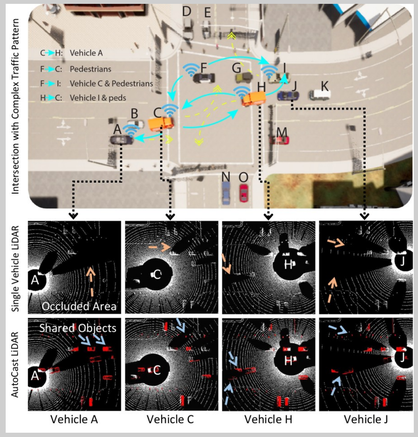
Privacy-Preserving, Community-Based Trust for Cooperative Autonomous Vehicles

Namo Asavisanu[1], Konstantinos Psounis[1], Ramesh Govindan[1], Fawad Ahmad[2], Hang Qiu
[1] University of Southern California, [2] Rochester Institute of Technology

Cooperative Autonomy



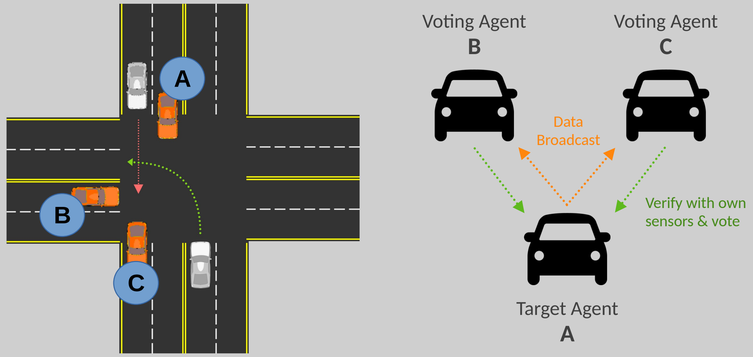
- Goal: Better overall **efficiency** and **safety** with multi-agent communication & cooperation
- Multiple ways to do so (at different layers in the stack)
  - Perception: sharing sensor data
  - Planning: sharing intent
  - Control: explicit cluster based control

Security & Privacy Challenges

- How can we trust other agents in the network, in real time, without relying on always-available connectivity?
- With the amount of potentially sensitive (e.g., location) data being shared to accomplish cooperative autonomy goals, how do we preserve the privacy of system users?

Community Based Trust

- Similar to how people trusts each other in online communities, we assign each agent a dynamic trust score
- To influence the trust score, we use a voting system – other agents, when possible, validates the data sent (or action taken) by an agent, then collectively upvote or downvote
- This score can then be embedded and signed by the system (using standard PKI), then broadcasted by the participants in each data frame, enabling rapid trust evaluations



Location Data Privacy

- Precise location is needed in-situ for cooperative autonomy
- Outside observers (ideally including the system itself) should not have historical or real-time location data access
- ID/certificate rotations, as well as in-situ voting can potentially create a system to satisfy this need

Identity Rotation for Tracking Prevention

- While keeping long-term “identities” consistent (for the purpose of trust), we can use pseudonyms (short-term identities) that we can rotate frequently as what we present to the network
- This works when we have a centralized authority server (they are now the only entity able to map pseudonyms to actual vehicle identities)
- Work is ongoing on determining how this can be achieved in a distributed fashion, while preserving everyone’s privacy

Security

- We increase robustness towards vote collusion by requiring multiple voters, and keeping track of vehicles that have voted for each other (in a limited period of time). More votes for a target = less vote weight for that target
- We also increase robustness towards spoofed sensor inputs by either utilizing in-situ votes with timing restrictions, or submission of the target agent’s signed beacon frames (which includes the timestamp among other data)
- The system is designed on top of standard PKI primitives, and does not get in the way of additional security systems (i.e., data link encryption). Embedded score validation can be done in less than 5 milliseconds, enabling real time use

ProperData Frontier 2nd Annual Symposium
Dec 1-2, 2022 | Irvine, California

SaTC Frontiers: Collaborative: *1956393* [1], *1955227* [2], *2103439* [3], *1956435* [4]
Institutions: UC Irvine [1], Northeastern Univ. [2], UC Davis [3], USC [4]
Lead PIs: A. Markopoulou [1], D. Choffnes [2], Z. Shafiq [3], K. Psounis [4]