Hybrid Routing and Security Framework for High Speed Vehicular Networks based on BESO Algorithm

Kusuma G S
Department of Electronics and Communication Engineering,
The Oxford College of Engineering
Bengaluru, Karnataka,India.
E-mail:kusuma.gs1988@gmail.com

Manju Devi
Department of Electronics and Communication Engineering,
The Oxford College of Engineering
Bengaluru, Karnataka,India.
E-mail:manju3devi@gmail.com

***Abstract*—The VANET architecture is highly dynamic due to the constant movement of vehicles, which complicates routing and data scheduling for high-speed communication. Incorporating security measures further adds to the complexity, often leading to increased delays and decreased throughput. To tackle these challenges, the proposed system focuses on reducing the overhead of key generation and utilizes a fog computing platform combined with lightweight encryption techniques. Specifically, the Batched Eagle Spotting Optimizer (BESO) algorithm is employed for efficient route selection, optimizing parameters like packet transmission timing and hash-based key creation. For security, a lightweight encryption method called ROTR is used, enabling faster data transmission by generating smaller keys. Overall, the integrated BESO-ROTR approach enhances routing efficiency and security while minimizing processing delays, with performance validated through metrics such as packet loss, transmission success, and throughput in high-mobility VANET environments.

***Index Terms*—Vehicular Ad-hoc Network (VANET), Batched Eagle Spotting Optimizer (BESO), and Key pattern generation.**

I. INTRODUCTION

Incorporating fog computing into VANETs plays a crucial role in enhancing the overall efficiency of data transmission within the network. By positioning computing and storage resources at the edge, near the vehicles, the system reduces the time it takes to process and analyze data, leading to lower latency and quicker decision-making. This localized processing allows vehicles to communicate more rapidly and securely, minimizing delays that are common in centralized cloud-based architectures. The fog layer acts as a vital intermediary, managing data, performing computations, and handling services locally before transmitting information to the cloud when necessary. This setup not only accelerates data transfer but also helps in maintaining secure and reliable communication, even in highly dynamic environments where vehicle positions and network conditions constantly change. Overall, this architecture makes VANETs more responsive, scalable, and capable of supporting high-speed data exchange essential for safety applications and intelligent transportation systems.

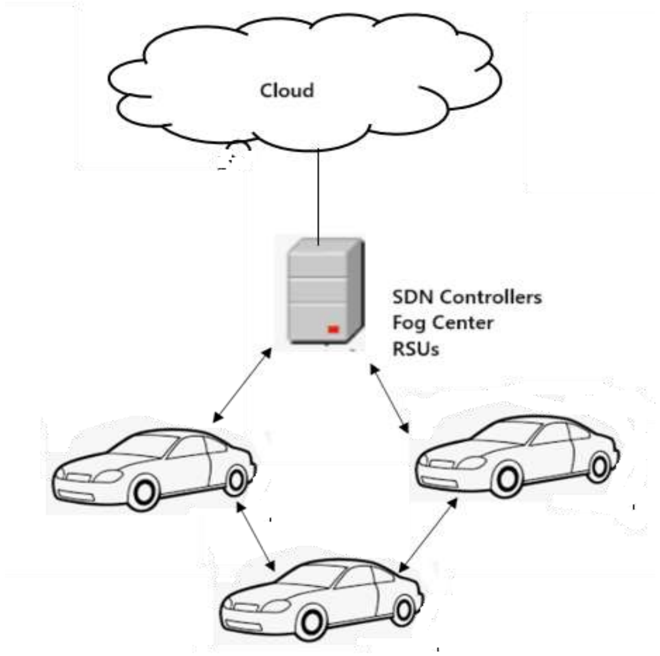

Fig 1. VANETs Architecture

In this Fig 1, the architecture of the VANET model was sub-divided into 3 stages such as, cloud environment, Fog computing and the end-user of vehicle nodes. The nodes are connected to the RSU unit to retrieve data from the cloud to local system while at the dynamic network structure. The Fog computing and the other controllers are done in the RSUC unit that controls the flow of data transmission to the nodes and cloud storage. Here, the data security can also process under the controlling unit which forms the secure network combination. The RSU placement and the structure are referred to route the vehicle nodes based on the position and coverage size. In that, some of the protocol used for routing model such as Adaptive Data Dissemination Protocol (AddP) [1], intelligent forwarding method [2], Random Fire-Fly [3], map-based relaying algorithm (MBR) [4], adaptive beacon generation rate (ABGR) [5], etc. are implementing the optimal feature selection for routing path identification with the network security problem.

From these arrangement, to achieve the better transmission rate and to improve the throughput parameters in the network formation, the routing path selection needs to select with the best optimal path that is leads to best matching with the parameters that are related to the packet transmission. This can also combine with the Fog computing technique to enhance the routing experience and enhance the high speed packet transmission. This was enhanced in the proposed technique based on the batching process of optimization algorithm to achieve the parameters range. The network security in the proposed architecture are can be achieved by using the light-weight key generation model and the hashing key pattern to enhance the speed of performance and the secure data transmission rate.

The objective of the proposed model of optimal routing and the VANET security are can be listed as

- To estimate the network properties and the node characteristics for optimal path selection and routing system in VANET.
- To perform the optimal selection of best routing path by using the Batched Eagle Spotting Optimizer (BESO) Algorithm that works batch process of the particles for each iteration of time count.
- To identify the most effective routing paths, relevant network features such as node location, velocity, and link quality are analyzed and weighted to select an optimal route that minimizes overall transmission cost.
- Network security is improved by dynamically generating encryption keys at fog nodes based on recent network parameters and patterns, thereby reinforcing data protection through intelligent key pattern extraction integrated with fog computing capabilities.
- For rapid and secure data transfer, a lightweight encryption method employing a ROTR-based rotation cipher is utilized, offering high-speed performance while maintaining data confidentiality through efficient, minimal-overhead encryption.

The full description about the proposed architecture and the algorithm descriptions are explained in the following sections. According to that, the survey of various types of network security system and the routing protocols are explained with its merits and demerits in section II. the BESO and the ROTS based secure optimal routing protocol are explained in the section III. The simulation parameters and the performance validation of the proposed model with the comparison chart and the table results are described in the section IV. Finally, the conclusion of proposed model was justified and the future work are presented in section V.

II. RELATED WORKS

The reviewed works encompass various approaches aimed at enhancing routing efficiency[6], security, and privacy in VANETs. Many algorithms, such as the weighted inertia-based dynamic virtual bat algorithm (WIDVBA) [7], have demonstrated the ability to optimize route selection processes, thereby reducing unwanted data flooding and improving data delivery, especially in dynamic network topologies. These protocols significantly contribute to maintaining efficient communication within high-mobility environments.

On the security front, multiple schemes have been developed to safeguard data integrity and user privacy. Techniques like batch verification with certificate-less ring signatures [12], identity-based encryption models [16], and blockchain-based edge computing [17] offer robust mechanisms to prevent attacks and ensure data authenticity. Additionally, trust management frameworks [20, 21] are employed to detect malicious activities, such as DOS or DDOS attacks, thereby strengthening the overall security posture of VANETs. However, these algorithms also bear notable limitations. Many security schemes, particularly those involving cryptographic operations and blockchain consensus, tend to introduce high computational overhead, which can lead to delays and increased resource consumption incompatible with the fast-paced environment of VANETs. Scalability is another critical issue; protocols like OLSR with multipoint relay schemes [18] may struggle to maintain efficiency as network size increases. Furthermore, despite these advancements, vulnerabilities[19] such as privacy breaches and attack exploitation remain, especially when security mechanisms are resource-intensive or not fully integrated. Lastly, most existing algorithms are optimized for static or semi-dynamic scenarios, making their performance less effective in real-world VANET[20][21] environments where topology changes rapidly and unpredictably. These constraints highlight the necessity for developing more lightweight, adaptive, and scalable routing and security solutions tailored specifically for high-mobility VANET applications.

III. PROPOSED METHODOLOGY

The proposed system enhances VANET performance by integrating the Batched Eagle Spotting Optimization (BESO) algorithm with fog computing to efficiently identify the best routing paths amidst high vehicle mobility. BESO evaluates network parameters such as node velocity, delay, and packet loss through an iterative, batch-based process that quickly converges on optimal routes. By leveraging fog nodes near vehicles, the system performs real-time analysis and route selection, adapting swiftly to the dynamic topology and ensuring minimal transmission delay while maximizing throughput and packet delivery ratio. This approach addresses the challenges of rapid topology changes and resource constraints in VANETs, enabling reliable high-speed data transmission.For security, the system employs a lightweight ROTR encryption model that reduces encryption and decryption complexity by generating smaller, dynamic keys based on hash patterns and randomization. This encryption scheme, combined with fog computing, facilitates fast and secure data transmission without adding significant overhead, making it suitable for the high-speed requirements of vehicular networks. By integrating optimized routing with efficient cryptography, the methodology ensures data integrity, privacy, and low latency, providing a robust solution for simultaneous high-speed communication and security in highly dynamic VANET environments.

A. Batched Eagle Spotting Optimizer,
B. Random Off-The-Record.

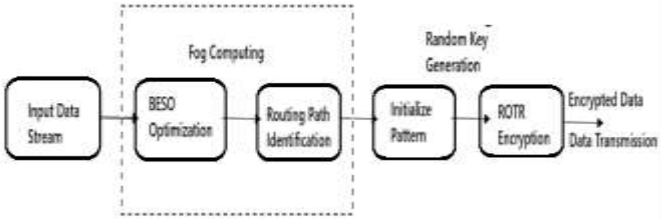

Fig 2. Overall flow of the proposed system

A. *Batched Eagle Spotting Optimizer*

The BESO algorithm is designed as a multi-objective optimizer that balances parameters such as transmission time and packet loss to select the most efficient routing path in VANETs. By incorporating fog computing into its objective function, the algorithm leverages edge-based processing to achieve better computation efficiency compared to traditional distance-based evaluation methods. It evaluates network conditions at each iteration to identify the convergence point, specifically targeting routes that minimize packet loss. The optimal path is determined by the convergence curve reaching the lowest packet transmission loss, ensuring reliable and swift data delivery across the highly dynamic vehicular network. The detailed step-by-step procedure and mathematical model of the BESO algorithm are provided in Algorithm 1, illustrating its systematic approach to real-time route optimization.

Algorithm 1: BESO algorithm

Input: Node array, $N = \{N_1, N_2, \dots N_n\}$ and Fog parameters $F_p = \{F_1, F_2, \dots F_n\}$

Output: Best nodes selection with enhanced speed transmission.Inputs include an array of nodes and fog parameters.

Step1:Iterative Optimization Process:

The outer loop runs until the maximum number of iterations (max_Iter) is reached or convergence is achieved.For each iteration, multiple particles (candidate routes) (q) are evaluated.

Step 2:Calculations for Each Particle:

Transmission time is calculated based on current network parameters.The time taken for each node (via a time cycle) and packet transmission over time samples are evaluated.Response times and packet counts per fog node (FOG) are computed, considering the number of nodes (NT) and service rate (SR).The average and total packets are derived from these calculations.Upper and lower limit fog nodes are estimated based on packet series and resource utilization.

Step 3:Path Selection:

Potential routing paths are collected from the lower to upper limit fog nodes.

Paths are sorted based on resource utilization and packet sizes.

Additional iterations adjust the parameters (angle difference calculation) for the upper limit fog nodes, selecting the best candidate path.

Step4: Evaluation and Convergence:

The fitness value (e.g., based on transmission delay or packet loss) is calculated.Particle positions are updated (i.e., candidate paths are refined).The best route candidates are assigned based on utilization.

Step 5:Convergence Check:

The standard deviation of the particles' positions is computed to estimate the convergence point.

If the system's performance measures indicate convergence (e.g., minimal packet loss or delay), the process terminates; otherwise, it continues.

This process enables dynamic, real-time selection of optimal routing paths in VANETs by balancing transmission efficiency and resource utilization, leveraging fog computing for edge processing.

Let the initial coordinates of the particles are initialized as $X_0.X_0 = X_{min} + (X_{max} - X_{min}) \times rand$ (1)

In the optimal routing protocol, the parameter update and weight value are derived from the transmission time, which is mathematically represented by equation (2). This equation likely relates to the transmission time between nodes, incorporating factors such as sending time and fetching time, to optimize routing decisions based on these temporal parameters.

$$T_{ij}(t) = FT\big(N(j)\big) - ST\big(N(j)\big) \qquad (2)$$

Where, ST – Sending time

FT – Fetching Time

$i = 1,2, \dots n$ // Index of nodes list

$j = 1,2, \dots m$ // Index of FOG list.

From this, the parameter extraction allows the calculation of the average packet transmission time along that temporary path, as described by equation (3). This involves measuring the total transmission duration across the selected route, considering factors such as node processing and link delays, to evaluate the efficiency of the path in terms of data transfer.

(3).

$$Average\ Transmission_F = \frac{\sum_{i=1}^{n} T_{(ij)}(t)}{Time_C \times m} \qquad (3)$$

Since, the objective function based on the Fog computing in equation (4).

$$L(F_j, t) = \frac{NT(T,t)}{SR(VM_j,t)} \qquad (4)$$

From this, the upper limit and the lower limit of the particle update can be validated and assigned to the relevant parameters are can be estimate by (5).

$$UL_{VM(j)} = \begin{cases} F(j), & if\ (L(j) > S(j) \\ \phi, & otherwise \end{cases} \qquad (5)$$

$$LL_{VM(j)} = \begin{cases} F(j), & if\ (L(j) < (S(j) - B) \\ \phi, & otherwise \end{cases} \qquad (6)$$

Where, S(j) – Maximum size of each FOG.

B – Boundary limit of FOG.

UL – Upper-limit of FOG.

LL – Lower-limit of FOG.

Validation of similarity matching with the parameters that are relevant to each factor. This can be represented as in the equation (7).

$$\theta = \alpha \times P_a + (1-\alpha) \times \frac{T_{CT(ij)}}{Time_C} \tag{7}$$

Where,

α – Similarity constant to find the boundary limit.

The similarity can be identified by using the cosine similarity index between the parameters.

$$angle = \cos^{-1}\left(T_{CT(ij)} \times \frac{P_{R_x}}{\left(\left|P_{R_y}\right|\left|P_{R_x}\right|\right)}\right) \tag{8}$$

The fitness value of the overall optimization function for the particles update was calculated by the ratio of Average data samples to the time required to transmit the data as in (9).

$$Fit = \frac{1}{Time_C} \times Average\ (N_F) \tag{9}$$

Then from the 'σ' parameter estimation, the convergence point can be find and select the best path as in (10).

$$\sigma = \sqrt{\frac{1}{m}\sum_{i=1}^{m}\left(T_j - T\right)^2} \tag{10}$$

Where,

$$SN = \frac{L(F_i,t)}{\sum L/t}, ST_N = \sum_{j=1}^{m} SN_j \tag{11}$$

From this parameter validation, the best routing path was selected in the VANET architecture and it was ready for the data transmission with enhanced speed of operation.

B. Network Security using ROTR

From the optimal routing system, the best path is to transmit the data with higher the transmission rate. Then to secure the data transmission with reduced size of data and the efficient key management, ROTR model of pattern generation technique was used to perform the light weighted hash pattern extraction. This design of data encryption system focused on the higher transmission quality and the better delivery ratio. Compare to the traditional model such as AES, DES, ECC and other types of encryption techniques, the key size was managed and the size was optimally used according to the properties of data streams that are to transmit over the network structure.

The detailed steps for the ROTR based data encryption model was described in the algorithm 2.

Algorithm 2: Random Off-The-Record (ROTR)

```
Input: Data input, $D_r$
Output: Encrypted Result $E_T$.
Step 1:Initialize Data Packet Loop
For each data packet, where 'n' is the total number of data packets or data chunks:

Step 2: Process Each Resource
For each resource involved in transmission:

Step 3:Calculate Key Pattern
Generate a random weight value for each related parameter of the data structure.
Use these weights to compute the key formation pattern, which will influence encryption.
Step 4:Manage Data Bins
While there are key bins available in the current data set: a. Find Data Bins
Identify the bins of data samples based on their timestamps or time-related parameters. b. Select Key Bits
Determine the appropriate key bits for encrypting the current data samples. c. Assign Coordinates
Map or assign coordinates for these key bits within a random sequence. d. Zero Out Irrelevant Bits
Set bits that do not contribute to the pattern to zero, optimizing the key size and pattern.

Step 5: Update Parameters
After processing each resource, update relevant parameters for all resources to adapt to the new key patterns and data states.

Step 6:Encrypt Data
Perform XOR operation between the data and the generated key to produce the encrypted data packet.

Step 7: Continue this process for all data packets and resources to ensure complete secure data transmission.

This stepwise breakdown facilitates understanding of how key patterns are dynamically generated and applied for lightweight encryption in high-speed VANET environments.
```

IV. RESULTS AND DISCUSSION

The simulation results and analysis of the proposed VANET routing system were conducted to evaluate and compare key performance parameters, specifically Packet Delivery Ratio (PDR) and delay rate, against existing routing protocols and security mechanisms. These parameters serve as indicators of throughput and the efficiency of packet transmission within the VANET architecture. The simulated VANET topology, depicted in Fig 3, comprises fog nodes at positions {2, 7, 12, 17} serving as connection points, and access points located at nodes {3, 10, 19}. The entire simulation was implemented using MATLAB/Simulink (version R2011b), and the results derived from data transmission structures demonstrate the Quality of Service (QoS) achieved by the proposed model in the network. The parameters that are considered for the comparison are can be listed as

1. Packet Delivery Ratio % (PDR),
2. Packet Loss Ratio % (PLR) and
3. Average Delay (ms)

A. Packet Delivery Ratio

The Packet Delivery Ratio (PDR) of equation (12) in VANET simulations measures the effectiveness of data transmission, indicating the percentage of packets successfully received at the destination relative to those sent by the source. It is calculated by taking the ratio of received packets to transmitted packets, as expressed in equation (12), and then multiplying by 100 to convert it into a percentage. A higher PDR reflects more reliable communication within the network.

$$PDR = \frac{Total\ No.\ of\ packets\ received\ at\ the\ receiver\ node}{Total\ No.\ of\ packets\ sent} \qquad (12)$$

The line graph in the Fig 4 and 5 shows the comparison result of proposed model with the other existing models of VANET routing system from [22] and [23] respectively.

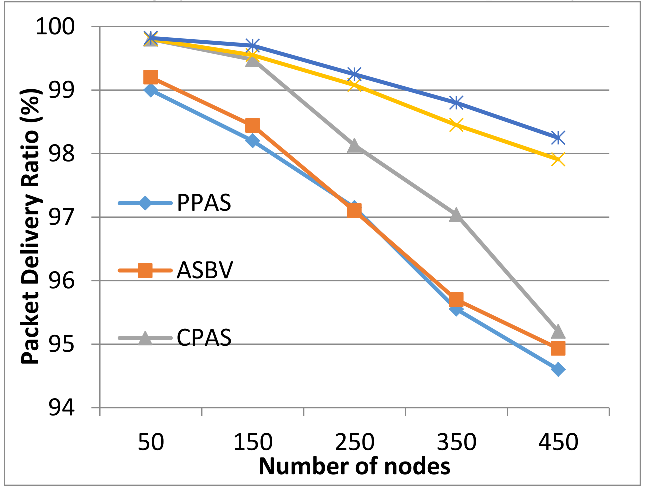

Fig 4. PDR analysis from [22]

This was also represented in the table result to find the linearity of this parameter and validate the performance of proposed routing model. The results are evaluated for the various number of node sequences such as {50, 150, 250, 350, 450}. This parameter refers the quality of data transmission by the proposed work with minimum amount of data loss than the other routing model.

Table 1. Comparison of PDR for the dynamic vehicle nodes from [22]

Number of nodes	Packet Delivery Ratio (%)				
	PPAS	ASBV	CPAS	PDS-QF	Proposed
50	99	99.2	99.8	99.8	99.82
150	98.2	98.44	99.48	99.55	99.7
250	97.15	97.1	98.13	99.08	99.25
350	95.55	95.7	97.04	98.45	98.8
450	94.6	94.93	95.2	97.91	98.25

Table 2. Comparison of PDR for the dynamic vehicle nodes from [23]

Number of nodes	Packet Delivery Ratio (%)				
	EIB	CPAS	ABAKA	SAES	Proposed
50	99.48	99.9	99.58	99.75	99.9
100	99.07	99.65	99.4	99.52	99.785
150	98.5	98.2	98.91	99	99.15
200	98.15	97.45	95.75	97.96	98.25

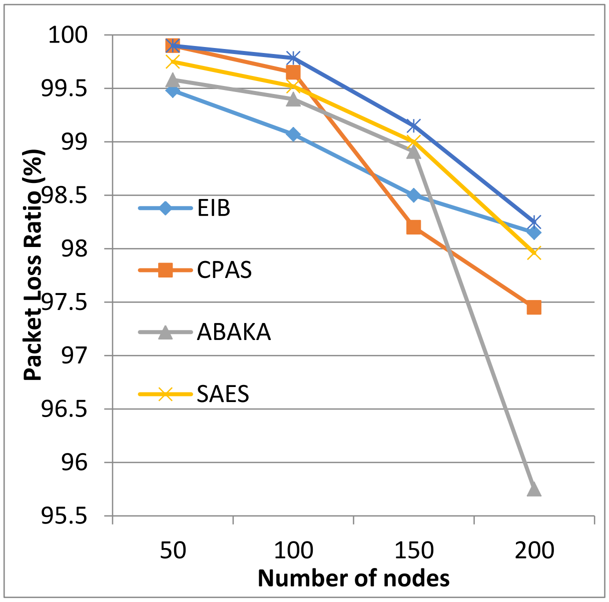

Fig 5. PDR analysis from [23]

B. *Packet Loss Ratio*

The BESO-ROTR based optimal routing system achieved the better transmission rate by referring the packet loss ratio. This parameter is to calculate the amount of packet that are not able to reach the destination which may failed to data loss. This is interpreted as in the equation (13).

$$PLR = 1 - PDR \qquad (13)$$

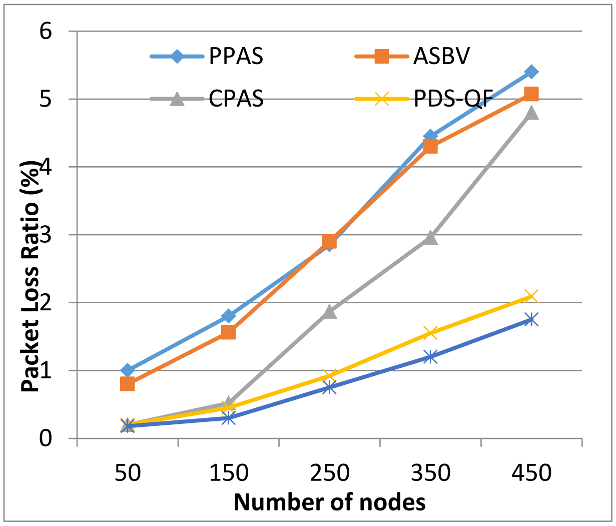

Fig 6. Packet loss ratio analysis from [22]

The Fig 6 and 7 shows the graphical representation of linear line plot with the comparison of PPAS, CPAS, ASBV and PDS-QF methods of routing and security system in the VANET architecture. In that graph results, it shows that the proposed work achieved less packet loss than other methods.

This was also shown in the Table 3 result for the nodes from 50 to 450 number of vehicles.

Table 3. Comparison of Packet Loss Ratio (%) with different methods in VANET architecture from [22]

Number of nodes	Packet Loss Ratio (%)				
	PPAS	ASBV	CPAS	PDS-QF	Proposed
50	1	0.8	0.2	0.2	0.18
150	1.8	1.56	0.52	0.45	0.3
250	2.85	2.9	1.87	0.92	0.75
350	4.45	4.3	2.96	1.55	1.2
450	5.4	5.07	4.8	2.09	1.75

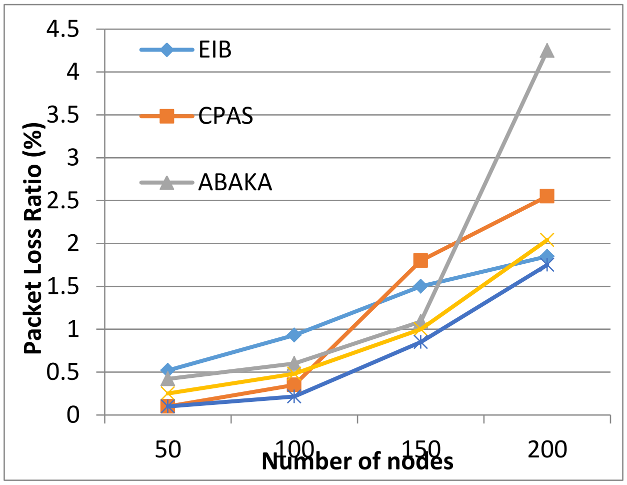

Fig 7. Packet loss ratio analysis from [23]

Table 4. Comparison of Packet Loss Ratio (%) with different methods in VANET architecture from [23]

Number of nodes	Packet Loss Ratio (%)				
	EIB	CPAS	ABAKA	SAES	Proposed
50	0.52	0.1	0.42	0.25	0.1
100	0.93	0.35	0.6	0.48	0.215
150	1.5	1.8	1.09	1	0.85
200	1.85	2.55	4.25	2.04	1.75

C. *Average Delay Rate*

The transmission delay in the VANET network was evaluated under conditions simulating dynamic node structures consistent with the designed VANET architecture. This analysis focused on assessing system throughput and related performance parameters by measuring the delay rate for packet transmission from sender to receiver. The evaluation considered scenarios involving high-speed moving vehicles and the coverage range parameters of the network model. The results indicated that the proposed approach achieves lower delay rates within the millisecond range compared to existing methods, demonstrating improved efficiency in high-mobility environments.

The Fig 8 and 9 shows the comparison graph of average delay for the VANET architecture for different number of node arrangement. The table 5 and 6 shows the table representation of the comparison result from [22] and [23]. From these parameter analysis, the proposed model achieved less delay rate (ms) than other existing methods.

Table 5. Average Delay (ms) comparison with [22]

Number of nodes	Average Delay (ms)				
	PPAS	ASBV	CPAS	PDS-QF	Proposed
50	0.95	0.78	0.75	0.745	0.735
150	0.98	0.85	0.81	0.8	0.79
250	1.35	1.03	0.84	0.825	0.81
350	2.15	1.95	1	0.83	0.815
450	2.9	2.55	1.85	1.02	0.95

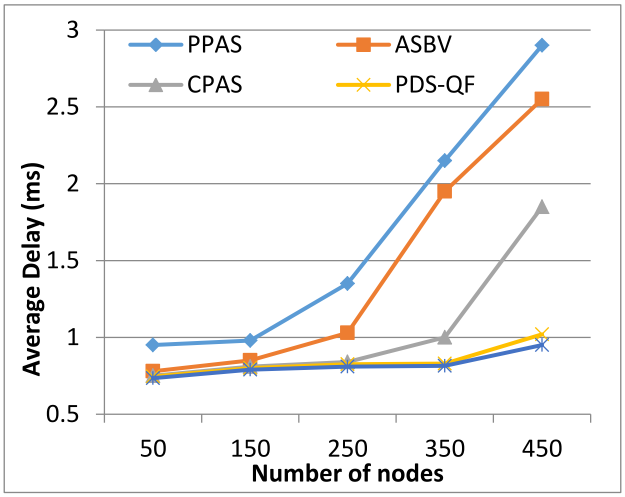

Fig 8. Average Delay (ms) chart comparison with [22]

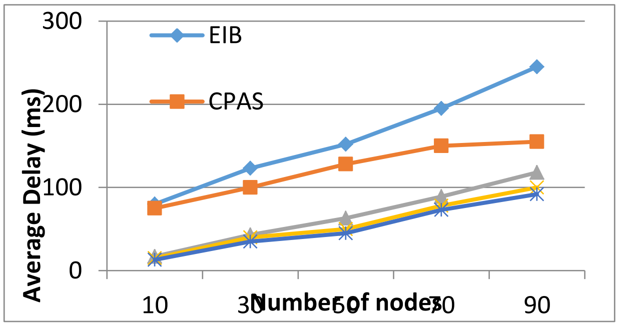

Fig 9. Average Delay (ms) chart comparison with [23]

Table 6. Average Delay (ms) comparison with [23]

Number of nodes	Average Delay (ms)				
	EIB	CPAS	ABAKA	SAES	Proposed
10	80	75	17	15	13
30	123	100	43	40	35
50	152	128	63	50	45
70	195	150	89	78	73
90	245	155	118	100	92

Based on comprehensive analysis, the BESO optimization algorithm demonstrated superior performance in predicting and selecting optimal routing paths. Additionally, the ROTR-based security mechanism improved key management during data transmission within the VANET framework that leverages fog computing architecture.

V. CONCLUSION

This Paper introduces an innovative VANET security framework that incorporates an optimal routing protocol to facilitate high-speed data transfer. The proposed Batched Eagle Spotting Optimizer (BESO) algorithm efficiently identifies the best routing paths within a highly dynamic network, resulting in superior packet delivery ratios compared to existing protocols. By integrating fog computing, the system enhances prediction accuracy and improves the routing process for effective data retrieval from cloud platforms. Additionally, the use of the Light-Weight Random Off-The-Record (ROTR) encryption scheme ensures faster data transmission and higher throughput. Analytical evaluations demonstrate that the proposed approach reduces delay times and minimizes packet loss across varying vehicle densities, effectively accommodating the continuous mobility and velocity changes of vehicles within the network coverage.
Future improvements in VANET architectures can be achieved by integrating advanced machine learning techniques with optimization functions within fog computing environments, enabling adaptive and predictive routing protocols that dynamically respond to network conditions and security threats. Additionally, focusing on space complexity through efficient key management schemes—such as lightweight, scalable, and dynamic key distribution methods—can enhance security while minimizing storage and computational overhead, ensuring high-speed, reliable, and secure data transmission essential for VANET applications.

ACKNOWLEDGEMENT

We sincerely thank Vemana Institute of Technology for their resources and support during this research.

REFERENCES

[1] R. Oliveira, C. Montez, A. Boukerche, and M. S. Wangham, “Reliable data dissemination protocol for VANET traffic safety applications,” *Ad Hoc Networks*, vol. 63, pp. 30-44, 2017.

[2] M. Chahal, and S. Harit, “A stable and reliable data dissemination scheme based on intelligent forwarding in VANETs,” *International Journal of Communication Systems*, vol. 32, no. 3, pp. e3869, 2019.

[3] P. Manickam, K. Shankar, E. Perumal, M. Ilayaraja, and K. S. Kumar, "Secure data transmission through reliable vehicles in VANET using optimal lightweight cryptography," *Cybersecurity and secure information systems*, pp. 193-204: Springer, 2019.

[4] J. Wu, H. Lu, Y. Xiang, R. Wu, and F. Wang, “MBR: A Map-Based Relaying Algorithm For Reliable Data Transmission Through Intersection in VANETs,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 10, pp. 3661-3674, 2018.

[5] W. Li, W. Song, Q. Lu, and C. Yue, “Reliable congestion control mechanism for safety applications in urban VANETs,” *Ad Hoc Networks*, vol. 98, pp. 102033, 2020.

[6] J. Aredla, S. Zhang, and E. Liu, "An Adaptive and Reliable Communication Method for Road Safety Applications of VANET." pp. 1-6.

[7] A. Amuthan, and R. Kaviarasan, “Weighted inertia-based dynamic virtual bat algorithm to detect NLOS nodes for reliable data dissemination in VANETs,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 11, pp. 4603-4613, 2019.

[8] M. Kim, and C. Joo, “Prediction-based reliable data forwarding method in VANET,” *The Journal of Korean Institute of Communications and Information Sciences*, vol. 42, no. 1, pp. 128-139, 2017.

[9] A. Katiyar, D. Singh, and R. S. Yadav, “State-of-the-art approach to clustering protocols in vanet: a survey,” *Wireless Networks*, vol. 26, no. 7, pp. 5307-5336, 2020.

[10] S. A. Rashid, M. M. Hamdi, and S. Alani, "An overview on quality of service and data dissemination in VANETs." pp. 1-5.

[11] V. Velmurugan, and J. M. L. Manickam, “A efficient and reliable communication to reduce broadcast storms in VANET protocol,” *Cluster Computing*, vol. 22, no. 6, pp. 14099-14105, 2019.

[12] S. Bouakkaz, and F. Semchedine, “A certificateless ring signature scheme with batch verification for applications in VANET,” *Journal of Information Security and Applications*, vol. 55, pp. 102669, 2020.

[13] S. Wang, K. Mao, F. Zhan, and D. Liu, “Hybrid conditional privacy-preserving authentication scheme for VANETs,” *Peer-to-Peer Networking and Applications*, vol. 13, pp. 1600-1615, 2020.

[14] M. Usha, and B. Ramakrishnan, “Robust MPR: a novel algorithm for secure and efficient data transmission in VANET,” *Wireless Personal Communications*, vol. 110, no. 1, pp. 355-380, 2020.

[15] M. N. Yasir, and M. S. Croock, “Software engineering based self-checking process for cyber security system in VANET,” *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 10, no. 6, 2020.

[16] A. Malik, and B. Pandey, “CIAS: a comprehensive identity authentication scheme for providing security in VANET,” *International Journal of Information Security and Privacy (IJISP)*, vol. 12, no. 1, pp. 29-41, 2018.

[17] X. Zhang, R. Li, and B. Cui, "A security architecture of VANET based on blockchain and mobile edge computing." pp. 258-259.

[18] P. Agarwal, “Technical review on different applications, challenges and security in VANET,” *J. Multimed. Technol. Recent Adv*, vol. 4, no. 3, pp. 21-30, 2017.

[19] M. B. Mansour, C. Salama, H. K. Mohamed, and S. A. Hammad, “VANET security and privacy-an overview,” *International Journal of Network Security & Its Applications (IJNSA) Vol*, vol. 10, 2018.

[20] X. Yao, X. Zhang, H. Ning, and P. Li, “Using trust model to ensure reliable data acquisition in VANETs,” *Ad Hoc Networks*, vol. 55, pp. 107-118, 2017.

[21] C. A. Kerrache, N. Lagraa, C. T. Calafate, and A. Lakas, “TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs,” *Vehicular Communications*, vol. 9, pp. 254-267, 2017.

[22] Soleymani, Seyed Ahmad, et al. "A security and privacy scheme based on node and message authentication and trust in fog-enabled VANET." *Vehicular Communications* 29 (2021): 100335.

[23] Jiang, Haobin, Lei Hua, and Lukuman Wahab. "SAES: a self-checking authentication scheme with higher efficiency and security for VANET." *Peer-to-Peer Networking and Applications* 14.2 (2021): 528-540.