Social-Psychology Based Consensus Model for Secure Connected Vehicle Networks

Gianna Voce[1]

Mentors: Dr. Henry Griffith and Dr. Heena Rathore[2]

1. Department of Computer Science, Syracuse University, NY, USA
2. Department of Computer Science, Texas State University, TX, USA

Introduction and Motivation

- Connected Vehicles (CVs) are estimated to comprise 95% of new vehicle sales by 2030, and as such require better security solutions.
- Performance of state of the art methodologies to determine if a vehicle is malicious is impacted in majority-corrupt conditions.
- Equations from social psychology can be adapted for CVs to better handle majority-corrupt conditions.

Goal: Apply a mathematical model of opinion dynamics to improve identification of malicious vehicles within majority-corrupt CV networks.

Background

Consensus-Based Trust:

- CVs reports kinematic data through Basic Safety Messages (BSMs).
- Peer vehicles form their own estimates of these BSMs.
- Each vehicle then compare the reports and estimates to determine if a vehicle is "corrupt."
- The vehicle is assigned a "reputation score" that dictates how "trustworthy" it is.

DeGroot Learning[1]: $x(t) = A \cdot x(t\text{-}1)$

Where: x is a vertical array of opinions for agent i; A is a square, stochastic matrix that represents each agent's trust in the other agents' opinions of agent i

Model of opinion spreading used in psychology

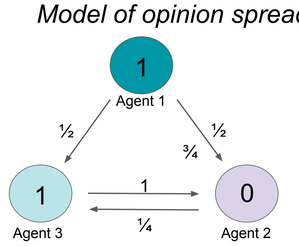

Fig 1: Agents 1 and 3 have opinion 1; agent 2 has opinion 0. Agent 1 trusts 3 and 2 equally, 2 puts ¾ of its trust in 3, and ¼ in 1. Agent 3 puts all its trust in 2. As t approaches infinity, the system will reach consensus of .529

Proposed Model

Proposed model is decentralized, convergences faster, is robust to failure.

Modified Equation for CV: $x_i(t) = A \cdot x_i(t\text{-}1) \cdot W$

Where: $x_i(t)$ is the reputation for agent i at time t, A is a square, stochastic matrix that represents each vehicle's trust in the other agents' reputation calculations for agent i, W is a weight matrix determined by how much self-reports and peer estimations differ

Modifications: adjacency, internal validity, external validity

Results

Motion Model Simulation

- Model coded in Python to simulate motion, lane changing, etc. Tested with 4, 10, or 20 vehicles in 75-98% corruption. Average F1-score: .97

Open-Source Traffic Simulation

- Data generated in an open-source traffic simulation[2] on two courses (closed loop with 95 vehicles, and on-ramp with a total of 67 vehicles). Average F1 score: .98

Real-World Data

- Dataset[3] from Tampa, Florida, that includes BSMs and peer reports from CVs. Average F1-Score: .93

Proposed DeGroot model was successful in identifying malicious and benevolent vehicles in systems up to 98% corrupt in three different datasets

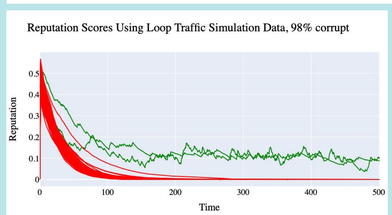

Fig 2: Reputations in a 98% corrupt network from traffic simulation. Uncorrupted vehicles are shown in green, corrupted show in in red. Time is in seconds.

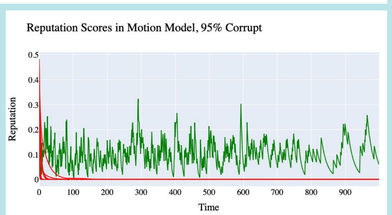

Fig 3: Reputations in a 95% corrupt network using motion model. Uncorrupted vehicles are shown in green, corrupted show in in red. Time is in seconds.

Comparison

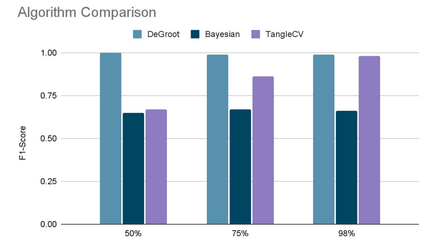

Fig 4: DeGroot performance compared to TangleCV[4] (a social-psychology-inspired algorithm) and Bayesian-based Distributed Trust Management System[5]

Discussion

- Applying the DeGroot equation of opinion dynamics to CV consensus-based trust algorithms successfully identifies malicious and benevolent vehicles in majority-corrupt systems
- In conditions that are 50%, 75%, or 98% malicious, the proposed DeGroot model consistently outperforms comparable algorithms
- Future work includes applying a variable weighted scheme on other kinds of majority-corrupt conditions such as spike, outlier, stuck-at, drift and others.

Acknowledgements

Thanks is given to the REU program at Texas State University. This work is made possible by the National Science Foundation under Grant No. CNS-2149950.

References

[1] "Lecture 5: The DeGroot Learning Model (PDF) | Networks | Economics." *MIT OpenCourseWare*
[2] Microsimulation of traffic flow. https://traffic-simulation.de/
[3] H. Griffith et al. "A Data Generation Workflow for Consensus-Based Connected Vehicle Security", *IEEE ICCE*, 2023.
[4] H. Rathore et al. "Social Psychology Inspired Distributed Ledger Technique for Anomaly Detection in Connected Vehicles", *IEEE Transactions on Intelligent Transportation Systems*, 2023.
[5] G. Rawat and K. Singh, "A bayesian-based distributed trust management scheme for connected vehicles' security". *Peer-to-Peer Networking and Applications*, 2023.