A Framework for Secure Vehicular Network using Advanced Blockchain

Vikas Hassija[1], Vinay Chamola[2], Vatsal Gupta,[1] and G. S. S Chalapathi[2]
[1]Department of CSE and IT, Jaypee Institute of Information Technology, Noida, India
[2]Department of Electrical and Electronics Engineering, BITS-Pilani, Pilani Campus, India

***Abstract*— Vehicular Ad-hoc Network (VANET) poses to be a promising technology for the future since it increases the comfort level of the drivers while also enhancing the safety measures for them. The main aim of VANETs is to enable communication among vehicles and roadside units (RSUs) using vehicle-to-vehicle (V2V) and vehicle-to-RSU (V2R) networks. VANET applications have a vast potential for growth owing to the increasing number of smart cities around the globe and advancement taking place in the technology sector. However, with all their benefits, VANETs also face several security challenges. The sensitive nature of data being transferred turns VANETs prone to malicious attacks. To overcome the security challenges, this paper proposes a distributed Directed Acyclic Graph (DAG) enabled vehicular network comprising several requesting vehicles and RSUs. The proposed model is based on advanced blockchain and therefore provides a strong level of security and data immutability. Furthermore, the interactions between the requesting vehicles and the RSUs have been modeled using an auction-based game-theoretic smart contract deployed on the blockchain.**

***Index Terms*— Directed Acyclic Graph, Blockchain, Game theory, Consensus mechanism, Distributed applications, Internet of vehicles, VANET, IOTA.**

I. Introduction

The VANET application has become a topic of enormous interest in the past few years and is being researched extensively. VANET works on the vehicle domain of the ad-hoc network and consists of RSUs, sensor-enabled vehicles and wireless interconnection to enable communication between them. As one of the major components of Intelligent Transportation System (ITS), VANET - 1) helps in integrating technology to increase safety, 2) enables inter-vehicle communication, and 3) provides mechanisms for effective traffic management. In addition to this, VANET enables drivers to make the right decisions by making them aware of the traffic conditions in advance. Figure 1 illustrates the basic architecture of VANETs [1]. VANET consists of two different types of networks: 1) infrastructure oriented networks that deal with the RSUs and 2) infrastructure-less networks that deal with the ad-hoc vehicles. Sensors called On-Board Units (OBU) are embedded in the vehicles and are tasked with the responsibility of storing and processing the information [2], [3]. Furthermore, OBUs forward the messages to vehicles or RSUs in the V2V and V2R networks. Vehicles also carry a multiple application unit (MAU) or a single application unit (SAU) that makes use of the communication capabilities of the OBU to use the applications provided by the provider.

Communication between VANETs can be represented using three different domains: Roadside domain (RSD), ad hoc domain (AHD), and in-vehicle domain (IVD). RSD consists of RSUs, internet, and other gateway components. Some of the major attacks that RSD is prone to include routing and DDoS attacks. In routing attacks, the attackers send several messages to the RSUs in order to exhaust the resources in the VANET network. AHD is the domain that facilitates V2V and V2R communication. Major attacks faced by AHD include routing and authentication attacks. In authentication attacks, the attackers generate fake IDs from the original ones and transfer false information. IVD enables the interaction of an SAU or an MAU with OBUs. In IVD, the attackers try to gain information from the OBUs by generating fake IDs or cause malfunctioning of the application units by sending some harmful viruses into the VANET network. Besides these, VANETs are prone to several other attacks, as discussed in [4] and [5].

Communication and information sharing is an essential aspect of VANETs; therefore, efficient and precise data sharing using trustworthy resources is very important. Furthermore, to prevent a major crisis in the VANETs, security and privacy issues need to be considered [6]. Every domain of VANET is equally important and needs to be secured from all kinds of malicious attacks. The need for security in VANETs arises due to the following reasons [7]:

1. Attackers are attracted towards VANETs owing to the sensitive nature of the data being shared.

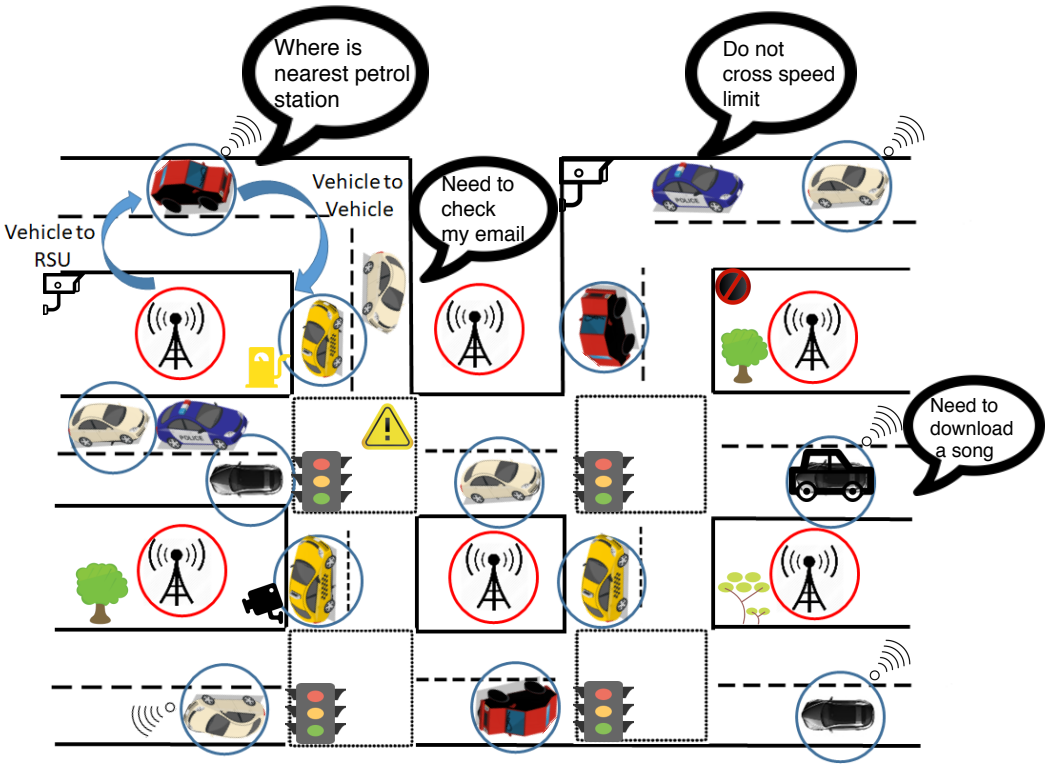

Fig. 1: A network of vehicles communicating with each other.

2. The presence of several wireless links in the infrastructure of VANETs makes them very susceptible to malicious attacks.
3. Security and privacy of a user is at threat.
4. Spoofing of valid IDs and intrusion in VANET communication is easy for malicious attackers.

To overcome these limitations, in this paper, we propose a DAG-enabled vehicular network consisting of several vehicles and RSUs. Since our model leverages a distributed ledger technology (DLT), it is privacy-preserving by design.

The rest of the paper is organized as follows. Existing work done in the direction of securing VANET applications has been described in Section II. Section III presents the proposed distributed model for secure vehicular communication. In section IV, the proposed game-theoretic smart contract is established for optimal price formulation for data sharing among vehicles and RSUs. The numerical analysis is presented in Section V, and the paper is eventually concluded in section VI.

II. Related Work

This section summarizes the various works done in the direction of securing VANETs and the various domains in which they are applied.

Lei Zhang *et al.* [8] have proposed a tamper-proof privacy-preserving mechanism for VANETs, which reduces the required vehicular storage space by compressing signatures and verifying several messages together. Instead of using ideal TPDs (tamper-proof devices), their model uses realistic TPDs. They have used the NS-2 simulator for the purposes of simulation and evaluation.

The authors of [9] have discussed safety applications for the VANETs, such as cooperative awareness messages (CAM). Vehicle tracking is possible through the spatiotemporal and periodic information given by CAM. Various schemes concerned with privacy in the VANETs have been evaluated in their research, and the impact of those schemes on safety applications has also been analyzed. Furthermore, a privacy metric based on distortion has also been proposed in the paper. The accuracy of the proposed privacy metric is analyzed by comparing it to many famous privacy metrics.

In [10], Bhakti Pawar *et al.* have established an attack-resistant trust (ART) scheme for secure and high-quality VANET communication. The authors have also presented a comparison between their

proposed model and the baseline method in regards to QoS metrics like throughput and communication overhead.

The authors of [11] have presented a comprehensive survey of the several security and privacy challenges that hinder the performance of VANETs. Their work also evaluates the efficiency of a number of cryptographic solutions that have been suggested in existing literature for securing VANETs.

Mohammad Wazid *et al.* [12] have proposed a mechanism demonstrating three different mutual authentications between vehicles, cluster heads, and roadside units (RSUs). For maintaining a secure communication, a secret key is also maintained between RSUs as per their scheme. In the proposed model, in-depth details about the registration phase, authentication, and key agreement phase, RSU2RSU key establishment phase, password update phase, and dynamic RSU addition phase have been provided. The authors have demonstrated the feasibility of their proposed mechanism in the VANET environment with the help of the NS-2 simulator.

In [13], the authors have proposed a new ciphertext policy attribute-based encryption (CP-ABE) scheme, which overcomes the challenges faced by the traditional CP-ABE. In the proposed scheme, RSUs perform nearly all the computation to improve the vehicles' efficiency of decryption. To enhance the factors like computational cost, communication, and distance from RSUs, deep learning techniques such as decision trees have been used. In addition, the authors have thoroughly discussed the security issues and the access control scheme in VANETs.

Rawat *et al.*, in [14], have proposed a scheme to detect data falsification attacks made by malicious users in VANETs. In this scheme, hashes are used to detect the attacks and further enhance the security level of the vehicles. The performance is improved by enabling on-time forwarding of correct and precise information to the vehicles in the neighborhood. The simulation results presented demonstrate that their proposed approach reduces delay and increases the throughput in the VANETs.

The authors of [15] have introduced an end-to-end authentication mechanism for protecting VANETs from malicious attacks that also helps in confirming confidentiality-integrity-availability (CIA) services. In their approach, CIA security has been achieved by transferring the data in an encrypted form.

Although there are various works in the direction of securing vehicular communication, all these works are based on centralized architectures. Such architectures are highly prone to a single point of failure and other malicious attacks such as DDoS. Therefore, this paper proposes a distributed network based on advanced blockchain to secure communication in vehicular networks. A sample smart contract based on game theory is also proposed to model the interaction between vehicles and RSUs.

III. Proposed Model for Decentralized V2V communication

IOTA enables the creation of a secure distributed network with support for a large number of nodes. IOTA uses a DAG, more specifically, a tangle, to store the transactions occurring between the nodes in the network [16]. Even though blockchain is a tamper-proof, and open data structure, IOTA has been preferred over conventional blockchain in our model to avoid forking and pruning issues. Besides, IOTA provides several unique features that set it apart from the traditional blockchain, including high scalability, zero-fee transactions, and secure data transfer [17]. Since nodes in an IOTA network, in this case, the vehicles and the RSUs, operate directly with one another without involving any central authority, the security of the data being transferred is ensured.

In any DLT, a consensus algorithm is required to achieve reliability in the network and establish trust between the unknown nodes. IOTA has recently adopted a new consensus mechanism named coordicide that is extremely scalable and truly decentralized. Using the coordicide mechanism, consensus finality can be achieved in seconds without having to wait for confirmation by external entities. Coordicide mechanism further increases the reliability of transactions by reducing the need for reattachments [18].

IV. Optimal price formulation

In a V2R model, any vehicle inside the range of an RSU can request it for information like the location details of other vehicles. The requesting vehicle can get the location data of other vehicles through two routes: 1) location data is transferred directly from the nearby vehicle to the requesting vehicle 2) location data is first transferred from the queried vehicles to the nearby RSU, and then from the RSU to the vehicle requesting for the data. Fig. 2 shows the transfer of data via the two routes, as mentioned above.

In the following section, an auction-based game-theoretic approach to minimize the cost incurred by

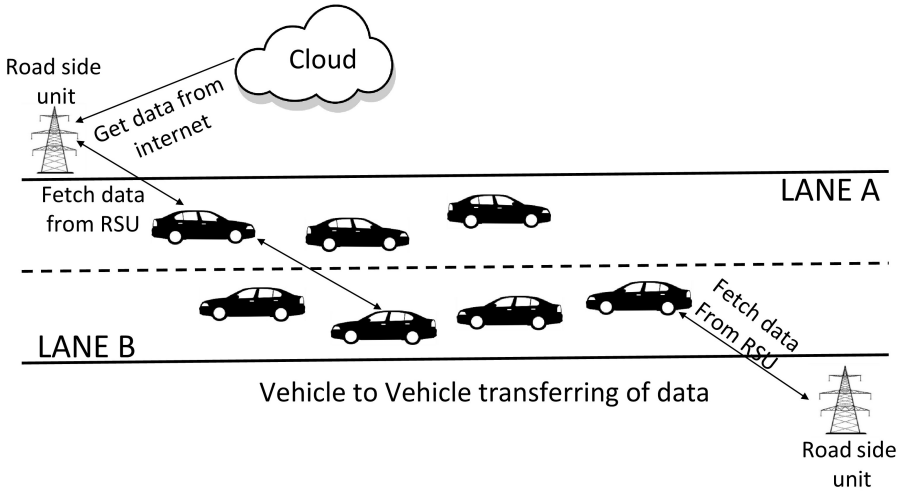

Fig. 2: Bandwidth sharing among vehicles and RSUs.

the requesting vehicle to request data from the RSU is presented.

A. Auction based game theory for bandwidth allocation

Consider a model consisting of several vehicles and a single internet-connected RSU. Whenever a vehicle comes within the range of the RSU, it can query the RSU for information such as traffic details, weather data, GPS data of other vehicles, etc. If there are a total of v vehicles within the range of a single RSU, then $\mathcal{V} = \{\mathcal{V}_1, \mathcal{V}_2, ..., \mathcal{V}_i..., \mathcal{V}_v\}$ represents the set of vehicles where $i \in (1, v)$ denotes the index of the vehicle $\mathcal{V}_i$.

Each vehicle $\mathcal{V}_i$ queries the RSU for certain information that is measured quantitatively in terms of the bandwidth requested by that vehicle. Since the total bandwidth, χ that the RSU can allocate is limited, χ needs to be divided among the v vehicles. The bandwidth requested by each vehicle is represented by γ_i where,

$$\gamma_i < \chi \tag{1}$$

$$\Lambda = \sum_{i=1}^{v} \gamma_i \tag{2}$$

Along with the bandwidth request, the requesting vehicles also submit the prices that they are willing to pay in order to acquire the requested bandwidth. If $\mathcal{P}_i$ denotes the price offered by the vehicle $\mathcal{V}_i$, then:

$$\Phi = \sum_{i=1}^{v} \mathcal{P}_i \tag{3}$$

Consider two cases pertaining to the total bandwidth requested:

Case 1: If $\Lambda \leqslant \chi$, then there is no need for an auction since the bandwidth requirement of each vehicle can be satisfied at the offered price itself.
Case 2: If $\Lambda > \chi$, then a conflict will arise since each vehicle will try to maximize the bandwidth that it can acquire and minimize the price at which it can acquire that bandwidth.

To solve the problem, as mentioned in the second case, there is a need for an auction-based game-theoretic model. Let $\pi = (\gamma, \mathcal{P})$ be a vector representing the bid of each vehicle in the game theory model such that $\pi_i = (\gamma_i, \mathcal{P}_i)$ represents the bid of the vehicle $\mathcal{V}_i$. Allocation of bandwidth to each vehicle $\mathcal{V}_i$ takes place when all the vehicles have submitted their bid and depends on the bids of all the requesting vehicles. The allocated bandwidth, α_i can be calculated using:

$$\alpha_i = \min\left(\gamma_i, \frac{\mathcal{P}_i}{\Phi}\chi\right), \ \forall \ \gamma_i < \chi \tag{4}$$

The cost, $\mathcal{C}_i$, of the bandwidth allocated to the vehicle $\mathcal{V}_i$ can be mathematically modeled as:

$$\mathcal{C}_i = \alpha_i \mathcal{P}_i \tag{5}$$

Since all vehicles are not within the range of the RSU at all instances, a valuation function δ_i for each vehicle $\mathcal{V}_i$ is introduced. If $\mathcal{T}_{i,in}$ and $\mathcal{T}_{i,out}$ denote the time spent by the vehicle $\mathcal{V}_i$ inside and outside the range of the RSU respectively, then the valuation function can be calculated as:

$$\delta_i = \mathcal{T}_{i,in} + \mathcal{T}_{i,out} \tag{6}$$

where,

$$\mathcal{T}_{i,in} = \tau_{in} * c \log\left(1 + \varrho\alpha_i\right) \tag{7}$$

$$\mathcal{T}_{i,out} = \mu(\tau_{out}) \tag{8}$$

Here c and ϱ are logarithmic constants and μ is a satisfaction function which is further discussed in the section below. τ_{in} and τ_{out} represent the summation of time-in and time-out of the vehicle $\mathcal{V}_i$ respectively.

To simultaneously maximize the bandwidth acquired and minimize the price paid to acquire it, a QoE function θ has been defined. θ is calculated as the difference between the cost, $\mathcal{C}_i$ and the valuation, δ_i as formulated in eqns. 5 and 6 respectively. If $\mathcal{P}_{-i}$ denotes the prices offered by all vehicles other than $\mathcal{V}_i$ then θ is formulated as:

$$\theta_i(\mathcal{P}_i, \mathcal{P}_{-i}) = \delta_i - \mathcal{C}_i \tag{9}$$

B. User Satisfaction and Nash Equilibrium

Let τ_o denote the time duration for which the vehicle is unable to fetch the data from RSU. The user satisfaction function, μ, used in eqn. 8 is defined as a function of τ_o and can be mathematically modeled as follows:

$$\mu\left(\tau_o\right) = 1 - \frac{1}{1 + \exp\left(-\rho\left(\tau_{out} - \upsilon\right)\right)} \tag{10}$$

where ρ and υ are constants. The suitable cost that can maximize the QoE delivered to each vehicle is given by Nash Equilibrium and can be calculated as follows:

$$\mathcal{P}_i^* = \sigma_i\left(\mathcal{P}_{-i}^*\right) \tag{11}$$

where σ_i denotes the best response made by the vehicle $\mathcal{V}_i$ and can be mathematically formulated as:

$$\sigma_i(\mathcal{P}_i) = \arg\max_{\mathcal{P}_i} \theta_i(\mathcal{P}_i) \tag{12}$$

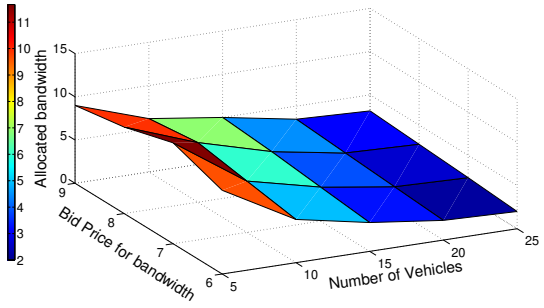

Fig. 3: The change in allocated bandwidth with the change in bid price and the network size.

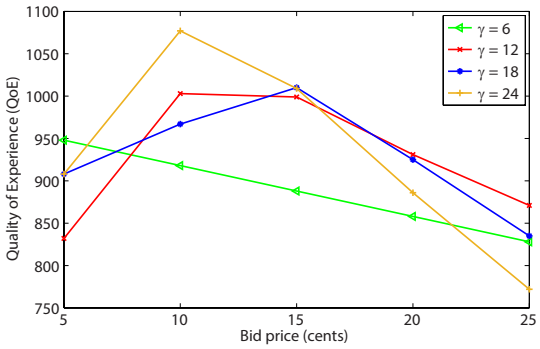

Fig. 4: Variation in QoE with Changing Bid Prices Keeping Bandwidth Requirement Fixed

V. Numerical Analysis

For the evaluation of our V2R model, we have considered four vehicles having different time-in and time-out in the DAG-enabled network. The time-out of a vehicle is calculated as the difference in total time and time-in of that vehicle. The time-in of vehicles is assumed to be in the range of [10, 50] minutes in the frame window of 60 minutes. The required bandwidth of four vehicles while entering in the network is assumed to be $\gamma_i = \{6, 12, 18, 24\}$ bits per second and the corresponding price offered by each vehicle is taken as $P_i = \{30, 40, 50, 60\}$ cents. For every iteration, we increase the number of vehicles in the network and consider the change in QoE of the four vehicles under consideration. Finally, each vehicle is allocated its required bandwidth at a minimum possible price and maximum possible QoE.

Fig. 3 demonstrates that the bandwidth allocated by the RSU to any vehicle $\mathcal{V}_1$ varies with the price offered by that vehicle and the total number of vehicles in the network. It can be observed that the bandwidth allocated to the vehicle $\mathcal{V}_1$ decreases with an increase in the number of vehicles in the network and vice versa.

The variation in QoE with the change in the bid prices at a fixed bandwidth requirement (γ) is shown in Fig. 4. Since the QoE of the vehicles depends on the bids of all the vehicles in the network, there is no guarantee that the QoE will increase with an increase in the offered price. It can be seen in the figure that, initially, the QoE of vehicles increases with an increase in the bid price. However, at a certain price point, the bandwidth allocation by the RSU to a particular vehicle saturates. For example, the saturation point of the first vehicle (with $\gamma = 6$) occurs during the first bid itself. Therefore, the subsequent increase in bid prices causes the QoE of that vehicle to decline.

VI. Conclusion

In this paper, we propose a secure and distributed framework for vehicular communication. In addition to providing all the security features present in blockchain, this DAG-enabled framework also resolves the scalability issues of the traditional blockchain. A sample auction-based smart contract is also proposed to model the V2R cost bargaining for data offloading. The simulation results show that the proposed model enhances the QoE of the vehicles in the network while minimizing the costs incurred by them. Furthermore, complicated smart contracts can be deployed in the same network to model different interactions between different parties involved in the network.

References

[1] W. Liang, Z. Li, H. Zhang, S. Wang, and R. Bie, "Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends," *International Journal of Distributed Sensor Networks*, vol. 11, no. 8, p. 745303, 2015.

[2] G. Bansal, V. Hassija, V. Chamola, N. Kumar, and M. Guizani, "Smart stock exchange market: A secure predictive decentralised model," *Proceedings of the 2019 IEEE Globecom, Big Island, HI, USA*, pp. 9–13, 2019.

[3] V. Hassija, V. Chamola, G. Han, J. J. P. C. Rodrigues, and M. Guizani, "Dagiov: A framework for vehicle to vehicle communication using directed acyclic graph and game theory," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4182–4191, April 2020.

[4] G. Samara and Y. Al-Raba'nah, "Security issues in vehicular ad hoc networks (VANET): a survey," *CoRR*, vol. abs/1712.04263, 2017. [Online]. Available: http://arxiv.org/abs/1712.04263

[5] R. Kaur, T. P. Singh, and V. Khajuria, "Security issues in vehicular ad-hoc network(vanet)," in *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, 2018, pp. 884–889.

[6] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Vanet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7–20, 2017.

[7] R. Mishra, A. Singh, and R. Kumar, "Vanet security: Issues, challenges and solutions," in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, 2016, pp. 1050–1055.

[8] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516–526, 2016.

[9] K. Emara, "Safety-aware location privacy in vanet: Evaluation and comparison," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 10 718–10 731, 2017.

[10] B. V. Pawar and M. M. Dongre, "Performance enhancement for vanet security using attack-resistant trust (art)," in *Innovations in Electronics and Communication Engineering*. Springer, 2019, pp. 219–228.

[11] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on vanet security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[12] M. Wazid, A. K. Das, N. Kumar, V. Odelu, A. G. Reddy, K. Park, and Y. Park, "Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks," *IEEE Access*, vol. 5, pp. 14 966–14 980, 2017.

[13] Y. Xia, W. Chen, X. Liu, L. Zhang, X. Li, and Y. Xiang, "Adaptive multimedia data forwarding for privacy preservation in vehicular ad-hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2629–2641, 2017.

[14] A. Tolba, "Trust-based distributed authentication method for collision attack avoidance in vanets," *IEEE Access*, vol. 6, pp. 62 747–62 755, 2018.

[15] G. Kumar, R. Saha, M. K. Rai, and T.-H. Kim, "Multidimensional security provision for secure communication in vehicular ad hoc networks using hierarchical structure and end-to-end authentication," *IEEE Access*, vol. 6, pp. 46 558–46 567, 2018.

[16] V. Hassija, V. Saxena, and V. Chamola, "Scheduling drone charging for multi-drone network based on consensus time-stamp and game theory," *Computer Communications*, vol. 149, pp. 51–61, 2020.

[17] V. Hassija, V. Chamola, S. Garg, N. G. K. Dara, G. Kaddoum, and D. N. K. Jayakody, "A blockchain-based framework for lightweight data sharing and energy trading in v2g network," *IEEE Transactions on Vehicular Technology*, pp. 1–1, 2020.

[18] S. Popov, H. Moog, D. Camargo, A. Capossele, V. Dimitrov, A. Gal, A. Greve, B. Kusmierz, S. Mueller, A. Penzkofer *et al.*, "The coordicide," 2020.