



BITS Pilani

Pilani | Dubai | Goa | Hyderabad



A Framework for Secure Vehicular Network using Advanced Blockchain

Vikas Hassija, Vinay Chamola, Vatsal Gupta, and G.S.S. Chalapathi

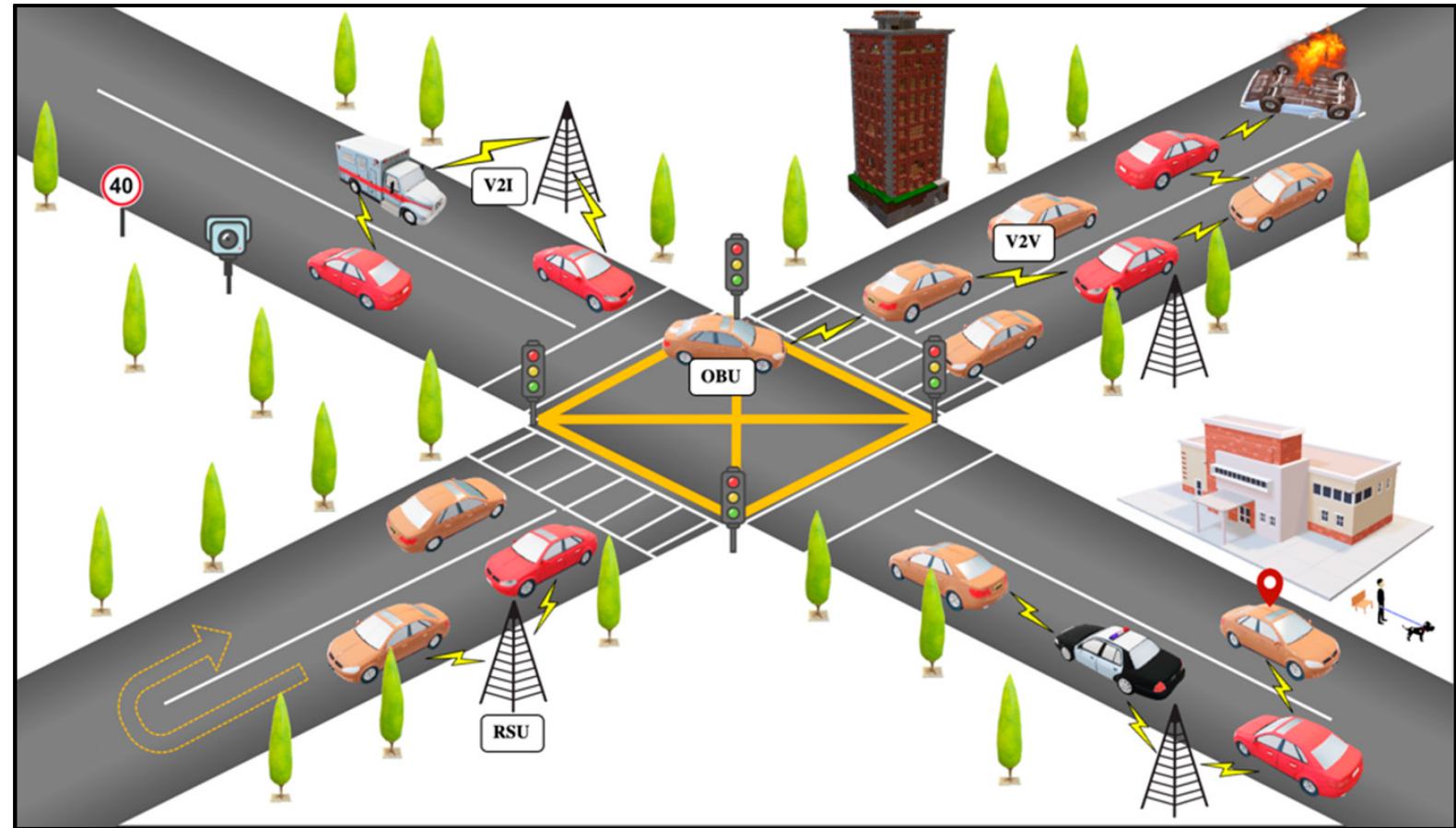
Introduction

Vehicular Ad Hoc Networks (VANETs)

Work on the vehicle domain of the ad-hoc network.

Benefits:

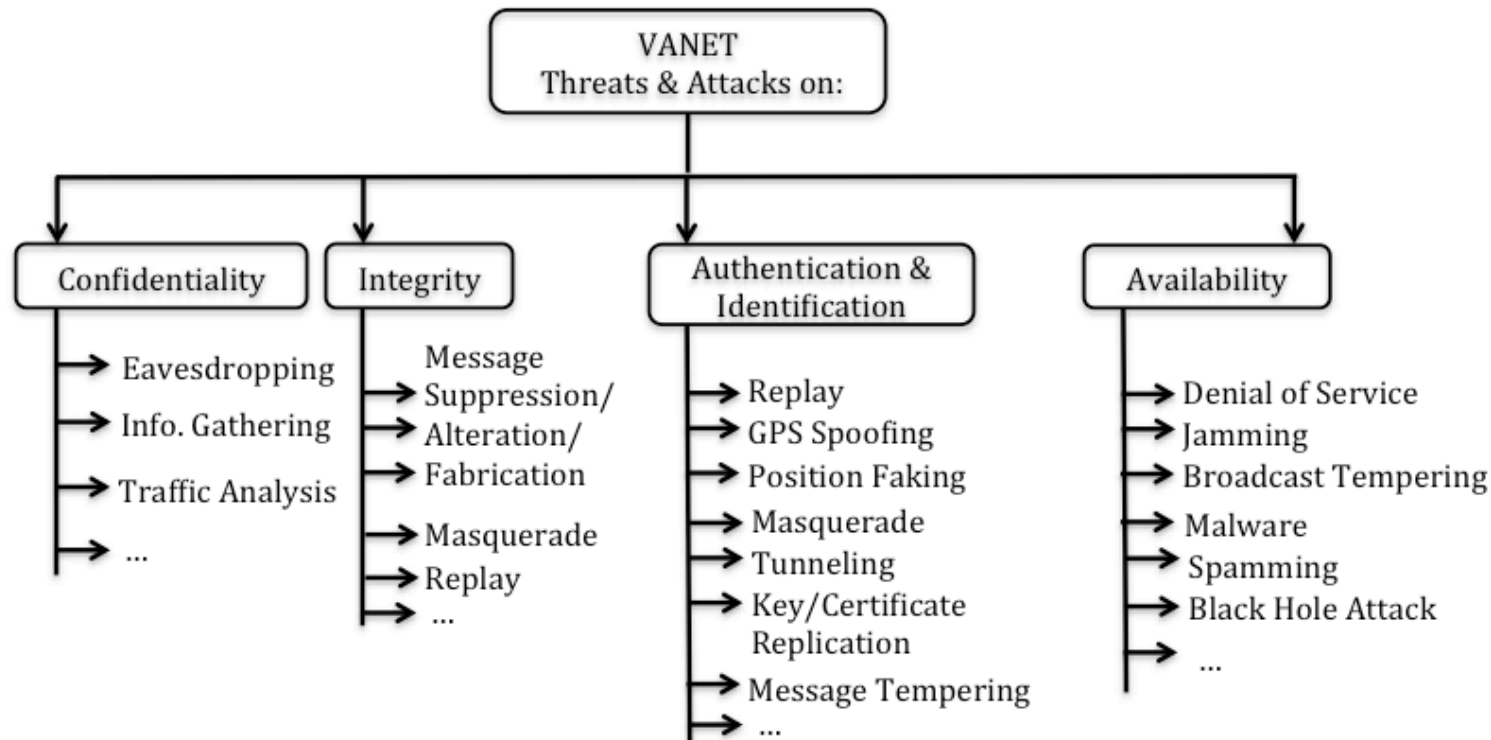
- enable safe driving
- enable an intelligent traffic system
- early warning signals to minimize road mishaps
- increase road conditions advisement



Security Concerns in VANETs...

VANETs face several security concerns since:

- Data being shared in VANETs is sensitive.
- Infrastructure-less model renders VANETs susceptible to several types of malicious attacks.
- Spoofing of valid IDs and intrusion in VANET communication is easy.



Existing Solutions for Securing VANETs

- Distributed Aggregate Privacy-Preserving Authentication in VANETs
 - Lei Zhang et al.
- Design of Lightweight Authentication and Key Agreement Protocol for Vehicular Ad-Hoc Networks
 - Mohammad Wazid et al.
- Adaptive Multimedia Data Forwarding for Privacy Preservation in Vehicular Ad-Hoc Networks
 - Yingjie Xia et al.

Problems in existing approaches

One major pitfall in all the existing solutions is their dependence on centralized architectures.

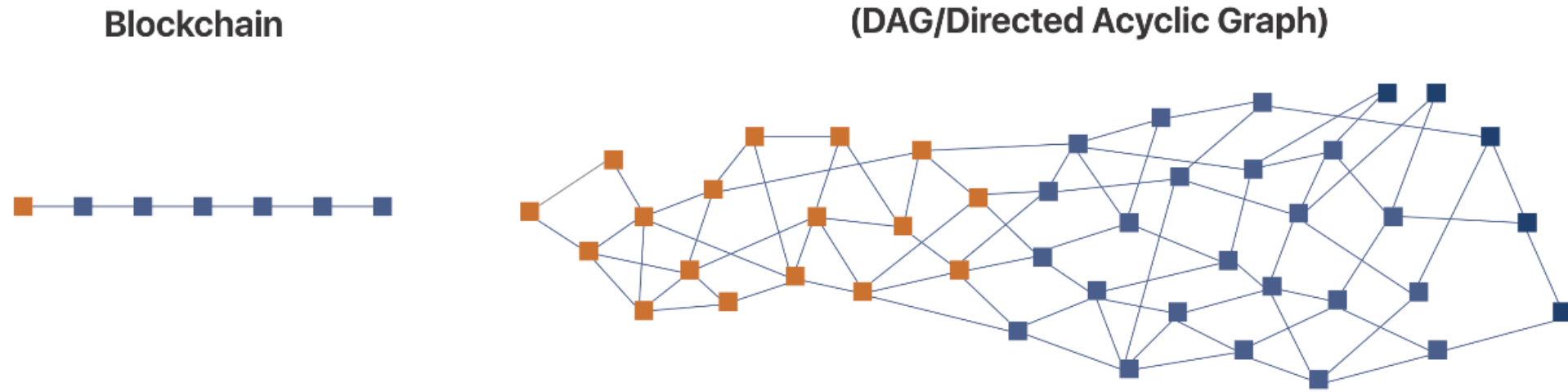
- The traditional centralized VANET architectures are prone to several kinds of malicious attacks.
- Such architectures are not future-proof since they may not be efficient in handling massive amounts of traffic data generated by smart vehicles such as video and sensor data.

Proposed solution

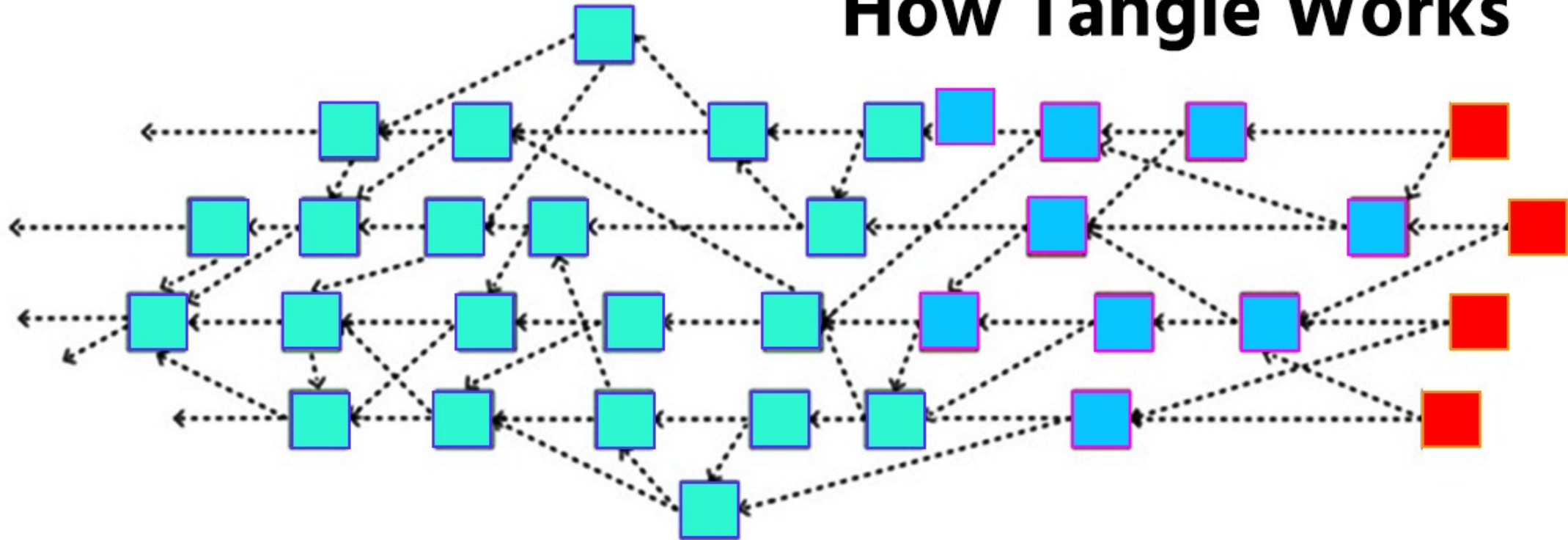
To overcome the limitations faced by traditional centralized architectures, we propose the creation of a distributed VANET based on the tangle data structure to secure communication in vehicular networks. A sample smart contract based on game theory is also proposed to model the interaction between vehicles and RSUs.




What is a Tangle?

Tangle, based on the concept of Directed Acyclic Graph (DAG), is the data structure behind IOTA's distributed ledger and protocol. Tangle adopts some elements from the traditional blockchain and realizes some entirely new ones that allow it to overcome the limitations of traditional blockchain.



How Tangle Works



-  Fully confirmed transactions in green nodes
-  Partially confirmed transactions in blue nodes
-  Unconfirmed transactions (also known as tips) in red nodes

Every transaction represented by a node is validated by two previous transactions connected via edges (arrows) moving in a particular direction

Why not use the Traditional Blockchain?

As blockchain transaction volumes grow, storage and network bandwidth requirements increase. 'Proof of Work' can also consume large amounts of computing power and electricity. There are of course different consensus algorithms, but 'the perfect' consensus algorithm is yet to emerge (if it ever does). Scalability is another issue that severely hinders the efficiency of any blockchain-based application. Furthermore, most blockchain architectures suffer from forking and pruning issues that severely hamper their reliability.

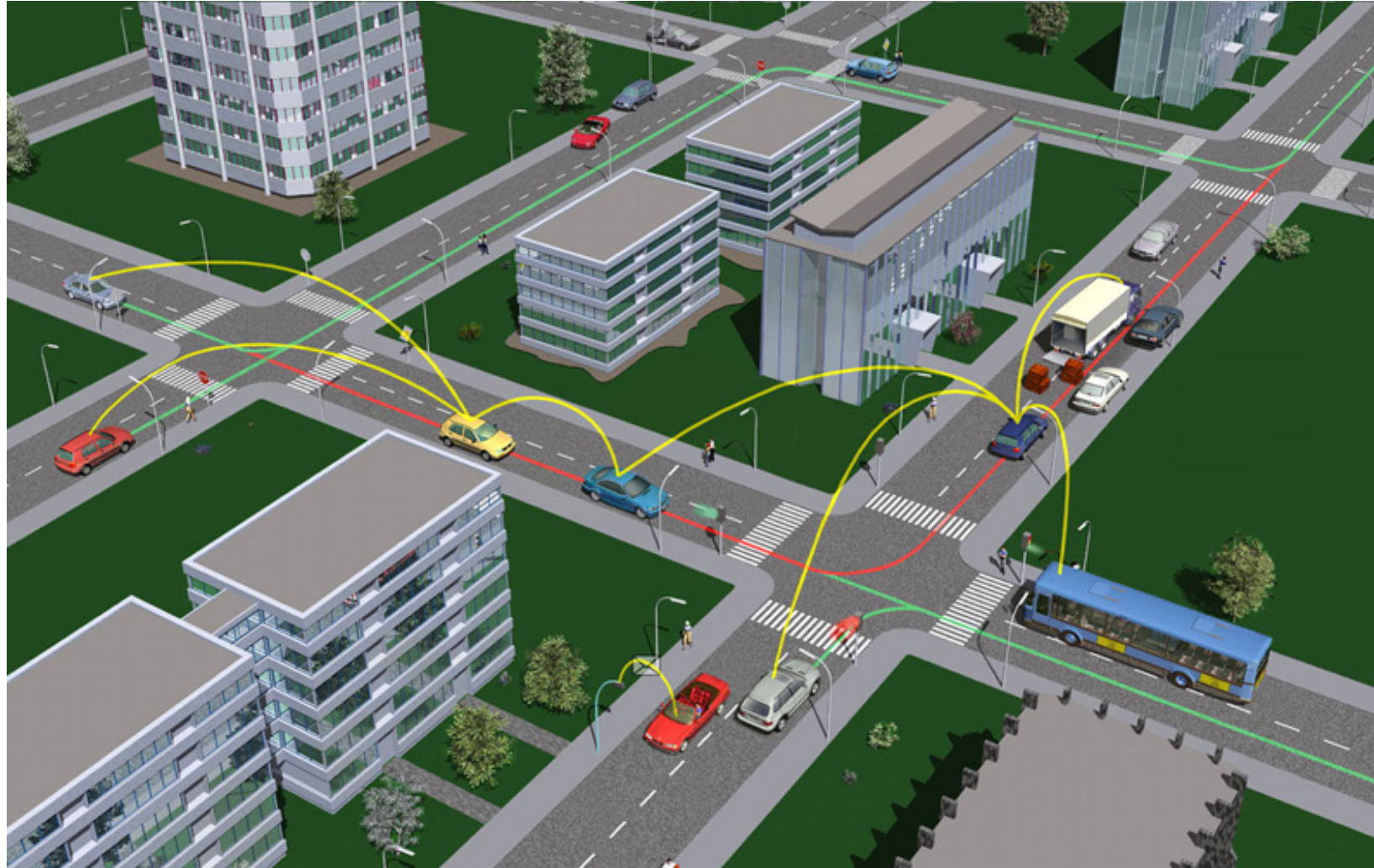
CATEGORY	BLOCKCHAIN	TANGLE (DAG)
DATA STRUCTURE	Data structured in blocks in order of transactions which are validated by miners in the ecosystem.	Data structured in a way that ensures that each transaction is independent.
CONSENSUS	Participants have the ability to mint new tokens via different consensus algorithms.	The present transaction validates the preceding transactions to achieve consensus.
TRANSACTIONS PER SECOND (TPS)	Highly limited in terms of scalability and TPS.	Ensures that scalability and TPS are high.
VALIDATION OF TRANSACTIONS	Miners have the power to postpone a transaction or cancel it entirely.	The success of the present transaction depends on its ability to validate two previous transactions.

Proposed Model

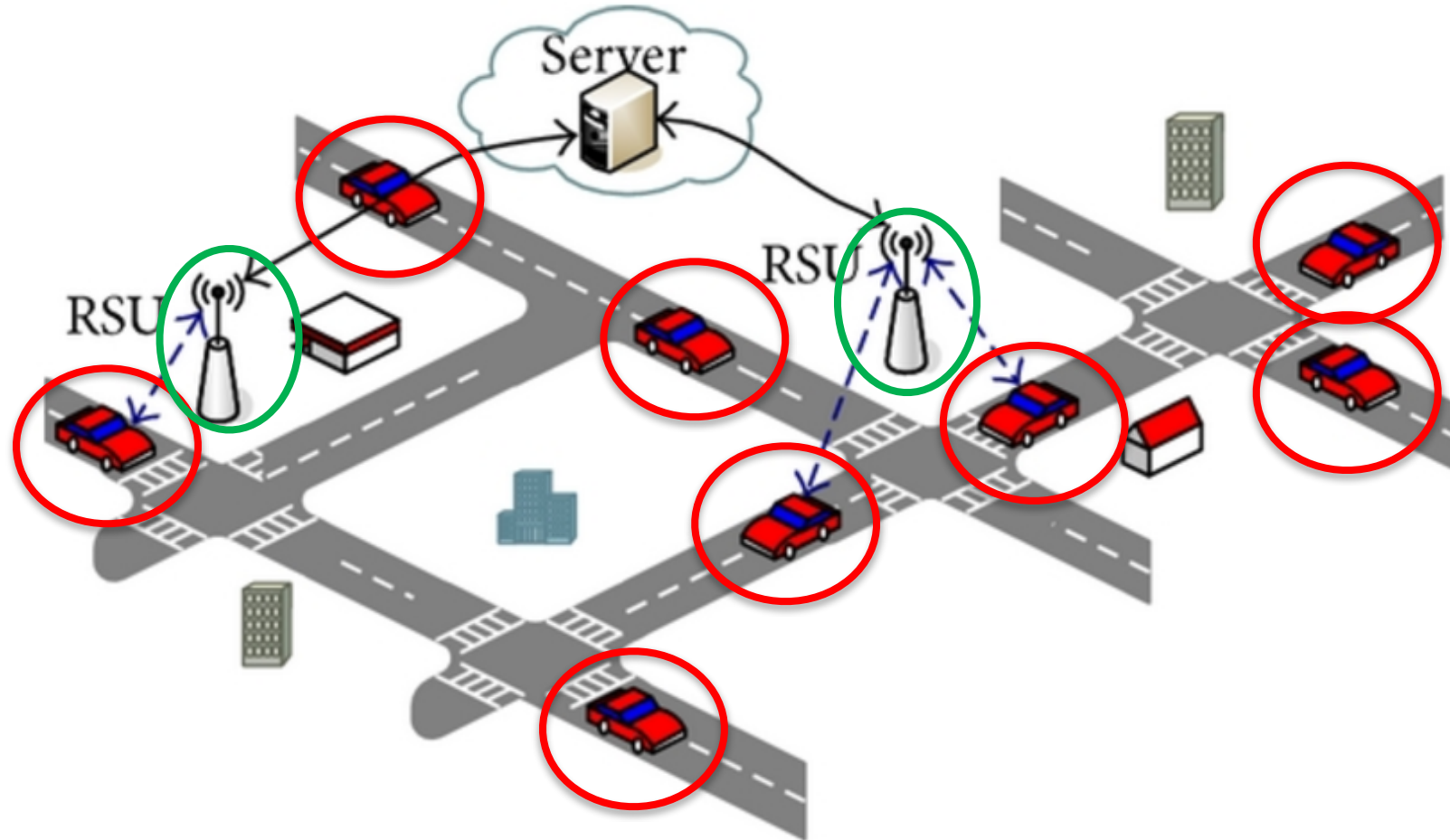
In our work, we consider a model in which any vehicle inside the range of a Road-Side Unit (RSU) can request it for information like the location data of other vehicles. The requesting vehicle can get the desired data of other vehicles through two routes:

- 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.

Scenario 1 – Direct Vehicle-to-Vehicle Communication



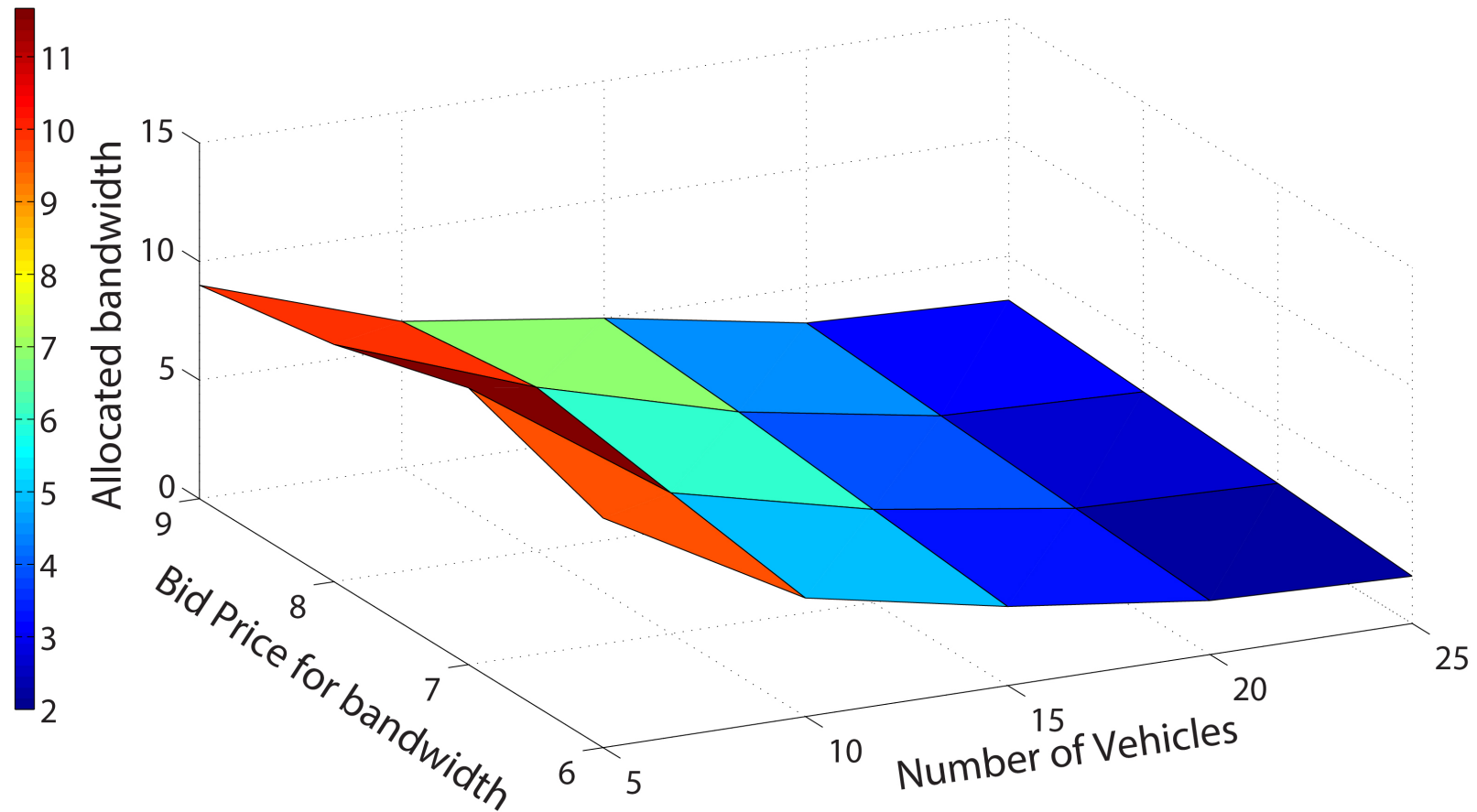
Scenario 2 – Vehicle-to-RSU (V2R) Communication



To model the financial interactions between the RSUs and the vehicles in a V2R model, we include an auction-based game theory in our work. The deployment of a game-theoretic smart contract on the IOTA network ensures that requesting vehicles are allotted bandwidth at the minimum possible price while ensuring maximum possible Quality of Experience (QoE).

For the evaluation of our V2R model, we have considered four vehicles in proximity to a single RSU in a DAG-enabled V2R network. The required bandwidth of four vehicles while entering 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.

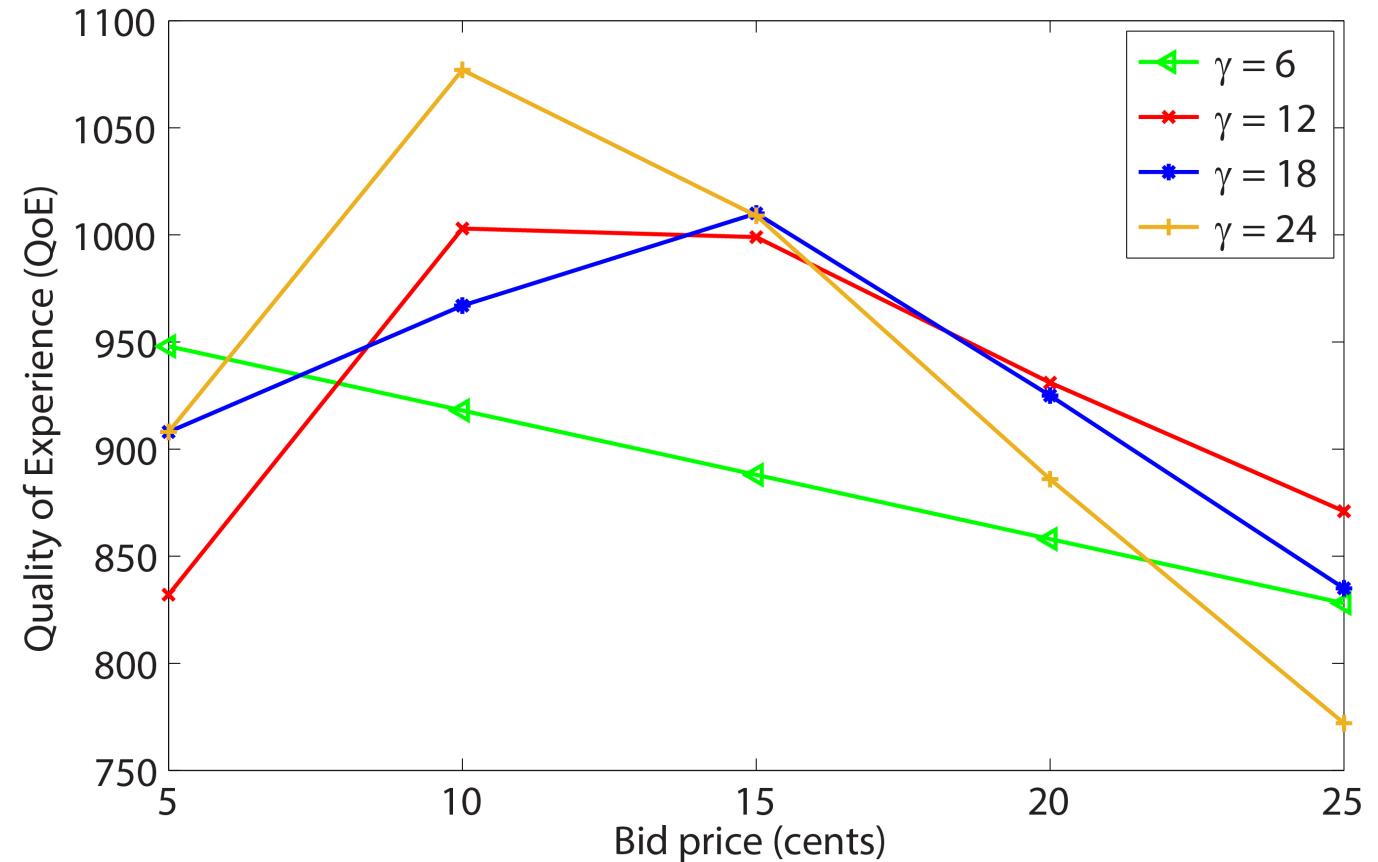
Results



The figure above demonstrates that the bandwidth allocated by the RSU to any vehicle 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 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 this figure. 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.



Conclusion

- ❑ Existing solutions in the direction of securing VANETs are based on centralized architectures, and therefore, face several challenges in terms of reliability and scalability.
- ❑ In this paper, we propose a secure and distributed framework for vehicular communication in VANETs.
- ❑ To resolve the scalability issues associated with traditional blockchain, we propose the use of a DAG-based tangle data structure.
- ❑ 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.

Future Work

- ❑ In this work, we only model the financial interactions between vehicles and RSUs. In the future, sophisticated smart contracts can be deployed in the proposed network to model different interactions between the parties involved.
- ❑ This security aspect of the model needs to be evaluated more comprehensively to establish the reliability of our model.



BITS Pilani

Pilani | Dubai | Goa | Hyderabad

Thank you