Bulletin of Electrical Engineering and Informatics
Vol. 12, No. 5, October 2023, pp. 2993~2999
ISSN: 2302-9285, DOI: 10.11591/eei.v12i5.5223

On the design of trust and mobility based evaluation for intelligent collaborative UAVs assisted VANETs

Sami Abduljabbar Rashid, Ahmed Shamil Mustafa, Abdulkareem Dawah Abbas, Hamza Qasim Abdullah, Mohammed Jassim Mohammed
Department of Computer Engineering Techniques, Al-Maarif University College, Ramadi, Iraq

Article Info

Article history:

Received Nov 13, 2022
Revised Dec 16, 2022
Accepted Feb 16, 2023

Keywords:

Crow swarm optimization
Genetic algorithm
Multipath greedy routing
UAVs assisted VANETs
Vehicular adhoc network

ABSTRACT

In recent days, vehicles usage and speed are highly increased that leads to an increase in energy consumption, delay, and overhead in the network. In this paper, a novel trajectory is introduced to achieve maximum reliability namely trust and mobility-based evaluation for intelligent collaborative (TMIC)-UAVs assisted VANETs. Reactive multipath greedy routing protocol (RMGR) is the hybrid routing protocol and it is the combination of ad hoc on-demand multipath distance vector (AOMDV) with greedy geographic forwarding (GGF) which is used for routing in frequently changeable network topology. To protect the network from malfunctions, effective trust evaluation (ETE) is performed by calculating the direct trust and indirect trust. Finally, to achieve effective communication among the UAVs, hybrid optimization is performed which is the combination of the genetic algorithm (GA) and the crow swarm optimization (CSO) algorithm. For validation network simulator (NS3) is used and the results show that this approach achieves high energy efficiency, delivery ratio, and reduction in delay when compared with the earlier research.

Corresponding Author:

Sami Abduljabbar Rashid
Department of Computer Engineering Techniques, Al-Maarif University College
Wattana, Radamdi, Iraq
Email: sami25.6.1989@gmail.com

1. INTRODUCTION

Vehicular ad hoc network (VANET) is the subset class of mobile ad hoc networks (MANET) which follows the mechanism of mobile vehicles to develop communication between huge numbers of mobile devices to exchange information in a cost-effective manner. Nowadays the vehicles which are used in road safety application are highly increasing so it becomes highly essential to concentrate on trust ability and communication protocols. At the initial stage of VANETs communication, the simple network consists of two types of communication models in order to perform the data transmission. They are vehicle-to-vehicle and vehicle to roadside unit (RSU) [1]. These are considered a ground-level communication models which provide a successful transmission during the process of communication between the source and the destination. Later on to improve critical road-safety information as well as to manage the usage of the vehicles in the network routing protocols are introduced [2]. The most challenges in this kind of network are managing the communication among the high-speed vehicles hence it gets affected by ground-level obstacles during communication. To that in recent days, unmanned aerial vehicles (UAVs) are introduced in VANETs so that the network gets free from ground-level obstacles where the communication is proceeded in ground to air (G-A) medium [3]–[5]. Furthermore, UAVs need separate routing protocols so it is essential to develop a reliable routing protocol for UAVs to achieve effective communication in the network. In general, UAVs

maintain highly flexible mobility and it helps to address the like failures, delays and routing overhead which is occurred during the transmission in VANETs [6]. Finally to improve the effectiveness of communication in UAVs assisted VANETs it becomes essential to concentrate on the vehicle's trust ability, mobility, and routing. So that in this paper a novel design is developed for the UAVs assisted VANETs and its contribution is described.

In this paper, to improve the effectiveness of the UAVs assisted VANETs a novel trust and mobility based evaluation for an intelligent collaborative approach. To perform data transmission in UAVs effective routing protocol is essential that reactive multipath greedy routing protocol (RMGR) is introduced which is a combination of the ad hoc on-demand multipath distance vector (AOMDV) and greedy geographic forwarding (GGF). The trust evaluation method is the combination of direct and indirect trust computation which helps to improve the trustworthiness among the vehicles. Mobility prediction is performed according to the input parameters using the weight value is calculated to predict the mobility of the vehicle. To proceed effective communication in the ground-to-air medium hybrid optimization is performed which is the combination of the genetic algorithm (GA) and the crow swarm optimization (CSO) algorithm. The remainder of this paper is organized as follows. In section 2 the related work about the UAVs assisted VANETs and the earlier trust and mobility models of VANETs are discussed. In section 3, the proposed trust and mobility aware intelligent collaborative UAVs assisted VANETs approach is detailed. In section 4 the performance analysis and results are discussed. Finally, in section 5 the paper is concluded and the future direction of the research is given.

2. RELATED WORKS

Several earlier works are present in terms of UAVs assisted VANETs such as UAV-assisted content distribution method [7], VRU protocol [8], low-cost UAV radar-based highway monitoring application [9], mobility and energy-aware joint optimization method for data routing in UAV-aided VANETs [10], multi-objective optimization [11], and 3D routing for UAV assisted VANETs [12]. To improve the effectiveness of communication in VANETs in earlier research several trust models are introduced in VANETs. They are trust cascading-based emergency message dissemination (TCEMD) model [13], risk-based trust evaluation advanced model (RTEAM) [14], trust model for location privacy protection [15], context-aware trust management model [16], anonymous cloaking zone creation approach based on a trust mechanism [17], "VAR2" strategy that permits autonomous trust model [18], a vehicle trust evaluation approach based on a hidden markov model (HMM) that increases the accuracy in the identification of malicious activity [19], a trusted routing strategy based on block-chain and fuzzy logic to enhance the identification of rogue nodes in VANET [20], a consortium block-chain-based strategy for preventing insider assaults in the VANET system utilizing the trusted AODV protocol [21], adaptive traffic-management system (ATM), an effective active-detection trust management system [22], the trust model to protect the UAVs assisted VANETs [23], UAV-assisted ubiquitous trust evaluation (UUTE) framework [24], and lightweight attestation mechanism [25]. Once after analysis the earlier research which is based on trust in UAV assisted VANETs the major drawback which is identified are increased energy consumption, delay and overhead in the network. To overcome these drawbacks a new model is developed namely, trust and mobility-based evaluation for intelligent collaborative (TMIC)-UAVs assisted VANETs and it is detailed in the upcoming section.

3. TRUST AND MOBILITY AWARE INTELLIGENT COLLABORATIVE UAVs ASSISTED VANETs

To improve the effectiveness of the communication in UAVs assisted VANETs a novel approach is proposed in the research called TMIC-UAVs assisted VANETs. The primary concentration of this proposed approach is that to improve the trust worthiness and the mobility of the UAVs assisted VANETs. For that purpose certain segments are developed in this approach such as effective trust evaluation (ETE) which is based on direct and indirect computation, intelligent mobility prediction (IMP) based routing in RMGR protocol and optimal path prediction using genetic crow swarm optimization (GCSO) algorithm. The workflow of the proposed TMIC-UAVs is given in Figure 1.

3.1. Effective trust evaluation

The attackers from the blackhole attack and the link flooding attack mainly concentrate on the ground level communication which affects the data transmission between the vehicles. So in order to protect the communication between the vehicles the inter-vehicular trust model is focused which is based on the measurements and the evaluation of direct trust and indirect trust of the vehicles. The direct trust values of the vehicles are evaluated using the direct interactions between them where the indirect trust values of the

vehicles are evaluated using the direct interactions between vehicles according to the estimation of its neighbors.

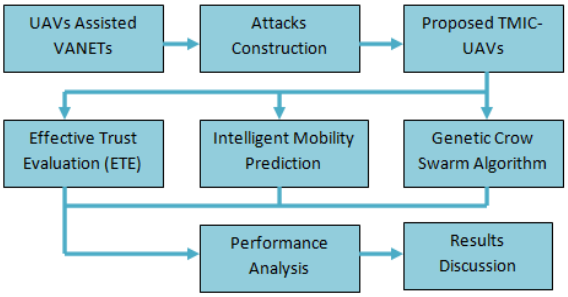


Figure 1. Workflow of the proposed TMIC-UAVs

3.1.1. Direct trust evaluation

The calculation of direct trust among any two vehicles are represented as $DT_{(V_1,V_2)}$ which is used to provide a truthful report about the authorized (A) and malicious (M) actions performed during communication. The mathematical expression for the calculation of the direct trust evaluation is described in (1):

$$DT_{(V_1,V_2)} = \frac{A_{(V_1,V_2)}}{M_{(V_1,V_2)} + A_{(V_1,V_2)}} \times \left[\alpha - \frac{1}{A_{(V_1,V_2)}+1}\right] \times \left[\beta - \frac{1}{M_{(V_1,V_2)}-1}\right] \quad (1)$$

Where the terms $A_{(V_1,V_2)}$ and $M_{(V_1,V_2)}$ implies the authorized and malicious actions of the vehicles, α and β are the experimental constants which satisfies the condition $\alpha + \beta = 1$, $\frac{A_{(V_1,V_2)}}{M_{(V_1,V_2)} + A_{(V_1,V_2)}}$ implies the quantity of authorized communication to the total number of communication, $\left[\alpha - \frac{1}{A_{(V_1,V_2)}+1}\right]$ implies the increase of authorized communication and $\left[\beta - \frac{1}{M_{(V_1,V_2)}-1}\right]$ implies the decrease of the malicious communication. From (1) the trust level and its improved is indentified.

3.1.2. Indirect trust evaluation

The calculation of indirect trust among any two vehicles are represented as $IDT_{(V_1,V_2)}$ which is based on the trustful (T) and harmful (H) estimation of the neighbors for each instant of time. The mathematical expression for the calculation of the indirect trust evaluation is described in (2):

$$IDT_{(V_1,V_2)} = \sum_{N=1}^{V_n} DT_{(V_1,V_n)} \times \left[\alpha_1 - \frac{1}{T_{(V_1,V_n)}}\right] \times \left[\beta_1 - \frac{1}{H_{(V_1,V_n)}}\right] \quad (2)$$

Where the terms $T_{(V_1,V_n)}$ and $H_{(V_1,V_n)}$ implies the trustful and harmful estimation of the neighbor V_n, N implies the total number of recommendations of the neighbors, α_1 and β_1 are the experimental constants which satisfies the condition $\alpha_1 + \beta_1 = 1$. Using (1) and (2) the total trust estimation $TRUST_{(V_1,V_2)}$ of the vehicles are calculated and it is expressed in (3):

$$TRUST_{(V_1,V_2)} = \left[\left(C_1 - \frac{1}{I_{count}}\right) \times DT_{(V_1,V_2)}\right] + \left[\left(C_2 - \frac{1}{I_{count}}\right) \times IDT_{(V_1,V_2)}\right] \quad (3)$$

Where the terms C_1 and C_2 implies the constants, I_{count} implies the number of interactions performed among the vehicles. According to (3) the total trust level of the vehicles is measured and it gets updated at each instant of time. This is the process of direct and indirect trust calculation in the ETE process.

3.2. Intelligent mobility prediction in RMGR protocol

To improve the stability of the RMGR protocol, the parameter-based IMP method is combined with it. The parameters which are considered for the calculation of the position of the vehicles are distance, time interval, neighbor angle, velocity, and acceleration. The steps to implement the IMP-RMGR protocol are described:

- Step 1: according to the defined parameters such as distance, time interval, neighbor angle, velocity and acceleration the weight of the source node is calculated.

- Step 2: through HELLO packets transmission the neighbor detection is performed.
- Step 3: the distance and the neighbor angles which are considered to reach the destination are calculated.
- Step 4: finally using those parameters the weight of the neighbor to reach the destination is measured as well as the path to reach the destination is selected.
- Step 5: route request (RREQ) is transmitted in the selected path. Once after reaching the destination, the vehicle transmits the route reply (RREP). In case any link failure occurs then the route error (RERR) is transmitted to the destination and the source. Then to find the current best path it steps from 1 to 4 are repeated.

3.3. Genetic crow swarm optimization algorithm

The GCSO algorithm is one among the hybrid algorithm which works which the combination of the GA and the CSO algorithm which is designed to find an optimal path between the vehicles to reach their respective UAV. In general, GA is the process of natural path selection between source and destination. It works with the generated population then the best solution is optioned using the selection, crossover, and mutation process. In the CSO algorithm, the intelligence of crows is utilized to find the optimal path among the vehicles. Commonly the crows live in the form of a flock by hiding their location which follows each other to perform communication and it intelligently protects their caches. At the initial condition to find the path between the source and the destination the CSO algorithm is used and to validate the path GA algorithm is applied in it. The process of CSO algorithm is illustrated in the pseudo-code below.

```
START
Create flock position in a random manner where all the crows (V) are located at the
sample crow space
Crows location finding
Memory allocation for the crows
While iter_num < iter_max
   For i = 1: v (v → crows count)
   Neighbor selection is random
   Measure the awareness:
        if r_v1 ≥ A^(v1,iter_num)
           v^(i,iter_num+1) = v^(i,iter_num) × (m^(i,iter_num − v^(i,iter_num))
        Else,
           v^(i,iter_num+1) → Select any position in the sample crow space
           End if
   End while
```

4. SIMULATION ENVIRONMENTS AND PERFORMANCE ANALYSIS

For the process of experimentation, the simulator which is preferred for the implementation is network simulator (NS3) and simulation of urban mobility (SUMO) in an ubuntu operating system 20.04. Using open street maps (OSM) the input real-time traffic is captured and the performance of the proposed TMIC-UAVs approach is analyzed in the NS3 simulation environment. The network is observed for the run time of 300 seconds. That observation is applied to the comparative study and the performance of the proposed TMIC-UAVs approach is have been compared with that of three other recently developed approaches such as traveling salesman problem (TSP)-UAVs [18], universal target control station (UTCS)-UAVs [19] and space-time adaptive processing (STAP)-UAVs [20]. Furthermore, the performance is analyzed in terms of energy efficiency, packet delivery ratio and end to end delay.

4.1. Energy efficiency calculation

In Figure 2(a) the effect of energy efficiency is investigated for the proposed TMIC-UAVs approach and it is compared with the earlier research. To achieve effective network performance it is essential to attain maximum energy efficiency. From the figure it is understood that the proposed TMIC-UAVs approach produced high energy efficiency when compared with the earlier approaches. The energy efficiency achieved by the proposed TMIC-UAVs approach is 92.69% whereas for the earlier methods such TSP-UAVs, UTCS-UAVs, and STAP-UAVs it reaches up to 76.54%, 82.23%, and 85.17% respectively. So the energy efficiency of the proposed TMIC-UAVs approach is 16% higher than TSP-UAVs, 10% higher than UTCS-UAVs, and 7% higher than STAP-UAVs.

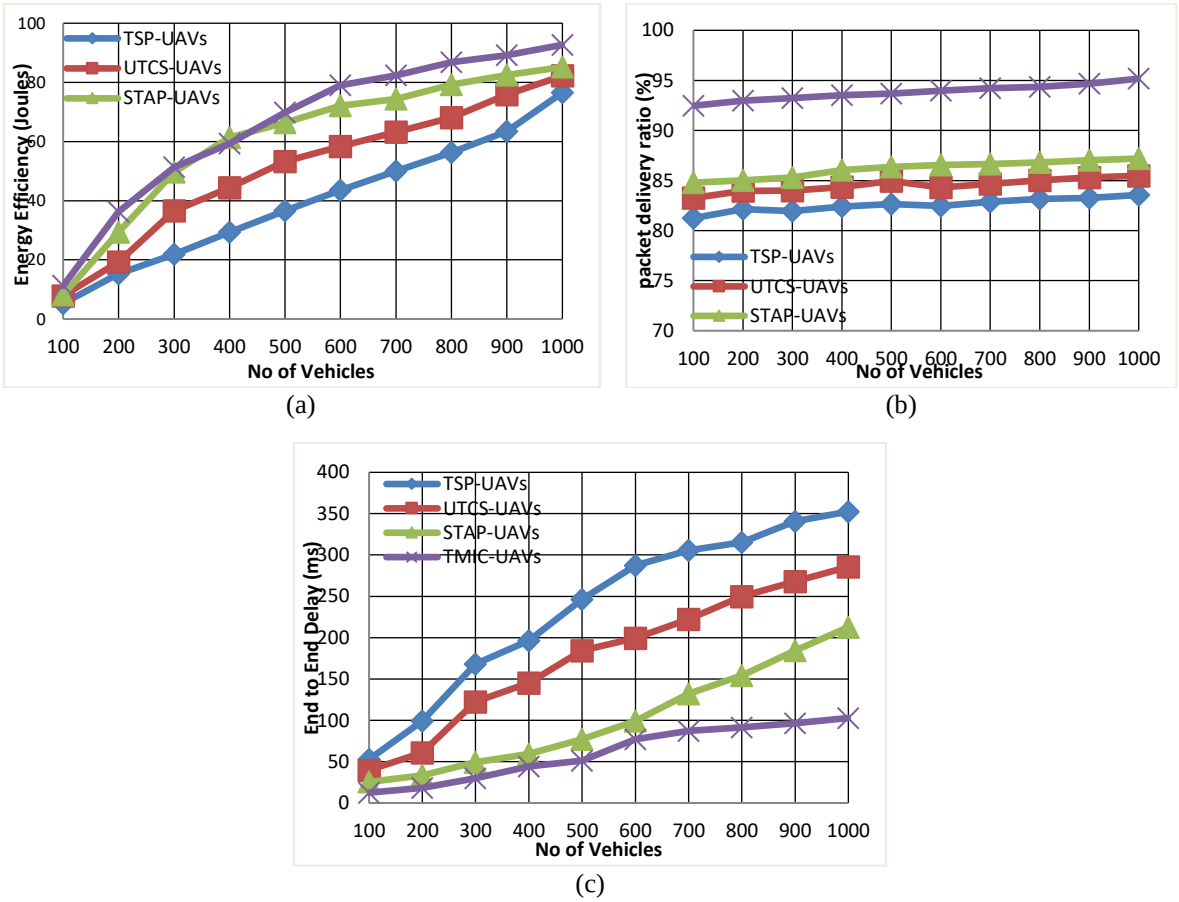
4.2. Packet delivery ratio calculation

In Figure 2(b) the calculation of the packet delivery ratios is performed in terms of (%) and the performance of the proposed TMIC-UAVs approach is compared with the earlier research. Achieving a high packet delivery ratio reflects in the improvement of the overall performance of the UAV assisted VANETs.

From the figure it is proven that the proposed TMIC-UAVs approach achieved a high packet delivery ratio when compared with the earlier approaches. The packet delivery ratio achieved by the proposed TMIC-UAVs approach is 95.17% whereas for the earlier methods such TSP-UAVs, UTCS-UAVs, and STAP-UAVs it reaches up to 83.56%, 85.47%, and 87.19% respectively. So the packet delivery rate of the proposed TMIC-UAVs approach is 12% higher than TSP-UAVs, 10% higher than UTCS-UAVs, and 8% higher than STAP-UAVs.

4.3. End to end delay calculation

In Figure 2(c) the calculation of the end-to-end delays is performed in terms of (ms) and the performance of the proposed TMIC-UAVs approach is compared with the earlier research. The core objective of the proposed method is to reduce the end-to-end delay during the time of data transmission between the vehicles and the UAVs. From figure it is shown that the proposed TMIC-UAVs approach produced low delay when compared with the earlier approaches. The end-to-end delay produced by the proposed TMIC-UAVs approach during the process of data transmission between the UAVs and the vehicles is 102.79 ms whereas for the earlier methods such TSP-UAVs, UTCS-UAVs, and STAP-UAVs it reaches up to 352.48 ms, 285.75 ms, and 212.76 ms respectively.



(a) (b)

(c)

Figure 2. Performance analysis (a) energy efficiency, (b) packet delivery ratio, and (c) end to end delay calculations

5. CONCLUSION

In this paper, the novel TMIC approach is developed for UAVs assisted VANETs. To improve the network from the earlier routing issues like delay and overhead a hybrid routing is performed to achieve better performance called RMGR is introduced which is the combination of the AOMDV and GGF. The proposed approach works with three major segments they are trust evaluation, mobility prediction, and hybrid optimization. Trust evaluation is introduced to protect the network from ground level malicious activities and obstacles. To reduce the congestion and delay in the network mobility prediction is performed and this improves the packet delivery ratio and reduces the delay issues. To provide an optimal solution in

the ground-to-air level communication hybrid optimization is performed which is the combination of the GA and the CSO algorithm. The simulation is performed in terms of a varying number of vehicles and the outcome is showen and it is compared with the TSP-UAVs, UTCS-UAVs, and STAP-UAVs. In terms of a number of vehicles, the proposed TMIC-UAVs achieve 4% to 13% high energy efficiency, 7% to 18% high packet delivery ratio, and 100 ms to 220 ms lower end-to-end delay, in a real-time traffic scenario. As a result the overall performance of the proposed TMIC-UAVs is higher compared with the earlier approaches. In the future direction to improve the coverage area and the number of UAVs in the network clustering can be implemented.

REFERENCES

[1] S. Li, F. Wang, J. Gaber, and X. Chang, "Throughput and energy efficiency of cooperative ARQ strategies for VANETs based on hybrid vehicle communication mode," *IEEE Access*, vol. 8, pp. 114287–114304, 2020, doi: 10.1109/ACCESS.2020.3003813.

[2] N. M. A. -Kharasani, Z. A. Zukarnain, S. K. Subramaniam, and Z. M. Hanapi, "An adaptive relay selection scheme for enhancing network stability in VANETs," *IEEE Access*, vol. 8, pp. 128757–128765, 2020, doi: 10.1109/ACCESS.2020.2974105.

[3] A. K. Kazi, S. M. Khan, and N. G. Haider, "Reliable group of vehicles (RGoV) in VANET," *IEEE Access*, vol. 9, pp. 111407–111416, 2021, doi: 10.1109/ACCESS.2021.3102216.

[4] Y. Cao, H. Zhang, Y. Fang, and D. Yuan, "An adaptive high-throughput multichannel MAC protocol for VANETs," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8249–8262, 2020, doi: 10.1109/JIOT.2020.2990568.

[5] S. Jiang, Z. Huang, and Y. Ji, "Adaptive UAV-assisted geographic routing with Q-learning in VANET," *IEEE Communications Letters*, vol. 25, no. 4, pp. 1358–1362, 2021, doi: 10.1109/LCOMM.2020.3048250.

[6] O. S. Oubbati, N. Chaib, A. Lakas, P. Lorenz, and A. Rachedi, "UAV-assisted supporting services connectivity in Urban VANETs," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 3944–3951, 2019, doi: 10.1109/TVT.2019.2898477.

[7] A. A. -Hilo, M. Samir, C. Assi, S. Sharafeddine, and D. Ebrahimi, "UAV-assisted content delivery in intelligent transportation systems-joint trajectory planning and cache management," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5155–5167, 2021, doi: 10.1109/TITS.2020.3020220.

[8] H. Fatemidokht, M. K. Rafsanjani, B. B. Gupta, and C.-H. Hsu, "Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular ad hoc networks in intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4757–4769, 2021, doi: 10.1109/TITS.2020.3041746.

[9] F. Z. Rabahi, S. Boudjit, C. Bemmoussat, and M. Benaissa, "UAVs-based mobile radars for real-time highways surveillance," in *2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, 2020, pp. 80–87, doi: 10.1109/MASS50613.2020.00020.

[10] H. Ghazzai, A. Khattab, and Y. Massoud, "Mobility and energy aware data routing for UAV-assisted VANETs," in *2019 IEEE International Conference on Vehicular Electronics and Safety (ICVES)*, 2019, pp. 1–6, doi: 10.1109/ICVES.2019.8906323.

[11] Y. He, D. Zhai, Y. Jiang, and R. Zhang, "Relay selection for UAV-assisted urban vehicular ad hoc networks," *IEEE Wireless Communications Letters*, vol. 9, no. 9, pp. 1379–1383, 2020, doi: 10.1109/LWC.2020.2991037.

[12] Y. C. Sehgelmeble and S. Fischer, "A different perspective in routing for VANETs," in *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, 2020, pp. 1–4, doi: 10.1109/ISNCC49221.2020.9297351.

[13] Z. Liu *et al.*, "TCEMD: a trust cascading-based emergency message dissemination model in VANETs," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4028–4048, 2020, doi: 10.1109/JIOT.2019.2957520.

[14] R. J. Atwa, P. Flocchini, and A. Nayak, "RTEAM: risk-based trust evaluation advanced model for VANETs," *IEEE Access*, vol. 9, pp. 117772–117783, 2021, doi: 10.1109/ACCESS.2021.3107467.

[15] B. Li, R. Liang, D. Zhu, W. Chen, and Q. Lin, "Blockchain-based trust management model for location privacy preserving in VANET," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3765–3775, 2021, doi: 10.1109/TITS.2020.3035869.

[16] J. Guo *et al.*, "TROVE: a context-awareness trust model for VANETs using reinforcement learning," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6647–6662, 2020, doi: 10.1109/JIOT.2020.2975084.

[17] B. Luo, X. Li, J. Weng, J. Guo, and J. Ma, "Blockchain enabled trust-based location privacy protection scheme in VANET," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 2, pp. 2034–2048, 2020, doi: 10.1109/TVT.2019.2957744.

[18] F. H. Kumbhar and S. Y. Shin, "VAR^2: novel vehicular ad-hoc reliable routing approach for compatible and trustworthy paradigm," *IEEE Communications Letters*, vol. 25, no. 2, pp. 670–674, 2021, doi: 10.1109/LCOMM.2020.3032753.

[19] H. Liu, D. Han, and D. Li, "Behavior analysis and blockchain based trust management in VANETs," *Journal of Parallel and Distributed Computing*, vol. 151, pp. 61–69, 2021, doi: 10.1016/j.jpdc.2021.02.011.

[20] Y. Inedjaren, M. Maachaoui, B. Zeddini, and J.-P. Barbot, "Blockchain-based distributed management system for trust in VANET," *Vehicular Communications*, vol. 30, p. 100350, 2021, doi: 10.1016/j.vehcom.2021.100350.

[21] S. Kudva, S. Badsha, S. Sengupta, H. La, I. Khalil, and M. Atiquzzaman, "A scalable blockchain based trust management in VANET routing protocol," *Journal of Parallel and Distributed Computing*, vol. 152, pp. 144–156, 2021, doi: 10.1016/j.jpdc.2021.02.024.

[22] F. Li, Z. Guo, C. Zhang, W. Li, and Y. Wang, "ATM: an active-detection trust mechanism for VANETs based on blockchain," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 4011–4021, 2021, doi: 10.1109/TVT.2021.3050007.

[23] Y. Su, "A trust based scheme to protect 5G UAV communication networks," *IEEE Open Journal of the Computer Society*, vol. 2, pp. 300–307, 2021, doi: 10.1109/ojcs.2021.3058001.

[24] M. Huang, A. Liu, N. N. Xiong, and J. Wu, "A UAV-assisted ubiquitous trust communication system in 5G and beyond networks," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 11, pp. 3444–3458, 2021, doi: 10.1109/JSAC.2021.3088675.

[25] G. Bansal and B. Sikdar, "Secure and trusted attestation protocol for UAV fleets," in *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2022, pp. 1–6, doi: 10.1109/INFOCOMWKSHPS54753.2022.9798087.

BIOGRAPHIES OF AUTHORS

Sami Abduljabbar Rashid was born in Al-Anbar, Iraq. He received the B.Eng. degree in computer engineering technology from Al-Maarif University College, Iraq and the M.Sc. degree in communication and compute engineering from University Kebangsaan Malaysia (UKM), Malaysia. He is currently pursuing the Ph.D. degree in the department of Communication engineering, University Tun Hussein Onn Malaysia (UTHM), Malaysia. His Research interests include wireless and mobile communications and VANET. He can be contacted at email: sami25.6.1989@gmail.com.

Ahmed Shamil Mustafa received his Master of Communication and Computer Engineering from Universiti Kebangsaan Malaysia (UKM), Malaysia in 2015. Currently serving as a lecturer in the Department of Computer Engineering Techniques at Al Maarif University College. He is highly interested in communication, computer engineering, VANET, and digital signal processing (DSP). He can be contacted at email: ahmedshamil90@gmail.com.

Abdulkareem Dawah Abbas received his Master of Electrical Engineering, Electrical Engineering University Belgrade republic of Serbia1988. Currently serving as a lecturer in the Department of Computer Engineering Techniques at Al Maarif University College. He is highly interested in - Signal and System Processing and Mathematical for Engineering and Science and Digital Fundamentals and Electronic electrical Elements. He can be contacted at email: k.d.a@uoa.edu.iq.

Hamza Qasim Abdullah was born in Al-Anbar, Iraq. He received the B.Eng. degree in Computer Engineering Technology from Al-Maarif University College. He can be contacted at email: hamza.q.abd@gmail.com.

Mohammed Jassim Mohammed was born in Al-Anbar, Iraq. He received the B.Eng. degree in Computer Engineering Technology from Al-Maarif University College. He can be contacted at email: mohammed.j.mo25@gmail.com.