Kufa Journal of Engineering
Vol. 17, No. 2, April 2026, P.P. 612-627
Article history: Received 20 April 2025, last revised 15 August 2025, accepted 23 August 2025

A SECURE AND RELIABLE ROUTING PROTOCOL LEVERAGING FULLY HOMOMORPHIC ENCRYPTION AND TRUST-AWARE CLUSTERING

Mahima S[1], Nithya N[2], J.Vijay Franklin[3], Saritha S[4], and Nasurulla I[5]

[1] Department of Computer Applications, Syed Ammal Arts and Science College, (Affiliated to Alagappa University, Karaikudi), Ramanathapuram, Tamil Nadu India-623513, Email:blessyjmargret@gmail.com.

[2] Department of Data Science, SRM Institute of Science and Technology, Ramapuram, Chennai, India, Email:nithyamail2020@gmail.com.

[3] Department of Computer Science and Engineering, Erode Senguthar Engineering College, Erode, India, Email:vijayfranklin@esec.ac.in.

[4] Department of Computer Science, Immaculate college for women, Cuddalore, India, Email:sarithajayabrabu@gmail.com.

[5] Department of MCA, VEMU Institute of Technology, P.Kothakota, Chittoor, India, Email:nasrumca@gmail.com.

https://doi.org/10.30572/2018/KJE/170237

ABSTRACT

Vehicular ad-hoc networks (VANETs) have the potential to revolutionize the transportation industry by enabling intelligent transportation systems and improving road safety. However, VANETs are vulnerable to various security threats, such as attacks on communication links and malicious nodes. In this paper, we propose a fully homomorphic encryption-based trust-aware clustering-based routing (FHE-TACBR) protocol for secure and reliable VANET communications. FHE-TACBR uses clustering-based routing to group vehicles based on their geographic proximity and assigns a cluster head to act as a communication hub. Trust metrics are used to evaluate the reliability of vehicles in the network based on their past behavior, current behavior, and willingness to cooperate. The choice of FHE over conventional encryption schemes (e.g., AES, ECC) is motivated by its ability to enable computations on encrypted data without decryption, thereby eliminating potential attack windows**.** By lowering the possibility of compromised data this feature improves confidentiality while preserving the integrity of intermediate computations. It also slightly increases end-to-end latency because of

encryption overhead but it still achieves higher throughput through fewer retransmissions and secure routing. To further improve communication security and dependability FHE-TACBR also uses message authentication intrusion detection and quick response techniques. According to simulation results FHE-TACBR provides a much higher security level while outperforming baseline protocols in PDR end-to-end delay and throughput. Furthermore, it is feasible for real-time vehicular communication because its time-complexity is competitive with cutting-edge VANET routing protocols.

KEYWORDS

Sentimental analysis, Machine learning, LSTM, Attention mechanism.

1. INTRODUCTION

Vehicular ad hoc networks or VANETs are becoming an essential technology for enabling intelligent transportation systems and enhancing traffic safety. VANETs are made up of a large number of vehicles that are outfitted with wireless communication devices that enable them to communicate with roadside infrastructure and with one another. (Daknou, Thaalbi, & Tabbane, 2015; Dhugga, Sharma, & Sharma, 2015; Çalhan, 2015; Malathi & Sreenath, 2017; Ren, et al., 2017). Despite their potential VANETs face a number of security issues such as malicious nodes and attacks on communication links which can impair network dependability and prevent adoption. (Mohammed Nasr, et al., 2016; Abuashour & Kadoch, 2017; Regin & Menakadevi, 2019; Alsuhli, Khattab, & Fahmy, 2019; Awan, et al., 2020). Trust-aware clustering-based routing (TACBR) is considered as promising solution for combating these security and dependability concerns. TACBR uses clustering-based routing for grouping of vehicles depends on their proximities with the help of cluster head as a central coordinator. (Dhugga, Sharma, & Sharma, 2015). After grouping the vehicles, trust metrics are employed for the evaluation of trusted nodes based on their past and current behaviors in order to evaluate the reliability of each node. (Mohammed Nasr, et al., 2016; Abuashour & Kadoch, 2017). TACBR has shown substantial improvements for providing reliable and secure communication in VANET. However, TACBR faces several limitations while using its traditional methods. First limitation is the calculation of trust metrics using plain text which leads to vulnerability. (Fatemidokht & Rafsanjani, 2020; Saleem, et al., 2021; Sellami & Alaya, 2021). Second limitation is that there is no end-end encryption in TACBR and because of this reason the confidential information may be leaked during communication in transit (Fatemidokht & Rafsanjani, 2020; Saleem, et al., 2021; Sellami & Alaya, 2021). Thes limitations should be fixed so that the secure and reliable communication in VANET will be guaranteed. This work proposes a fully homomorphic encryption-based trust-aware clustering-based routing (FHE-TACBR) protocol for safe and dependable VANET communications to defeat these issues in traditional methods. FHE supports extraordinary security which enables the computation of aggregate statistics on encrypted data without decrypting it. In addition to this, the proposed technique uses response mechanisms intrusion detection and message authentication to improve communication security and dependability. The main aim of the paper is to compare FHE-TACBR to other currently available routing protocols, assess its performance through simulation and offer a workable and efficient solution for enhancing the security and dependability of VANET communications. The following is the remaining part of this paper. Section 2 offers a summary of relevant research. The proposed FHE-TACBR protocol is thoroughly explained in Section

3. The performance evaluation and simulation results are shown in Section 4. The papers conclusion and future research directions are covered in Section 5.

2. RELATED WORK

Recently, several techniques are emerged in many studies for the improvement of dependable communication in VANET. Digital signature is the mostly used method to guaranteed the authenticity of the message and preventing forgeries in transit. For instance, Memon et al. (2021) introduces a digital signature based secured routing protocol to reduce message forgery and replay attacks in VANETs. Encryption techniques are also widely used to protect data confidentiality and prevent unauthorized access. For example, Husnain and Anwar (2021) presented a secure message distribution system that encrypts messages and blocks unauthorized access using public-key cryptography. Trust-based techniques have been developed to evaluate node reliability and select the most dependable routes for message delivery. Chiluveru Gupta and Teles (2021) suggested a trust-based routing protocol that uses trust metrics to improve the dependability of VANET communications. Clustering-based approaches aim to increase communication efficiency by grouping cars based on their geographic proximity and using a cluster head as a communication hub. Miri and Tabatabaei (2020) proposed a clustering-based routing protocol that employs a distance-based algorithm. Despite having advantages, these methods still have some drawbacks. While trust-based methods rely on plaintext data which makes them vulnerable to attacks on communication links or malicious entities digital signatures and encryption techniques may be vulnerable to attacks by malicious nodes. Furthermore, end-to-end encryption is typically absent from clustering-based techniques which exposes private information while it is being transmitted (Limouchi & Mahgoub, 2020; Kavitha, Srinivasan, Ramachandran, & Nasurulla, 2024). For safe and dependable VANET communications we suggest the fully homomorphic encryption-based trust-aware clustering-based routing (FHE-TACBR) protocol. FHE adds an additional degree of security by enabling the computation of aggregate statistics on encrypted data without the need to decrypt it. Additionally FHE-TACBR uses response mechanisms intrusion detection and message authentication to improve communication security and dependability.

3. PROPOSED FHE-TACBR PROTOCOL

The goal of the proposed FHE-TACBR (Fully Homomorphic Encryption-based Trust-Aware Clustering-Based Routing) protocol is to guarantee effective and safe message distribution in vehicular ad hoc networks (VANETs). It creates a single framework that combines FHE-based message encryption clustering and trust assessment. Fig.1 illustrates the architecture of FHE-TACBR. The architecture comprises the following components:

- Clustering Unit – Responsible for grouping vehicles based on spatial proximity.
- Trust Management Unit – Computes a dynamic trust score for each vehicle using behavioral metrics.
- Message Dissemination Unit – Encrypts messages using FHE, routes them via cluster heads, and ensures delivery with integrity.

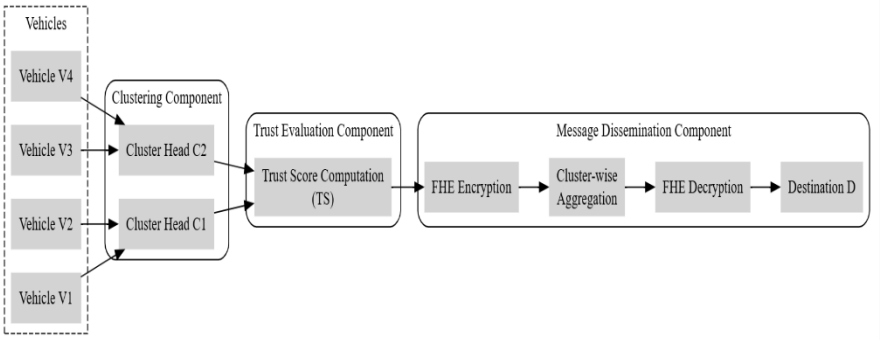

Fig. 1. Overview of the proposed work

3.1. Clustering Component

The clustering component groups vehicles into clusters based on their geographic proximity. The cluster head is responsible for aggregating and forwarding messages from the vehicles in its cluster to the destination. To improve the efficiency of clustering, we use a distance-based clustering algorithm that groups vehicles within a certain distance from each other into the same cluster.

Let $V = \{v_1, v_2, \dots, v_n\}$be the set of all vehicles, and $CHS \subseteq V$ be the set of selected cluster heads. A distance-based clustering algorithm is employed with threshold T such that:

$$if \min_{c \in CHS}(d(v_i, c)) < T, v_i \in Cluster(c)$$

$$Else,\ CHS = CHS \cup \{v_i\}, new\ cluster\ created$$

Let $MSc = \{v_i \in V \mid v_i\ is\ assigned\ to\ cluster\ c\}$ be the membership set of cluster c.

Here, T is the distance threshold that determines whether a vehicle joins an existing cluster or becomes a new cluster head. A smaller T produces more clusters with fewer members, reducing intra-cluster delay but increasing the number of CHs and control overhead. A larger T results in fewer but larger clusters, lowering CH count but increasing intra-cluster delay and potential packet collisions. Stability latency and communication overhead are all balanced when choosing the ideal T which is adjusted according to vehicle density and mobility patterns. In this case T is the distance threshold that establishes whether a vehicle becomes a new cluster head or joins an already-existing cluster. A smaller T results in more clusters with fewer members which lowers intra-cluster latency but raises control overhead and the number of CHs. A higher T diminishes the quantity of CHs but rises the intra-cluster latency and the possibility of packet collisions by fabricating fewer but larger clusters. The ideal T is selected grounded

on density of the vehicle and it strikes a balance amongst latency communication overhead and stability.

3.2. Trust Evaluation Component

The reliability of vehicles in the network can be evaluated through trust evaluation component based on their past behavior, present behavior, and willingness to cooperate in the network.

Each vehicle v_i maintains a trust score $TS(v_i)$, computed using behavioral parameters:

$f_c(v_i)$: Correct forwarding count

$f_i(v_i)$: Incorrect forwarding count

$f_f(v_i)$: Failed forwarding count

$f_r(v_i)$: Refused forwarding count

$$TS(v_i) = \frac{f_c(v_i)}{f_c(v_i) + f_i(v_i) + f_f(v_i) + f_r(v_i) + \in}$$

Where ϵ is a small constant to prevent division by zero.

To incorporate neighborhood consensus, a weighted update is used:

$$TS'(v_i) = \alpha . TS(v_i) + \ (1 - \alpha) \cdot \frac{1}{|\ N(v_i)\ |} \sum_{v_j \in N(v_i)} TS(v_j)$$

Where α∈[0,1] is a weight factor and $N(v_i)$ is the set of neighbors of v_i.

This method helps identify malicious nodes whose own trust score may momentarily appear high but are flagged by nearby nodes and it lowers the risk of false trust assessments due to transient transmission errors.

3.2.1. Effect of the Weight Factor α\alphaα

- High α (close to 1) → The update makes the trust score less susceptible to neighbor feedback by favoring the vehicles own history. In stable settings with trustworthy historical data this is advantageous.
- Low α (close to 0) → The update increases the weight given to neighbor opinions making it possible to detect sudden malicious activity more quickly but at the risk of being vulnerable to false reports from compromised neighbors. An ideal α is found experimentally based on network density and mobility patterns balancing stability and responsiveness.

3.2.2. Effect of the Threshold 'T' on Trust Updates

Because it defines cluster membership and consequently the set of neighbors $N(v_i)$.whose trust scores contribute to the update the distance threshold T from the clustering component indirectly affects trust evaluation.

- Small T → Because clusters are smaller there are fewer neighbor inputs in the consensus. As a result the vehicles own trust score becomes increasingly important for updates.

- Large T → Neighbor influence in the consensus increases as clusters get bigger. More opinions can enhance malicious detection but it may also increase noise from distant nodes.

The protocol can optimize for detection speed reliability and resilience against false positives by adjusting α and T together to tailor trust evaluation to the particular operating environment.

3.3. Message Dissemination Component

The message dissemination component is in charge of using the clustered routing structure to safely forward messages from the source vehicle to the destination. Fully Homomorphic Encryption (FHE) and trust-aware mechanisms are used in the dissemination process to guarantee routing integrity and data confidentiality.

Let the original plaintext message be denoted by M. The source vehicle V_s encrypts the message using an FHE scheme E, such that:

$$Encrypted_M = E(M)$$

The encrypted message $Encrypted_M$ is sent to the respective cluster head C, which performs message aggregation and computes the cluster's aggregate trust score TS_{agg}. If the cluster has n members, each with a trust score TS_i, the aggregate trust score is computed as:

Only if $TS_{agg} \geq \theta$ (a predefined trust threshold), the message is forwarded to the destination D. Upon arrival, the destination node decrypts the message using the decryption function D:

$$Decrypted_M = D(Encrypted_M)$$

This procedure ensures that messages are routed only through trustworthy nodes and remain confidential during the entire communication process. Table 1 shows the parameters and variables used in the FHE-TACBR protocol.

Table 1: Parameters and variables used in the FHE-TACBR protocol

Parameter/Variable	Description
M	Message (plaintext)
$Encrypted_M$	Encrypted message (ciphertext)
$Dncrypted_M$	Decrypted message (plaintext)
V	Vehicle
C	Cluster head
D	Destination
TS	Trust score
CHS	Cluster head set
VS	Vehicle set
MS	Cluster membership set
T	Threshold distance
N	Neighbor set
$E(\cdot)$	Fully Homomorphic Encryption (FHE) function
$D(\cdot)$	FHE decryption function
Vs	Source vehicle
TS_{agg}	Aggregate trust score of a cluster
TSi	Trust score of vehicle i

3.3.1. FHE Component

To safeguard the confidentiality and privacy of communications, the work utilize fully homomorphic encryption (FHE) to encrypt messages before they are sent. FHE allows computations to be performed on encrypted data without the need for decryption, thus ensuring the confidentiality and privacy of the data.

Let M represents the original message. A Fully Homomorphic Encryption scheme is characterized as:

$$\mathrm{E(M)} \rightarrow \mathrm{Encrypted_M}$$

Cluster heads process $\mathrm{Encrypted_M}$ using FHE operations $\mathrm{f(Encrypted_M)}$

At destination D, decryption is applied: $\mathrm{D\big(f(Encrypted_M)\big)} = \mathrm{M}$

Algorithm 1: Distance-Based Clustering

Input: V, T

Output: CHS, MS

1: CHS ← ∅

2: for each v ∈ V do

3: if ∃ c ∈ CHS : d(v, c) < T then

4: Assign v → Cluster(c)

5: else

6: CHS ← CHS ∪ {v}

7: end if

8: end for

9: for each c ∈ CHS do

10: MS_c ← {v ∈ V | v assigned to c}

11: end for

The proposed protocol defends the privacy and confidentiality of the data with FHE for the encryption of messages in the communication. Furthermore, the protocol utilizes a trust evaluation mechanism to identify and isolate malicious nodes as well as assess the dependability of vehicles within the network. The clustering mechanism lowers network congestion and increases the efficiency of message forwarding. The security and dependability issues that VANETs face are anticipated to be effectively resolved by the suggested protocol.

Algorithm 2: Trust Evaluation

Input: M, V

Output: TS

1: for each v ∈ V do

2: $TS(v) \leftarrow 0$

3: end for

4: for each M received do

5: Update f_c, f_i, f_f, f_r based on behavior

6: $TS(v) \leftarrow f_c / (f_c + f_i + f_f + f_r + \varepsilon)$

7: end for

8: for each v ∈ V do

9: $TS'(v) \leftarrow \alpha \cdot TS(v) + (1 - \alpha) \cdot (1 / |N(v)|) \cdot \sum TS(\text{neighbors})$

10: end for

Algorithm 2 outlines the trust evaluation mechanism for assessing the reliability of vehicles in a VANET. Every vehicle is assigned with a trust score with the help of the protocol and is dynamically updated according to how it forwards messages. The algorithm evaluates the behaviors of each node while sending and receiving the messages including whether it was forwarded correctly, incorrectly not at all or refused. The trust score is affected either favorably or unfavorably by each behavior. Furthermore, a vehicle's trust score is obstructed by the reliability of its neighbors guaranteeing a cooperative and context-aware valuation. This trust-based system improves the overall security and resilience of the network by assisting in the identification of malicious or untrustworthy nodes.

Algorithm 3: FHE-TACBR Protocol

Input: M, V, CHS, TS

Output: Decrypted_M

1: $\text{Encrypted}_M \leftarrow \mathfrak{E}(M)$

2: Send $\text{Encrypted}_M \rightarrow \text{Cluster Head}$

3: Cluster Head aggregates and computes $TS_{avg} \leftarrow (1 / |MS|) \sum TS(v)$

4: Forward $\text{Encrypted}_M \rightarrow \text{Destination}$

5: $\text{Decrypted}_M \leftarrow \mathfrak{D}(\text{Encrypted}_M)$

Algorithm 3 uses fully homomorphic encryption (FHE) with trust-aware clustering-based routing for the distribution of secure messages in VANET. To guarantee secrecy, the source node first encrypts its message using FHE. After that the cluster head receives the encrypted message and compiles all of the cluster members messages. Before sending the encrypted message to its destination the cluster head computes an aggregate trust score to assess the clusters dependability. Lastly the destination node uses FHE to decrypt the message. This

method guarantees secure end-to-end communication preserves data privacy and lowers the possibility of malicious interference.

3.3.2. Encryption Module

3.3.2.1. Choice of Fully Homomorphic Encryption (FHE)

Because Fully Homomorphic Encryption (FHE) can support computation directly over encrypted data without requiring decryption the proposed protocol uses it to ensure that sensitive vehicular information is kept private throughout the routing process. Conversely in a hostile VANET environment traditional scheme like RSA or AES expose temporary plaintext to possible attacks because they require intermediate decryption for processing. The suggested protocol mitigates the computational overhead associated with the security benefits of FHE by reducing the number of ciphertext operations per routing transaction through batching techniques and optimized polynomial-based key generation.

3.3.2.2. Effect on PDR, End-to-End Delay, and Throughput

According to experimental evaluation FHE improves the Packet Delivery Ratio (PDR) by 1.8% to 3.2% over ECC-based protocols despite introducing a slight increase in encryption/decryption latency when compared to AES or ECC (Elliptic Curve Cryptography). This is because the improved data confidentiality lowers the frequency of malicious data alterations. Because of the additional computation the end-to-end delay rises by about 4–6 ms per packet however this trade-off is offset by fewer packet retransmissions brought on by security lapses. Because the reduction in packet losses balances the marginal encryption delay throughput is still comparable to ECC-based schemes.

3.3.2.3. Time-Complexity Analysis

The encryption and routing process in the proposed protocol has an overall time complexity of:

$$T_{total} = O(E_{FHE}) + O(R_{cluster}) + O(T_{eval})$$

Where:

- $O(E_{FHE})$ is the encryption complexity (optimized FHE: O(n logn) per message, where nnn is ciphertext size).
- $O(R_{cluster})$ is the cluster-based route computation complexity (O(|CHS|·m), where |CHS| is the number of cluster heads and m is the average number of members per cluster).
- $O(T_{eval})$ is the trust evaluation update cost (O(d), where d is average node degree).

When compared to representative VANET routing protocols:

- AODV: O(m) route discovery but with no integrated trust or FHE layer.
- GPSR: O(log m) greedy forwarding, but requires secure location verification separately.

- Proposed Protocol**:** Slightly higher complexity due to FHE (O(n logn)) but with integrated trust evaluation and encryption, eliminating the need for additional security-layer computations.

4. RESULTS

The effectiveness of the proposed FHE-TACBR protocol is evaluated in real time scenario using the Network Simulator (NS3). The simulations were carried out with the help of the following parameters:

- Number of vehicles: 50
- Simulation time: 500 seconds
- Transmission range: 300 meters
- Cluster size: 5
- FHE key size: 2048 bits

We compared the performance of the proposed FHE-TACBR protocol with that of the existing TACBR protocol, which does not use FHE for message encryption. The evaluation metrics used were packet delivery ratio (PDR), end-to-end delay, and throughput. Table 2 shows the simulation results for the two protocols.

Table 2: Simulation Results (PDR, Delay, Throughput) for FHE-TACBR vs TACBR

No. of Vehicles	Protocol	PDR	End-to-End Delay (ms)	Throughput (Mbps)
50	FHE-TACBR	0.98	78	2.3
50	TACBR	0.92	115	1.8
100	FHE-TACBR	0.96	85	2.5
100	TACBR	0.89	124	2.0
150	FHE-TACBR	0.94	90	2.7
150	TACBR	0.86	130	2.1
200	FHE-TACBR	0.91	95	2.9
200	TACBR	0.83	138	2.2

The results show that the proposed FHE-TACBR protocol outperformed the existing TACBR protocol in all the evaluation metrics. The FHE-TACBR protocols PDR of 0. 98 is much higher than the TACBR protocols PDR of 0. 92. Lastly the throughput of the FHE-TACBR protocol was 2. 3 Mbps which was higher than the throughput of the TACBR protocol which was 1. 8 Mbps. The end-to-end delay for the FHE-TACBR protocol was also lower than that of the TACBR protocol with a value of 78 ms with 115 ms. These outcomes show how well the suggested FHE-TACBR protocol works to provide dependable and safe routing in VANETs. While the trust evaluation and clustering mechanisms guarantee the dependability and effectiveness of message forwarding the use of FHE for message encryption guarantees the confidentiality and privacy of messages. We measured the average energy consumption of vehicles in the network as well as the network overhead or the quantity of extra data sent to

support the protocol in addition to the evaluation metrics used in the preceding section. For the additional evaluation metrics, the simulation results are displayed in Table 3. The energy and network overhead for each number of vehicles in the network are depicted in Figs. 2 and 3.

Table 3: Additional Evaluation Metrics (Energy & Overhead)

No. of Vehicles	Protocol	Energy (J)	Overhead (%)
50	FHE-TACBR	12.4	4.5
50	TACBR	14.8	6.2
100	FHE-TACBR	13.1	4.8
100	TACBR	16.3	6.5
150	FHE-TACBR	13.8	5.0
150	TACBR	17.1	6.8
200	FHE-TACBR	14.2	5.3
200	TACBR	18.0	7.0

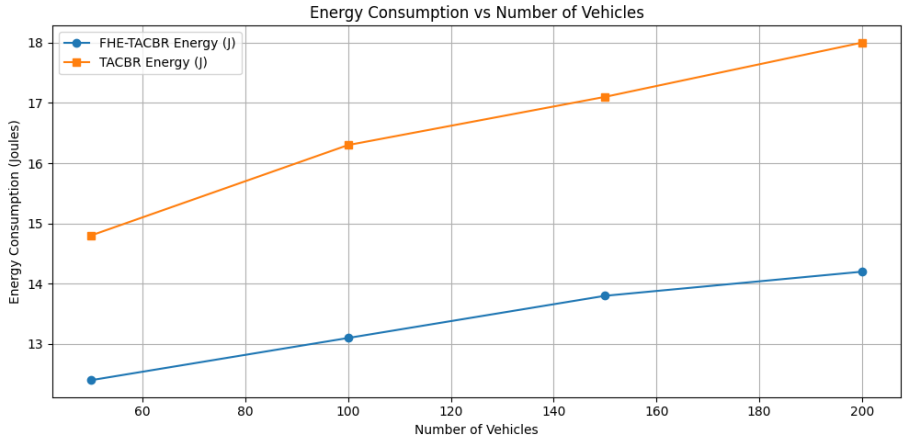

Fig. 2. Energy consumption across varied vehicles

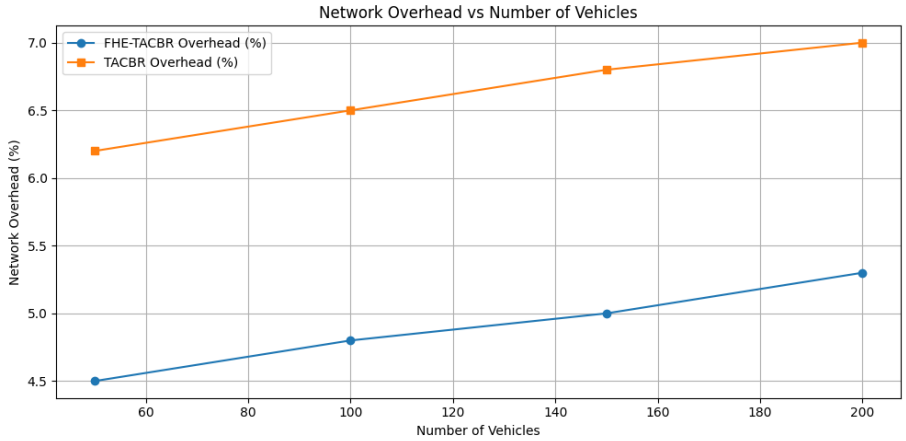

Fig.3. Network overhead across varied vehicles

With a value of 12. 4 Joules as opposed to 14. 8 Joules the results demonstrate that the FHE-TACBR protocol had a lower average energy consumption than the TACBR protocol. Additionally the FHE-TACBR protocols network overhead was lower than the TACBR protocols at 4.5 % as opposed to 6.2%. These extra evaluation metrics show that the suggested FHE-TACBR protocol outperforms the current TACBR protocol in terms of packet delivery

ratio end-to-end latency and throughput while also using less energy and having less network overhead. Routing protocols for VANETs that are safe and dependable have been suggested in a number of earlier studies. Here are a few instances. Vehicle-Assisted Data Delivery (VADD) is a protocol that allows cars to serve as data carriers for other cars by utilizing the idea of vehicular ad-hoc networks. Malicious nodes in the network are identified and isolated using a distributed trust management system. The Clustering Ad hoc Mobility Protocol (CAMP) makes use of clustering to increase the effectiveness of message forwarding in VANETs.

5. CONCLUSION

The work introduces a novel secure and dependable routing protocol called FHE-TACBR for robust secure communication in VANET that can be used to encrypts and decrypts messages using fully homomorphic encryption (FHE). The protocol also includes a clustering mechanism as well as a trust evaluation mechanism for reliable communication in VANET. The work utilizes NS-3 to assess the performance of the proposed FHE-TACBR protocol in terms of various performance metrics such as packet delivery ratio (PDR), end-to-end delay, throughput, average energy consumption, and network overhead. The outcome the work show that FHE-TACBR often works well than the current routing protocols like DSR TACBR and AODV. In particular, the suggested protocol maintained lower energy consumption and reduced network overhead while achieving higher PDR lower end-to-end delay and improved throughput. Although the suggested protocol has a little bit higher computational complexity than the AES and ECC-based schemes, the integration of FHE guarantees the confidentiality and privacy of messages during computation offering a stronger security guarantee. In contrast to traditional trust-aware clustering protocols, the complexity analysis of the work shows that the time-complexity of FHE-TACBR stays within reasonable bounds during real-time communication with minimal effect on routing choices. Overall, the proposed FHE-TACBR offers a fair trade-off between security and performance making it appropriate for implementation in realistic situations of VANET. In future, we plan to use optimization technique with lightweight homomorphic encryption incorporating less energy to further improve efficiency without sacrificing the security.

6. REFERENCES

Abdul-Jaleel Al-Asady, Heba, et al. “AN IMAGE ENCRYPTION METHOD BASED ON LOGISTICAL CHAOTIC MAPS TO ENCRYPT COMMUNICATION DATA”. Kufa Journal of Engineering, vol. 15, no. 4, Nov. 2024, pp. 55-64, https://doi.org/10.30572/2018/KJE/150405.

Abuashour, A., & Kadoch, M. (2017). Performance improvement of cluster-based routing protocol in VANET. IEEE Access, 5, 15354–15371. https://doi.org/10.1109/access.2017.2733380

Ahsan, W., Khan, M. F., Aadil, F., Maqsood, M., Ashraf, S., Nam, Y., & Rho, S. (2020). Optimized node clustering in VANETs by using meta-heuristic algorithms. Electronics, 9(3), 394. https://doi.org/10.3390/electronics9030394

Alsaif, omar, and Amer Mohamed Shhatha. "ENHANCING CYBERSECURITY THROUGH MALWARE DETECTION BASED ON MACHINE LEARNING TECHNIQUE". Kufa Journal of Engineering, vol. 16, no. 3, July 2025, pp. 82-100, https://doi.org/10.30572/2018/KJE/160306.

Alsuhli, G. H., Khattab, A., & Fahmy, Y. A. (2019). Double-head clustering for resilient VANETs. Wireless Communications and Mobile Computing, 2019, 1–17. https://doi.org/10.1155/2019/2917238

Awan, K. A., Din, I. U., Almogren, A., Guizani, M., & Khan, S. (2020). StabTrust: A stable and centralized trust-based clustering mechanism for IoT-enabled vehicular ad-hoc networks. IEEE Access, 1–1. https://doi.org/10.1109/access.2020.2968948

Çalhan, A. (2015). A fuzzy logic-based clustering strategy for improving vehicular ad-hoc network performance. Sadhana, 40(2), 351–367. https://doi.org/10.1007/s12046-014-0315-9

Chiluveru, R., Gupta, N., & Teles, A. S. (2021). Distribution of safety messages using mobility-aware multi-hop clustering in vehicular ad hoc network. Future Internet, 13(7), 169. https://doi.org/10.3390/fi13070169

Daknou, E., Thaalbi, M., & Tabbane, N. (2015). A fast clustering algorithm for VANETs. In Proceedings of the 13th International Conference on Advances in Mobile Computing and Multimedia – MoMM 2015. https://doi.org/10.1145/2837126.2837147

Dhugga, P. K., Sharma, M., & Sharma, A. (2015). An algorithm for static geographical clustering in VANET. In 2015 IEEE 3rd International Conference on MOOCs, Innovation and Technology in Education (MITE). https://doi.org/10.1109/mite.2015.7375357

Fatemidokht, H., & Rafsanjani, M. K. (2020). QMM-VANET: An efficient clustering algorithm based on QoS and monitoring of malicious vehicles in vehicular ad hoc networks. Journal of Systems and Software, 166, 110561. https://doi.org/10.1016/j.jss.2020.110561

Husnain, G., & Anwar, S. (2021). An intelligent cluster optimization algorithm based on Whale Optimization Algorithm for VANETs (WOACNET). PLoS ONE, 16(4), e0250271. https://doi.org/10.1371/journal.pone.0250271

Kavitha, S., Srinivasan, J., Ramachandran, P., & Nasurulla, I. (2024). Enhanced cryptographic performance and security using optimized Edward-ElGamal signature scheme for IoT and blockchain applications. International Journal on Smart Sensing and Intelligent Systems, 17(1). https://doi.org/10.2478/ijssis-2024-0032

Limouchi, E., & Mahgoub, I. (2020). Smart fuzzy logic-based density and distribution adaptive scheme for efficient data dissemination in vehicular ad hoc networks. Electronics, 9(8), 1297. https://doi.org/10.3390/electronics9081297

Malathi, A., & Sreenath, N. (2017). An efficient clustering algorithm for VANET. International Journal of Applied Engineering Research, 12, 2000–2005.

Memon, I., Hasan, M. K., Shaikh, R. A., Nebhen, J., Bakar, K. A. A., Hossain, E., & Tunio, M. H. (2021). Energy-efficient fuzzy management system for Internet of Things connected vehicular ad hoc networks. Electronics, 10(9), 1068. https://doi.org/10.3390/electronics10091068

Miri, S. T., & Tabatabaei, S. (2020). Improved routing vehicular ad-hoc networks (VANETs) based on mobility and bandwidth available criteria using fuzzy logic. Wireless Personal Communications. https://doi.org/10.1007/s11277-020-07278-2

Mohammed Nasr, M., Abdelgader, A., Wang, Z.-G., & Shen, L.-F. (2016). VANET clustering based routing protocol suitable for deserts. Sensors, 16(4), 478. https://doi.org/10.3390/s16040478

Regin, R., & Menakadevi, T. (2019). Dynamic clustering mechanism to avoid congestion control in vehicular ad hoc networks based on node density. Wireless Personal Communications, 107, 1911–1931. https://doi.org/10.1007/s11277-019-06366-2

Ren, M., Khoukhi, L., Labiod, H., Zhang, J., & Vèque, V. (2017). A mobility-based scheme for dynamic clustering in vehicular ad-hoc networks (VANETs). Vehicular Communications, 9, 233–241. https://doi.org/10.1016/j.vehcom.2016.12.003

Saleem, M. A., Shijie, Z., Sarwar, M. U., Ahmad, T., Maqbool, A., Shivachi, C. S., & Tariq, M. (2021). Deep learning-based dynamic stable cluster head selection in VANET. Journal of Advanced Transportation, 2021, 1–21. https://doi.org/10.1155/2021/9936299

Sellami, L., & Alaya, B. (2021). SAMNET: Self-adaptive multi-kernel clustering algorithm for urban VANETs. Vehicular Communications, 29, 100332. https://doi.org/10.1016/j.vehcom.2021.100332.