Original scientific paper
https://doi.org/10.33180/InfMIDEM2025.402

Informacije MIDEM
Journal of Microelectronics, Electronic Components and Materials
Vol. 55, No. 4(2025), 219 – 228

Smart Prediction and Trust-based Transmission in Delay-Targeted Networks for Aviation Communication

Shanmugavel Deivasigamani[1], Rajinigirinath Dhandapani[2]

[1]Department of Artificial Intelligence and Data Science, JEPPIAAR Institute of Technology, Chennai, Tamilnadu, India.
[2]Department of Computer Science and Engineering, Sri Muthukumaran Institute of Technology, Chennai, India

Abstract: Delay Targeted Networking (DTN) facilitates communication in environments with sporadic connectivity and long delays, such as space missions and isolated locations. The rise of 5G technology has increased the demand for in-flight services, challenging aviation communication to provide reliable data through satellite systems and traditional macro-cellular networks. However, airborne communication's dynamic nature poses significant challenges, including irregular connections and variable delays. To tackle these challenges, a novel Smart Prediction and trAnsmission mechanism for delay taRgeted networK (SPARK) technique has been proposed to enhance the efficiency and reliability of DTNs in aviation communication. The proposed SPARK method includes a comprehensive node trust evaluation system, utilizing direct and indirect trust metrics to ensure network reliability. After evaluating node trustworthiness, the proposed method restricts heavy load traffic based on trustworthiness. The Prediction and Transmission Module incorporates the Cooperative Watchdog System (CWS) to dynamically update each node's reputation score. Nodes are classified into cooperative, partially cooperative, neutral, mislead, and selfish nodes. Experimental results demonstrate the effectiveness of the suggested SPARK framework utilizing evaluation parameters including delivery rate, delay, overhead, hop count, throughput, complexity, and resource utilization. The delay rate of the proposed SPARK method is 18.67%, 19.87%, and 14.45% is lower than the existing OPRNET, IDRL, and CCMA, techniques respectively. The distribution of the proposed SPARK framework attains a forwarding rate of 11% for selfish, and 9.2% for misleading based on their packet forwarding behavior.

Keywords: Delay Targeted Network; transmission; routing; prediction; communication

Pametno napovedovanje in prenos na podlagi zaupanja v omrežjih z zamikom za letalsko komunikacijo

Izvleček: Omrežje z zamikom (DTN) olajšuje komunikacijo v okoljih z naključno povezljivostjo in dolgimi zamiki, kot so vesoljske misije in izolirane lokacije. Razvoj tehnologije 5G je povečal povpraševanje po storitvah med letom, kar predstavlja izziv za letalsko komunikacijo, da zagotovi zanesljive podatke prek satelitskih sistemov in tradicionalnih makrocelularnih omrežij. Vendar pa dinamična narava letalske komunikacije predstavlja pomembne izzive, vključno z nepravilnimi povezavami in spremenljivimi zamiki. Za reševanje teh izzivov je bila predlagana nova tehnika Smart Prediction and trAnsmission mechanism for delay taRgeted networK (SPARK), ki izboljšuje učinkovitost in zanesljivost DTN v letalski komunikaciji. Predlagana metoda SPARK vključuje celovit sistem ocenjevanja zaupanja vozlišč, ki uporablja neposredne in posredne metrike zaupanja za zagotavljanje zanesljivosti omrežja. Po oceni zanesljivosti vozlišč predlagana metoda omeji promet z veliko obremenitvijo na podlagi zanesljivosti. Modul za napovedovanje in prenos vključuje sistem Cooperative Watchdog System (CWS) za dinamično posodabljanje ocene ugleda vsakega vozlišča. Vozlišča so razvrščena v sodelujoča, delno sodelujoča, nevtralna, zavajajoča in sebična vozlišča. Rezultati poskusov dokazujejo učinkovitost predlaganega okvira SPARK, ki uporablja parametre ocenjevanja, vključno s hitrostjo dostave, zamudo, režijskimi stroški, številom skokov, prepustnostjo, kompleksnostjo in izkoriščenostjo virov. Stopnja zamude predlagane metode SPARK je 18,67%, 19,87% in 14,45% nižja od obstoječih tehnik OPRNET, IDRL in CCMA. Porazdelitev predlaganega okvira SPARK doseže stopnjo posredovanja 11% za sebične in 9,2% za zavajajoče vozlišča na podlagi njihovega vedenja pri posredovanju paketov.

Ključne besede: Mreža z zamikom; prenos; usmerjanje; napovedovanje; komunikacija

** Corresponding Author's e-mail: shankan2005@gmail.com*

How to cite:
D. Shanmugavel et al., "Smart Prediction and Trust-based Transmission in Delay-Targeted Networks for Aviation Communication", Inf. Midem-J. Microelectron. Electron. Compon. Mater., Vol. 55, No. 4(2025), pp. 219–228

1 Introduction

Delay Targeted Networking (DTN) is a networking protocol that is intended to function well across very long distances and in conditions that conventional networking may find challenging [1,2]. In the realm of aviation communication, the advent of 5G technology has raised passenger expectations for in-flight services [3-5]. Presently, data services for both passenger and airline operations are facilitated through macro-cellular networks, inflight satellite systems, or air-to-ground (A2G) links [6-8]. However, the considerable financial expense and propagation delays associated with satellite communication, notably the Ad hoc Network utilizing Air-to-Air (A2A) radio broadcasts [9-11]. This approach offers power and transmission rate advantages over traditional methods, which is especially crucial for air traffic management and offshore coverage enhancement [12-15].

Despite its potential benefits, the dynamic nature of airborne communication poses significant challenges, including irregular connections, inadequate links, and variable delays during data transfer [16-19]. Moreover, existing research often overlooks the intermittent nature of connections, limiting the exploration of flexible transmission methods and impeding the development of efficient DTNs [20-23]. To address these challenges, this paper focuses on assessing the interactions among key network properties within a DTN framework, considering its fast-changing topology and occasional connectivity. By enabling opportunistic transmissions and employing realistic transatlantic data traces, aim to quantify the efficacy of DTNs, with a particular emphasis on data flow, transmission delays, and system overhead. In this paper, a novel SPARK method has been proposed to enhance the efficiency and reliability of DTNs in aviation communication. The major contributions of the proposed method are as follows:

- Nodes within the DTN are evaluated for trust using both direct and indirect trust metrics.
- After trust evaluation, heavy load traffic is restricted based on node trustworthiness. The prediction and Transmission Module incorporates the CWS which dynamically updates each node's reputation score based on several factors and categorizing nodes into five types: cooperative, partially cooperative, neutral, mislead, and selfish.
- After classification, cooperative, partially cooperative, and neutral nodes proceed to data forwarding.
- This process involves efficiently routing data packets through the network to ensure reliable delivery to the destination node.

The rest of the work are ordered in the following manner. Section II provides the literature evaluation, while Section III describes the proposed methodology. Section IV examines the experiment results. Section V contains the paper's conclusion.

2 Literature review

In recent years, numerous models have been introduced to improve the efficiency of DTNs. This section discusses some of the most prominent models and their respective benefits and limitations.

In 2021, Parameswari et al., [24] introduced OPRNET, an Opportunistic Routing Protocol that utilizes global location data for routing verdicts. OPRNET aims to enhance network capacity, while also increasing distribution opportunities and reducing latency and overhead. In 2021, Chourasia et al., [25] created a routing technique that gives packet scheduling priority over copy distribution counts in the network. The results indicate that the suggested method performs better than the current VDTN routing techniques.

In 2023, Gupta and Khaitan [26] introduced a queueing network model to depict message dissemination in hybrid VANET architecture. The paper offers an analysis of hybrid VANET with two conventional VANET architectures. In 2023, Yu et al., [27] presented a MANET routing technique for high-speed applications. The outcomes demonstrate that the suggested algorithm reducing communication delays by 75% and increasing data arrival rates by 15%.

In 2023, Han et al., [28] presented a hybrid routing technique with dynamic addressing that integrates the concepts of static setup. Then, an analysis and comparison are conducted on the performance metrics of each algorithm. In 2023, Upadhyay et al., [29] presented a routing method for enhanced deep reinforcement learning (IDRL) that minimizes augmented control overhead. The suggested IDRL routing strategy performs better than the innovative in terms of data dependability, PDR, and latency.

In 2024, Nakayima et al., [30] offered a cutting-edge method for improving VANET performance using a centralized-controller multi-agent (CCMA) algorithm that combines Reinforcement Learning (RL) with SDN and DTN principles. Evaluations show that the suggested approach performs better in a variety of VANET circumstances. Table 1 describes the comparison of existing techniques.

Table 1: Comparison of existing techniques

Techniques	Aim	Strengths	Weaknesses
OPRNET [24]	To enhance network capacity, including energy consumption, optimization latency, and storage	Reducing latency and overhead	Increased energy consumption
Routing technique [25]	VDTNs that limits the number of copies distributed to enhance efficiency.	Improved delivery performance, reduced network congestion, and enhanced packet prioritization.	High buffer usage, increased processing overhead.
Queueing network model [26]	Analyze end-to-end delay and backlog in a hybrid VANET	Improving network performance	Increased computational complexity
MANET routing technique [27]	To enhance routing decisions and network stability	Reducing communication delay and increasing data arrival rates	High computational complexity
A hybrid routing technique [28]	To reduce network overhead and increase network longevity	Lower routing discovery delay, and improved reliability.	Increased processing load, and potential routing inefficiencies.
IDRL [29]	To reduce control overhead and transmission delay.	Reduced latency, improved PDR, enhanced data reliability.	Increased resource consumption.
CCMA [30]	Enhance VANET performance	Reduced latency, and better buffer management,	High computational complexity

However, several significant studies have been undertaken on efficiency issues in DTNs. Despite notable advancements, existing approaches exhibit limitations such as scalability challenges, high overhead, complexity, delay, etc. To overcome these challenges, a novel SPARK technique has been suggested in this paper, which is covered in the following section 3 and the subsections.

3 Smart prediction and transmission mechanism for delay-targeted network

In this section, a novel SPARK technique has been suggested to enhance the efficiency and reliability of DTNs in aviation communication.

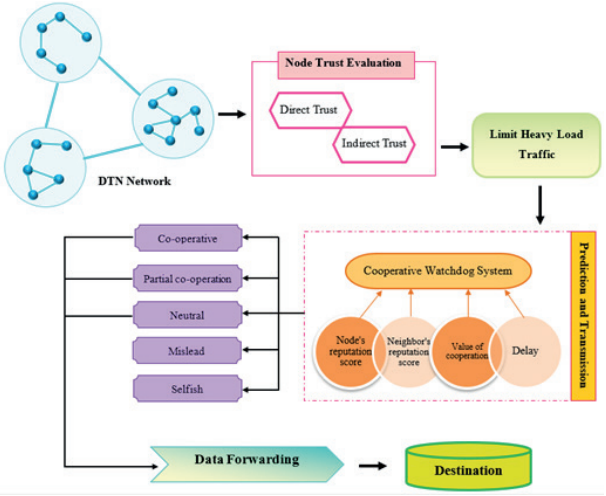

Figure 1: Proposed SPARK Methodology

Direct and indirect trust metrics are used to assess nodes in the DTN for trustworthiness. While indirect trust considers the opinions of nearby nodes to enhance overall network stability, direct trust assesses node behavior based on direct interactions. Following the trust assessment, heavy load traffic is limited according to the trustworthiness of the node. The CWS, which dynamically adjusts each node's reputation score depending on several variables, is incorporated into the Prediction and Transmission Module. Five node categories such as cooperative (class 0), partially cooperative (class 1), neutral (class 2), misleading (class 3), and selfish (class 4) are created from the CWS scores assigned to nodes. Cooperative, moderately cooperative, and neutral nodes move on to data forwarding after classification. Data packets are effectively routed through the network during this step to guarantee dependable delivery to the destination node. The overall workflow of the suggested SPARK model is given in Figure 1.

Node trust evaluation

Nodes' trustworthiness is evaluated through a combination of direct and indirect trust. Direct trust is based on the actual interactions between nodes, while indirect trust considers past behaviors and the level of confidence in those assessments. Ultimately, weighted values of both are used to compute the overall trust value.

3.1 Direct trust (DT)

DT is the immediate impression of the assessed node by the evaluation node. For the direct trust computation, the three elements listed as trust factors, where x stands for trust in the assessed node and y for the node that has to be assessed.

3.1.1 Direct trust bayesian trust degree (BTD)

BTD model uses the trust degree as an arbitrary variable with a possibility circulation to predict future node behavior (posterior) based on past node interactions (prior). The parameter b indicates the number of unsuccessful interactions. Equation (1) gives the Bayesian trust degree, which used to visually represent the node's packet forwarding success rate and trend.

$$BTD_{xy} = \frac{a}{a+b} = \frac{o_s + 1}{o_s + o_u + 2} \tag{1}$$

Where o_s is the record of effective y connections and o_u denotes the record of failed y interactions.

3.1.2 Data similarity degree (DSD)

The degree of comparison among 2 nodes transmitting data is indicated by data similarity; and incorporating resemblance into the trust value control might help mitigate malicious assaults to some extent. The calculation is done using equation (2).

$$DSD_{xy} = \frac{MsgSame}{\left(List_x + List_y\right)/2} \tag{2}$$

Where *MsgSame* indicates how many comparable packets there are between nodes x and y and ($List_x$ + $List_y$)/2 indicates how many packets on average are stored in each node's cache.

3.1.3 Node activity degree (NAD)

The quantity of nodes encountered in a given amount of time determines a node's activity level inside the network. To prevent malicious assaults, node activity is zeroed at the beginning of each unit time. This is its calculating in equation (3).

$$NAD_{xy} = \frac{t}{\varnothing} \times \frac{Internum}{No} + \left(1 - \frac{t}{\varnothing}\right) \times NAD_{xyOld} \tag{3}$$

Where *t* is the time in units, *Internum* is a representation of the number of nodes encountered in the network. The entire number of nodes in the present network is denoted as *No* and NAD_{xyOld} is the activity of the node at the most recent reset. As a result, equation (4) can be used to define the DT value (D).

$$D_{xy} = V_1 \times BTD_{xy} + V_2 \times DSD_{xy} + V_3 \times NAD_{xy} \tag{4}$$

The weight coefficients are the parameters V_1, V_2 and V_3. Depending on the network environment, the weights may have varying values allocated to them.

3.2 Indirect trust

A Node x should reflect the "view" of neighboring nodes on y, just like in social life, to evaluate node y more completely. Let x and y be two nodes that have neighbors in common. The trust threshold is determined by averaging the trust values found in the node x's trust table, which is given in equation (5).

$$H_{threshold} = \frac{\sum_{i=1, i\neq x}^{m} H_{xi}}{m-1} \tag{5}$$

Where H_{xi} is the node x's direct trust value to its common neighbor nodes, where m is the number of common nodes at present. Afterward solving equation (5), m co-neighboring nodes remain. The departure of the number of contacts between node y and nearby nodes from the number of connections between node x and node y, which is determined as in equation (6).

$$\rho = \frac{\sqrt{\sum_{r=1}^{n}\left(IN_{r,y} - IN_{x,y}\right)^2}}{n} \tag{6}$$

$$I_{xy} = \frac{\sum_{i=1}^{c} D_{x,i} \times D_{i,y}}{c} \tag{7}$$

The above equation (7) provides the ultimate indirect trust computation algorithm. Where ρ defines the calculated metric, *n* represents the total number of elements, $IN_{r,y}$ is the number of interactions that a neighbor node r has had. At node r, the "view" will be deemed invalid if $IN_{r,y} < IN_{x,y-} - \rho$, c indicates the remaining shared neighbor nodes.

3.3 Limit heavy load traffic

Limiting heavy load traffic after Node Trust Evaluation involves a crucial assessment process aimed at enhancing network reliability and security. This ensures that only nodes deemed trustworthy are allowed to handle heavy loads, thereby reducing the risk of network congestion, and potential breaches. Once heavy load traffic is limited, it enters the prediction and transmission phase where nodes are categorized for efficient data transmission.

3.4 Prediction and transmission

After reducing heavy traffic load, optimized input is fed into the prediction and transmission phase for efficient data transfer. The core of the Prediction and Transmission module is the CWS, which aims to ensure network access while identifying non-compliant nodes. The node's reputation score (RSI), its neighbors' reputation score (RS_N), a value of cooperation offered by the watchdog (CV_W), and Delay. The node's associated cooperative value (CV_W). Eq. (8) determines a cooperative value for node *n*.

$$CV_{w_n} = \beta.\gamma_n \tag{8}$$

Where γ represents the punctuation that the classification module assigns to node *n* is the node performance coefficient represented by β. Eq. (9) is used by the classification module to generate this value, where R_{Bi} is the number of bundles that have been relayed from node *i*, D_{Bi} is the number of packages that have already been delivered from node *i* and D_{pBi} is the number of bundles that have already been dumped from node *i*. Eq. (10) is used to determine the value.

$$x = \frac{\sum_{i=I}^{N}\left(R_{B_i} - D_{B_i}\right)}{\sum_{i=I}^{N}\left(R_{B_i} - DP_{B_i}\right)} \tag{9}$$

$$\beta = \frac{x - \min\left(x\right)}{\max\left(x\right) - \min\left(x\right)} \tag{10}$$

The neighbor assessment module establishes the RS_N of each node. The module for neighbor evaluation polls *N* neighbors (N_g) for feedback on the participating nodes at each contact opportunity. These neighbors provide the corresponding RS_N value in response to the evaluation module request from the neighbor. Each time a neighbor creates a direct communication channel with a node (*n*), the node's RS_N value is modified is given in equation (11).

$$RS_N\left(n\right) = \frac{\sum_{i=I}^{N} RS_{R_i}}{N} \tag{11}$$

The reputation score that the node itself (RS_I), the neighbor's evaluation module (RS_N), and the categorization module (CV_W) have seen are all taken into consideration by the decision module when updating a network node's reputation score () following a contract opportunity. An updated node reputation scores (∞_n) which is the sum of the three ratings and is determined as follows in equation (12).

$$\propto_n = \theta.RS_{I_n} + \left(I - \theta\right).RS_{N_n} + CW_{W_n} \tag{12}$$

where ∞_n represents the degree to which the CWS relies on nodes' self-reported observations and ranges from [0,1]. The classification module updates its classification table after receiving the decision module's updated nodes' reputation scores. Using this score finally the nodes are classified into 5 types they are class 0, class 1, class 2, class 3, and class 4. Subsequently, the classified output is transferred to the data forwarding phase.

3.5 Data forwarding

After node prediction, if classified as class 0, class 1, or class 2, nodes proceed to data forwarding. Immediate neighbors of the downstream node assist in this process. The next upstream sender is noted in the failed node's Pending Credit Table. Once the forwarder timer expires, a neighboring node broadcasts the data packet to lower-layer nodes using the credit table. When the designated lower-layer node retransmits the packet, nearby nodes with the same data in their credit table delete their cache and stop their timers. This process reduces transmission delays, prevents redundant transmissions, and enhances the interest satisfaction ratio. The process of data packet forwarding and routing is shown in Figure 2.

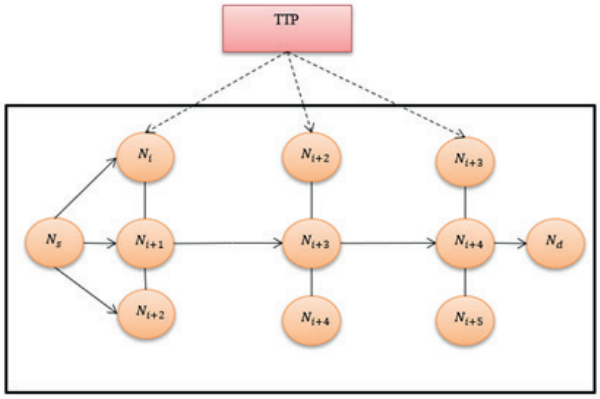

Figure 2: Data forwarding and routing mechanism

Algorithm: Proposed SPARK model data forwarding in DTN network
Input Data: DTN network topology, Node interaction data, Trust evaluation parameters
Output: Data forwarding to the destination
Step-1: Initialize the DTN network and establish communication links.
Step-2: Perform node trust evaluation
Step-2.1: Determine direct trust based on the past node interactions (prior) using equation (1)
Step-2.2: Determine indirect trust from neighboring nodes using equation (5).
Step-3: Limiting heavy load traffic to enhance network reliability and security
Step-4: Perform prediction and transmission to identify optimal paths.
Step-4.1: Compute the node's reputation score based on forwarding behavior
Step-4.2: Analyze neighbor's reputation score to assess cooperation level
Step-4.3: Evaluate the value of cooperation to identify malicious nodes
Step-4.4: Measure delay to detect misbehavior
Step-5: Classify the network nodes using cooperative watchdog system (CWS)
Step-6: Forward data based on trust scores and cooperative behavior
Step-7: Deliver data to the destination efficiently and securely.

4 Results and discussion

The suggested SPARK model's simulation findings are examined and a discussion of efficacy is done in terms of numerous evaluation parameters within this section. The effectiveness of the proposed SPARK method is tested using the ONE (opportunistic network environment) simulator. The efficacy of the suggested SPARK approach is examined using four metrics: hop count, overhead, delivery ratio, delivery delay throughput, complexity, and resource utilization. All of the significant factors that were utilized in the simulation are enumerated in Table 2.

Figure 3 presents the distribution of the proposed SPARK model categories based on their packet forwarding behavior. This provides how node behaviors are evaluated and categorized within the DTN. A cooperative node is defined as one that forwards packets in 39.4% of interactions, while a partially cooperative node forwards packets in 26.6% of the time. Nodes that attain a forwarding rate of 13.8% are neutral, and misleading nodes are forward less than 9.2% of packets. Finally, selfish nodes that function correctly in 11% of interactions within the DTN.

Table 2: Parameter setup

Parameter	Value
Region	5000m*5000m
Data size	500 KB
Interval	40s
TTL	4 hours
Time	10 hours
Transmission range	10 m
Transmission speed	250 KB/s

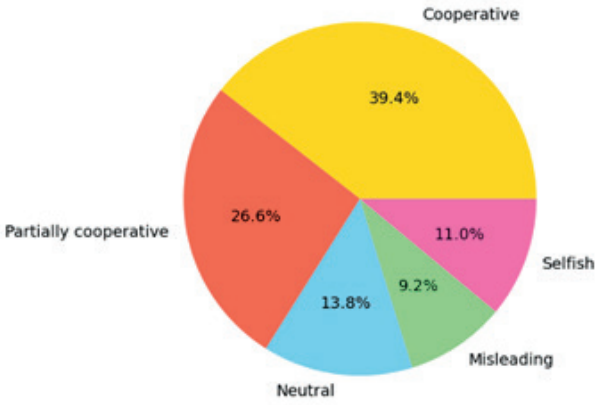

Figure 3: Classification distribution of the proposed SPARK framework

4.1 Comparative analysis

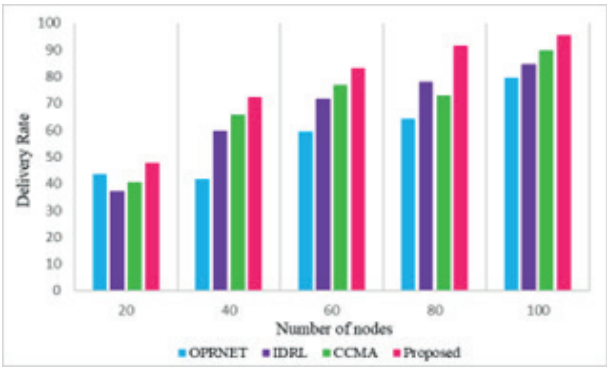

Figure 4: Comparison in terms of delivery rate

Figure 4 illustrates a comparison of delivery rates between existing methods and the proposed SPARK method. Our proposed work effectively minimizes the packet drops by utilizing an optimized routing mechanism, which selects the most reliable route dynamically. This demonstrate that the greater performance of

the proposed SPARK method in ensuring higher delivery rates under the given conditions.

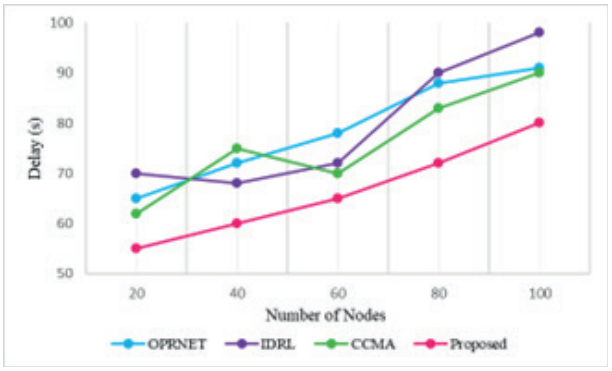

Figure 5: Comparison in terms of delay

Figure 5 presents a comparative analysis of delay times with existing techniques and a proposed method. By implementing the efficient path selection, our proposed SPARK method reduces the time required for packet transmission. The delay rate of the proposed SPARK method is 18.67%, 19.87%, and 14.45% is lower than the existing OPRNET, IDRL, and CCMA techniques respectively.

Figure 6 illustrates a comparative analysis of overhead. For reducing the network control traffic, the suggested work employs a routing mechanism through optimized control message transmission. It shows that the suggested model's effectives significant efficiency in reducing overhead, highlighting its potential advantages over the other methods.

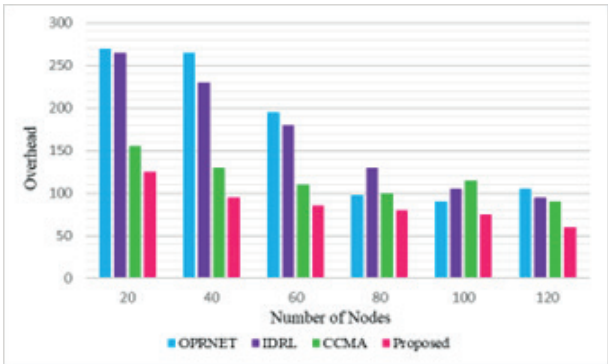

Figure 6: Comparison in terms of overhead

Figure 7 presents a comparison of hop counts. The proposed method constantly attains advanced hop counts associated with the other protocols, particularly noticeable at larger network sizes. OPNET consistently results in the lowest hop counts across all network sizes, demonstrating a more efficient routing performance in terms of hop count.

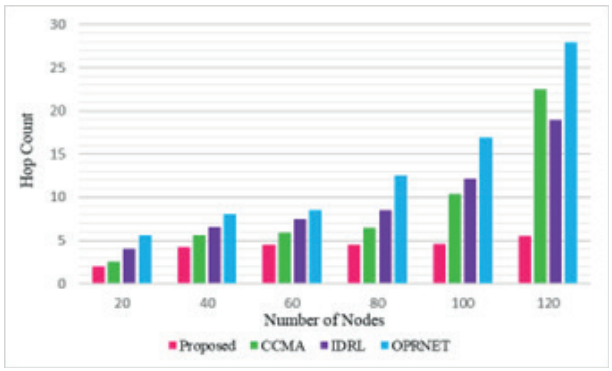

Figure 7: Comparison in terms of Hop Count

Figure 8 illustrates a comparison of throughput among the proposed SPARK method and the existing methods. The proposed SPARK method maintains a relatively stable and high throughput. Overall, the proposed SPARK method shows superior presentation in terms of maintaining consistent and high throughput related to the other protocols.

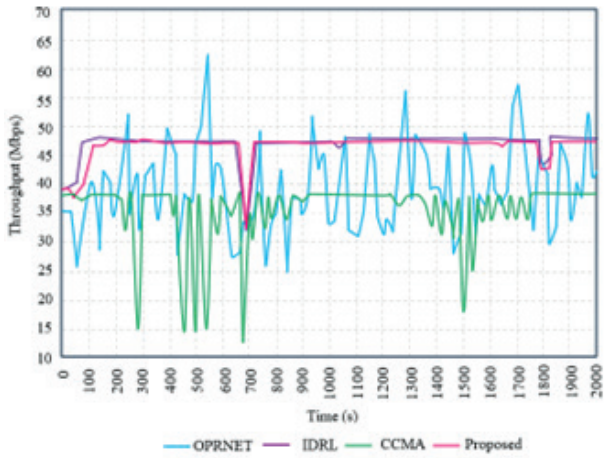

Figure 8: Comparison in terms of Throughput

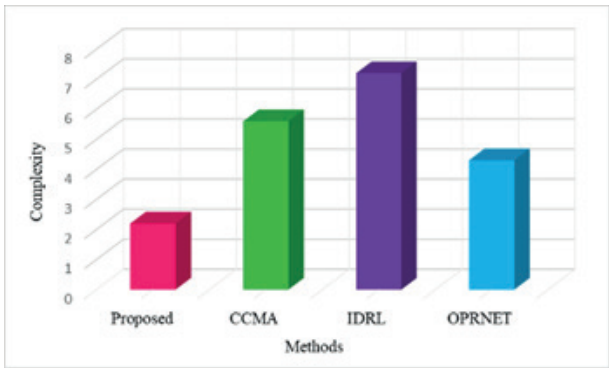

Figure 9: Comparison in terms of Complexity

Figure 9 illustrates the comparation of complexity between the suggested SPARK approach and current methods. The proposed method shows the lowest complexity, while IDRL is the most complex. This shows

the proposed SPARK method's maintaining lower complexity compared to the others.

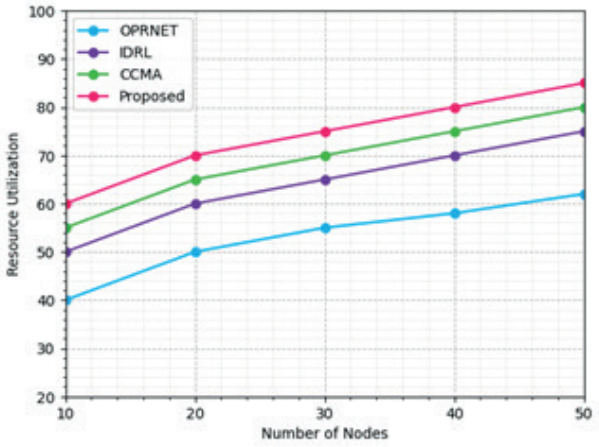

Figure 10: Comparison of Resource utilization

Figure 10 shows the comparation of resource utilization between the proposed SPARK method and existing approaches. It is evident that the Proposed model consistently achieves higher resource utilization across all node counts compared to the other models. The increasing trend in resource utilization for all Models indicates that they scale with the number of nodes, with the Proposed model demonstrating superior efficiency and scalability.

5 Conclusions

In this paper, a novel SPARK technique has been proposed to enhance the efficiency and reliability of DTNs in aviation communication. By incorporating a robust node trust evaluation system, the methodology ensured that only trustworthy nodes handle heavy traffic loads, thereby enhancing overall network security and performance. The proposed SPARK method was assessed using various performance parameters including delivery rate, delay, overhead, hop count, throughput, complexity, and resource utilization. The proposed SPARK approach consistently achieved higher delivery rates, lower delays, reduced overhead, and higher hop counts, indicating its effectiveness in managing the unique challenges of DTNs in aviation environments. The delay rate of the proposed SPARK method is 18.67%, 19.87%, and 14.45% is lower than the existing OPRNET, IDRL, and CCMA, techniques respectively. Future research should focus on integrating AI and machine learning methods for anomaly detection, traffic control, and predictive analytics to further improve the resilience and effectiveness of DTNs.

6 Acknowledgments

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

7 Conflict of interest

No financial or interpersonal conflicts have been reported by the authors that would have affected the study's finding

8 References

1. S. Ullah and A. Qayyum, "Socially-aware adaptive delay tolerant network (dtn) routing protocol", *PloS one*, vol. 17, no. 1, pp. 0262565, 2022. http://dx.doi.org/10.1371/journal.pone.0262565
2. G. Koukis, K. Safouri and V. Tsaoussidis, "All about Delay-Tolerant Networking (DTN) Contributions to Future Internet", *Future Internet*, vol. 16, no. 4, pp. 129, 2024. http://dx.doi.org/10.3390/fi16040129
3. E.M. Malathy, V. Sathya, P.E. David, P. Ajitha, V.T. Noora, and A. Ahilan, 5G Network with Hexagonal SDN Control for Highly Secure Multimedia Communication. IETE Journal of Research, vol. 70, no. 12, pp. 8492-8507, 2024.
4. H. Kopetz and W. Steiner, "Real-time communication. In Real-time systems: Design principles for distributed embedded applications", *Cham: Springer International Publishing*, pp. 177-200, 2022. http://dx.doi.org/10.1007/978-3-031-11992-7_7
5. N. Tepylo, A. Straubinger and J. Laliberte, "Public perception of advanced aviation technologies: A review and roadmap to acceptance", *Prog. Aerosp. Sci.*, vol. 138, pp. 100899, 2023. http://dx.doi.org/10.1016/j.paerosci.2023.100899
6. A. Shaverdian, S. Shahsavari and C. Rosenberg, "Air-to-ground cellular communications for airplane maintenance data offloading", *IEEE Trans. Veh. Technol.,* vol. 71, no. 10, pp. 11060-11077, 2022. http://dx.doi.org/10.1109/tvt.2022.3185562
7. M.A. Khalifa, M. Ali and M. Naeem, "Buoyant airborne turbines in B5G/6G wireless networks: Opportunities, challenges, applications, and future directions", *Comput. Electr. Eng.,* vol. 111, pp. 108962, 2023. http://dx.doi.org/10.1016/j.compeleceng.2023.108962
8. P.P. Ray, "A review on 6G for space-air-ground integrated network: Key enablers, open challenges,

and future direction", *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 9, pp. 6949-6976, 2022. http://dx.doi.org/10.1016/j.jksuci.2021.08.014

9. R.E. Śliwa, P. Dymora, M. Mazurek, B. Kowal, M. Jurek, D. Kordos, T. Rogalski, P. Flaszynski, P. Doerffer, K. Doerffer and S. Grigg, "The latest advances in wireless communication in aviation, wind turbines, and bridges", *Inventions*, vol. 7, no. 1, pp. 18, 2022. http://dx.doi.org/10.3390/inventions7010018
10. T. Wei, W. Feng, Y. Chen, C.X. Wang, N. Ge, and J. Lu, "Hybrid satellite-terrestrial communication networks for the maritime Internet of Things: Key technologies, opportunities, and challenges", IIEEE *Internet Things J.,* vol. 8, no. 11, pp. 8910-8934, 2021. http://dx.doi.org/10.1109/jiot.2021.3056091
11. A. Baltaci, E. Dinc, M. Ozger, A. Alabbasi, C. Cavdar and D. Schupke, "A survey of wireless networks for future aerial communications (FACOM)", *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2833-2884, 2021. http://dx.doi.org/10.1109/comst.2021.3103044
12. P. Park, P. Di Marco, J. Nah and C. Fischione, "Wireless avionics intracommunications: A survey of benefits, challenges, and solutions", *IEEE Internet Things J.,* vol. 8, no. 10, pp. 7745-7767, 2020. http://dx.doi.org/10.1109/jiot.2020.3038848
13. Z. Xiao, Z. Han, A. Nallanathan, O.A. Dobre, B. Clerckx, J. Choi, C. He and W. Tong, "Antenna array enabled space/air/ground communications and networking for 6G", *IEEE J. Sel. Areas Commun.,* vol. 40, no. 10, pp. 2773-2804, 2022. http://dx.doi.org/10.1109/jsac.2022.3196320
14. S.A.H. Mohsan, M.A.Khan and H. Amjad, "Hybrid FSO/RF networks: A review of practical constraints, applications, and challenges", *Opt. Switching Networking.,* vol. 47, pp.100697, 2023. http://dx.doi.org/10.1016/j.osn.2022.100697
15. S.A. Al-Ahmed, T. Ahmed, Y. Zhu, O.O. Malaolu and M.Z. Shakir, "UAV-Enabled IoT Networks: Architecture, Opportunities, and Challenges", *Wireless Networks and Industrial IoT: Applications, Challenges and Enablers,* pp.263-288, 2021. http://dx.doi.org/10.1007/978-3-030-51473-0_14
16. J.O. Ogbebor, A.L. Imoize and A.A.A. Atayero, "Energy-efficient design techniques in next-generation wireless communication networks: emerging trends and future directions", *Wireless Commun. Mobile Comput.,* vol. 2020, no. 1, pp. 7235362, 2020. http://dx.doi.org/10.1155/2020/7235362
17. M.Y. Arafat, S. Poudel and S. Moh, "Medium access control protocols for flying ad hoc networks: A review", *IEEE Sens. J.,* vol. 21, no. 4, pp. 4097-4121, 2020. http://dx.doi.org/10.1109/jsen.2020.3034600
18. A. Salh, L. Audah, N.S.M. Shah, A. Alhammadi, Q. Abdullah, Y.H. Kim, S.A. Al-Gailani, S.A. Hamzah, B.A.F. Esmail and A.A. Almohammedi, "A survey on deep learning for ultra-reliable and low-latency communications challenges on 6G wireless systems", *IEEE Access,* vol. 9, pp. 55098-55131, 2021. http://dx.doi.org/10.1109/access.2021.3069707
19. A. Förster, J. Dede, A. Könsgen, K. Kuladinithi, V. Kuppusamy, A. Timm-Giel, A. Udugama and A. Willig, "A beginner's guide to infrastructure-less networking concepts", *IET Networks*, vol. 13, no. 1, pp. 66-110, 2024. http://dx.doi.org/10.1049/ntw2.12094
20. M. Usha, T. Mahalingam, A. Ahilan and J. Sathiamoorthy, "EOEEORFP: Eagle optimized energy efficient optimal route-finding protocol for secure data transmission in FANETs". *IETE J. Res.,* vol. 70, no. 5, pp. 4867-4879, 2024.
21. Vishnu Karthik Ravindran, "QUICK-CHAIN: Blockchain Enabled Secure Data Transmission In IoT-WSN Environment," *International Journal of Computer and Engineering Optimization*, vol. 02, no. 02, pp. 35-39, 2024.
22. R. R. Sathiya, S. Rajakumar and J. Sathiamoorthy, "Secure Blockchain Based Deep Learning Approach for Data Transmission in IOT-Enabled Healthcare System," *International Journal of Computer and Engineering Optimization*, vol. 01, no. 01, pp. 15-23, 2023.
23. Hari Krishna Kalidindi, "Crow Search Optimized DNA Encryption for Secure Medical Data Transmission," *International Journal of Computer and Engineering Optimization*, vol. 02, no. 03, pp. 80-85, 2024.
24. S. Parameswari, "Opportunistic Routing Protocol for Resource Optimization in Vehicular Delay-Tolerant Networks (VDTN)", Turk. J. Comput. Math. Educ., vol. 12, no. 11, pp. 3665-3671, 2021. http://dx.doi.org/10.17762/turcomat.v12i6.5685
25. V. Chourasia, S. Pandey and S. Kumar, "Packet priority-based routing approach for vehicular delay tolerant network", In I*nnovations in Computational Intelligence and Computer Vision: Proceedings of ICICV 2020 Springer Singapore*, pp.294-301, 2021. http://dx.doi.org/10.1007/978-981-15-6067-5_32
26. S. Gupta and V. Khaitan, "End-to-end delay and backlog bound analysis for hybrid vehicular ad hoc network: a stochastic network calculus approach", Int. J. Veh. Inf. Commun. Syst., vol. 8, no. 3, pp. 191-216, 2023. http://dx.doi.org/10.1504/ijvics.2023.132925
27. Y. Yu and X. Sun, "A Routing Algorithm for High-Speed Mobile Ad Hoc Network Based on Deep

Q Network", *In 2023 IEEE 13th International Conference on Electronics Information and Emergency Communication (ICEIEC)*, pp. 65-69, 2023, http://dx.doi.org/10.1109/iceiec58029.2023.10199694
28. Z. Han, L. Liu, Z. Guo, Z. Su, L. Suo, S. Cai, and H. Han, "A Dynamic Addressing Hybrid Routing Mechanism Based on Static Configuration in Urban Rail Transit Ad Hoc Network". *Electron.*, vol. *12*, no. 17, p.3571. 2023.
29. P. Upadhyay, V. Marriboina, S.J. Goyal, S. Kumar, E.S.M. El-Kenawy, A. Ibrahim, A.A. Alhussan and D.S. Khafaga, "An improved deep reinforcement learning routing technique for collision-free VANET", *Sci. Rep.,* vol. 13, no. 1, pp. 21796, 2023. http://dx.doi.org/10.3390/electronics12173571
30. O. Nakayima, M.I. Soliman, K. Ueda and S.A.E. Mohamed, "Combining Software-Defined and Delay-Tolerant Networking Concepts with Deep Reinforcement Learning Technology to Enhance Vehicular Networks", *IEEE Open J. Veh. Technol.,* 2024. http://dx.doi.org/10.1038/s41598-023-48956-y

Copyright © 2025 by the Authors. This is an open access article distributed under the Creative Commons Attribution (CC BY) License (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Arrived: 05. 10. 2024
Accepted: 01. 10. 2025