ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
https://doi.org/10.17559/TV-20211216115635
Original scientific paper

Efficient Privacy-Preserving Red Deer Optimization Algorithm with Blockchain Technology for Clustered VANET

Kalimuthu VINOTH KUMAR*, Balaganesh DURAISAMY

Abstract: Vehicular Adhoc Network (VANET) is a version of Mobile Adhoc Network (MANET). Owing to an increase in road accidents, VANET offers safety to road vehicles through appropriate coordination with vehicles and road side units. Along with the security guidelines of the vehicles in the network, privacy and security become vital parameters that need to be accomplished for secure data transmission in VANET. This study develops an efficient privacy-preserving data transmission architecture using red deer optimization algorithm based clustering with blockchain technology (RDOAC-BT) in cluster-based VANET. The proposed RDOAC-BT technique involves the design of RDOA based clustering technique to elect cluster heads (CHs) and construct clusters. In addition, blockchain technology is employed for secured transmission in VANET. Moreover, the blockchain is utilized to perform intra-cluster and inter-cluster communication processes. A wide range of simulations take place and the results are examined under varying aspects. The resultant outcome portrayed the betterment of the RDOAC-BT technique over the recent techniques.

Keywords: blockchain technology; CH selection; clustering; privacy; security; VANET

1 INTRODUCTION

In the last few years, vehicular ad hoc network (VANET) is becoming most appropriate dynamic wireless topology for worldwide business [1]. Urban VANET is extremely mobile adhoc wireless network which has been performed for providing emergency alert services, passenger safety, and driver assistance. VANET is developed for guarantying the infrastructure-based vehicle network, viz. vehicle centralized to infrastructure (V2I) at a time and self-organized vehicle training, viz., decentralized vehicle-to-vehicle communication (V2V) [2]. The urban VANET networks contribute to a huge amount of network traffics because numerous vehicle users (VU) share or utilize data enormously. A huge amount of applications from VANET network is now utilized, namely video on demand (VoD) and realtime streaming services [3]. Various methods for eHealth systems, sensor networks, intelligent network communications, and vehicle communications are introduced. But this presented system does not consider the privacy of users of VANET network and no longer considers limited bandwidth, dynamic topology, energy use, and limited physical security. Hence, it is very important but complex for designing an efficient method protecting the security and privacy of VANET network [4]. Fig. 1 depicts the architecture of VANET.

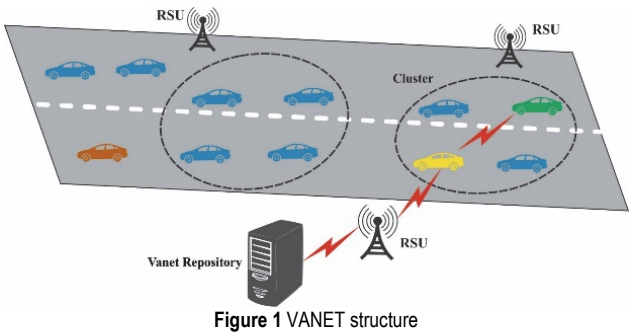

Figure 1 VANET structure

Privacy is one of the critical areas of concern which should be studied beforehand in the implementation of VANET technique [5]. Security needs are categorized based on the application kinds utilized in VANET. In this study, we focus mainly on security-based applications. Moreover, fundamental security messages are transmitted each 100-300 ms as recommended by the DSRC [6]. Therefore, the security needs immediate verification where a vehicle needs to validate huge quantity of messages, and non-repudiation must be assisted by the validation system for preventing users from being denied that they have not sent or received messages. The 3rd requirement is message integrity i.e., employed to guarantee the content of messages has not been changed at the time of transition and the final requirement is accessibility where attacker tries to do the network busy by introducing attacks like Denial of Service (DoS) [7]. The 2 methods are used for meeting the needs. Initially, asymmetric key cryptographic systems employ digital signatures. All the vehicles have a set of keys recognized as private and public keys that are utilized for generating and verifying digital signatures correspondingly. The next method is symmetric key authentication system.

Authentication should be attained at 2 stages - initially at node level, described as node authentication, and next at the message level, represented as message authentication [8]. The main objective of message authentication could be easier signing a message through the sender and later verifying the integrity and authenticity of the messages at the receiver end [9]. Authentication needs like strong and scalable authentication, efficient and scalable certificate revocation lower computation overhead should be solved and addressed for ensuring secured transmission in VANET [10]. Guaranteeing security of vehicle (driver) is the major problem where effective solutions need to be determined otherwise an adversary can track vehicle's traveling paths by analyzing and capturing its messages and recognize the vehicles (drivers) that might contain dramatic impact on the driver.

This study develops an efficient privacy-preserving data transmission architecture using red deer optimization algorithm based clustering with blockchain technology (RDOAC-BT) in cluster-based VANET. The proposed RDOAC-BT technique involves the design of RDOA based clustering technique to elect cluster heads (CHs) and construct clusters. In addition, blockchain technology is employed for secured transmission in VANET. Moreover,

the blockchain is utilized to perform intra-cluster and inter-cluster communication processes. A wide range of simulations take place and the results are examined under varying aspects. The increase in traffic once a day is a major test for the general population of developing nations. Accordingly, the capable experts should concentrate on road security to make the road traffic as efficient as could reasonably be expected. Information broadcasting from such a large number of sources with the limitation of message causes blockage issue in vehicular communication, in this way guaranteeing packet dropping, low energy efficiency and broadened delay. The proposed research work has been committed to the optimal routing structure in an energy-efficient way by optimizing the energy consumption parameter.

2 THE PROPOSED MODEL

In this study, a new RDOAC-BT technique is derived for efficient privacy-preserving data transmission architecture in VANET. The proposed RDOAC-BT technique involves the design of RDOA based clustering technique to elect CHs and construct clusters. In addition, blockchain technology is employed for secured transmission in VANET. Moreover, the blockchain is utilized to perform intra-cluster and inter-cluster communication processes.

2.1 Steps Involved in RDOAC Technique

Modified red deer algorithm (MRDA) has been presented. No such metaheuristics technique is to be in the works which are similarly retained explorations as well as exploitations. Distinct steps of the modified type of this technique were related to the subsequent subsection. As the original RDA, this modified form is also fixed for finding the global or near optimum solution in terms of certain issues. During the solution space (P), some possible solution has been assumed as red deer (RD) and it can be determined as:

$$RD = \left[P_1, P_2, P_3, \ldots, P_D\right] \tag{1}$$

During the primary stage, the population has been designed by making NP amount of RD solutions. According to the fitness value, an optimum RD is assumed as N_{male} and the rest of solutions have been assumed as N_{hind}. At this point, the elitism property has been monitored to elect RD in these 2 sets. According to these assets, the amount of males have been assumed as

$$N_{\text{male}} = \text{round}\left\{\alpha_1 . NP\right\} \tag{2}$$

where, α_1 implies the arbitrary constant value and $\alpha_1 \in \left[0.2,\ 0.5\right]$. The amount of hinds ($N_{\text{hind}}$) are represented as $N_{\text{hind}} = NP - N_{\text{male}}$. The places of male RDs, considered as optimum solutions have been tried to upgrade for getting optimum solutions from the neighbourhood. The natural observation of original technique was preserved and the arbitrariness to upgrade the place of male RDs is also integrated. In preference to utilized 3 constant values, individuals have been created arbitrarily from the original version of technique. Only one arbitrary constant value was implemented. For providing a Gradient in adaptability, and assist a progressively lower rate. The subsequent formulas have been projected for updating the places of males

$$male_{\text{new}} = \begin{cases} male_{\text{old}} - (1-a) * (ub - lb) * \dfrac{n}{i^2 + n}, & a < 0.5 \\ male_{\text{old}} + a * (ub - lb) * \dfrac{n}{i^2 + n}, & a \geq 0.5 \end{cases} \tag{3}$$

where, a refers to the arbitrarily created real number $a \in \left[0,\ 1\right]$ the present generation and the entire amount of generations have been represented as i and n correspondingly. According to the original RD technique, commanders and stags are 2 kinds of RD which are regarded in this modified type. The amount of commander males (N_{cm}) have been resolved from the subsequent manner:

$$N_{\text{cm}} = \text{round}\left\{\alpha_2 . N_{\text{male}}\right\} \tag{4}$$

where, α_2 represents the arbitrary constant value and $\alpha_2 \in \left[0.2,\ 0.5\right]$. Therefore, 20% to 50% of males are chosen as commanders. The rest of males have been assumed as the stags and the count of stags (N_{stag}) are calculated as:

$$N_{\text{stag}} = N_{\text{male}} - N_{\text{cm}} \tag{5}$$

The mathematical process is distinctively engineered to conserve further of the dominant features and less of recessive features with certain objective of availing gradient modification in values. During this case of Stag, it could be permitted for mating arbitrarily with some hind from the populations. Fig. 2 showcases the flowchart of RDA.

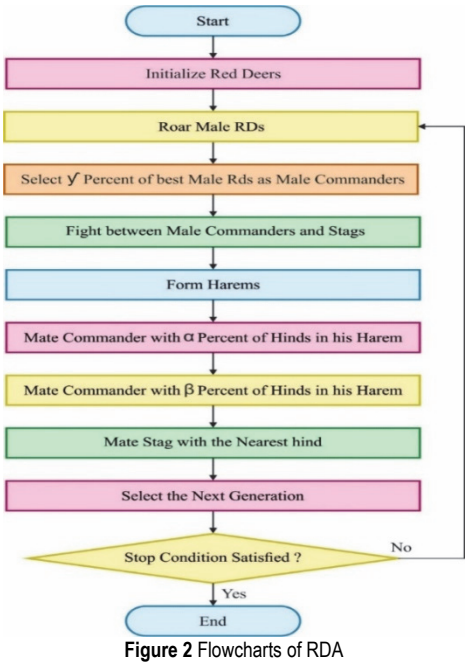

Figure 2 Flowcharts of RDA

For selecting the population for the next generation, the quality of the offspring *RD* has been estimated on the fundamental fitness value. According to the fitness value of present off-springs and the *RD* of the earlier generation, an optimum *RD* has been chosen for the next generation. The roulette wheel selection technique has been utilized in this chosen procedure. These steps remain to a particular count of iteration.

$$F = MaximizeFitness = \alpha * f_1 + \beta * f_2 + \gamma * \frac{1}{f_3} + \delta * \frac{1}{f_4} \quad (6)$$

where, α, β, γ, and δ refer the weighted coefficient to f_1, f_2, f_3, and f_4 FF parameter correspondingly. The range of weighted coefficients is diverse from the interval of 0 and 1.

2.2 Data Transmission using Blockchain Technology

At this stage, the blockchain is utilized to perform intra-cluster and inter-cluster communication processes. A blockchain is a dispersed public dataset of each digital event which had been achieved and distributed amongst contributing nodes. It has verifiable and definite records of entire events ever happened. All the events in the blockchain databases are authenticated by the consensus of most of the nodes in the network. There are primarily 2 kinds of blockchain, viz.., private blockchain and public blockchain. The public blockchain is an open blockchain where everyone could join up and communicate with the blockchain without getting authorization from central control. Conversely, the private blockchain depends on an access control method. It enables administrators to control the participant in networks and things like who can write, join and view the blockchain. During the private blockchain, the administrators might generate a consensus group. Therefore, the private blockchain could converge to be centralized and that generates it to be susceptible to a certain point of failure. But the public blockchain is a completely decentralized blockchain which does not have a certain point of failure problems and can resist malicious attacks [11].

The core of the blockchain is a genesis block i.e., the initial block in the blockchain. It is the popular source of each block and comprises the data i.e., usually recognized to each node. The block comprises cryptographic hashes of record, with every block having the data regarding the forming a chain of data, creating a blockchain, and prior block hash. The block body comprises list of transactions and further information, based on the requirements of the blockchain. All the present blocks are connected to the prior block, with the hashes of prior blocks such as chain.

The Merkle hash has been drawn in the Merkle approach, i.e., a cryptographic system which hashes each transaction of the blocks to attain the Merkel root. The advantage of Merkel tree is that it can confirm transaction as needed and does not involve the body of each transaction in the block header when providing an approach to authenticate the entire blockchain. It creates a distinctive hash value which validates the integrity of each transaction under it, and the size of the Merkel hash is smaller than the entire size of each transaction. The blockchain has achieved enormous popularity because of its security characteristics of utilizing cryptography.

3 EXPERIMENTAL VALIDATION

The experimental validation of the ROAC-B with existing techniques takes place in terms of varying aspects. Tab. 1 and Fig. 3 illustrate the ETE delay analysis of the ROAC-B with recent techniques under varying node counts. The results demonstrated that the ROAC-B technique has gained a lower ETE delay.

Table 1 ETE delay analysis of ROAC-B model with number of nodes

End to End Delay / s				
Number of Nodes	HEPPA	LASKAP	ASC	ROAC-B
20	0.288	0.131	0.142	0.115
40	0.301	0.184	0.221	0.193
60	0.338	0.281	0.251	0.203
80	0.432	0.374	0.328	0.298
100	0.475	0.522	0.361	0.308

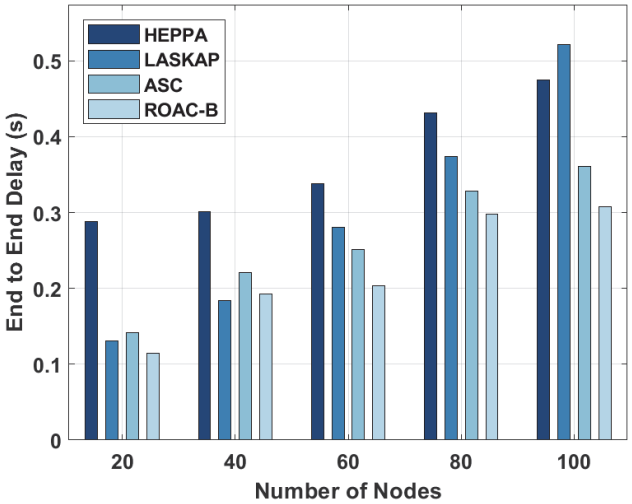

Figure 3 ETE analysis of ROAC-B model with existing techniques

For instance, with 20 nodes, the ROAC-B technique has accomplished a lower ETE delay of 0.115 s whereas the HEPPA, LASKAP, and ASC techniques have reached a higher ETE delay of 0.131 s, 0.142 s, and 0.115 respectively. Likewise, with 60 nodes, the ROAC-B method has accomplished a lower ETE delay of 0.203s whereas the HEPPA, LASKAP, and ASC systems have attained a superior ETE delay of 0.338 s, 0.281 s, and 0.251 correspondingly. At the same time, with 100 nodes, the ROAC-B approach has accomplished a lower ETE delay of 0.308s whereas the HEPPA, LASKAP, and ASC manners have reached a superior ETE delay of 0.475 s, 0.522 s, and 0.361 correspondingly.

Table 2 PDR analysis of ROAC-B model with number of nodes

Packet Delivery Ratio				
Number of Nodes	HEPPA	LASKAP	ASC	ROAC-B
20	0.841	0.699	0.758	0.900
40	0.731	0.680	0.630	0.761
60	0.701	0.641	0.581	0.751
80	0.671	0.640	0.571	0.699
100	0.573	0.575	0.531	0.632

The PDR analysis of the ROAC-B technique with several methods takes place in Tab. 2 and Fig. 4. The

results have shown that the ROAC-B technique has resulted in an increased PDR under varying nodes. For instance, with 20 nodes, the ROAC-B technique has offered a higher PDR of 0.900 whereas the HEPPA, LASKAP, and ASC techniques have reached a lower PDR of 0.841, 0.699, and 0.758 respectively. In addition, with 60 nodes, the ROAC-B methodology has increased PDR of 0.751 whereas the HEPPA, LASKAP, and ASC methodologies have attained a minimum PDR of 0.701, 0.641, and 0.581 correspondingly. Finally, with 100 nodes, the ROAC-B technique has offered a higher PDR of 0.632 whereas the HEPPA, LASKAP, and ASC techniques have reached a minimum PDR of 0.573, 0.575, and 0.531 correspondingly.

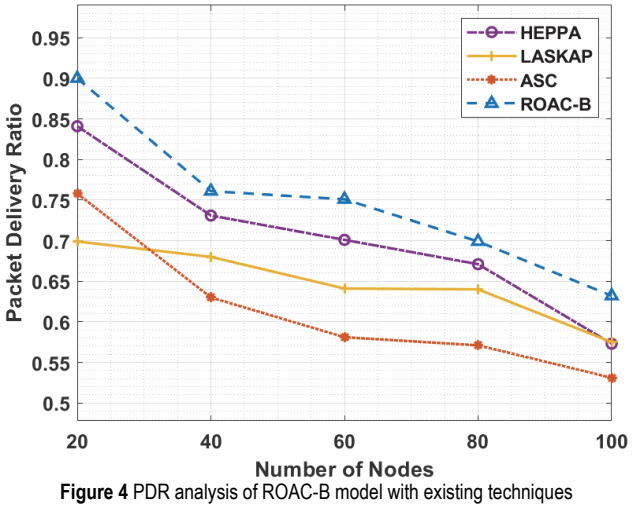

Figure 4 PDR analysis of ROAC-B model with existing techniques

Table 3 PLR analysis of ROAC-B model with count of nodes

Packet Loss Ratio				
Number of Nodes	Number of Nodes	Number of Nodes	Number of Nodes	Number of Nodes
20	0.159	0.301	0.242	0.100
40	0.269	0.320	0.370	0.239
60	0.299	0.359	0.419	0.249
80	0.329	0.360	0.429	0.301
100	0.427	0.425	0.469	0.368

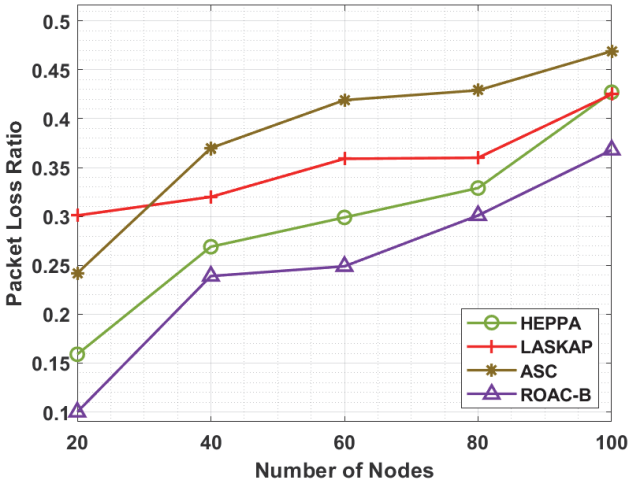

Figure 5 PLR analysis of ROAC-B model with existing techniques

Tab. 3 and Fig. 5 demonstrate the PLR delay analysis of the ROAC-B with recent manners under varying node counts. The results demonstrated that the ROAC-B technique has gained a lower PLR delay. For instance, with 20 nodes, the ROAC-B approach has accomplished a minimum PLR delay of 0.100 whereas the HEPPA, LASKAP, and ASC methods have reached a higher PLR delay of 0.159, 0.301, and 0.242 respectively.

Followed by, with 60 nodes, the ROAC-B technique has accomplished a minimum PLR delay of 0.249s whereas the HEPPA, LASKAP, and ASC approaches have gained a maximum PLR delay of 0.299, 0.359, and 0.419 individually. At last, with 100 nodes, the ROAC-B technique has accomplished a lower PLR delay of 0.368 whereas the HEPPA, LASKAP, and ASC techniques have reached a higher PLR delay of 0.427, 0.425, and 0.469 correspondingly.

The throughput analysis of the ROAC-B approach with several manners takes place in Tab. 4 and Fig. 6. The outcomes exhibited that the ROAC-B system has resulted in an increased throughput under varying simulation times. For instance, with 20 simulation time, the ROAC-B approach has offered a higher throughput of 14.87% whereas the HEPPA, LASKAP, and ASC techniques have obtained a decreased throughput of 7.85%, 6.02%, and 10.90% respectively.

Table 4 Throughput analysis of ROAC-B model with existing techniques

Throughput / %				
Simulation Time / s	HEPPA	LASKAP	ASC	ROAC-B
5	1.44	1.44	3.58	8.16
10	3.27	2.97	5.10	8.16
15	6.32	4.80	9.38	13.04
20	7.85	6.02	10.90	14.87
25	10.29	12.12	15.18	19.15
30	18.23	24.03	20.67	23.73
35	22.20	27.09	37.47	39.60
40	26.17	28.61	50.60	53.34
45	29.22	29.53	52.73	57.01
50	34.11	35.33	54.56	60.06
55	38.99	41.13	58.23	60.67
60	41.44	47.24	60.37	62.50
65	48.15	52.43	60.98	64.03
70	53.95	61.59	64.33	67.39
75	60.06	66.17	70.75	75.33
80	65.56	69.83	75.33	78.99
85	70.75	73.19	78.99	83.26
90	72.58	75.33	81.43	84.79
95	75.33	80.21	84.79	89.07
100	80.21	83.26	89.98	94.26

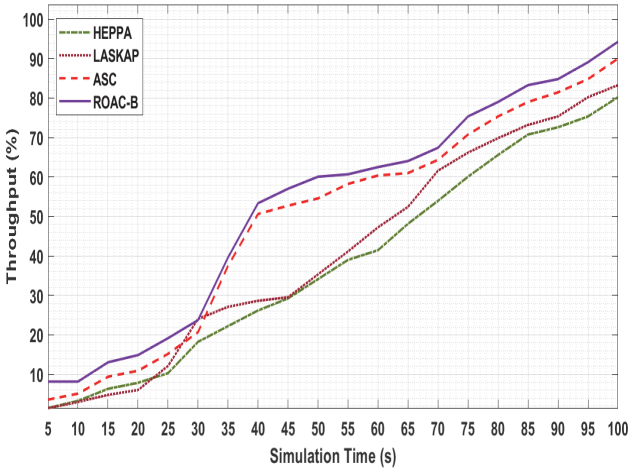

Figure 6 Throughput analysis of ROAC-B model with existing techniques

Finally, with 100 simulation time, the ROAC-B methodology has obtainable an increased throughput of 94.26% whereas the HEPPA, LASKAP, and ASC

techniques have attained a lesser throughput of 80.21%, 83.26%, and 89.98% correspondingly.

4 CONCLUSION

In this study, a new RDOAC-BT technique is derived for efficient privacy-preserving data transmission architecture in VANET. The proposed RDOAC-BT technique involves the design of RDOA based clustering technique to elect CHs and construct clusters. Besides, blockchain technology is employed for secured transmission in VANET. Furthermore, the blockchain is utilized to perform intra-cluster and inter-cluster communication processes. A wide range of simulations take place and the results are examined under varying aspects. The resultant outcome portrayed the betterment of the RDOAC-BT technique over the recent techniques. In future, data aggregation concepts can be employed to enhance the energy efficient performance of the VANET.

5 REFERENCES

[1] Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H., & Zedan, H. (2014). A comprehensive survey on vehicular ad hoc network. *Journal of network and computer applications, 37*, 380-392. https://doi.org/10.1016/j.jnca.2013.02.036

[2] Li, F. & Wang, Y. 2007. Routing in vehicular ad hoc networks: A survey. *IEEE Vehicular technology magazine*, *2*(2), 12-22. https://doi.org/10.1109/MVT.2007.912927

[3] Yousefi, S., Mousavi, M. S., & Fathy, M. (2006). Vehicular ad hoc networks (VANETs): challenges and perspectives. *6th international conference on ITS telecommunications*, 761-766. https://doi.org/10.1109/ITST.2006.289012

[4] Rasheed, A., Gillani, S., Ajmal, S., & Qayyum, A. (2017). Vehicular ad hoc network (VANET): A survey, challenges, and applications. *Vehicular Ad-Hoc Networks for Smart Cities*, 39-51. https://doi.org/10.1007/978-981-10-3503-6_4

[5] Tanwar, S., Vora, J., Tyagi, S., Kumar, N., & Obaidat, M. S. (2018). A systematic review on security issues in vehicular ad hoc network. *Security and Privacy*, *1*(5), 39. https://doi.org/10.1002/spy2.39

[6] Kumar, A. & Sinha, M. (2014). Overview on vehicular ad hoc network and its security issues. *International conference on computing for sustainable global development (INDIACom)*, 792-797. https://doi.org/10.1109/IndiaCom.2014.6828071

[7] Saha, A. K. & Johnson, D. B. (2004). Modeling mobility for vehicular ad-hoc networks. *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, 91-92. https://doi.org/10.1145/1023875.1023892

[8] Kumar, A., Varadarajan, V., Kumar, A., Dadheech, P., Choudhary, S. S., Kumar, V. A., Panigrahi, B. K., & Veluvolu, K. C.(2021). Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. *Microprocessors and Microsystems*, *80*, 103352. https://doi.org/10.1016/j.micpro.2020.103352

[9] Sheikh, M. S., Liang, J., & Wang, W. (2020). Security and privacy in vehicular ad hoc network and vehicle cloud computing: a survey. *Wireless Communications and Mobile Computing*, *2020*. https://doi.org/10.1155/2020/5129620

[10] Günay, F. B., Öztürk, E., Çavdar, T., & Hanay, Y. S. (2021). Vehicular ad hoc network (VANET) localization techniques: a survey. *Archives of Computational Methods in Engineering*, *28*(4), 3001-3033. https://doi.org/10.1007/s11831-020-09487-1

[11] Kumari, A., Gupta, R., Tanwar, S., & Kumar, N. (2020). A taxonomy of blockchain-enabled softwarization for secure UAV network. *Computer Communications*, *161*, 304-323. https://doi.org/10.1016/j.comcom.2020.07.042

Contact infomation:

Dr. Kalimuthu VINOTH KUMAR, Post-Doctoral Research Fellow
(Corresponding author)
Department of ECE, Faculty of Computer Science and Multimedia,
Lincoln University College, Malaysia
E-mail: vinodkumaran87@gmail.com

Dr. Balaganesh DURAISAMY, Dean
Faculty of Computer Science and Multimedia,
Lincoln University College, Malaysia
E-mail: balaganesh@lincoln.edu.my