**DECENTRALIZED TRUST MANAGEMENT SYSTEM FOR VANETS**

Vivaash Koundal ~ 23BCE5095

**Abstract**

Vehicular Ad-Hoc Networks (VANETs) face significant challenges in ensuring the trustworthiness and security of information exchanged between vehicles. Traditional centralized trust management systems are inadequate for the highly dynamic and distributed nature of VANETs, while existing decentralized approaches often suffer from scalability issues and high computational overhead.  
This project proposes a novel, lightweight, and scalable blockchain-based trust management system for VANETs, integrated with adaptive routing algorithms (AODV, GyTAR, TMR). The system effectively mitigates security threats such as false information dissemination and Sybil attacks while maintaining network efficiency. The model demonstrates improved safety message reliability, reduced delay, and robust detection and isolation of malicious vehicles.

**Keywords:** VANET, Blockchain, Trust Management, Routing Algorithms, Security, AODV, GyTAR, TMR

**Introduction**

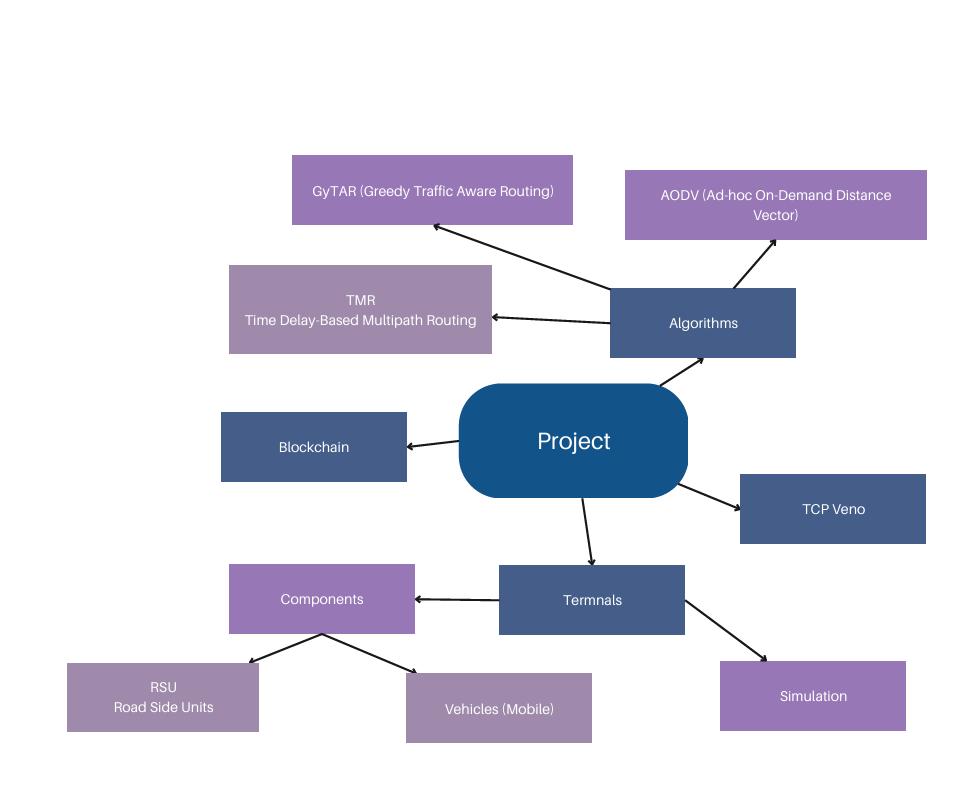
The need for secure and reliable communication in VANETs is paramount, given their application in road safety and traffic management. Existing trust management solutions either rely on centralized authorities or are not scalable for real-world vehicular networks.  
This project addresses these limitations by integrating a decentralized blockchain-based trust management system with adaptive routing, enabling secure, efficient, and scalable communication. The novelty lies in the lightweight blockchain design, custom consensus mechanism, and dynamic routing algorithm selection based on real-time network conditions, ensuring both security and performance in VANET environments.

**Literature Survey**

* **Yang et al., "Blockchain-Based Decentralized Trust Management in Vehicular Networks" (IEEE IoT Journal):**  
  Purpose: To propose a blockchain-based trust management system for VANETs.  
  Method: Lightweight blockchain with reputation scoring and consensus tailored for vehicular networks.  
  Key Findings: Enhanced security and scalability, effective against Sybil and false data attacks.  
  Conclusion: Blockchain can provide decentralized, tamper-resistant trust management for VANETs.
* **Karanam et al., "Overlay based fault tolerant peer to peer multicasting for emergency data communication in VANETS":**  
  Purpose: To improve emergency data dissemination in VANETs.  
  Method: Fault-tolerant peer-to-peer multicasting overlay.  
  Key Findings: Improved reliability and reduced delay in emergency scenarios.  
  Conclusion: Overlay multicasting can enhance VANET robustness for critical communications.

**Conclusion for Literature Survey:**  
The literature supports the use of blockchain and adaptive routing for secure, scalable, and efficient VANET communication, motivating the proposed integrated solution.

**Methodology**

****

* **Data Collection:**  
  Simulation-based data generation with configurable network parameters (number of vehicles, speeds, RSU radius, etc.).
* **System Architecture Diagram:**  
   Architecture includes Mobile Domain, Infrastructure Domain, and Generic Domain, with V2V, V2I, and V2B communications.
* **Discussion of the Diagram:**  
  Vehicles equipped with OBUs communicate with each other (V2V) and with RSUs (V2I). RSUs connect to broader networks (V2B). Blockchain ensures data integrity and trust, while routing modules enable efficient message delivery.
* **Methodology Used:**
  1. Develop a lightweight blockchain for trust management.
  2. Implement reputation scoring and malicious vehicle detection.
  3. Integrate three routing algorithms (AODV, GyTAR, TMR).
  4. Use TCP Veno for congestion control.
  5. Simulate accident scenarios and dynamic route selection at a T-junction.
  6. Measure V2V and V2I delays, isolate malicious vehicles, and report performance.
* **Modules of the Proposed Work:**
  1. Blockchain Module
  2. Configuration Module
  3. RSU Module
  4. Vehicle Module
  5. Routing Algorithms (AODV, GyTAR, TMR)
  6. Simulation Module
  7. Requirements Module

**Results & Discussion**

* Performance Parameters:
  + Average V2V and V2I communication delays
  + Number of isolated malicious vehicles
  + Total simulation time
  + Algorithm-specific performance (AODV, GyTAR, TMR)
* Findings:
  + The blockchain-based system-maintained data integrity and enabled real-time trust scoring.
  + Adaptive routing (GyTAR/TMR) reduced delays in medium/high-density scenarios compared to AODV.
  + Malicious vehicles were successfully detected and isolated, improving network reliability.
* Graphs/Tables:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| S.no | Configuration | | Sim Results | | |
| Algo Used | # of vehicle | Total Time | Avg V2V Delay | Avg V2I Delay |
| 1 | 1 | 11 | 11 | 100.48 | 27.27 |
| 2 | 2 | 11 | 11 | 102.35 | 27.65 |
| 3 | 3 | 11 | 11 | 102.06 | 27.51 |
| 4 | 1 | 45 | 11.01 | 108.01 | 27.57 |
| 5 | 2 | 45 | 11.01 | 104.84 | 27.36 |
| 6 | 3 | 45 | 11.01 | 105.25 | 27.27 |
| 7 | 1 | 100 | 11.03 | 104.63 | 27.6 |
| 8 | 2 | 100 | 11.02 | 104.75 | 27.57 |
| 9 | 3 | 100 | 11.02 | 104.79 | 27.54 |
| 10 | 1 | 11 | 31 | 104.17 | 28.01 |
| 11 | 2 | 11 | 31 | 103.59 | 27.62 |
| 12 | 3 | 11 | 31 | 105.44 | 27.54 |
| 13 | 1 | 45 | 31.01 | 104.66 | 27.49 |
| 14 | 2 | 45 | 31.01 | 105.12 | 27.48 |
| 15 | 3 | 45 | 31.01 | 104.69 | 27.5 |
| 16 | 1 | 100 | 31.02 | 104.99 | 27.47 |
| 17 | 2 | 100 | 31.02 | 105 | 27.48 |
| 18 | 3 | 100 | 31.03 | 104.98 | 27.46 |
| 19 | 1 | 100 | 901.04 | 104.95 | 27.51 |
| 20 | 2 | 100 | 901.12 | 104.98 | 27.46 |
| 21 | 3 | 100 | 901.12 | 104.99 | 27.5 |

**Conclusion**

The project demonstrates that a blockchain-based, decentralized trust management system combined with adaptive routing algorithms can significantly enhance the security, reliability, and efficiency of VANETs. Key achievements include successful detection and isolation of malicious vehicles, reduced communication delays, and robust operation across varying network densities.

**Future Directions:**

* Integration with real vehicular hardware for field testing
* Enhanced privacy mechanisms for vehicle identities
* Advanced incentive schemes for honest participation
* Cross-network trust management for heterogeneous vehicular networks
* Trust score can be used by insurance companies to

formulate packages based on usability

References: 1 Yang, Y. T., et al. "Blockchain-Based Decentralized Trust Management in Vehicular Networks." IEEE Internet of Things Journal.2 Karanam, V., Maheswari, B. U., & Sudarshan, T. S. B. "Overlay based fault tolerant peer to peer multicasting for emergency data communication in VANETS." 2017 International Conference On Smart Technologies For Smart Nation.