SBA-GT: A Secure Bandwidth Allocation Scheme with Game Theory for UAV-Assisted VANET Scenarios

Yuyang Cheng[1,2], Shiyuan Xu[1,3], Yibo Cao[1,4], Yunhua He[1,5(✉)], and Ke Xiao[1]

[1] School of Information Engineering, North China University of Technology, Beijing, China
heyunhua@ncut.edu.cn
[2] Department of Electrical Engineering, The University of Sydney, Sydney, Australia
[3] Department of Computer Science, The University of Hong Kong, Hong Kong, Hong Kong
[4] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, China
[5] Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

Abstract. Unmanned Aerial Vehicles (UAVs) are widely utilized for wireless communication services, promoting the emergence of promising UAV-assisted vehicle networks. However, due to the ever-increasing traffic data and diversified wireless service requirements of vehicles, there are also privacy issues caused by fraud, which challenges the effective allocation of limited security bandwidth for secure communications. In this article, to solve these two problems, we firstly propose a secure bandwidth allocation scheme based on the game theory on the Internet of Vehicles assisted by UAVs. Secondly, the proposed blockchain-based system introduces an emerging consensus mechanism that can significantly reduce the delay in exchanging information and protect data privacy. Furthermore, to allocate the limited safe bandwidth, based on the real-time feedback of each UAV, we design an optimal decision search algorithm based on gradient descent to achieve Stackelberg equilibrium. Finally, the simulation results show the superiority of improving the utility's security bandwidth allocation scheme.

Keywords: Vehicular Ad-Hoc Network (VANET) · Bandwidth allocation · UAV · Game theory · Information security · Privacy protection

1 Introduction

With the rapid popularity of UAVs equipped with wireless transceivers, a promising UAV-assisted vehicle network has been advocated to provide vehicles with ubiquitous wireless communications [1, 2, 6, 7 14], . The traditional mobile network uses ground base stations to adapt to the wireless access of vehicles [13, 15–18]. High data rate wireless communication for drones. Therefore, the Internet of Vehicles composed of base stations and drones has become a new paradigm for the next generation of communication networks.

Specifically, most current data management systems use a Proof-of-Work (PoW) mechanism in blockchain systems [3]. However, the bandwidth allocation of secure

L. Wang et al. (Eds.): WASA 2022, LNCS 13472, pp. 356–364, 2022.
https://doi.org/10.1007/978-3-031-19214-2_29

spectrum resources is essential for providing vehicles with satisfactory Quality-of-Experience (QoE) wireless data services [4].

The Proof of Stake (PoS) mechanism has many advantages [5]. In a PoS-based network, vehicles are essential for maintaining the operation and safety of the network. Therefore, we propose a model based on the Stackelberg game to jointly maximize utility and secure bandwidth allocation, and then design an optimal decision search algorithm based on gradient descent to find Stackelberg equilibrium. Finally, simulations verify the feasibility and effectiveness of the proposed scheme.

We propose a blockchain-based network and game-theoretic security bandwidth allocation scheme. The contribution of this paper can be summarized as follows:

- We propose a secure bandwidth allocation scheme with game theory to provide secure data services to vehicles in VANET, which jointly considers the cooperation and competition between drones and vehicles.
- We develop a novel PoS-based framework for service management, including smart contracts, enabling all vehicles to send feedback messages without any privacy leaks and get safe bandwidth allocation.
- We design utility functions for vehicles and drones, and we utilize the Stackelberg game to study the complex interaction between drones and vehicles.
- An optimal decision search algorithm based on gradient descent is designed to find Stackelberg equilibrium. Finally, through simulation performance, we compare with other methods to prove the superiority and effectiveness of our method.

2 Our Proposed Scheme

2.1 Network Model

As shown in Fig. 1, we consider a UAV-based VANET, consisting of a single ground base station, a roadside unit, multiple drones, and vehicles.

The set of UAVs is represented as $U = \{1, 2, \cdots, U\}$ and the bandwidth of the UAV is B_0. We apply the UAV-to-X communication protocol in the connections between UAVs and the RSU. During the provision of wireless service, the serving UAV hovers over the vehicles. In the time slot t, the location of the UAV u is denoted as $l_u(t) = \{x_u(t), y_u(t), z_u(t)\}$, where z is the height of the UAV. Due to vehicles' mobility, the number of vehicles under each UAV varies over time. At the time slot t, the set of vehicles under UAV u is denoted as $N_u^t = \{1, 2, \cdots, n_u^t, \cdots, N_u^t\}$. The location of the vehicle n_u^t is $l_{n_u^t} = \{x_{n_u^t}, y_{n_u^t}, 0\}$. As such, the distance between UAV u and vehicles n_u^t at a time slot t is given by

$$d_{u,n_u^t}(t) = \sqrt{(x_u(t) - x_{n_u^t}(t))^2 + (y_u(t) - y_{n_u^t}(t))^2 + z_u^2} \tag{1}$$

We assume that the Line-of-Sight (LOS) chain-link dominates the channel between the drone and each vehicle. Therefore, the channel gain from UAV u to vehicle n_u^t is $g_{u,n_u^t(t)}(t) = g_0(d_{u,n_u^t}(t))^{-\mu}$ where g_0 is the UAV-to-ground channel gain with the unit

distance and μ is the path loss parameter of the LOS link. Then, the signal to interference plus noise ratio (SINR) at the vehicle n_u^t is

$$\beta_{n_u^t}(t) = \frac{P_u g_{u,n_u^t(t)}(t)}{\sigma^2 + \sum_{u'=1,u'\neq u}^{U} P_{u'} g_{u',n_u^t(t)}(t) + P_0 g_{0,n_u^t}(t)} \tag{2}$$

where P_u represents the transmission power from the UAV u to each vehicle and σ^2 denotes the white Gaussian noise power. P_0 and $g_{0,n_u^t}(t)$ represents the power of each vehicle and power gain from the base station to the vehicle. At the time slot t, the bandwidth data rate from UAV is $R_{n_u^t} = \log_2(1 + \beta_{n_u^t}(t))$.

Fig. 1. Network model

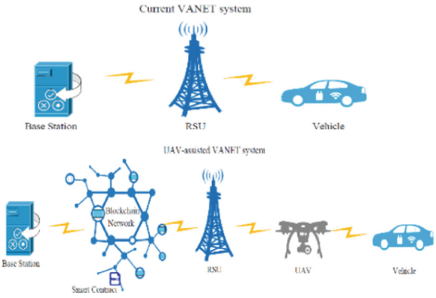

Fig. 2. VANET system and UAV-assisted system

2.2 Our Proposed UAV-Based VANET System

Our proposed UAV-assisted VANET system maximizes the efficiency of secure bandwidth allocation and provides smart contracts in the storage server for protection. The current VANET [12] system and the UAV assistance system elaborates in Fig. 2. The process of management includes the following steps:

Step 1. The communication protocol between the base station and the RSU is stored in the storage server as a smart contract, the program that defines the vehicle. The communication protocol will be automatically executed when the conditions specified by the smart contract are met. **Step 2.** When one vehicle desires the RSU for road traffic information services, the vehicle inquires the RSU through UAV to receive information about the service. **Step 3.** If the vehicle decides to enable the service, the request information and verification information will hear the address sent to the smart contract by the RSU. **Step 4.** Once successfully sent to the smart contract, the RSU will grant the vehicles access to traffic information directly or through the UAV. **Step 5.** When one vehicle finishes using the information service, RSU will send a data packet containing the provided service to the smart contract address. **Step 6.** The smart contract will be

automatically calculated and sent to the base station. It also triggers the information transmitted from the base station to the RSU.

2.3 The Secure Bandwidth Allocation System

To find the best bandwidth allocation for vehicles and drones. The utility of vehicles and drones should be designed separately. Their utilities consist of the revenue from the sale of secure bandwidth and the cost of providing wireless services. Therefore, the utility function of UAV in the time slot is expressed as

$$U_u(P_u(t)) = \sum_{n_u^t}^{N_u^t} P_u(t) b_{n_u^t}(t) - \sum_{n_u^t=1}^{N_u^t} c_u(t) b_{n_u^t}(t) \tag{3}$$

Among them, $P_u(t)$ is the security bandwidth price of the drone u $c_u(t)$ is the cost of providing unit security bandwidth for the drone u and $b_{n_u^t}(t)$ is the security bandwidth obtained by the vehicle n_u^t in a time slot t. The utility of each vehicle consists of the satisfaction of obtaining safe bandwidth and the cost of purchasing safe bandwidth from the associated drone. $\gamma_{n_u^t}$ is the satisfaction parameter of the vehicle n_u^t, and $R'_{n_u^t}(t)$ is the data rate requirement of a vehicle n_u^t in the time slot t. Formally, the utility function of a vehicle n_u^t in the time slot t is

$$U_{n_u^t}(b_{n_u^t}(t)) = \gamma_{n_u^t} \log(1 + \frac{R_{n_u^t}(t) b_{n_u^t}(t)}{R'_{n_u^t}(t)}) - p_u(t) b_{n_u^t}(t) \tag{4}$$

2.4 Security Analysis of the Proposed Roaming System

By adopting the Ouroboros consensus mechanism, our roaming management system can achieve a minimal data exchange delay compared with the current roaming system. In particular, it takes about 20 s to add a block to the chain and 3 min to confirm the transaction. Therefore, compared with traditional roaming fraud protection systems, fraud attacks can be detected approximately 4 h earlier. In addition, the Ouroboros consensus mechanism has been proven to resist multiple types of attacks, such as double-spending attacks and grinding attacks [6].

Data authentication and unforgeability: Attackers cannot be used as a legitimate tool to destroy the trust evaluation storage server because it cannot forge any vehicle to apply for verification, and maliciously authorized vehicles are also problematic to destroy the storage server since it is almost impossible to control most entities due to high costs. Malicious attack: A group of malicious vehicles may produce unfair feedback to deal with the security bandwidth allocation of the target vehicle. In our system, the UAV iterative algorithm obtains the allocation, and thus the continuous feedback sent by the malicious vehicle will not be effective.

3 Game Theory Analysis

3.1 Game Modeling

In the Stackelberg game, the goal is to maximize their utility. Therefore, we define the following two problems:

Problem 1.

$$\max \ \{ \ U_u(p_u(t)), p_u(t)\} \geq 0, B_0 \geq \sum_{n_u^t=1}^{N_u^t} b_{n_u^t}(t) \tag{5}$$

The local condition means that the bandwidth price should be greater than or equal to zero, and the amount of bandwidth allocated should be less than the owned by the drone.

Problem 2.

$$\max\{U_{n_m^t}(b_{n_m^t}(t)), b_{n_m^t}(t)\} \geq 0 \tag{6}$$

Among them, the condition means that the amount of bandwidth obtained by vehicles should be greater than zero.

Assumption 1: $b_{n_u^t}(t)'$ and $p_u(t)$ are respectively the solutions of UAV n_u^t **problem 2** and **problem 1** in time slot t. Let $b_u(t)$ be the bandwidth demand vector of vehicles in the coverage area of UAV u, and $b_{-n_u^t,u}(t)'$ be the vehicle bandwidth demand vector except for vehicle n_u^t. We have these two inequalities $U_u(p_u(t)', b_u(t)') \geq U_u(p_u(t), b_u(t)')$ and $U_{n_u^t}(b_{n_u^t}(t)', b_{-n_u^t,u}(t)', p_u(t)') \geq U_u(b_{n_u^t}(t), b_{-n_u^t,u}(t)', p_u(t)')$.

3.2 Follower Strategy

By solving **problem 2**, we obtain the optimal bandwidth purchase strategy for vehicles according to the following theorem.

Theorem 1: Given the bandwidth price, the optimal bandwidth purchase strategy for the UAV covered by the vehicle n_u^t at time t is

$$b_{n_u^t}(t)' = \max(\frac{\alpha_{n_u^t}}{p_u(t)} - \frac{R'_{n_u^t}(t)}{\log(1+\gamma_{n_u^t}(t))}, 0) \tag{7}$$

Proof: We need to know if the utility function has the extremum. The processing of proof elaborates in Table 1.

Case 1: Low Bandwidth Price Regime. The low price situation corresponds to the situation where the bandwidth price provided by UAV u is not greater than $\frac{\alpha_{n_u^t} R_{n_u^t}(t)}{R'_{n_u^t}(t)}$. Therefore, the utility function $U_{n_u^t}(b_{n_u^t}(t))$ initially increases and then declines $b_{n_m^t}(t)$. The optimal bandwidth requirement at the time slot t can be obtained by solving $\frac{\partial U_{n_u^t}(b_{n_u^t}(t))}{\partial(b_{n_u^t}(t))} = 0$. Therefore, within the coverage of UAV u in a time slot t, the optimal bandwidth requirement of a vehicle n_u^t is $b_{n_u^t}(t)' = \frac{\alpha_{n_u^t}}{p_u(t)} - \frac{R_{n_u^t}(t)}{R'_{n_u^t}(t)}$.

Case 2: High Bandwidth Price Regime. The high bandwidth price system means that the bandwidth price provided by UAV u is greater than . So $\lim_{b_{n_m^t}(t)\to 0} \frac{\partial U_{n_m^t}(b_{n_m^t}(t))}{\partial(b_{n_m^t}(t))} < 0$, the first derivative of the utility remains negative as the bandwidth demand enhances. The optimal bandwidth requirement of the vehicle n_u^t in the UAV u coverage of time slot t is $b'_{n_m^t}(t) = 0$.

Table 1. Proof of Theorem 1.

Proof: The max-min value judgment
1: **For** $\frac{\partial U_{n_u^t}(b_{n_u^t}(t))}{\partial(b_{n_u^t}(t))} = \frac{\alpha_{n_u^t} R_{n_u^t}(t)}{R'_{n_u^t}(t)+R_{n_u^t}(t)b_{n_u^t}(t)} - p_u(t)$
2: And $\frac{\partial^2 U_{n_u^t}(b_{n_u^t}(t))}{\partial(b_{n_u^t}(t))^2} = -\frac{\alpha_{n_u^t}(R_{n_u^t}(t))^2}{(R'_{n_u^t}(t)+R_{n_u^t}(t)b_{n_u^t}(t))^2}$ is less than 0
3: **Therefore**, the utility function is concave
4: **For** $\lim_{b_{n_u^t}(t)\to\infty} \frac{\partial U_{n_u^t}(b_{n_u^t}(t))}{\partial(b_{n_u^t}(t))} = -p_u(t)$ is less than 0
5: And $\lim_{b_{n_u^t}(t)\to 0} \frac{\partial U_{n_u^t}(b_{n_u^t}(t))}{\partial(b_{n_u^t}(t))} = \frac{\alpha_{n_u^t} R_{n_u^t}(t)}{R'_{n_u^t}(t)} - p_u(t)$
6: **Therefore**, it has a max or min value

Then, we further analyze the optimal bandwidth price strategy of each UAV is

$$\begin{aligned} U_u(p_u(t)) &= (p_u(t) - c_u(t)) \sum_{n_u^t=1}^{N_u^t} \max\left(\frac{\alpha_{n_u^t}}{p_u(t)} - \frac{R'_{n_u^t}(t)}{\log(1+\beta_{n_u^t}(t))}, 0\right) \\ &= (p_u(t) - c_u(t)) \sum_{n_m^t=1}^{N_m^t} \left(\frac{\alpha_{n_u^t}}{p_u(t)} - \frac{R'_{n_u^t}(t)}{\log(1+\beta_{n_u^t}(t))}\right) \end{aligned} \tag{8}$$

The second derivative of the UAV utility function relative to the bandwidth price $p_u(t)$ can be expressed as $\frac{\partial^2 U_u(p_u(t))}{\partial(p_u(t))^2} = -2\sum_{n_u^t=1}^{N_u^t} \left(\frac{c_u \alpha_{n_u^t}}{(p_u(t))^3}\right) < 0$.

We propose an optimal decision search algorithm based on gradient descent to find the optimal bandwidth pricing strategy for each UAV. By adjusting the policy to improve the utility, the price of the drone u is updated to $p_u(t)[\tau+1] = p_u(t)[\tau]+\varepsilon\nabla U_u(p_u(t)[\tau])$, where $p_u(t)[\tau]$ is the bandwidth price of the UAV m in the $\tau-th$ iteration, ε is the number of iterations of bandwidth price, and $\nabla U_u(p_u(t)[\tau])$ is the gradient value. The iterative process of optimal bandwidth pricing strategy shows in **Algorithm 1**.

Algorithm 1: Iterative algorithm based on gradient descent

1: **Initialization:** Each UAV determines its initial bandwidth price $p_u(t)$ and bandwidth capacity B_0 . $\tau = 0$

2: **repeat**

3: Vehicles within the coverage of each UAV determines their bandwidth requirements $b_{n_u^i}(t)$ by (8)

4: **if** the total bandwidth requirement of vehicles is more extensive than B_0 **then**

5: Each UAV updates its bandwidth price by $p_u(t)[\tau+1] = p_u(t)[\tau] + \rho_p$, where ρ_p is a small value

6: **else**

7: Each UAV updates its price by $p_u(t)[\tau+1] = p_u(t)[\tau] + \varepsilon \nabla U_u(p_u(t)[\tau])$

8: **end if**

9: $\tau = \tau + 1$

10: **until** Each $pm(t)$ has no significant changes

4 Simulation Performance

Table 2 elaborates the parameters of our experimental environment.

Figure 3 shows the comparison result of the UAV's utility. When B_0 is fixed, the utility of the UAV in our proposed scheme is greater than that of the other two conventional schemes. In the linear-based allocation scheme, the bandwidth price is determined according to the linear pricing mechanism. As a result, this bandwidth price is not optimal, and drones cannot have the most excellent utility. In our proposed scheme, the bandwidth price is determined based on the game theory of the optimal bandwidth price.

The performance of the proposed scheme is evaluated by comparing it with the many-to-one scheme [8] scheme, the maximum signal-strength-indicator (max-RSSI) [9] scheme, the maximum signal-to-interference-plus-noise-ratio (max-SINR) [10] scheme, the Auction-Based UAV Swarm Many-to-Many scheme (AMMA) and UE-Optimal Many-to-One Matching scheme (UMOA) [11].

Table 2. Experimental parameters and value.

Parameters	Value	Parameters	Value
Square network	1000 m × 1000 m	Gain between BS and vehicle	10 mW–30 mW
Number of UAV	10, 12, 15	Gain between UAV and ground g_0	−50 db
Desired data rate	1 Mbps–15 Mbps	Path loss μ	−2
AWGN variance	10^{-14} W	Number of iterations	0.1

The system throughput among UAVs and vehicles of our scheme specifies in Fig. 4. The figure elaborates that our scheme has the highest system throughput. The second one is about 40.2% lower than ours compared with other schemes.

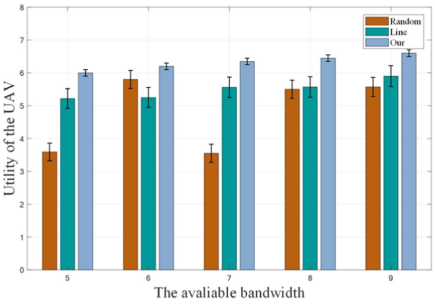

Fig. 3. Utility of the UAV

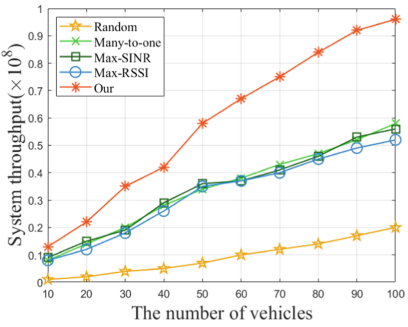

Fig. 4. System throughput

5 Conclusion

In this paper, we propose a novel security bandwidth allocation scheme based on the storage server and smart contracts in UAV-assisted VANET with game theory. Specifically, we firstly developed a secure bandwidth allocation framework. To allocate the secure bandwidth of drones, we design an iterative-based algorithm based on the needs of vehicles and the real-time bandwidth of drones, to maximize utility by Stackelberg equilibrium. Furthermore, we not only elaborate the security analysis of the smart contracts in the network, and resist fraud and malicious attacks, respectively, but also achieve privacy protection and secure bandwidth allocation. Finally, we conduct simulation experiments to verify the effectiveness of our scheme.

Acknowledgment. This work was supported in part by the R&D Program of Beijing Municipal Education Commission under Grant KM202010009010, in part by the Yunnan Key Laboratory of Blockchain Application Technology under Grant 2021105AG070005 (YNB202102), in part by the Beijing Municipal Natural Science Foundation under Grant M21029 and in part by the National Key Research and Development Program of China under Grant 2018YFB1800302.

References

1. Liang, J., Ma, M.: An efficiency-accuracy tradeoff for IDSs in VANETs with markov-based reputation scheme. In: Proceedings of ICC, pp. 1–6 (2021)
2. Bhabani, B., Mahapatro, J.: A delay-efficient channel allocation scheme for disseminating alert messages using WBAN and VANET. In: Proceedings of ICC, pp. 1–6 (2021)
3. Xu, S., Chen, X., He, Y.: EVchain: an anonymous blockchain-based system for charging-connected electric vehicles. Tsinghua Sci. Technol. **26**(6), 845–856 (2021)
4. Wen, Y., Shi, J., Zhang, Q., Tian, X., Huang, Z., Yu, H., et al.: Quality-driven auction-based incentive mechanism for mobile crowd sensing. IEEE Trans. Veh. Technol. **64**(9), 4203–4214 (2015)

5. Nguyen, C.T., Hoang, D.T., Nguyen, D.N., Niyato, D., Nguyen, H.T., Dutkiewicz, E.: Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals. Appl. Opport. IEEE Access. **7**, 85727–85745 (2019)
6. Shen, Y., Liu, Y., Yang, H., Sang, L., He, W.: Cell-cluster network-assisted adaptive streaming media optimization over wireless network. In: Proceedings of WCNC, pp. 1–6 (2021)
7. Yang, X., Zhang, H., Ji, H., Li, X.: Hybrid cooperative caching based iot network considering the data cold start. In: Proceedings of WCNC, pp. 1–6 (2021)
8. Meng, Y., Zhang, Z., Huang, Y., Zhang, P.: Resource allocation for energy harvesting-aided device-to-device communications: a matching game approach. IEEE Access. **7**, 175594–175605 (2019)
9. Elshaer, H., Kulkarni, M.N., Boccardi, F., Andrews, J.G., Dohler, M.: Downlink and uplink cell association with traditional macrocells and millimeter wave small cells. IEEE Trans. Wirel. Commun. **15**(9), 6244–6258 (2016)
10. Guvenc, I.: Capacity and fairness analysis of heterogeneous networks with range expansion and interference coordination. IEEE Commun. Lett. **15**(10), 1084–1087 (2011)
11. Zhang, Q., Wang, H., Feng, Z., Han, Z.: Many-to-many matching-theory-based dynamic bandwidth allocation for UAVs. IEEE Internet Things J. **8**(12), 9995–10009 (2021)
12. Cao, Y., Xu, S., Chen, X., He, Y., Jiang, S.: A forward-secure and efficient authentication protocol through lattice-based group signature in VANETs scenarios. Comput. Netw. **124**, 109149 (2022)
13. Cheng, Y., Xu, S., Zang, M., Jiang, S., Zhang, Y.: Secure authentication scheme for VANET based on blockchain. In: Proceedings of ICCC, pp. 1526–1531 (2021)
14. Cheng, Y., Xu, S., Zang, M., Kong, W.: LPPA: a lightweight privacy-preserving authentication scheme for the internet of drones. In: Proceedings of ICCT, pp. 656–661 (2021)
15. Xiong, Z., Cai, Z., Han, Q., Alrawais, A., Li. W.: ADGAN: protect your location privacy in camera data of auto-driving vehicles. IEEE Trans. Ind. Inform. **18**(2), 1310–1321 (2022)
16. Xiong, Z., Xu, H., Li, W., Cai., Z.: Multi-source adversarial sample attack on autonomous vehicles. IEEE Trans. Veh. Technol. **70**(3), 2822–2835 (2021)
17. Wang, J., Cai, Z., Yu., J.: achieving personalized k-anonymity based content privacy for autonomous vehicles in CPS. IEEE Trans. Ind. Inform. **16**(6), 4242–4251 (2020)
18. Cai, Z., Zheng, X.: A private and efficient mechanism for data uploading in smart cyber-physical systems. IEEE Trans. Netw. Sci. Eng. **7**(2), 766–775 (2020)