Whale optimization Algorithm and Blockchain Technology for Intelligent Networks

Shazia Sulthana[1+] and B N Manjunatha Reddy[2++],
shazia.sulthana@gat.ac.in *manjunatha_reddy@gat.ac.in*
Department of ECE, Global Academy of Technology, VTU, Karnataka, 560098, India

Summary
The proposed privacy preserving scheme has identified the drawbacks of existing schemes in Vehicular Networks. This prototype enhances the number of nodes by decreasing the cluster size. This algorithm is integrated with the whale optimization algorithm and Block Chain Technology. A set of results are done through the NS-2 simulator in the direction to check the effectiveness of proposed algorithm. The proposed method shows better results than with the existing techniques in terms of Delay, Drop, Delivery ratio, Overhead, throughout under the denial of attack.

Keywords:
VANET, Privacy, Block chain, Cluster size, Network simulator.

1. Introduction

In Mobile Ad-hoc Network, the emerging subclass intelligent transport system is VANET [1]. Many researchers started working for conserving the privacy of messages in intelligent wireless networks. The main advantage is to offer inter-vehicular and roadside unit communication to improve the road safety, avoids congestion and road accidents.

To progress the efficiency of the network entities, load balancing has to be maintained hence we go for smart clustering system, which should be adoptable, reliable and effective. Clustering in a network means vehicles are pooled as per their characteristics, uniqueness. In cluster-based architecture, each cluster contains cluster Head (CH) that is selected according to the power transmission, line-of-sight with the RSU mounted with antenna. Cluster Head is mid node to the grouping system, which carries out variety of functions like deploying the nodes in cluster, closing of a group, maintaining of system entities, and balancing of group configuration. The cluster head also manages both inside and outside communication through erstwhile nearby cluster. General Cluster based architecture is as shown in Fig.1.1, which contain Cluster Head and Cluster Node mounted with the On-Board Units (OBU), RSU mounted with isotropic or directional antenna and their connectivity is deployed through dedicated short-range communication (DSRC).

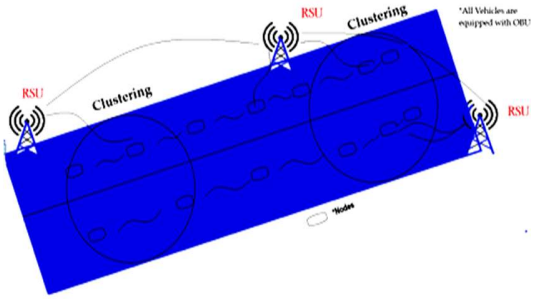

Fig. 1. General Cluster based architecture

2. Literature Survey

Bidiying and Amiya Nayak [2] have proposed a protocol that deals with the ambiguity and effectiveness issue in vehicular networks. It performs the low-cost security functions to validate legitimacy and legalization of ion messages. In addition to this protocol provides a technique for secret word change, it does not depend on any trusted authority, and it can refuse to accept offline secret word attack.

Mohammad Wazid et al., [3] proposed a skilled protocol for vehicular networks, it use single hash operations with bit-by-bit exclusive OR operation. They used proper safety analysis which is under the broadly used in Real-or-Random model together with a known safety algorithm.

Rajput et al., [4] adopted a technique that combines the features of pseudonym-specific models which depends on group signatures model with little ambiguity.

Lei ao et al., [5] Proposed an algorithm for managing the safe key within diverse network. In this safety manager Participate vital role in identifying the vehicle leaving information, encapsulating block for moving keys then compiling the rekeying to vehicles within an equivalent safety mechanism. The chief part of this structure is based on management of the group key with changing probability of moving nodes to leave existing area. Probability factor of vehicle is presented as method to realize a well-organized scheduling method and fewer keying costs. The next part of the structure is by the use of the database model towards the shortening of key.

Manuscript received July 5, 2022
Manuscript revised July 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.7.19

Cui et al., [6] offered a scheme for vehicular networks in addition through a cuckoo filter on the way to progress the safety and confidentiality of nodes with the minimization of the communication load.

Leiding et al., [7] modified the vehicular networks using Ethereum's Blockchain-based appliance and magnified algorithm which is monitoring by itself and no centralized unit. It uses intelligent convention technique for executing a Blockchain.

Dorri et al., [8] demonstrated a model based on the Blockchain for automotive safety using superimpose network inside the distributed database, as well as addition nodes which is placed on top block managers. The deployment of additional load on the top of the nodes resulted in a more delay; hence it became a centre for breakdown.

Rowan et al., [9] introduced Blockchain based database in order to secure the messages of the vehicle intelligence by means of the light medium. The Blockchain is engaged through the cryptographic session and public keys.

Guo et al., [10] synthesized a guaranteed authentication method to observe and attain the combined involvement for the moving vehicles. Besides, Blockchain is working to realize safe verification to obtain the secured confidentiality.

Sherazi et al., [11] determined a denial service of attack by improving the intrusion detection system for the vehicle connectivity in addition with Artificial Intelligence and Machine Learning model are identified allowing superior security data creation. Furthermore, a symbolic reason and neural network scheme is validating for scrutinizing the efficiency of existing technology.

Yang et al., [12] identified a verification-based result to compromise idea related to moving network rather than proof-of-authority methods. The congested information is accumulated throughout the fixed part and hence moving node will secure the accuracy on the receipt of broadcasting in addition to these two ways operations on Block chain is used for transmitting counsel messages towards the particular destination.

S. Mirjalili and A. Lewis [13] explained an innovative optimization method to invoke the procedures for searching humpback whales. It includes operators to reproduce the searching of victim, encompassing the victim and creating foraging by bubbling of whales. A general approach for controlling the standard functions and for examining the optimum searching, utilization of optimum solution and converging actions of the intended method is used. This method is originated to be sufficient viable among the other meta-heuristic methods.

Ying, B et al., [14] explained the ASC schemes, which are certificate-based, holds for V2V and V2I system. This scheme introduces login stage, register stage, data authentication stage, user authenticating stage, changing password phase.

3. Proposed Method

In the Proposed method, Block chain technology and whale optimization algorithms are used in vehicular network in which the vehicles are grouped by K nearest neighboring algorithm and the groups are called as clusters. It employs the crypto-currency hash function and will be considered moving vehicles cooperate with one another through V2V and V2I are towards the hook up with cluster successfully as depleted in Fig.2. Consider each one vehicle is embedded with communicating network and the validated RSU units are more than the intruder's RSU unit

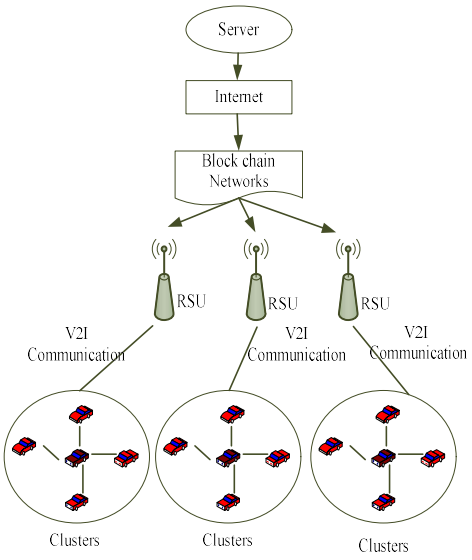

Fig. 2. Architecture of the WOA-based clustering using Block chain

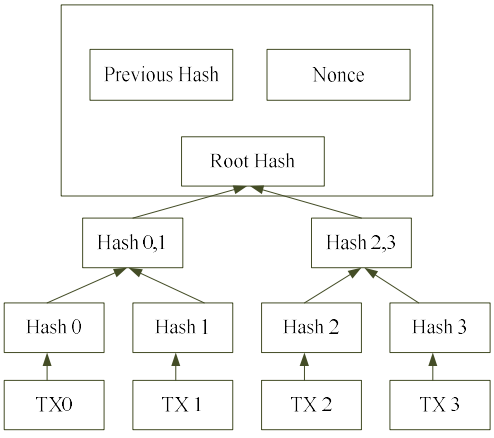

Fig. 3. Structure of Block chain

The Blockchain has been synchronized and monitored independently to trace the communication of all vehicles, broadcasting their locations with the valid messages as shown in Fig. 3. Location Certificate is employed as an accurate method for representing the moving vehicle at a particular distance. All vehicles require a Location Certificate to get authorization about their location from a valid RSU. Location certificate works as a location identifier for moving nodes, with in the given geographical area. Meantime Blockchain advertises the newly formed blocks together. The messages within the network do not cross the boundary of RSU, if the other moving nodes set up in a different position will not know any congestion and accident messages of a position. As a result, an alternative Blockchain system is necessary. With this self-governing database, all new blocks are reliable with the event occurring messages and forwarding the entire newly minted block within the distributed database. Hence, moving entity will send inquiry about its safety at any time necessary in the course of the distributed database. When the process is concluded, the new chunk of data is advertised, dynamic nodes within the system are validated with the updated parameters inside the distributed database. In this work, identified the clustering scheme where learning identifies a novel algorithm called as whale optimization algorithm (WOA) for optimizing which is based on the search performance of humpback whale. The simulated working behavior of whales is to search the best agent or to search the prey by the application of a searching mechanism. The efficient proposed algorithm with the Blockchain technology shows better results than the existing approaches.

3.1. Whale Optimization Algorithm

The WOA algorithm mimics the behavior of humpback whale especially the hunting behavior of this whale is analyzed. This uses the bubble-net hunting strategy for hunting the prey. This hunting strategy includes the spiral shaped bubble formation during hunting. Thus the way the cluster header is formed by hunting best prey and the cluster formation is done by the encircling behavior. The hunting strategies are shown in below section.

Exploration phase

Encircling the prey

Exploitation phase

Exploration phase: The whale search the best prey based on the prey position that is updated randomly than the best search agent [17]. The model of this stage is expressed as mathematically in equation (1; 2)

$$\vec{D} = \left| \vec{C} * \vec{X}_{rand} - \vec{X} \right| \tag{1}$$

$$X(t+1) = \vec{X}_{rand} - \vec{A} * \vec{D} \tag{2}$$

Where, the random position vector is denoted as $\vec{X}_{rand}$, and $\vec{C}$, $\vec{A}$ are coefficient vectors which shown in equations (3; 4).

$$\vec{A} = 2 * \vec{a} * \vec{r} - \vec{a} \tag{3}$$

$$\vec{C} = 2 * \vec{X}_{rand} \tag{4}$$

Where, the random number is between [0, 1], the control parameter is represented as ‘a ‘and if the iteration increases the value of ‘a’ is decreases from 2 to 0. The iteration is expressed in equation (5).

$$\vec{a} = 2 - \frac{2t}{T_{\max}} \tag{5}$$

Encircling model: In this model whale encircles the prey during hunting and the current best solution is obtained to update the position of other whales towards the search agent, nearest to the whale. The random position and best position is expressed mathematically in equation (6; 7)

$$\vec{D} = \left| \vec{C} * \vec{X}'(t) - \vec{X}(t) \right| \tag{6}$$

$$X(t+1) = \vec{X}'(t) - \vec{A} * \vec{D} \tag{7}$$

Where, the current iteration is denoted as t, best solution position is denoted as x(t).

Exploitation Phase (Bubble-Net Attacking Model): This section deals with the bubble net attacking of whale which consist of two phases as follows,

Shrinking encircling mechanism: Where, the random number is between [-1, 1], the control parameter is represented as ‘a ‘and if the iteration increases the value of ‘a’ is decreases from 2 to 0. In which the best search agent position is identified between search agent present and original position.

Position updating in spiral movement: The distance between humpback whale and the prey is analyzed for calculation. The movement between whale and prey is in helix-shaped which is analyzed in equation (8)

$$X(t+1) = \vec{D}'' * e^{bl} * \cos(2\pi l) + \vec{X}' \tag{8}$$

Where, l is the random number between [-1, 1] and b is the shape of spiral. Let's now define the mathematical model behind the humpback whales swimming style in the region of the prey which is expressed in equation (9)

$$\vec{X}(t+1) = \begin{cases} \vec{X'}(t) - \vec{A} * \vec{D} & if\ p < 0.5 \\ \vec{D''} * e^{bl} * \cos(2\pi l) + \vec{X'} & if\ p \geq 0.5 \end{cases} \quad (9)$$

The parameters for network performance are explained below.

1. Delay: The latency of a bit to move from starting point to ending point across the communication network.
2. Drop: the loss of packet bits arriving at their destination. The drop may due to congestion, noisy channel
3. Delivery Ratio: The delay ratio between the actual and desired response.
4. Overhead: data packet which is being encapsulated will contain additional information for reliable communication called overhead.
5. Throughput: measurement based on how many successful bits arrived at the destination out of transmitted bits depending on the networks.

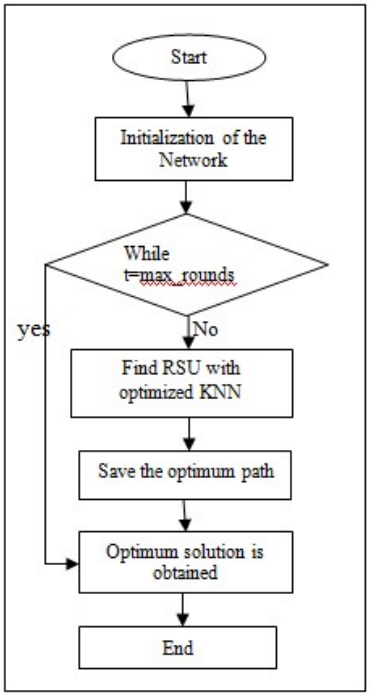

Fig. 4. Proposed optimized WAO model

Process1: fill data samples
Process2: Initialize every seek mediator to hold the K arbitrarily grouping centriods.
While $t < Iteration$ do
For every seek mediator i do
x_p do for every data vector
Process 3: Compute the data point between each cluster to their respective centroids.
Process 4: consign x_p to the group x_{ij} such that
$\left|x_p - Z_{ij}\right| = \min_{c=1,2,\ldots,k} \left|x_p - Z_{ic}\right|$
Process 5: Calculate the fitness.

$$Fitness = \sum_{j=1}^{k} \sum_{i=1}^{n} W_{ij} \left|X_{ij} - Z_{ij}\right|$$

$$W_{ij} = \begin{cases} 1 & if \left|X_i - Z_{ij}\right| = \min_{1 \leq m \leq k} \left|X_i - Z_{im}\right| \\ 0 & else \end{cases}$$

End for
End for
X^* is the best search agent?
Process 6: For each search agent
do
Update a, A, C, I and ρ
If $\rho < 0.5$ then
If $|A| < 1$ then
Process 7: Update search agent
Else if $|A| \geq 1$ then
Select random search agent.
Process 8: Update current search agent
End if
Else if $\rho < 0.5$ then
Process 9: Update the location of current search agent
End if
End for
$t = t + 1$
End while
Process 10: Return X^*
End Process
R is a random vector in [0, 1].

4. Results and Discussion

This section highlights the valuation of the proposed Whale Optimization method. Analysis has shown with the number of nodes and factors (Delay, Delivery Ratio, Overhead, Drop and Throughput). Network Simulator-2 Version 2.3.5 is used to get the results of the work. The

simulation model is shown in Fig.5. and the topology for 50 nodes, 6 RSU' S are deployed as shown in Fig. 6.

Fig. 7. shows Delay analysis for the various node counts. For 50 nodes, the WOA technique yields the lowest delay of 7.03, while ASC, HEPPA and ROAC methods resulted in higher delays of 11.71, 10.71 and 9.7 respectively. For 100 nodes, the proposed WOA algorithm yields the lowest delay of 10.84, while ASC, HEPPA and ROAC methods resulted in higher Delays of 15.23, 14.23 and 13.23 respectively.

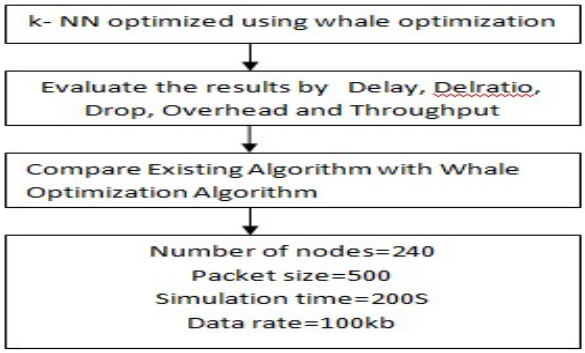

Fig. 5. Simulation Model

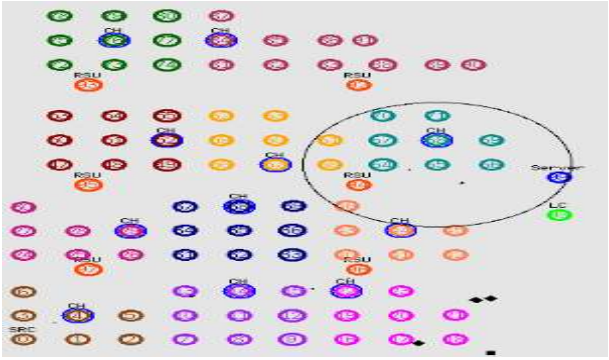

Fig. 6. Node Deployments for the 50 nodes.

For 150 nodes, the proposed WOA algorithm yields the lowest delay of 13.99, while ASC, HEPPA and ROAC methods resulted in higher Delays of 17.62, 16.62 and 15.62 respectively. For 200 nodes, the proposed WOA algorithm yields the lowest delay of 13.47, while ASC, HEPPA and ROAC methods resulted in higher delays of 18.39, 17.38 and 14.38 respectively. For 250 nodes, the proposed WOA algorithm yields the lowest delay of 15.39, while ASC, HEPPA and ROAC methods resulted in higher Delays of 19.39, 18.38 and 17.38 respectively.

Fig. 8. shows Overhead Analysis for the various node counts. for 50 nodes, the proposed WOA method yielded the lowest Overhead of 4395, while ASC, HEPPA and ROAC methods resulted in higher Overheads of 7527, 6527 and 5527 respectively. for 100 nodes, the proposed WOA method yielded the lowest Overhead of 3920, while ASC, HEPPA and ROAC methods resulted in higher Overheads of 7893, 6893 and 5893 respectively. For 150 nodes, the proposed WOA method yielded the lowest Overhead of 6253, while ASC, HEPPA and ROAC methods resulted in higher Overhead of 11648, 10648 and 9648 respectively. For 200 nodes, the proposed WOA method yielded the lowest Overhead of 6088, while ASC, HEPPA and ROAC methods resulted in higher Overheads of 12689, 11689 and 10689 respectively. for 250 nodes, the proposed WOA method yielded the lowest Overhead of 7962, while ASC, HEPPA and ROAC methods resulted in higher Overheads of 15777,14777 and 13777 respectively.

Fig. 9. shows for Drop analysis for various node count, for 50 nodes, the proposed WOA algorithm yields the lowest drop of 26, while ASC, HEPPA and ROAC methods resulted in higher drops of 54, 44 and 44 respectively. For 100 nodes, the proposed WOA algorithm yields the lowest drop of 45, while ASC, HEPPA and ROAC methods resulted in higher drops of 104,94and 84 respectively. For 150 nodes, the proposed WOA algorithm yields the lowest drop of 73, while ASC, HEPPA and ROAC methods resulted in higher drops of 108, 98 and 88 respectively. For 200 nodes, the proposed WOA algorithm yields the lowest drop of 61, while ASC, HEPPA and ROAC methods resulted in higher drops of 152,142 and 132 respectively. For 250 nodes, the proposed WOA algorithm yields the lowest drop of 7.03, while ASC, HEPPA and ROAC methods resulted in higher drops of 11.71, 10.71 and 9.7 respectively.

Fig. 10. shows Overhead Analysis, for number of nodes 50, the proposed WOA algorithm yields the lowest Overhead of 4395, while ASC, HEPPA and ROAC methods resulted in higher Overheads of 7527, 6527 and 5527 respectively. For number of nodes 100, the proposed WOA algorithm yields the lowest Overhead of 3920, while ASC, HEPPA and ROAC methods resulted in higher Overheads of 7893, 6893 and 5893 respectively. For number of nodes 150, the proposed WOA algorithm yields the lowest Overhead of 6253, while ASC, HEPPA and ROAC methods resulted in higher Overhead of 11648, 10648 and 9648 respectively. For number of nodes 200, the proposed WOA algorithm yields the lowest Overhead of 6088, while ASC, HEPPA and ROAC methods resulted in higher Overheads of 12689, 11689 and 10689 respectively. At node count of 250, the proposed WOA algorithm yields the lowest overhead of 7962, while ASC, HEPPA and ROAC methods resulted in higher Overheads of 15777, 14777 and 13777 respectively.

Fig. 11. shows Throughput analysis, for number of nodes 50, the proposed WOA algorithm yields the high throughput of 6085, while ASC, HEPPA and ROAC

methods resulted in lowest throughputs of 1254, 2254 and 3254 respectively. For number of nodes 100, the proposed WOA algorithm yields the high throughput of 3815, while ASC, HEPPA and ROAC methods resulted in low throughputs of 803,903 and 1903 respectively. For the nodes 150, the proposed WOA algorithm yields the highest throughput of 5495, while ASC, HEPPA and ROAC methods resulted in low throughput of 1696, 1796, 2796 respectively. For number of nodes 200, the proposed WOA algorithm yields the high throughput of 4225, while ASC, HEPPA and ROAC methods resulted in low throughput of 1780, 1880 and 2880 respectively. For node count 250, the proposed WOA algorithm yields the highest throughput of 4116, while ASC, HEPPA and ROAC methods resulted in lowest throughputs of 972, 1072, and 2072 respectively.

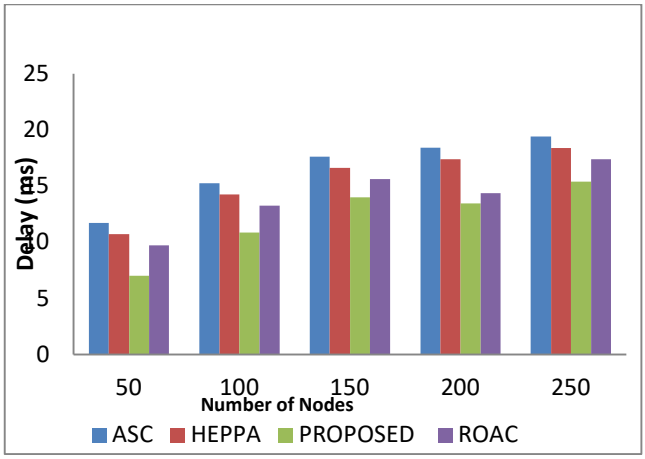

Fig.7..Delay Analysis in comparison between proposed and existing approaches

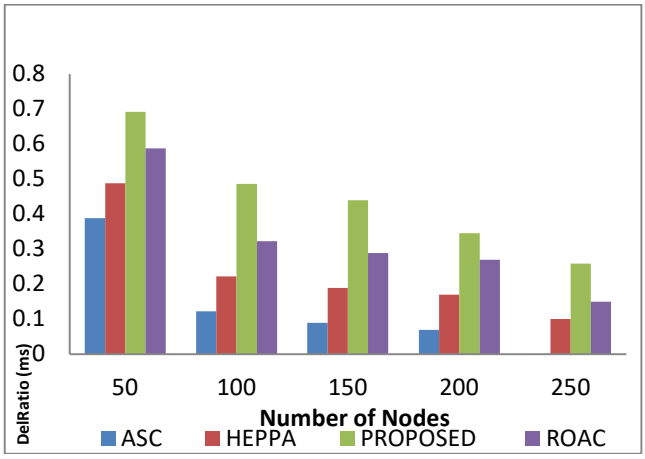

Fig. 8. Delivery Ratio Analysis in comparison between proposed and existing approaches

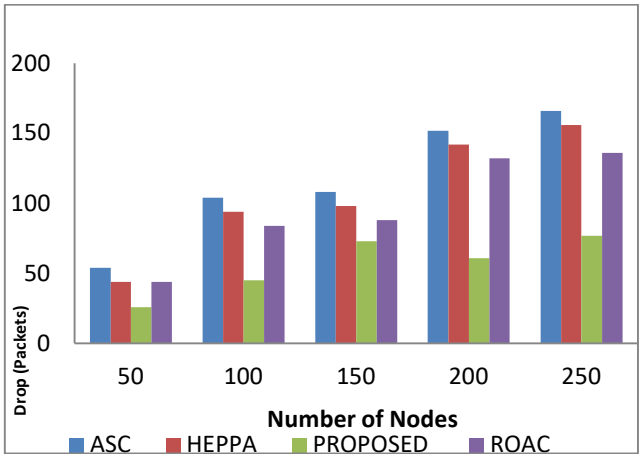

Fig. 9. Drop Analysis in Comparison between proposed and existing approaches

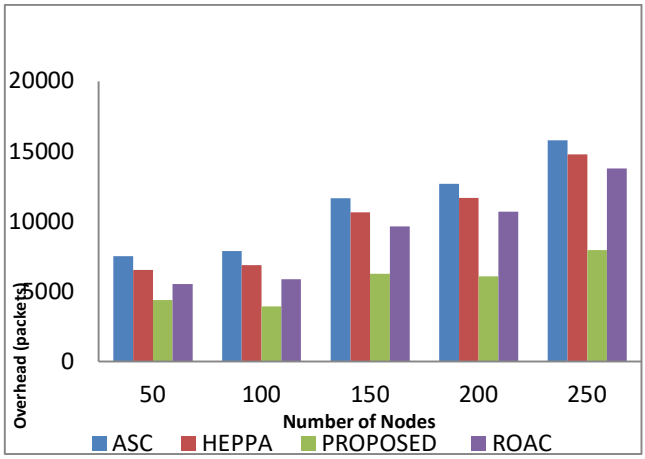

Fig. 10. Overhead Analysis in comparison between proposed and existing approaches

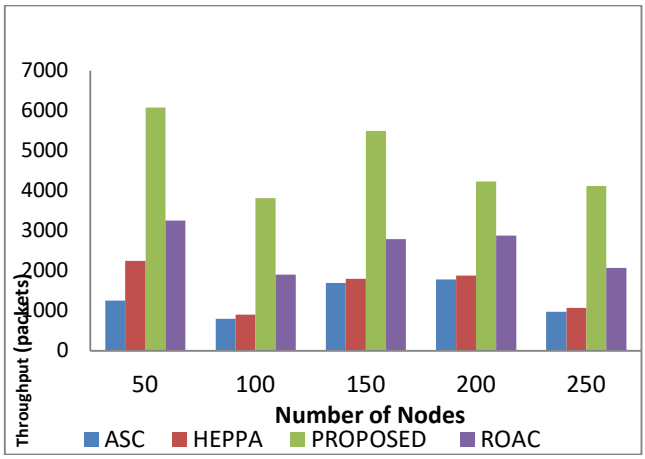

Fig. 11. Throughput Analysis in comparison between proposed and existing approaches

Acknowledgements

I would like to acknowledge and give my warmest thanks to my supervisor B N Manjunatha Reddy who made this work possible. His guidance and advice carried me through all the stages of writing my paper. I would also like to thank you my committee members for letting my defense be an enjoyable moment, and for your brilliant comments and suggestions, thanks to you.

References

[1] Bidiyng and Amiya Nayak:*Anonymous and Lightweight Authentication for Secure Vehicular Networks. IEEE Transactions on Vehicular Technology* Volume: 66, Issue: 12, Dec. 2017.

[2] Wazid, M.; Das, A.K.; Kumar, N.; Odelu,V.; Reddy, A.G.;Park, K.; Park,Y. :*Design of lightweight authentication and key agreement protocol for vehicular adhoc networks.*IEEE Access 2017 5, 14966–14980.

[3] Rajput, U.; Abbas, F.; Eun, H.; Oh, H,:*A hybrid approach for efficient privacy-preserving authentication in VANET*.IEEE Access 2017, 5, 12014–*12030.*

[4] Lei, A.; Ogah, C.; Al, E*, :A Secure Key Management Scheme for Heterogeneous Secure Vehicular Communication* Systems.ZteCommun, Mag. 2016, 111.

[5] Cui, J.; Zhang, J.; Zhong, H.; Xu, Y:*SPACF: A secure privacy-preserving authentication scheme for VANET with CUCKOO Filter.* IEEE Transmission Vehicle Technology, 2017, 66, 10283–10295.

[6] Leiding, B.; Memarmo shrefi, P.; Hogrefe, D.*:Self-managed and Block chain-based vehicular ad-hoc networks*. In Proceedings of the 2016 ACM Int. Jt. Conf.Pervasive Ubiquitous Comput. Adjun—UbiComp, Heidelberg, *Germany*, 12–16 September 2016; Volume 16, p. 137140.

[7] Dorri, A.:*Block chain: A Distributed Solution to Automotive Security and Privacy*. IEEE Commun. Mag. 2017, 55, 119–125.

[8] Rowan, S.; Clear, M.; Gerla, M.; Huggard, M.; Goldrick, C.M. :*Securing Vehicle to Vehicle Communications using Block chain through Visible Light and Acoustic Side Channels*. *arXiv* 2017, arXiv:1704.02553.

[9] Guo, S.; Hu, X.; Zhou, Z.; Wang, X.; Qi, F.; Gao, L.:*Trust access authentication in vehicular network based on Block chain.* China Commun. 2019, 16, 18–30.

[10] Sherazi, H.H.R.; Iqbal, R.; Ahmad, F.; Khan, Z.A.; Chaudary, M.H.:*DDoS attack detection: A key enabler forsustainable communication in internet of vehicles*.Sustain. Comput. Inf. Syst. 2019, 23, 13–20.

[11] Yang, Y.T.; Chou, L.D.; Tseng, C.W.; Tseng, F.H.; Liu, C.C. :*Block chain-based trace event validation and trust verification for VANETs*. IEEE Access 2019, 7, 30868–30877.

[12] Sherazi, H.H.R.; Khan, Z.A.; Iqbal, R.; Rizwan, S.; Imran,M.A.;Awan,K, :*A heterogeneous IoV architecture for data forwarding in vehicle to infrastructure communication*. Mob. Inf. Syst. 2019.

[13] S. Mirjalili and A. Lewis, :*the whale optimization algorithm*. Adv. Eng.Softw., vol. 95, pp. 51_67, May 2016.

[14] Ying, B. Nayak,:*An Anonymous and lightweight authentication for secure vehicular networks*. IEEE Trans.Veh. Technol. 2017, 66, 10626–10636

[15] Tangade, S.; Manvi, S.S. :*Scalable and privacy-preserving authentication protocol for secure vehicular communications*. International Proceedings of the 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems, Bangalore, India, 6–9 November 2016.

[16] Song, F.; Zhu, M.; Zhou, Y.; You, I.; Zhang, H. *:Smart collaborative tracking for ubiquitous power.* IoT inedge-cloud interplay domain. IEEE Int. Things J. 2019

[17] Moazzeni, A.R.; Khamehchi, E. :*Rain optimization algorithm (ROA): A new metaheuristic method for drilling optimization solutions.* J. Pet. Sci. Eng.2020.

[18] Shrestha, R.; Bajracharya, R.; Shrestha, A.P.; Nam, S.Y, :*A new type of Block chain for secure message exchange in VANET.* Digit. Commun. Netw. 2020, 6, 177–186.

[19] Prashar, D.; Jha, N.; Jha, S.; Joshi, G.P.; Seo, C:*Integrating IoT and Block chain for Ensuring Road Safety:An Unconventional Approach*. Sensors 2020, 20, 3296 [CrossRef]

[20] Dai, H.-N.; Zheng, Z.; Zhang, Y:*Block chain for Internet of Things: A Survey*. IEEE Internet Things J. 2019, 6,8076–8094. [CrossRef]

[21] Xuanxia Yao, Xinlei Zhang , Huansheng Ning and Pengjian Li:*Using Trust Model to Ensure Reliable Data Acquisition in VANETs*. Ad Hoc Networks, Vol. 55, pp. 107-118, 2017.

[22] Wafa Ben Jaballah, Mauro Conti and Chhagan Lal,:*Security and Design Requirements for Software-Defined VANETs",* Computer Networks. Vol. 169, No. 107099, 2020.

[23] R.Muthumeenakshi, T.R.Reshmi and K.Murugan:*Extended 3PAKE authentication scheme for value-added services in VANETs*.Computers & Electrical Engineering, Vol. 59, pp. 27-38, 2017.

[24] Dongyao Jia and Dong Ngoduy:*Enhanced cooperative car-following traffic model with the combination of V2V and V2I communication.* Transportation Research Part B: Methodological, Vol. 90, pp. 172-191, 2016.

[25] Ikram Ali, Mwitende Gervais, Emmanuel Ahene and Fagen Li:*A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs.* Journal of Systems Architecture, Vol. 99, No. 101636, 2019.

BIOGRAPHIES OF AUTHORS

Shazia Sulthana is Assistant Professor at the college of Global Academy of Technology, Visvesvaraya Technological University, Karnataka, India. She is having teaching experience of 15 years, currently perceiving Ph. D degree in the field of Wireless Networks under VTU, Karnataka, India. Her research areas are Vehicular Adhoc Networks, wireless Networks. she has published several papers in refereed International Journals and presented in National and International Conferences. she is a life member of IETE. she has attended several FDPs, conferences and workshops

Dr. B.N.Manjunatha Reddy has joined the Global Academy of Technology in the year 2004 and is currently working as a Professor in the Department of Electronics and Communication Engineering. His research and professional career spans about 23 years. He has completed his Ph.D. degree from VTU in the year 2018. His research interest is in the area of Low power VLSI and Embedded Systems. He has published several papers in refereed International Journals and presented in National and International Conferences. He has also visited many countries like Dubai, China, Thailand, Abu Dhabi and presented his research work. He is a life member of IETE. He has organized/attended several FDPs, conferences and workshops. He also had given several technical talks in many forums.