the standby head/intermediary head. The standby head serves as a backup in case the primary cluster head becomes unavailable due to node failure, ensuring the reliability of the cluster network. This means that each cluster will have a primary leader (cluster head) and a backup leader (standby head/intermediary node). The standby head/intermediary node is ready to take over the responsibilities of the cluster head if needed, which helps maintain the stability and reliability of the cluster network, especially in scenarios where the primary head node may fail or become unreachable.

Hierarchical Communication: Each cluster has a designated head (cluster head) responsible for collecting and aggregating information from member nodes within the cluster. This information is then relayed to other cluster heads, facilitating inter-cluster communication. By limiting route discovery packets to communication with cluster heads, our method significantly reduces network overhead compared to traditional approaches.

C. RBAC Mechanism

We propose an enhanced role-based access control (RBAC) mechanism tailored for vehicular ad hoc networks (VANETs) to address the dynamic nature of the space-ground integrated network. According to RBAC, each vehicle is assigned a particular role depending on its characteristics, such as height, weight, direction of movement, position on the road, and communication with the neighboring vehicles. Any of the vehicles try to modify the assigned role, then it will be treated as a malicious activity. Our approach incorporates dynamic parameters such as role magnitude, role weight, and time stamp to improve access control decisions and enhance security and reliability in VANETs.

Role Magnitude Integration: Roles in RBAC are assigned magnitudes to indicate their significance or importance within the network. Higher magnitude roles correspond to critical functions or responsibilities. The incorporation of role magnitude allows for prioritization of access permissions based on the importance of roles within the VANET cluster.

Role Weight Adjustment: Each role is assigned a weight factor reflecting its relative importance or priority compared to other roles. Role weight influences access control decisions, with roles of higher weight having greater authority or access privileges.

Dynamic Time Stamp Utilization: In VANETs, where vehicles are constantly moving and network topology is dynamic, a time stamp is utilized to track the temporal aspect of role assignments and access permissions. Time stamping ensures that access control decisions are based on the most current information, considering the real-time movement of vehicles within the cluster.

RBAC Framework Integration: Our proposed mechanism is integrated into the existing RBAC framework used in VANETs, ensuring compatibility with established access control architectures. The dynamic parameters of role magnitude, role weight, and time stamp are incorporated into the access control decision-making process within the RBAC framework.

The access control decision for a specific role assigned to a user in the VANET cluster is calculated as follows:

$$AccessControlDecision = \frac{(W_i \times M_i) \times TS_i}{RoleAssigned} \quad (4)$$

Where w_i represents the weight of the role assigned to the user, m_i represents the magnitude of the role assigned to the user. TS_i represents the time stamp associated with the access control decision, capturing the dynamic nature of the VANET environment. $RoleAssigned$ denotes the specific role assigned to the user within the VANET cluster. The equation 4 calculates the access control decision based on the weighted combination of role weight, role magnitude, and the time stamp relative to the specific role assigned to the user. Higher values of the access control decision indicate greater access privileges for the user within the VANET cluster.

Integrating enhanced RBAC into a space-ground integrated network provides security in two ways:

- Helps in preventing attacks on the cluster head from the vehicles in the same cluster.
- Helps in preventing attacks on the cluster head and other vehicles from other clusters and outside attackers.

The proposed reliable and secure multicast protocol for space-ground integrated networks is shown in Algorithm 1. The time complexity for cluster formation is $O(n)$, where n is the number of vehicles. The time complexity of cluster head selection is constant or $O(d)$. The time complexity of the RBAC mechanism is $O(nk)$, where n is the number of vehicles and k is the time for access control decisions. Thus, the total time complexity of the proposed protocol is $O(n)$.

V. Experimental Analysis

In this section, we first present the experimental setup before moving on to performance and accuracy analysis.

A. Experimental Setup

The experiments are conducted on a machine with an Intel core i7 10th generation CPU, Nvidia GTX 1080 GPU, and 16 GB RAM. The simulation is set up on the VANET framework within the NS-2 platform, which accurately models how vehicles move and talk to each other while changing the number of nodes (vehicles), clusters, and cluster heads (which are calculated dynamically). We have implemented the proposed modifications, including modified K-means clustering, hierarchical communication, dynamic cluster head selection, and the RBAC mechanism. We have defined metrics for performance evaluation, including average throughput, average packet loss, and end-to-end packet delay. For benchmarking, we compared the proposed method with existing solutions in the literature.

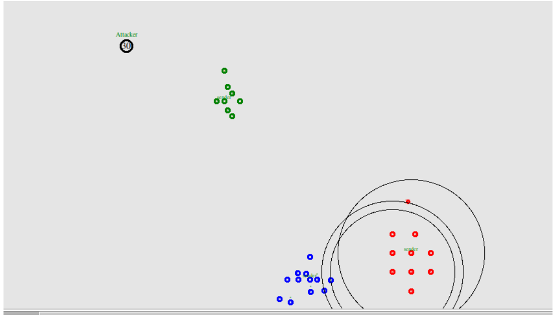

Fig. 3. Setup in NS-2 with multiple clusters and attacker nodes

B. Performance Analysis

We tested how well our proposed multicast transport protocol worked by finding out its throughput, transmission delay, packet drop, and execution time. We did this while taking into account changes in the network, such as node mobility, changing traffic densities, and dynamic topology changes. The simulation was run multiple times, and the throughput, packet drop, and delay values are calculated and presented in Figures 4, 5, and 6, respectively. Here, the simulation results are shown for 30 seconds. The throughput result is approximately 13.5 Mbps, the packet drop is 0.04% of the total number of messages exchanged between the satellite, cluster heads, and vehicles, and the packet delay is 0.03% of the total number of messages exchanged.

We have also compared the execution time of our proposed reliable and secure multicast protocol with the existing state-of-the-art research and the result is shown in Figure 7. The result indicates that our proposed model takes less execution time than the existing research, although it implements both security and reliability mechanisms, which is an advantage and is not present in any of the research work till now.

C. Accuracy Verification

To calculate the accuracy of our proposed model, we considered hundreds of attack samples of each of the attack types (spoofing, tampering, DoS, information disclosure, etc.). The proposed model is regarded as a true positive if it successfully

Algorithm 1 Cluster Formation, Cluster Head Selection, and RBAC Integration

```
Require: Number of Nodes ($n$), Number of Clusters ($k$), RBAC Parameters, Threshold Value
Ensure: Cluster Assignment, Cluster Heads, Access Control Decision
Initialize $k$ random cluster centroids
while not converged do
    for each node $i$ do
        Assign node $i$ to the nearest cluster centroid
    end for
    for each cluster centroid $j$ do
        Update centroid $j$ as the mean of all nodes assigned to it
    end for
end while
Compute Fitness Value for each node within the cluster (Algorithm 2)
Select cluster head based on the highest Fitness Value
Select standby head based on the second-highest Fitness Value
Check RBAC before multicasting:
for each role assigned to a user in the VANET cluster do
    Compute Access Control Decision using RBAC integration
        $$AccessControlDecision = \frac{(W_i \times M_i) \times TS_i}{RoleAssigned}$$
    if Fitness Value > Threshold Value then
        Magnitude $\leftarrow$ 1
        Role Weight $\leftarrow$ assigned weight according to cluster head or cluster member
        Time Stamp $\leftarrow$ current time
    end if
end for
```

identifies one attack; otherwise, it is a false negative. We consider one of the vulnerability indexes as the measure of true negative rate (TNR). TNR represents the proportion of scenarios that are mistaken for attacks. The TNR is described as follows:

$$TNR_{pi} = \frac{d(pi)}{A_i} \tag{5}$$

where A_i is the total attack samples for attack type i, and $d(pi)$ is the total number of incorrect attacks detected for attack type i. The proposed model finds TNRs for six hundred attack samples. Figures 8(a) and 8(b) present the results obtained during these experiments, which are the average TNR and TPR (true positive rates) values. It is observed that, out of the four attack types, tampering provides the highest TNR value of 1.002%.

VI. Conclusion

In this research, we propose a reliable and secure multicast transport protocol for space-ground integrated networks. The reliability of the protocol is ensured through a cluster head and an intermediary node for each cluster, and the security mechanism is designed using the role-based access (RBAC) mechanism. The role of each device, cluster, and network is defined, and any deviation from the defined role creates an alarm to detect anomalies in the space-ground integrated network. In the result analysis, we have shown the comparison of the execution time of our proposed protocol with the state-of-the-art research works. The results also confirm that our proposed approach increases network performance in terms of throughput (13.5 Mbps), PDR (0.004%), the energy con-

Algorithm 2 Fitness Value Computation

```
Require: Attributes: Stability ($w_1$), Speed Consistency ($w_2$), Direction of Movement ($w_3$), Time to Link ($w_4$), Connectivity ($w_5$)
Ensure: Fitness Value for Cluster Heads
Compute Average Speed Variation (ASV$_i$) for each vehicle $i$ within the cluster:
    $$ASV_i = \frac{1}{n}\sum_{j=0}^{n-1}(Vv_i - Vv_j)$$
Calculate Time to Link (TTL) for each vehicle $i$:
    $$TTL = \frac{F(V_i) \times \sqrt{(CD_x - V_i x)^2 + (CD_y - V_i y)^2}}{V_i}$$
Determine Direction Movement (Dir$_i$) for each vehicle $i$:
    $$F(V_i) = \begin{cases} 1; & \text{if } d1 \geq d2 \\ -1; & \text{if } d1 < d2 \end{cases}$$
Compute Fitness Value (F$_v$) for each vehicle $i$:
    $$F_v = \frac{w_1}{ASV_i} + \frac{w_2}{CD_i} + \frac{w_3}{TL_i} + w_4 \times NV_i + w_5 \times Dir_i$$
Select cluster head based on the highest Fitness Value
Select standby head based on the second-highest Fitness Value
```

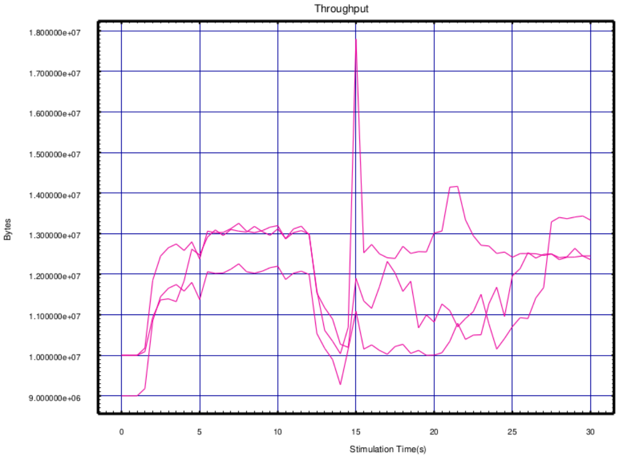

Fig. 4. Average throughput Vs. simulation time

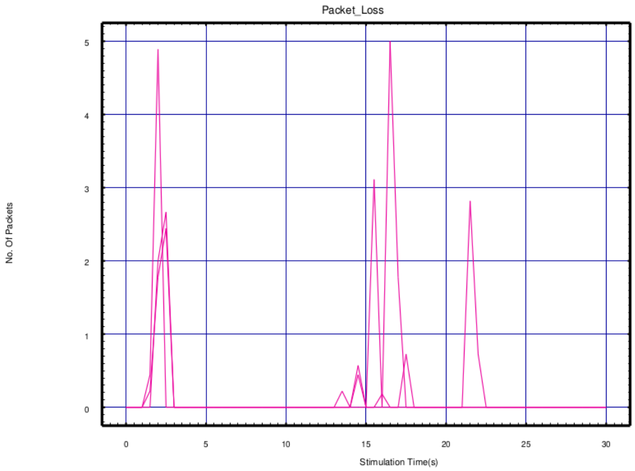

Fig. 5. Average packet loss Vs. simulation time

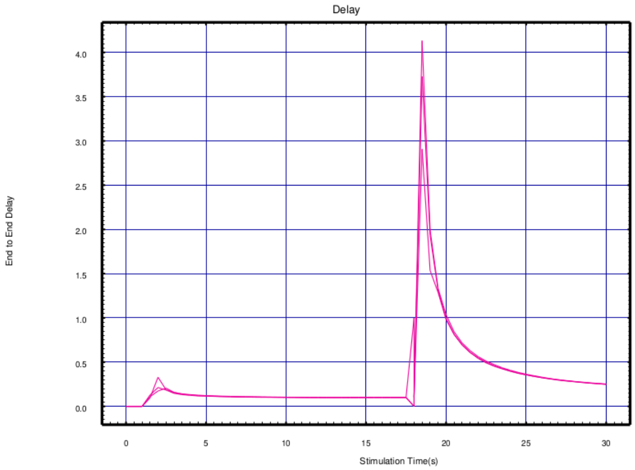

Fig. 6. Number of packet delay Vs. simulation time

sumption of the devices (12–15%), and execution time of the protocol (30s). As the simulation results are prominent, the proposed methodology can be implemented in the real-world satellite communication such as disaster response, commercial, defense and security, aerospace, etc.

One of the future directions of our proposed approach is to detect coordinated attacks by vehicles not present in the clusters.

REFERENCES

[1] M. Lv, F. Li, L. Zhang, K. Geng, and K. He, "A Reliable Multicast Transport Protocol for Device Management in Space-ground Integrated Network", 3rd International Conference on Multimedia Systems and Signal Processing, Pages 104–108, 2018.

[2] M.H. Junijo, AB A.B.Rahman, R. A. Shaikh, K. M. Yusof, S. Sadiah, "Trust Model for Reliable Grouping-Based Communications in Vehicular Ad-Hoc Networks", IEEE Access, Vol. 11, 2023

[3] M. Kalinin, V. Krundyshev, E. Rezedinova, and P. Zegzhda, "Role-based access control for vehicular ad-hoc networks", IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), 2018.

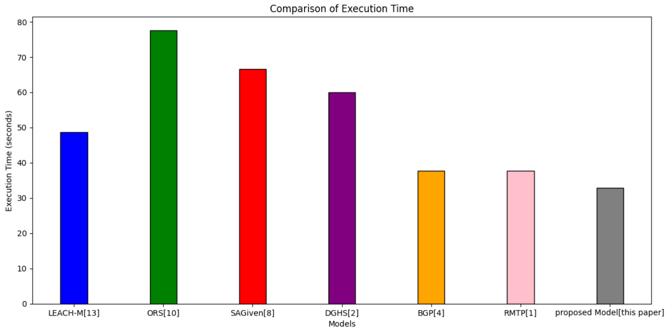

Fig. 7. Comparison of execution time of proposed model with State-of-the-art research

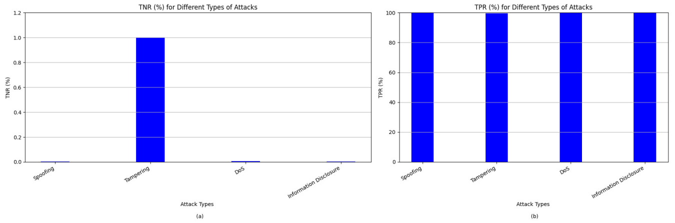

Fig. 8. (a) TNR for different attacks; (b) TPR for different attacks

[4] W. Han, B. Wang, Z. Feng, Z. Tang, B. Zhao, and W. Yu, "NCSR: Multicast Transport of BGP for Geostationary Satellite Network based on Network Coding", IEEE Aerospace Conference, 2015

[5] K. Kandali, L.Bennis, and H. Bennis, "A New Hybrid Routing Protocol Using a Modified K-Means Clustering Algorithm and Continuous Hopfield Network for VANET", IEEE Access, Vol. 09, 2021

[6] M. Sohail, Z. Latif, S. Javed, S. Biswas, S. Ajmal, U. Iqbal, M. Raza, and Abd U.Khan, "Routing protocols in Vehicular ad-hoc networks (VANETs): A comprehensive survey", Internet of Things, ELSEVIER, Vol. 23, 2023.

[7] T. Phillips, X. Yu, B. Haakenson, and X. Zou, "Design and Implementation of Privacy-Preserving, Flexible, and Scalable Role-based Hierarchical Access Control", First IEEE International Conference on Trust, Privacy, and Security in Intelligent Systems and Applications (TPS-ISA), 2019.

[8] Z. Niu, X. S. Shen, Q. Zhang, and Y. Tang, "Space-air-ground integrated vehicular network for connected and automated vehicles: Challenges and solutions", Intelligent and Converged Networks, Vol. 1, Issue 2, 2020.

[9] Y. Lu, W. Wen, K. K. Igorevich, P. Ren, H. Zhang, Y. Duan, H. Zhu, and P. Zhang, "UAV Ad Hoc Network Routing Algorithms in Space-Air-Ground Integrated Networks: Challenges and Directions", Drones, Vol. 7, MDPI, 2023.

[10] R. S. Kumar, P. Manimegalai, P. T. V. Raj, R. Dhanagopal, and A. J. Santhosh, "Cluster Head Selection and Energy Efficient Multicast Routing Protocol-Based Optimal Route Selection for Mobile Ad Hoc Networks", Hindawi Wireless Communications and Mobile Computing, Vol. 20, 2022.

[11] B. Raj, I. Ahmedy, M.Y. I. Idris, and R. Md. Noor, "A Survey on Cluster Head Selection and Cluster Formation Methods in Wireless Sensor Networks", Hindawi Wireless Communications and Mobile Computing, Vol. 2022, 2022

[12] K. Stefanovic, M. Malnar, and N. Jevtic, "Survey of Multicast Routing Protocols in VANET, 31st Telecommunications Forum (TELFOR), 2023

[13] L. Zhao, S. Qu, and Y. Yi, "A modified cluster-head selection algorithm in wireless sensor networks based on LEACH", EURASIP Journal on Wireless Communications and Networking, Article No. 187, 2018.