International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8159
***Article Received:** 25 June 2023 **Revised:** 18 August 2023 **Accepted:** 06 September 2023*

Secure Message Dissemination with QoS Guaranteed Routing in Internet of Vehicles

Tanuja Kayarga[1], Ananda Kumar S[2*]
[1,2]School of Computer Science and Engineering Vellore Institute of Technology-Vellore- India
tanuja.kayarga2017@vitstudent.ac.in
Corresponding Author: s.anandakumar@vit.ac.in

Abstract— Internet of Vehicles (IoV) is a variant of vehicular adhoc network (VANET) where vehicles can communicate with other vehicles, infrastructure devices, parking lots and even pedestrians. Communication to other entities is facilitates through various services like DSRC, C2C-CC. Fake messages can be propagated by attackers for various selfish needs. Complex authentication procedures can affect the propagation of emergency messages. Thus a light weight mechanism to ensure the trust of messages without affecting the delivery deadlines for emergency messages. Addressing this problem, this work proposes a clustering based network topology for IoV where routing is optimized for message dissemination of various classes using hybrid meta-heuristics. In addition, two stage message authentication technique combining collaborative authentication with Bayesian filtering is proposed to verify the authenticity of message. Through simulation analysis, the proposed solution is found to detect fake messages with an accuracy of 96% with 10% lower processing delay compared to existing works..

Keywords-Clustering, Meta heuristics, IoV, swarm intelligence algorithm, Grasshopper optimization algorithm(GSO).

I. INTRODUCTION

High vehicular density in most of cities is causing many challenges in congestion management, road safety and fuel consumption etc. Internet of Vehicles (IoV) which is an extension of vehicular adhoc network (VANET) is a promising technology to address these challenges. It is connected network of vehicles, city infrastructure, entities related to road network like pedestrians etc. Vehicles can communicate with any other entities in the network. Vehicles can connect to any entity within vehicular adhoc network (VANET) like Road Side Units (RSU), other vehicles and entities outside network like application servers, cloud etc. The connectivity is enabled using various mechanisms like dedicated short range communication (DSRC), car to car communication consortium (C2C-CC) etc. IoV is different from traditional IoT networks as it can generate information volume thousand times more than traditional IoT networks. IoV need to support messages of different categories like emergency messages, real time cooperative control messages, infotainment message etc with different delay and reliability constraints. With this enhanced communication reach, messages related to road safety and convenience can be exchanged in the network. The communication medium is also open to attackers who can exploit various security vulnerabilities to propagate false messages in the network for their selfish needs. Fake message propagation reduced the trustworthiness of the network and it become difficult to ascertain message creditability. Many authentication and trust verification based schemes have been proposed (discussed in survey section) to ascertain message creditability but their computational complexity introduces higher latency in message delivery. Latency can be reduced through two ways: light weight authentication and improving the QoS for message dissemination through network topology and routing optimization.

This work integrates these two approaches and proposes a secure message dissemination technique with QoS guaranteed routing in IoV. The network is partitioned to optimal clusters with use of hybrid meta-heuristics. QoS guaranteed routing over the clustered topology is done for service differentiated message class with respective timelines. The messages are validated in temporal and spatial context using two stage filtering combining collaborative and Bayesian filtering. Following are the novel contributions of this work.

(i) An integrated approach combining light weight message authentication and topology/routing optimization for secure message dissemination over IoV. The network topology is optimized using hybrid meta heuristics for latency minimization over the network.

(ii) Message authentication using a two stage authentication mechanism combining collaborative and Bayesian filtering is proposed which operates at two different levels. Low computational overhead collaborative filtering is realized at clustering head and the slightly higher computational overhead Bayesian filtering is realized at RSU. Bayesian filtering is trained based on spatial and temporal context of the message. With the two stage filtering, false messages are effectively filtered before propagation in the network

The rest of the paper is organized as follows. Section II presents the survey of existing techniques for secure message

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8159
***Article Received:** 25 June 2023 **Revised:** 18 August 2023 **Accepted:** 06 September 2023*

dissemination in VANET networks. Section III presents the proposed secure message dissemination technique. The results of the secure message dissemination technique and its comparison to existing work are presented in Section IV. The concluding remarks and future work scope are presented in Section V.

II RELATED WORK

Ullah et al [1] proposed a secure message dissemination scheme based trust scoring the nodes. Vehicular nodes are scored based social utilities and these scores are maintained at RSU. Vehicles send messages to RSU and RSU decides to forward or drop based on the trust score of the source vehicle. Trust needs to continuously computed and maintained at RSU and there is no mechanism to prevent from faking social utilities. Also capture and replay attacks cannot be prevented in this approach. Due et al [2] addressed the problem of message dissemination by forwarding on a reliable path instead of broadcast. Game theory is used for calculating the path reliability. Higher computational complexity and congestion in path are two important issues in this approach. Liu et al [3] constructed a machine learning classifier based on traffic flow theory to detect false messages and prevent its propagation in VANET. Bayesian classifier is trained to detect the likelihood of a event being false. The approach works only for traffic flow scenarios and not applicable for other events. Park et al [4] used cooperative scheme for false message detection based on events from vehicles traveling in both directions from a view of source vehicle. Though the method is distributed and does not necessitate any infrastructure, it is applicable only for highway scenarios. Arshad et al [5] proposed machine learning based false message detection scheme. The witness collected from the scene is used by the Bayesian classifier to classify the likelihood of the false event. But the work did not consider the trust of vehicles providing the witness. Mohamed et al [6] used cryptographic mechanism to authenticate messages and prevented false message propagation. Diffe-Hellman protocol was used for key exchange from RSU to vehicles. Every message from vehicle is encrypted with key and authenticated at RSU before propagation. The complexity of message authentication and key exchange is high and replay attacks were not considered. Chen et al [7] proposed a cooperative trust evaluation framework for verify the genuineness of the message. Due to involvement of multiple parties, the message validation has higher latency in this approach. Zhang et al [8] used Dempster-Shafer theory to validate trust of the message source and drops the message from the un-trusted source. But this method performs well only after a period of time and requires trust information to available globally across all RSU's. Asian et al [9] proposed a trust based message validation framework for vehicular network. Genetic programming is used in this work to classify the message. The approach performs only after a period of time and has zero day problems. Muhammad et al [10] verified the message genuineness based on radio signal strength (RSS). Distance estimated from RSS is checked the event consistency in the message to detect the message genuineness. Though the approach works for Sybil attacks it fails for capture and replay attacks. Rassam et al [11] detected the message genuineness using machine learning classifier. Context features extracted from the message and vehicular node is clustered using K-means algorithm to two classes of genuine and fake. Only spatial context is used without any temporal correlation. Similar to it, Ghaleb et al [12] used context information for detecting fake messages. Misbehaving context information is collected and a Bayesian model is constructed to classify fake messages. Computational complexity is higher in this approach. Sharshembiev et al [13] detected misbehaving vehicular nodes using flow sampling and entropy change. Statistical difference in flow between misbehaving and normal behavior is collected and classifier is built to detect misbehaving nodes. The model needs large volume of training dataset and outlier detection was not considered in this work. Guo et al [14] proposed trust management scheme to detect fake messages. The trust management scheme is continuously adapted using reinforcement learning. Fake messages related to driving conditions are detected. But latency is higher in this approach. Sedjelmaci et al [15] detected fake messages in VANET using rule based approach. The rules to detect malicious vehicular node is set at RSU and RSU detect malicious vehicular node. Though the scheme is simple to realize, it is not adaptive and requires frequent rule upgrade. Zaidi et al [16] proposed a statistical approach to detect fake messages in VANET. Attack scenario messages are collected and behavior features are extracted from it. Statistical rules are generated from it to detect attack scenarios. The approach is rigid and cannot accommodate minor changes in attack scenario. Liang et al [17] used hidden generalized mixture model for detecting fake messages in VANET. Future state of vehicle on processing of fake messages is predicted and based on it fake messages are detected. Temporal correlation between the messages over a period of time is detected.

The current approaches for false message detection can be categorized to two types: trust based and behavior based. In both of these approaches, computational complexity increased the delay and this can increase the delivery deadline for emergency messages. Thus the message authentication mechanism must be made light weight and latency in message verification can be compensated by reducing latency through routing optimization.

III INTEGRATED SECURE MESSAGE DISSEMINATION

The proposed integrated secure message dissemination (I-SMD) technique integrates machine learning based light weight

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8159
***Article Received:** 25 June 2023 **Revised:** 18 August 2023 **Accepted:** 06 September 2023*

message authentication and optimized network topology. The objective of this integration is to meet the delivery deadlines of different message classes. The proposed solution has two important functionalities: topology optimization and message authentication.

A. Topology optimization

The network is partitioned into clusters. Clustering is done to achieve multiple objectives of stability of cluster, maximize density and minimize inter cluster delay. The multi objective problem of selecting the best cluster heads is solved using Grasshopper optimization algorithm(GSO).

GSO is an recent swarm intelligence algorithm proposed in works of Saremi et al [22]. This algorithm is based on the grasshopper's foraging and swarming behavior. Grasshopper is a agricultural pest whose life cycle has two stage nymph and adulthood. In nymph stage, the grasshoppers move in small steps with less movement. In adulthood stage, grasshoppers make long rage movements and the movements are abrupt. GSO algorithm has two phases (i) intensification and (ii) diversification which are based on the movement pattern of grasshoppers in nymph and adulthood stage. Mathematically, GSO represents the swarming behavior of grasshoppers in terms of their social interaction (S_i), gravitational force (G_i) and wind advection (A_i) as

$$P_i = S_i + G_i + A_i \quad (1)$$

Where P_i is i^{th} grasshopper's position. S_i is calculated for N grasshoppers separated by a Euclidean distance (d_{ij}) with a social force s as

$$S_i = \sum_{\substack{j=1 \\ j\neq i}}^{N} s(d_{ij})\widetilde{d_{ij}} \quad (2)$$

The social force is represented in terms of attraction intensity(f) and attration length (l) as

$$s(r) = f\exp^{\frac{-r}{l}} - \exp^{-r} \quad (3)$$

Attraction and repulsion are the two themes based on which social interaction is measured. For a distance in range of 0 to 15, attraction is felt in range of 2.07 to 4 and repulsion is felt in range of 0 to 2.07. At the distance of 2.07, a comfort zone is realized where there is neither attraction nor distraction.

The gravity force G_i in equation (1) is calculated in terms of distance unit vector to center of earth($\hat{e}_g$) and gravitational constant (g)as

$$G_i = -g\hat{e}_g \quad (4)$$

The wind advection A_i in equation (1) is calculated in terms of distance unit vector to wind direction($\hat{e}_w$) and drift constant (u) is given by

$$A_i = u\hat{e}_w \quad (5)$$

Fitting each of the variables , the equation 1 is modified with upper bounds(ub_d) and lower bounds(lb_d) in the the d-th dimension and given as equation 6.

$$P_i^d = c\left(\sum_{\substack{j=1 \\ j\neq i}}^{N} c\frac{ub_d - lb_d}{2}\right) s(|P_j^d - P_i^d|)\frac{P_j - P_i}{d_{ij}}) + \hat{T}_d \quad (6)$$

$\hat{T}_d$ is the best solution found so far in the d-th dimension space. The parameter c is similar to inertia weight ω in PSO. This parameter controls the grasshopper's movement around food (target) and provides a fine balance between diversification and intensification. The parameter c is calculated as

$$c = c_{max} - t\frac{c_{max} - c_{min}}{t_{max}} \quad (7)$$

With the maximum value for c represented as c_{max} and minimum value for c represented as c_{min}. The position is updated for every iteration (t) for a maximum number of iterations (t_{max})

Grasshopper position is updated every iteration based on both local and global best solution. The iteration is stopped when they are no change in position of grasshopper.

Use of global best position prevents from getting trapped into local optimum.

The pseudo code of grass hopper optimization algorithm is given below

Algorithm 1: GOA Optimization

A. Random generation of initial population for n grasshoppers Pi
B. Initialize Cmin, Cmax, and a maximum number of iterationTmax
C. Evaluate the fitness f(Pi) of each grasshopper Pi
D. B= The best solution
E. **While** (t<tmax) **do**
F. Update c1 and c2
G. **For**i=1 to N, for all N grasshoppers in the population,
H. **do**
I. Distance between grasshoppers normalized in range of 1 to 4.
J. Update position using equation (7)
K. Rectify outlier and normalize grasshoppers position
L. **end for**
M. Update B with best solution so far
N. t=t+1

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8159
***Article Received:** 25 June 2023 **Revised:** 18 August 2023 **Accepted:** 06 September 2023*

O. **end while**
P. Return B

The fitness function of GSO (f(Pi)) for cluster head selection is designed to achieve multiple objectives of stability of cluster, maximize density and minimize inter cluster delay. The fitness function is designed based on following parameters

1. Average Stability of cluster (S)
2. Average effective hop count between clusters (h_c)
3. Average Degree difference (D_d)
4. Average uncovered vehicles on speed/direction variations. (U_C)

The fitness function is framed as

$$f(Pi) = w_1 S + w_2 h_c + w_3 \frac{1}{D_d} + w_4 \frac{1}{U_C} \quad (8)$$

The values of weights (w_1 to w_4) is selected depending on preference of system administrators for each of the objective parameters satisfying the following constraint of

$$w_1 + w_2 + w_3 + w_4 = 1 \quad (9)$$

The optimal cluster heads are selected using GSO and vehicular nodes join to their nearest cluster head. Vehicles send messages to their cluster head. From the cluster head the authenticated messages are forwarded to cluster heads in hop by hop manner for message dissemination. The message is authentication in a light weight manner in two level.

B. Message authentication

Messages are authenticated in light weight manner in one of two levels in the proposed work. Cluster heads authenticate the messages in a cooperative manner and propagate the authenticated messages. But when it does not have necessary information to cooperatively authenticate message, it forwards to RSU to authenticate based on spatial and temporal context. RSU forwards to cluster head once the message is validated. With this one of two levels, most of messages are authenticated at cluster head as clusters are constructed with higher density in proposed solution. Only when cluster head could not authenticate the message it is forwarded to RSU for authentication.

Cooperative confidence model is realized at the cluster heads to authenticate events. For every vehicle which is an event source, the confidence level or trust level is calculated based on its agreement of events with other sources over a period of time. The agreement factor is calculated in iteration averaging the agreement in past and current. The agreement coefficient between two sources (a and b) at time t ($\gamma_{ab}(t)$) is calculated based on probability of occurrence of event from view of $a(P_a)$ and $b(P_b)$ as

$$\gamma_{ab}(t) = \frac{1}{2}\left[\left(1 - 2 \times \left|\left(p_a(t) - p_b(t)\right)\right|\right) + \gamma_{ab}(t-1)\right] \quad (10)$$

$$p_a(t) = P\left(E_t \middle| M_a\right)$$

$$p_b(t) = P\left(E_t \middle| M_b\right)$$

The value of $\gamma_{ab}(t)$ for $t = 0$ is calculated as

$$\gamma_{ab}(0) = \frac{1}{2}\left[\left(1 - 2 \times \mathrm{abs}\left(p_a(0) - p_b(0)\right)\right)\right] \quad (10)$$

The value for γ_{ab} ranges from -1 to 1. For the case of complete agreement of events, the value is 1 and for the case there is no agreement, the value is 0.

Say there are N event sources, aggregation coefficient is calculated between each sources. The aggregation coefficient is clustered into two clusters using average link clustering with one cluster for agreement and another cluster for disagreement. Decision is made on the event as real or fake based on whether the event source falls in agreement or disagreement cluster.

The agreement coefficient between event sources is based on average link clustering. In average link clustering, the distance between one cluster and another cluster is calculated as the average distance from any member of one cluster to any member of the other cluster. When the event source falls into agreement cluster the event it sent is classified as trusty and forwarded to cluster head for propagation. When Cluster heads does not have enough evidences from nearby vehicles to validate the message using cooperative confidence model, it forwards to RSU for validation using Bayesian filtering.

The features of the event are reported location, reported time, Term frequency – inverted document frequency (TF-IDF) of event contents etc. A training dataset is constructed with the features corresponding to two classes of valid and fake messages. A Bayesian classifier is trained with the training data set. The posterior probability of the feature set M to belong to a class H is defined using Baiyes theorem as

$$P(H|M) = \frac{P(M|H).P(H)}{P(M)} \quad (11)$$

M is predicted to belong to class C_i if the probability if $P(C_i|M)$ is highest among all the $P(C_k|M)$ for all the classes and the $P(C_i|M)$ is above the threshold T. It is calculated as

$$P(C_i|M) = \frac{P(M|C_i).P(C_i)}{P(M)} \quad (12)$$

Bayesian classifier function is constructed for two classes of valid and fake message. Once the message arrives at RSU, features are extracted from message and the features are passed to Bayesian classifier function for valid and fake classes. The message is detected as fake when the value of Bayesian classifier function corresponding to fake class is higher than that of Bayesian classifier function for valid class. Fake messages are dropped and only valid message are processed for forwarding by sending to cluster head.

Authenticated messages can be captured and replayed by

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8159
Article Received: *25 June 2023* ***Revised:*** *18 August 2023* ***Accepted:*** *06 September 2023*

attacker creating denial of service attacks. To prevent this, the messages has to digitally signed and verified at receiving cluster heads before dissemination of message.

System wide public(P_b) and private key(P_r) is generated and the private key is known only at RSU. RSU creates a signature every T interval once as

$$S = RSA\_Encrypt(T, P_r)$$

This signature S is forwarded to cluster heads and authenticated messages are embedded with S before forwarding to other cluster heads for message dissemination. The cluster heads receiving the message, authenticate it by decrypting the S and checking it difference between T and current timestamp is less than tolerable delay. By this way, late message and capture replay messages are dropped at cluster heads.

To support messages for different deadlines or traffic priority classes, multiple queues are kept at RSU and cluster head. The incoming messages are queued in their corresponding queue. Processing of messages in queue is done differentially giving processing time proportional to priority of the queue. By this way, messages with higher priority are processed ahead of messages with lower priority.

IV RESULTS

NS2 simulator is used for measuring the effectiveness of the proposed solution. The vehicle traces are generated using SUMO and NS2 extension code implements the proposed solution on these traces.

The simulation was conducted against configuration parameters given in Table 1.

TABLE I SIMULATION CONFIGURATION

Parameter	Value
Length of road	4km
Topology	Highway
Number of lanes	3 each direction
Number of vehicles	25 to 200
Maximum vehicle speed	30m/s
Transmission range	250m
MAC specification	IEEE 802.11p
Data packet size	1000 bytes
Data rate	4 packet/second
Simulation time	1000 seconds

Messages are in three different priority levels. The performance of the solution is measured in two dimensions: false message filtering and QoS for message delivery. In terms of fake message filtering, parameters of false message detection accuracy, false detection rate and detection delay are measured. In terms of QoS message delivery and average latency for message dissemination are measured. The performance of proposed I-SMD is compared against traffic flow model approach proposed by Liu et al [6], context aware approach proposed by Rassam et al [14] and multifaceted context approach proposed by Ghaleb et al [15].

The accuracy of false message detection is measured varying the attack proportion and the result is given in Figure 1.

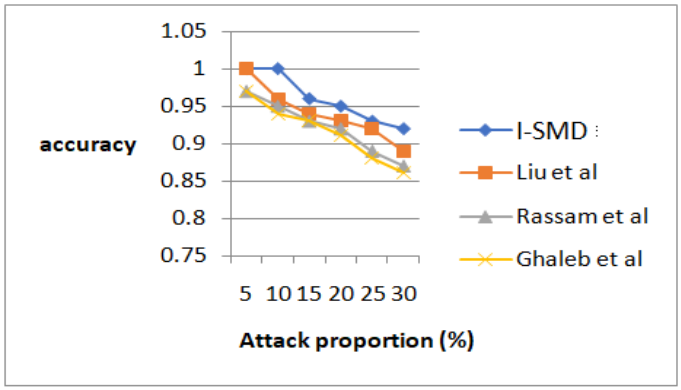

Figure 1 False detection accuracy

The proposed I-SMD detects false message with atleast 1.9% higher accuracy compared to existing works. Compared to Liu et al, the accuracy has increased by 1.9% due to proposed solution able to detect false messages based on content and context, while Liu et al detected false messages only for traffic flows. Compared to Rassam et al , the accuracy is higher by 4% in I-SMD due to consideration of spatial and temporal context in proposed solution while Rassam et al considered only spatial context. Compared to Ghaleb et al, the proposed solution has atleast 5% higher accuracy. This is because Ghaleb considered only temporal context while the I-SMD considered both content and context of the messages.

False positives are a degree of error recognizing genuine messages as fake messages. False positives are measured varying the attack proportion and the result is given in Figure 2.

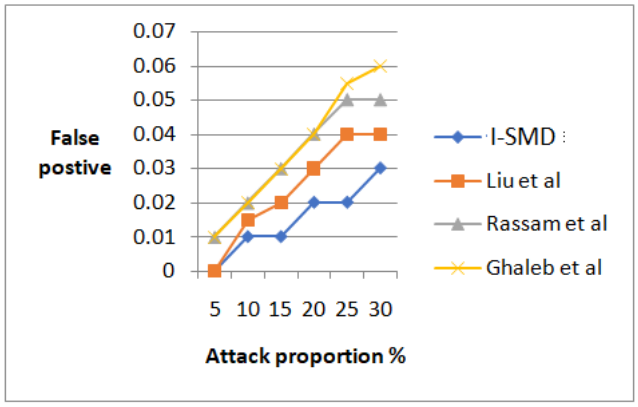

Figure 2 False positives

The proposed I-SMD has atleast 1.8% lower false positives compared to existing works. False positive has reduced in I-SMD due to cooperative detection scheme which involves scoring both event source and event over a temporal duration.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8159
***Article Received:** 25 June 2023 **Revised:** 18 August 2023 **Accepted:** 06 September 2023*

Also the I-SMD has increased the probability of more event sources in confidence measurement by maximizing the density of clusters. Existing works did not consider maximizing event confidence in the way addressed in proposed solution involving both event sources and event characteristics.

The average delay incurred for detection of a false message is measured varying the radius of attack sources and the result is given in Figure 3.

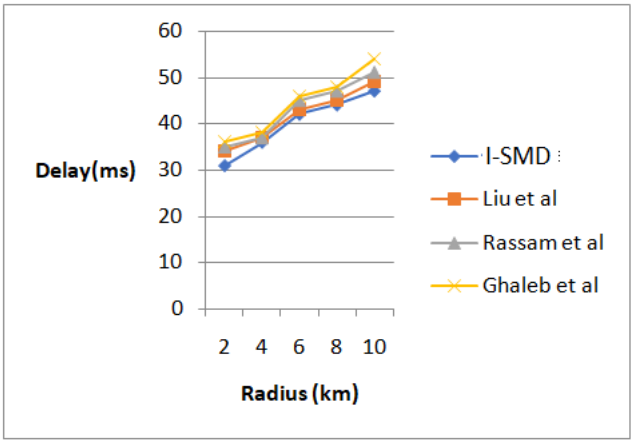

Figure 3 Average delay

The placement of cluster head is efficient in I-SMD, so that the first level of false event detection incurs only about 39 ms compared to more than 43 ms delay in false event detection in existing approaches. Only for the case of sufficient event evidences are not available, the proposed solution uses RSU to verify the messages based on spatial and temporal context.

The packet delivery ratio is measured varying the density of vehicles and the result is given in Table 2

TABLE 2 PACKET DELIVERY RATIO WITH VARYING DENSITY OF VEHICLES

No of vehicles	Proposed	Liu et al	Rasam et al	Ghaleb et al
50	94	87	82	81
100	93	86	81	79
150	92	85	79	78
200	91	84	78	77
250	90	83	77	76
Average	92	85	79.4	78.2

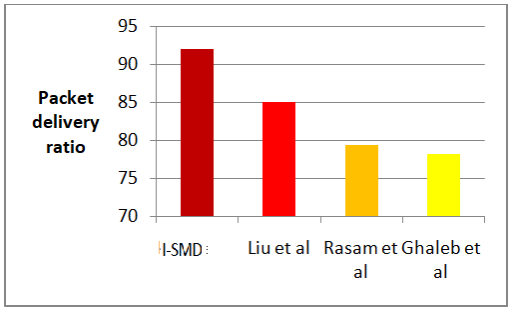

Figure 4 Average packet delivery ratio

The average packet delivery ratio in proposed I-SMD is atleast 7% higher compared to Liu et al, 12.6% higher compared to Rasam et al and 13.8% higher compared to Ghableb et al. The packet delivery ratio has increased in proposed solution as shown in the Figure 4, due to use of clustered topology with effective cluster head selection based on multiple objectives.

The delay for message dissemination is measured varying the vehicular density and the results are given in Figure 5.

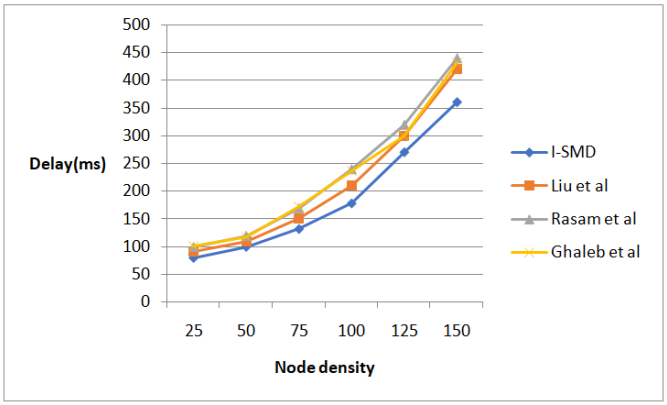

Figure 5 Average delay

The average delay in proposed I-SMD in proposed solution is atleast 1.4 times lower compared to existing works. The delay has reduced in proposed solution due to light weight message validation and topology optimized for message dissemination.

Packet delivery ratio is measured by varying the speed for fixed number of vehicles (100) and the result is given in Figure 6.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8159
***Article Received:** 25 June 2023 **Revised:** 18 August 2023 **Accepted:** 06 September 2023*

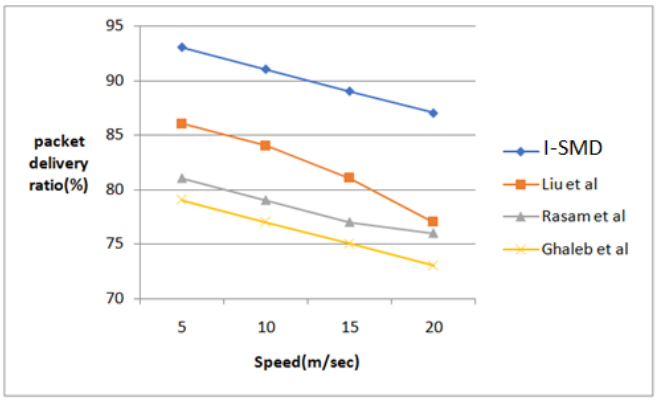

Figure 6 Packet delivery ratio vs speed

As the speed increases, packet delivery ratio drops but still the packet delivery is higher in proposed I-SMD compared to existing works. On average it is atleast 8% higher compared to existing works.

Message dissemination delay is measured by varying the speed for fixed number of vehicles (100) and the result is given in Figure 7.

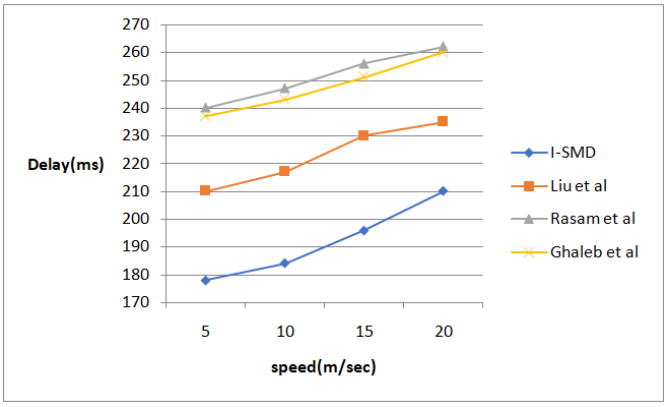

Figure 7 Delay vs speed

The delay increases with increase in speed, as mobility disrupts the links stability and alternate paths need to found. But the delay in proposed I-SMD is atleast 11% lower compared to existing works. Selection of stable clusters and clustering based message dissemination has reduced the delay even when speed increased in the proposed I-SMD.

V. CONCLUSION

A secure message dissemination technique combining light weight message validation and topology optimization was proposed in this work. The topology is optimized using multi objective based clustering using meta heuristics algorithm. A light weight message validation technique using one of two levels of collaboration based validation and spatial/temporal context based validation is realized to verify the genuineness of the message. The message validation technique proposed in this work does not involve complex cryptographic mechanisms and hence it is light weight. The proposed solution is able to detect false messages with an average accuracy of 96% which is atleast 1.9% higher compared to existing works. Also the latency for message validation is 10% lower in proposed solution compared to existing works.

REFERENCES

[1] S. Latif, S. Mahfooz, B. Jan, N. Ahmad, Y. Cao, M. Asif, A comparative study of scenario-driven multi-hop broadcast protocols for vanets, Veh. Commun. 12 (2018) 88–109

[2] S. Latif, S. Mahfooz, B. Jan, N. Ahmad, Y. Cao, M. Asif, A comparative study of scenario-driven multi-hop broadcast protocols for vanets, Veh. Commun. 12 (2018) 88–109

[3] W. Li, H. Song, Art: an attack-resistant trust management scheme for securing vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst. 17 (4) (2016) 960–969

[4] Ullah, Noor & Kong, Xiangjie & Tolba, Amr & Alrashoud, Mubarak & Xia, Feng. (2020). Emergency warning messages dissemination in vehicular social networks: A trust based scheme. Vehicular Communications. 100199. 10.1016/j.vehcom.2019.100199.

[5] A. Dua, N. Kumar, S. Bawa, Reidd: reliability-aware intelligent data dissemination protocol for broadcast storm problem in vehicular ad hoc networks, Telecommun. Syst. 64 (3) (2017) 439–458

[6] Liu J, Yang W, Zhang J, Yang C. Detecting false messages in vehicular ad hoc networks based on a traffic flow model. International Journal of Distributed Sensor Networks. 2020;16(2).

[7] S. Park and C. C. Zou, "Reliable Traffic Information Propagation in Vehicular Ad-Hoc Networks," *2008 IEEE Sarnoff Symposium*, Princeton, NJ, USA, 2008, pp. 1-6

[8] Arshad, M., Ullah, Z., Ahmad, N. et al. A survey of local/cooperative-based malicious information detection techniques in VANETs. J Wireless Com Network 2018, 62 (2018).

[9] Mr. R. Senthil Ganesh. (2019). Watermark Decoding Technique using Machine Learning for Intellectual Property Protection . International Journal of New Practices in Management and Engineering, 8(03), 01 - 09. https://doi.org/10.17762/ijnpme.v8i03.77.

[10] Mohamed TM, Ahmed IZ, Sadek RA. Efficient VANET safety message delivery and authenticity with privacy preservation. PeerJ Comput Sci. 2021 May 4;7:e519

[11] Chen Chen (2010). A Trust-based Message Evaluation and Propagation Framework in Vehicular Ad-Hoc Networks. UWSpace. http://hdl.handle.net/10012/4929

[12] C. Zhang, K. Chen, X. Zeng and X. Xue, "Misbehavior Detection Based on Support Vector Machine and Dempster-Shafer Theory of Evidence in VANETs," in *IEEE Access*, vol. 6, pp. 59860-59870, 2018

[13] Aslan, M., Sen, S. (2019). Evolving Trust Formula to Evaluate Data Trustworthiness in VANETs Using Genetic Programming. In: Kaufmann, P., Castillo, P. (eds) Applications of Evolutionary

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8159
***Article Received:** 25 June 2023 **Revised:** 18 August 2023 **Accepted:** 06 September 2023*

Computation. EvoApplications 2019. Lecture Notes in Computer Science(), vol 11454. Springer, Cham

[14] Mujahid Muhammad, Paul Kearney, Adel Aneiba, Junaid Arshad, Andreas Kunz. RMCCS: RSSI-based Message Consistency Checking Scheme for V2V Communications. In Sabrina De Capitani di Vimercati, Pierangela Samarati, editors, Proceedings of the 18th International Conference on Security and Cryptography, SECRYPT 2021, July 6-8, 2021. pages 722-727, SCITEPRESS

[15] Rassam, Murad & Ghaleb, Fuad & Zainal, Anazida & Maarof, Mohd. (2019). Detecting Bogus Information Attack in Vehicular Ad Hoc Network: A Context-Aware Approach.

[16] Mohannad O. Rawashdeh, Sayel M. Fayyad, Sulieman Abu-Ein, Waleed Momani, Zaid Abulghanam, A. M. Maqableh. (2023). Intelligent Automobiles Diagnostic System. International Journal of Intelligent Systems and Applications in Engineering, 11(4s), 458–465. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2703.

[17] Ghaleb, F.A.; Maarof, M.A.; Zainal, A.; Al-Rimy, B.A.S.; Saeed, F.; Al-Hadhrami, T. Hybrid and Multifaceted Context-Aware Misbehavior Detection Model for Vehicular Ad Hoc Network. IEEE Access 2019, 7, 159119–159140.

[18] Sharshembiev, K.; Yoo, S.M.; Elmahdi, E.; Kim, Y.K.; Jeong, G.H. Fail-Safe Mechanism Using Entropy Based Misbehavior Classification and Detection in Vehicular Ad Hoc Networks. In Proceedings of the 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Atlanta, GA, USA, 14–17 July 2019; pp. 123–128

[19] Guo, J.; Li, X.; Liu, Z.; Ma, J.; Yang, C.; Zhang, J.; Wu, D. TROVE: A context-awareness trust model for VANETs using reinforcement learning. IEEE Internet Things J. 2020, 7, 6647–6662.

[20] Sedjelmaci, H.; Senouci, S.M.; Abu-Rgheff, M.A. An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks. IEEE Internet Things J. 2014, 1, 570–577.

[21] Steffy, A. D. . (2021). Dimensionality Reduction Based Diabetes Detection Using Feature Selection and Machine Learning Architectures. Research Journal of Computer Systems and Engineering, 2(2), 45:50. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/32.

[22] Zaidi, K.; Milojevic, M.B.; Rakocevic, V.; Nallanathan, A.; Rajarajan, M. Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection. IEEE Trans. Veh. Technol. 2016, 65, 6703–6714

[23] Liang, J.; Lin, Q.; Chen, J.; Zhu, Y. A Filter Model Based on Hidden Generalized Mixture Transition Distribution Model for Intrusion Detection System in Vehicle Ad Hoc Networks. IEEE Trans. Intell. Transp. Syst. 2019, 10, 2707–2722.

[24] L. Kou, G. Markowsky, and L. Berman. A fast algorithm for steiner trees. Acta Informatica, 15:141–145, 1981

[25] S. Saremi, S. Mirjalili, and A. Lewis, ``Grasshopper optimisation algorithm: Theory and application," Adv. Eng. Softw., vol. 105, pp. 30_47, Mar. 2017.