Title

I. Prior Art

Dadras et al. [?] study behavior of a vehicle platoon in an adversarial environment. They consider insider attack where an adversary has control of a vehicle of the platoon and whose controller gains it can modify to destabilize or take control of the entire platoon. In the considered platoon, predecessor and follower vehicles distance and velocity information are used by a vehicle to compute its velocity and acceleration. The attack considered in the paper will influence the longitudinal control laws

II. Preliminaries and Problem Description

A. Car-Following Model of Truck Platoon

B. Attack Model

We consider an adversary that can control m out of n trucks (where, $m \leq n/2$) of a Driver Assistive Truck Platoon (DATP). The trucks uses radar and vehicle-to-vehicle (V2V) communication to drive longitudinally in a close-headway formation at highway speeds and to maintain a safe gap with the preceding vehicle. By remotely exploiting vulnerability in m truck's communication software, an attacker can hijack V2V's message transmission unit. Subsequently, by injecting malicious messages in the communication network of $(n-m)$ trucks, an adversary intends to impact the string stability of the platoon. We assume that the leader of the platoon is not attacked and we do not know the m attacked vehicles. Thus, the first goal is to detect the attacked trucks. The next goal is to identify the minimum number of trucks m, an adversary should attack to destabilize the platoon.

In the second attack model, we consider multiple vehicles communicating via V2V in a multilane highway. The vehicles broadcast Basic Safety Messages (BSM) to its neighboring vehicles. An adversary in control of one of the V2V equipped car can broadcast corrupted BSM with the intention of influencing the direction of motion of the vehicles. Thus, the goal is to design control law that can guarantee resilient coordinated motion of vehicles [?].