Final project

Compromised vehicle threat propagation simulator

Design and implement an application (using C language) that simulates how a malware propagates across a Vehicle-to-Vehicle (V2V) communication network. Vehicles are represented as nodes, and communication links as edges with weights capturing propagation characteristics. Edge weights may represent:

- Propagation time (delay)
- Infection probability
- Trust or vulnerability score
- Any other justified metric

Your program must analyse the spread of compromise, identify critical vehicles, and compute optimal propagation routes. Implement at least **four** of the following graph-based functionalities:

1. Infection spread wave from an initially compromised vehicle
2. Fastest or most-likely propagation path to a target
3. All-pairs propagation analysis
4. Detection of propagation clusters or communities
5. Backbone of propagation
6. Detection of problematic cycles

Compromised vehicle threat propagation simulator

UM6P University Mohammed VI Polytechnic

Submission (Dec. 4, before midnight on Canevas) Upload a single `.zip` containing:

- **PDF Report** (3–4 pages):
  - Graph modelling + assumptions + justification of edge weights
  - A detailed attack scenario (malware description, impacted asset, attacker profile..)
  - Justification of at least 4 selected graph/tree algorithms
  - Reference to 1+ research paper on graph theory in vehicular networks
  - Sample input–output
- **C Project Files**:
  - Clean, well-commented code
  - Proper header files
  - Acknowledgment of external sources

Demonstration (Dec. 5, afternoon)

- Teams of 2, **5-minute** demo
- One summary slide: modelled graph + key decisions
- Live run showing sample input/output