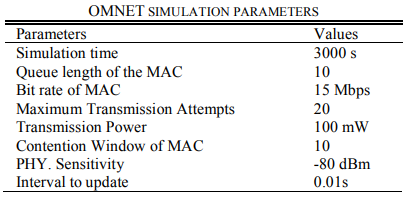
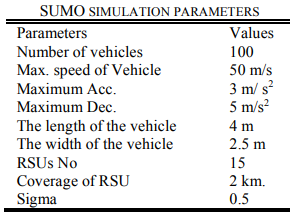
A Privacy-Preservation Framework based on Biometrics Blockchain (BBC) to Prevent Attacks in VANET

* Proposal: a biometrics blockchain (BBC) framework to secure data sharing among vehicles in VANET and to retain statuary data in a conventional and trusted system.
* Simulations in OMNeT++, Veins, and SUMO.
* Framework Components:
  + Trusted Authority (TA): initializes system, deploys smart contracts, registers vehicles and revokes registrations.
  + Motor Vehicle Department (MVD): vehicle registration, maintaining vehicle records, authorizes TA to issue certificates and public keys to the vehicles after verification process is completed from MVD.
  + Vehicle
  + RoadSide Unit (RSU)
  + Blockchain: responsible for secure handling of the transactions (safety messages) exchanged by vehicles across the network.
* Biometrics based Authentication:
  + OBU have finger print scanner which scans the finger print of the driver and send it with the driver’s information needed to register at TA.
  + Registration begins with obtaining real identity of the vehicle from the MVD, and sending the biometric data of the vehicle’s authorized user and vehicle ID to the TA. After verification, TA generates certificate holding pair of keys. After that vehicle can join the blockchain
* Simulation:
  + Parameters:





* + Compared Existing solutions: BC-VANET, ASC and LAKAP
  + Performance Analysis:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Without DoS | | With DoS | |
|  | Framework | Existing | Framework | Existing |
| Packet Delivery Rate | 0.99 | 0.9-0.98 | 0.96 | 0.7-0.94 |
| Computational Cost (20 vehicles) | 0.1 ms | 0.13 ms- 4 ms | 0.1 ms | 0.13 ms- 4 ms |

* + Security Analysis:
    - Secure Registration: ensures security using public and private keys. The keys are stored in the OBU which is a tamper proof memory. The vehicle is registered only when the registration data is verified with MVD. The data is sent to network by signing with private key of the vehicle.
    - Data Integrity: authentication and data are protected by hash function, signature and match functions.
    - Privacy Preservation and Traceability: real identity is not revealed to anyone, and data is traceable by the blockchain when any malicious activity occurs.

Blockchain-Based Pseudonym Management Scheme for Vehicular Communication

* Proposal: a lightweight pseudonym management scheme for vehicular authentication using blockchain.
* Simulation:
  + SUMO: to generate the vehicle traffic
  + OMNET++ with Veins: to simulate the network communication
  + Permissioned blockchain framework was implemented using hyperledger composer.
* Analysis:
  + Reduce authentication delay and computation overhead on vehicle OBUs.
  + Increased message exchange with the RSUs.
  + Effective under low to moderate channel loads.
  + Recommended that additional congestion control mechanisms should be implemented for higher loads.