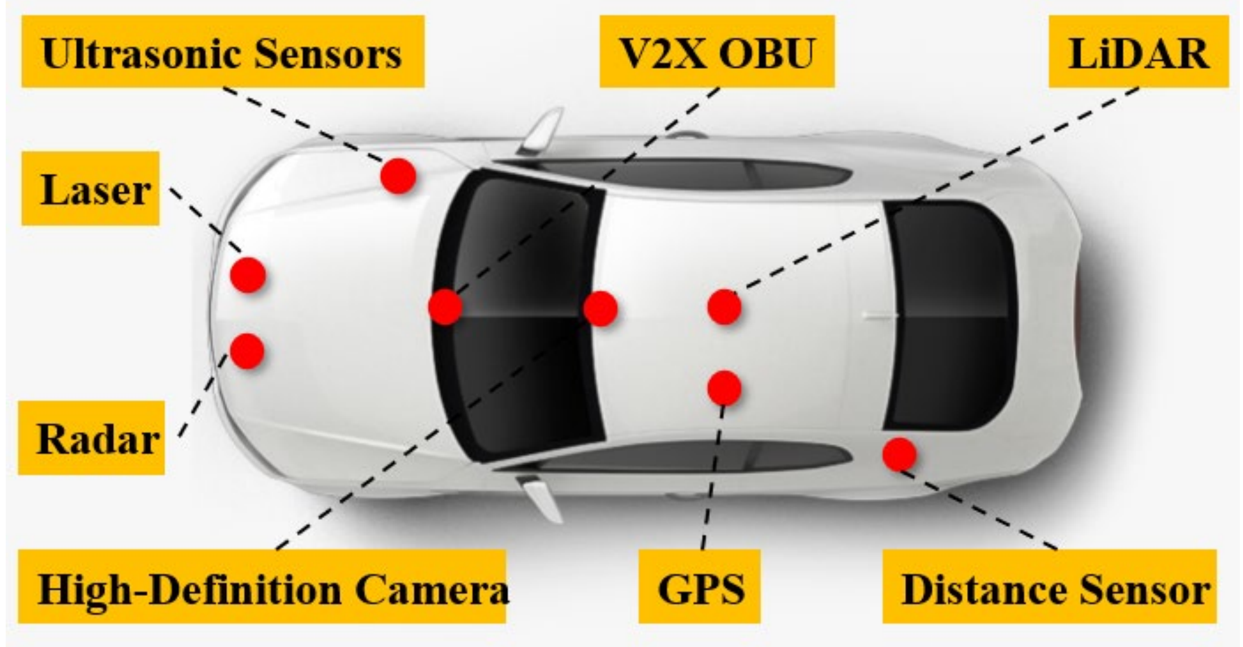
# Unmasking Deception in VANETs: A Decentralized Approach to Verifying Truth in Motion

**Susan Zehra, Syed R Rizvi, Steven Olariu**
***Old Dominion University***

## Abstract

VANET, which stands for "Vehicular Ad Hoc Network," is a wireless network that allows vehicles to communicate with each other and with infrastructure, such as Roadside Units (RSUs), with the aim of enhancing road safety and improving the overall driving experience through real-time exchange of information and data. VANET has various applications, including traffic management, road safety alerts, and navigation. However, the security of VANET can be compromised if a malicious user alters the content of messages transmitted, which can harm both individual vehicles and the overall trust in VANET technology. Ensuring the correctness of messages is crucial for the success of VANET, as fake messages pose a threat to traffic safety, human lives, and the credibility of VANET. This poster presents a novel framework for efficiently identifying vehicles that spread fake messages in VANET. The framework divides messages into two categories, urgent and non-urgent, and handles them using a decentralized priority queue consisting of trusted RSUs. The RSUs register dynamic security keys of the vehicles and broadcast the valid ones in their range for quick message exchange. The simulation results show that the framework is scalable and can efficiently identify vehicles that spread fake messages while providing secure communication and guaranteeing the QoS requirements of safety-related VANET applications.



## Concerns Due to Fake Messaging

Fake messaging impacts drivers' behavior, which can cause changes in the network topology

**Security concerns:**

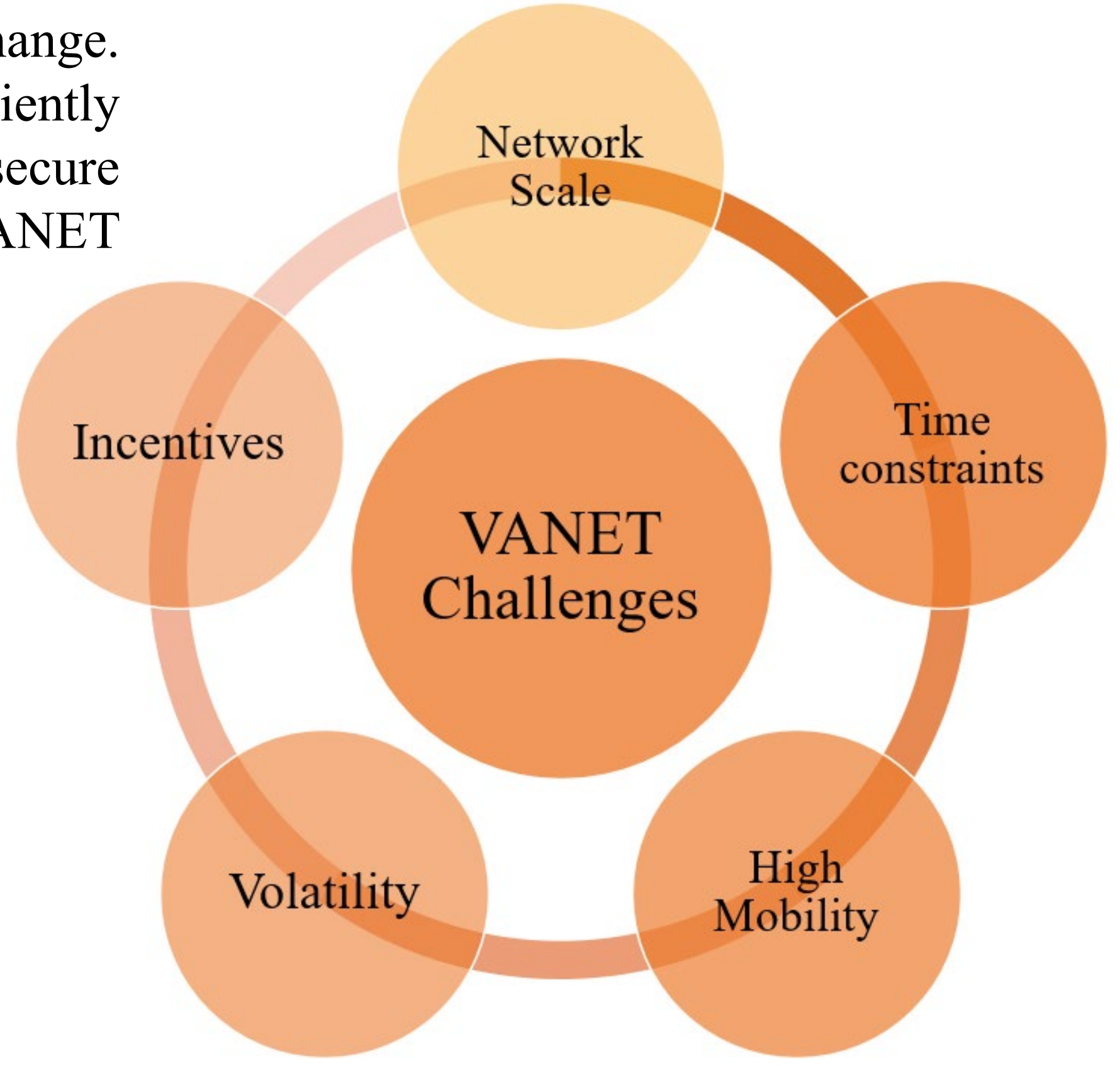
- For example, a malicious user alters message(s)
- Attacks could cause traffic jams by spreading bogus information
- Positioning information could be cheated, and data could be forged
- Hardware tampering

**Privacy concerns:**

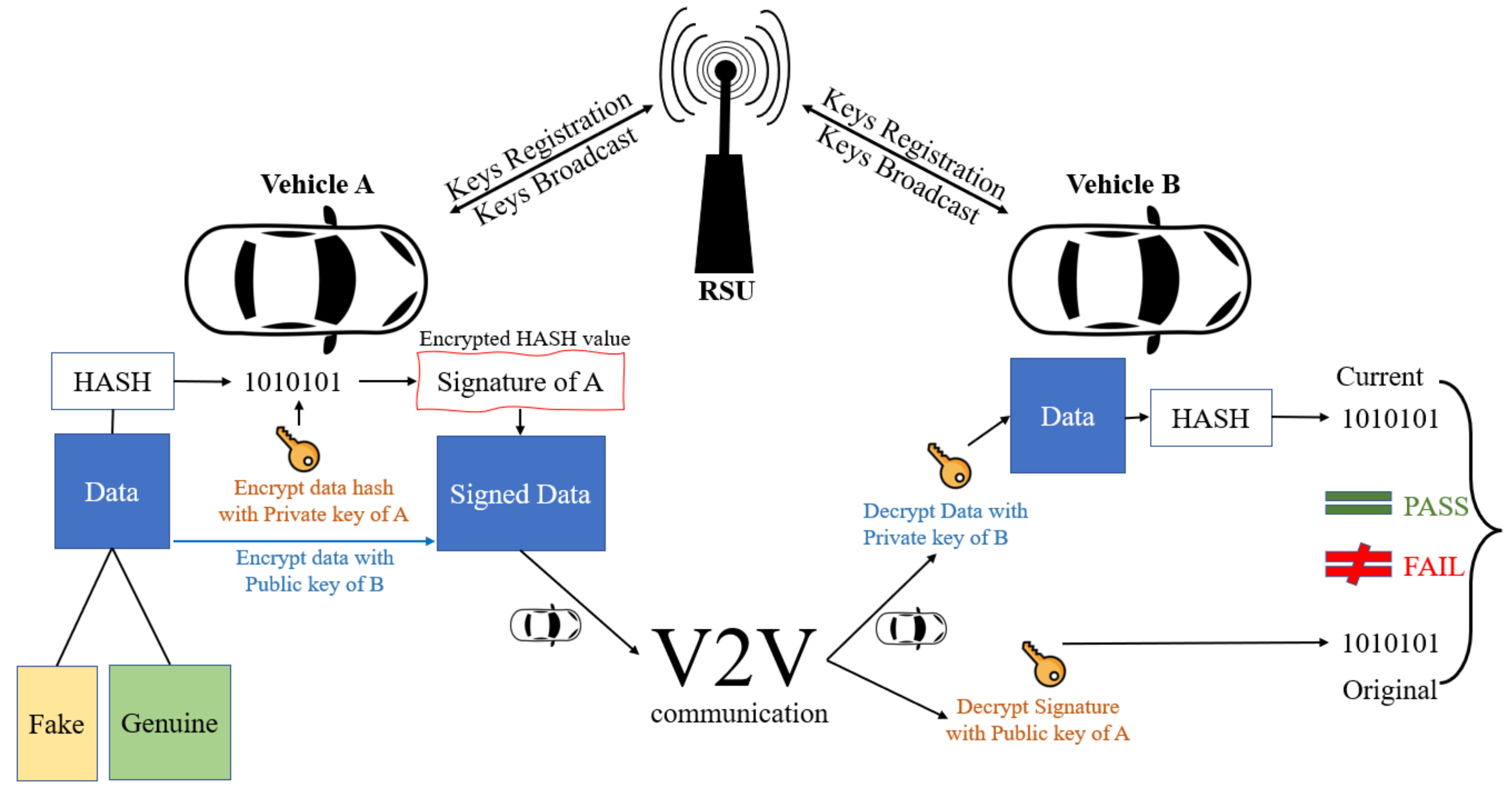
- Violation of privacy, or impersonation

**Negative Consequences of Fake Messaging:**

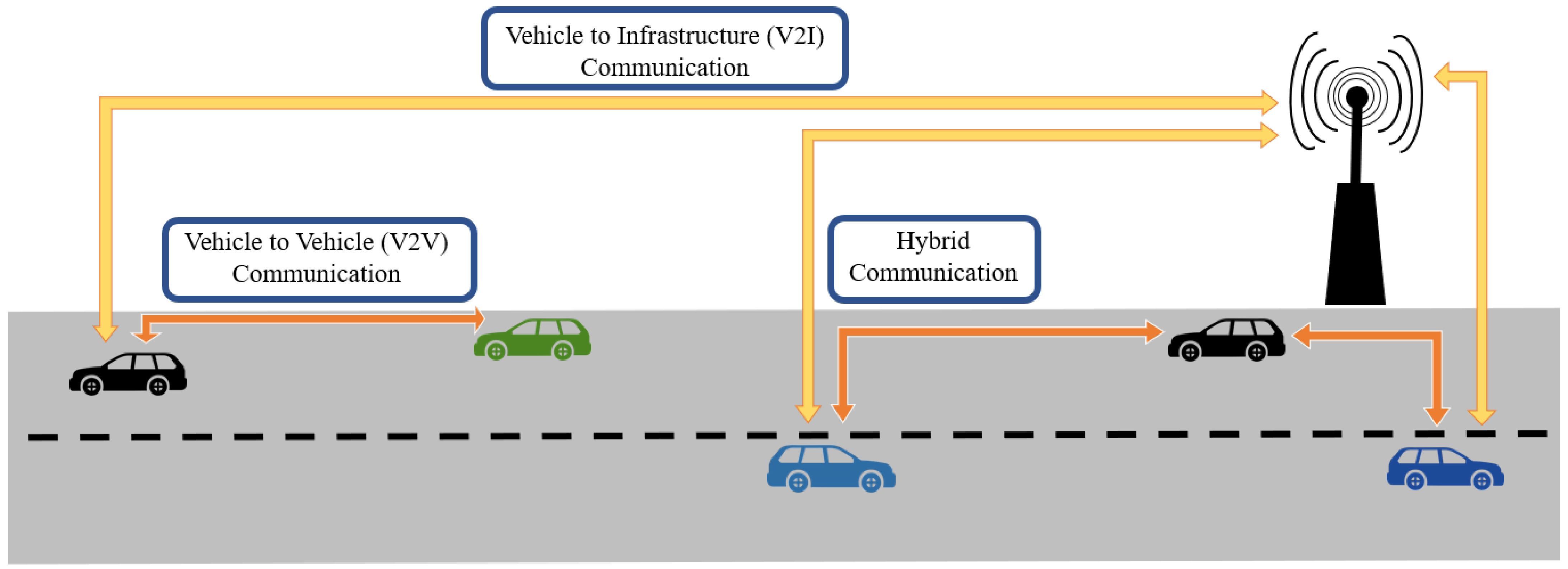
- Misleading drivers
- Causing unnecessary traffic congestion
- Disrupting emergency services
- Increasing the risk of accidents
- Wasting resources and time
- Damaging the credibility of the network and reducing trust



## Fake Message Testing

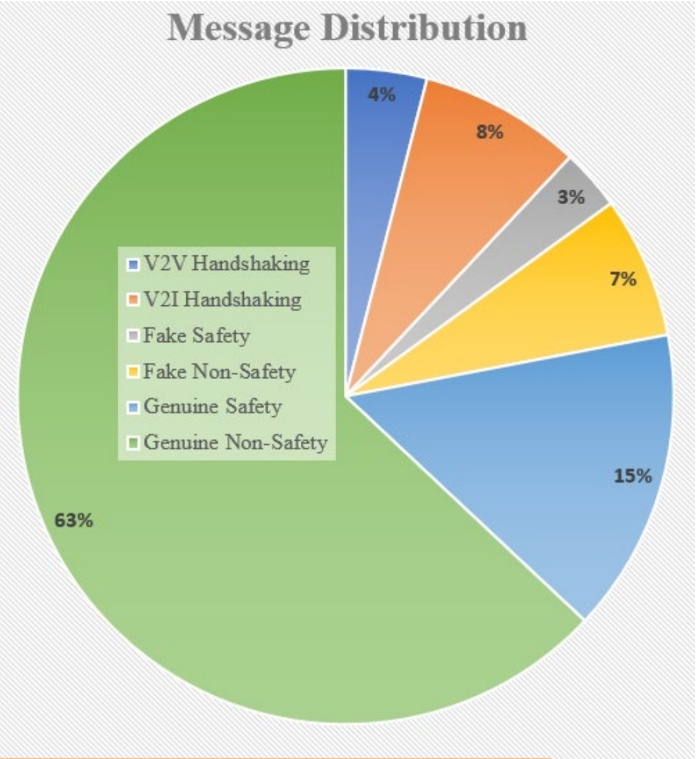


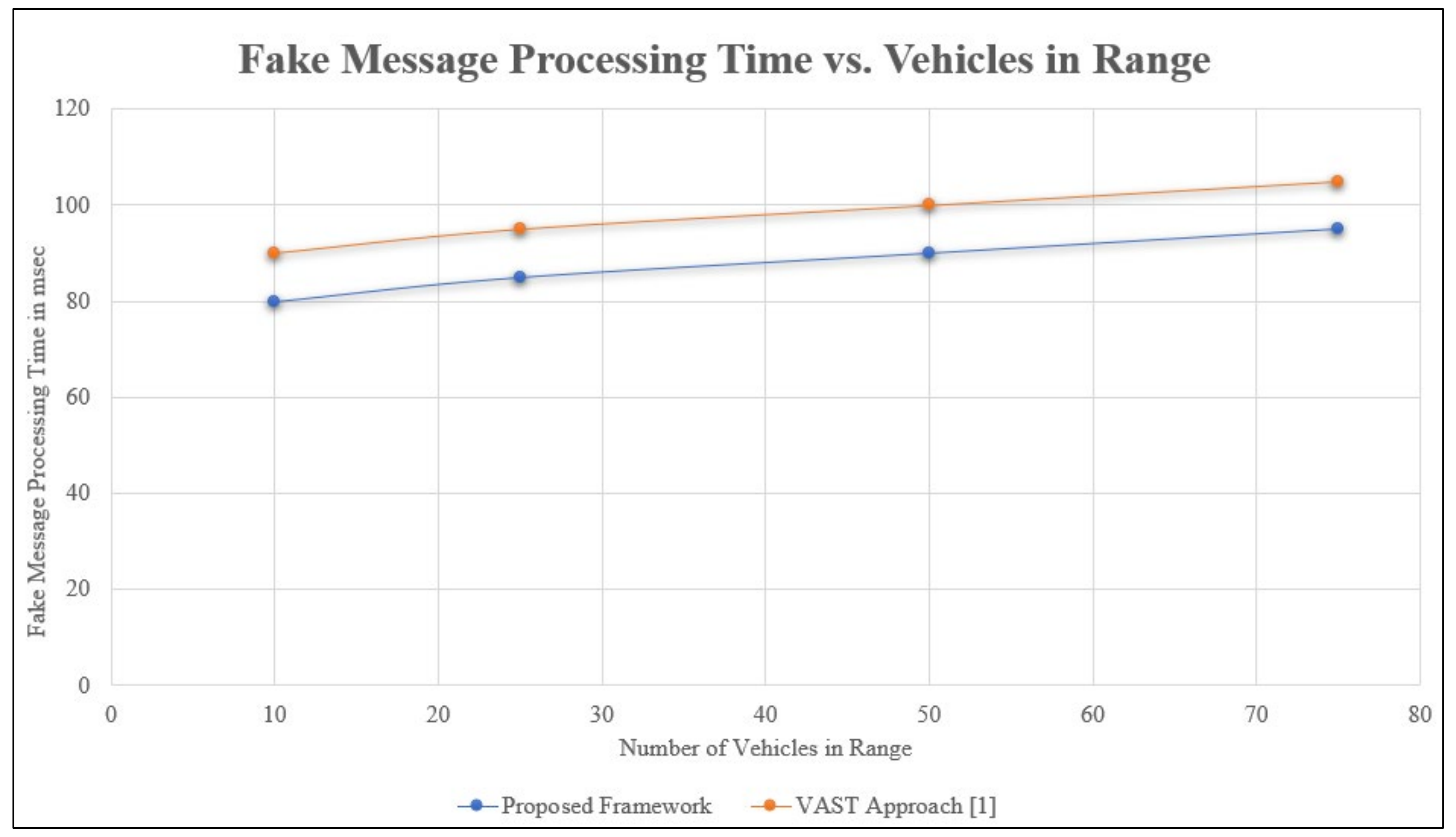
## Vehicular Ad Hoc Network (VANET)


Vehicle to Infrastructure (V2I) Communication
Vehicle to Vehicle (V2V) Communication
Hybrid Communication

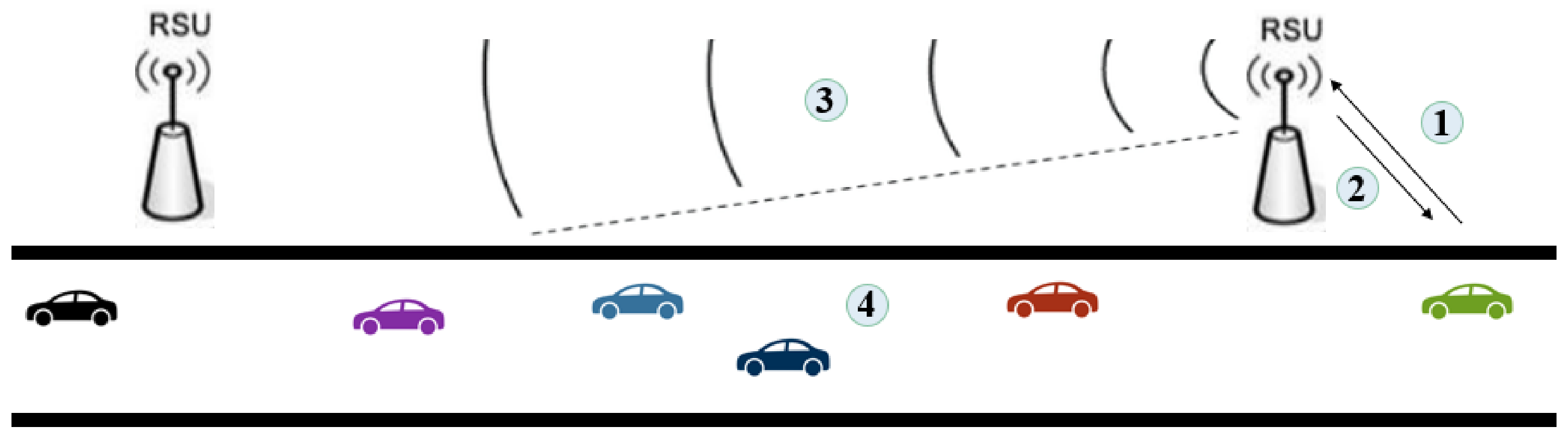
## Simulation and Results

| Parameters | Value |
|---|---|
| Area | 5000x5000 sq meter |
| Number of Vehicles | 100 to 200 |
| Traffic Density | 1-100 cars in radio range |
| Number of RSU | 10 |
| Speed of Vehicles | 30-60 km/hr |
| RSU Range | 1 km |
| OBU Range | 300 meter |
| Simulation Time | 100s |
| Minimum Distance of Separation between Vehicles | 20 meter |





## Framework



Legend
1 V2I Handshake: Vehicle provides its *Public Key* to the RSU
2 I2V Handshake: RUS provides a list of valid *Public Keys* to the vehicle
3 I2V Broadcast: RSU broadcasts a list of valid *Public Key*
4 V2V Handshake: Vehicles exchange messages

## Conclusion

VANET is a promising technology that can significantly enhance road safety and driving experience by enabling real-time communication between vehicles and infrastructure. However, the security of VANET is critical, and fake messages can compromise its effectiveness, endangering human lives and eroding trust in the technology. This poster presents a novel framework that efficiently identifies vehicles that spread fake messages in VANET, using a decentralized priority queue of trusted RSUs to handle urgent and non-urgent messages. The framework's simulation results demonstrate its scalability and effectiveness in guaranteeing the QoS requirements of safety-related VANET applications while providing secure communication. The proposed framework can contribute to the wider adoption of VANET and the realization of its full potential in enhancing road safety and improving driving experience.

## VANET Applications

**Safety Applications:**
1.Collision Avoidance
2.Emergency Vehicle Warning
3.Intersection Safety
4.Road Hazard Warning
5.Cooperative Adaptive Cruise Control
6.Pedestrian Safety
7.Lane Change Assistance

**Non-Safety Applications:**
1.Infotainment Services
2.Fleet Management
3.Traffic Management
4.Parking Management
5.Toll Collection
6.Eco-Driving
7.Autonomous Driving

## Security Requirements

AUTHENTICATION INTEGRITY CONFIDENTIALITY AVAILABILITY ACCESS CONTROL

## References

[1] A. Studer and F. Bai, "Flexible, extensible, and efficient vanet authentication," Journal of Communications and Networks, vol. 11, no. 06, pp.574–588, 2009.
[2] Alhilal at el., Distributed Vehicular Computing at the Dawn of 5G: a Survey. https://arxiv.org/pdf/2001.07077.pdf
[3] Soyturk, Mujdat, et al. "From vehicular networks to vehicular clouds in smart cities." Smart Cities and Homes. Morgan Kaufmann, 2016. 149-171.
[4] Weber, J., Neves, M. & Ferreto, T. VANET simulators: an updated review. J Braz Comput Soc 27, 8 (2021).

Contact Email(s): szehra@odu.edu, srizvi@odu.edu, olariu@odu.edu