Trustworthy Transportation Networked Control Systems

Saurabh Amin (MIT), Galina Schwartz (UC-Berkeley), Alex Kurzhanskiy (UC-Berkeley)

December 16, 2013

1 Introduction

The recent advances in computing and networking technologies have enabled the next generation of vehicular applications based on real–time measurements. These changes bring forward ubiquitous sensing and actuation capabilities, mobile and embedded computing with smartphones, and deep penetration of wireless communication networks. They resulted in real-time traveler information systems (e.g., dynamic message signs), field actuation mechanisms (e.g., ramp and signal controllers), and allowed to improve the responses to natural disasters and terrorist attacks. However, the drawback of this information technology (IT) modernization is lowered security of transportation networked control systems (NCS), caused by the exposure to IT insecurities.

Cyber-attacks against transportation NCS. A historical artifact from the pre-Internet era is that the existing transportation NCS commonly assume that the system operators are trustworthy, and the sensor–control data is genuine. As the automotive industry continues a trend of embedding computer controlled and networked devices into vehicles, new vulnerabilities of these embedded devices have emerged [1]. These attacks make vehicles susceptible to remote exploitation and thus, directly influence the security of transportation NCS. For e.g., in Dec 2011, hackers executed an attack on the Northwest railway systems for two days according to a recent TSA memo. Additionally, several hacking incidents have been reported in the Toronto subway system (where the traveler information was reprogrammed) and the Moscow subway system (where a hacker transferred revenue from the ticketing system). The emergence of network-based vehicle applications is expected to bring such threats to the forefront (e.g., vehicle-to-vehicle crash avoidance, e-payment transactions systems, and crowd-sourcing of probe data). Indeed, the security solutions for embedded devices in vehicles are necessary, but far from sufficient for the security of transportation NCS.

Threat Model. Traffic sensors can be broadly classified into three categories (see Fig. 1). The quantities $f(x,t)$ (flow), $v(x,t)$ (speed), and $\rho(x,t)$ (density) on a road segment of length L are distributed in space $x \in [0;L]$, and evolve in time $t \in \mathbb{R}_+$ according to hyperbolic conservation laws. They are generically represented by $u(x,t)$ in Fig. 1.

- **S1** *P-traffic*: Point sensors are deployed at fixed locations $x_{i1}, x_{i2}, \ldots$ along a roadway. They measure the flow f of vehicles passing through this location throughout the time for which they are active. Examples of point sensors are loop detectors and embedded wireless sensors.
- **S2** *S-traffic*: Space sensors take snapshots of traffic density ρ at a given moment of time and repeat such snapshots at multiple times $t_{j1}, t_{j2}, \ldots$. Examples of space sensors are surveillance cameras and satellite data.
- **S3** *M-traffic*: Mobile sensors are located in vehicles and thus, they move with the traffic flow. They collect the space and time samples (x_k, t_k), from which the vehicle speed v is computed. Examples of mobile sensors are GPS equipped vehicles and

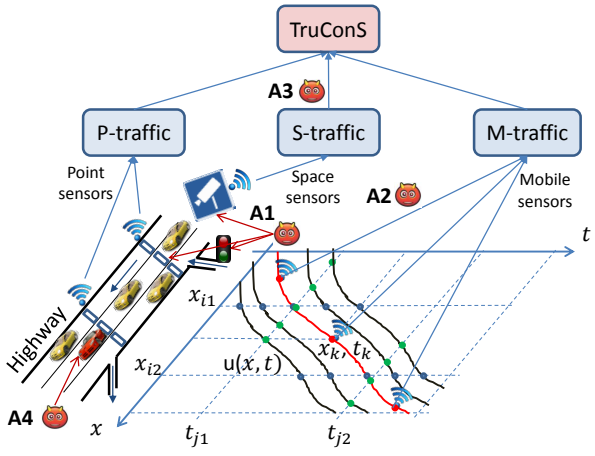

Figure 1: Threats to traffic sensors and measurement data.

automatic vehicle location techniques.

The threats to real-time traffic measurement data can be classified into four categories:

- **A1** Attacks (resp. faults) to the embedded traffic sensors due to adversarial (resp.) random disturbances; including loop-detectors, wireless sensors, GPS-equipped probes.
- **A2** Distributed DoS or deception attacks to the communication networks between traffic sensors, access points and traffic collection parties. These networks typically use open protocols making it easier for attackers to learn about NCS and thereafter interfere with its operation.
- **A3** Adversarial manipulations of automated tolling and ticketing systems and misconfigured data aggregation by traffic collection entities. In addition, numerous parties generate, use, and modify the traffic data, which allows for unauthorized access and manipulation.
- **A4** Field device compromises by fraudulent actors for identity theft, reconnaissance, and vandalism.

Modern transportation NCS depend on the availability and integrity of real-time measurement data. This data is used in four major domains of *operations planning*:

- **D1** *Traffic flow control* which implements ramp metering at freeway on-ramps and signal timing plans at signalized intersections to reduce congestion;
- **D2** *Demand management* which focuses on reducing the excess demand during peak hours;
- **D3** *Incident management* which targets resources to alleviate incident hot spots;
- **D4** *Traveler information* which is utilized to reduce traveler buffer time, i.e., the extra time the travelers must account for when planning trips.

Loss of availability and integrity of measurement data can be caused due to deception attacks and denial-of-service (DoS) attacks such as **A1**–**A4** to sensors **S1**–**S3**. This whitepaper presents the need for improving the operational resilience of transportation NCS against attacks on real-time measurement data for vehicular traffic networks.

2 Technical Challenges

We emphasize the need of security threat assessment for **A1**–**A4** to design resilient decision support for operations planning and control systems. These systems are responsible for traffic flow control (**D1**), demand management (**D2**), incident management (**D3**), and traveller information (**D4**). Especially important are the reliability failures (faults) and security failures (attacks) stemming from IT-driven failures in the traffic sensors **S1**–**S3**. We highlight three challenges for trustworthy transportation NCS:

Challenge 1: Compositions of dynamical network models of system operation using heterogeneous sensor data

To study different security and reliability scenarios, the integration of the physical traffic simulator [2] with communication network simulation and emulation capabilities, such as, ns-2 and the DETER testbed can be helpful. Such simulation-based approaches have been used for cyber-security testing and evaluation of networked systems with moderate success [3, 4]. New software tools are needed for automatic composition of security and reliability scenarios using real-time measurement data and historical knowledge of failure incidents. Such scenario compositions should account for the invariants and constraints specified by traffic management centers. The following aspects need to be considered (a) model-based invariants imposed by traffic flow theory, (b) event-based invariants imposed by communication protocols and architectures, and (c) constraints due to the uncertainty bounds of traffic state estimates and the available control strategies to the network managers. The challenge is to provide a semantically consistent, high-fidelity, and scalable platform for testing the safety and security of various operational control strategies.

Challenge 2: Model-based diagnostic tools to detect and characterize correlated security and reliability failures

The core component of a diagnostic tool for transportation NCS is a model-based scheme to facilitate the detection of correlated failures and isolating them. The focus should be placed on the diagnosis of false-data injection attacks to sensor data, where the adversary's goal is to compromise the safety of transportation NCS (e.g., by causing widespread congestion and traffic incidents) and yet evade detection. The traditional network intrusion detection systems rely on misuse-detection or anomaly-detection methods. They could fail to detect stealthy attacks, i.e., an adaptive adversary who can evade detection by learning typical response signals and exploiting the fact that detection guarantees are necessarily probabilistic. The challenge is to combine model-based fault detection tools with statistical techniques for

intrusion detection, while making mild assumptions on attacker statistics. We anticipate that such diagnostic schemes reduce the probability of misdiagnosis, and enable automatic triggering of safety-preserving control strategies.

Challenge 3: Operations planning and management based on robust control and game theoretic techniques

All domains **D1**–**D4** will benefit from improved NCS resilience to security and reliability failures, and will lead to system-wide improvements such as graceful degradation in response to extreme events (e.g., hurricanes). Here the challenge is to provide improved control and operational strategies for transportation NCS that will drive the network back to safe configuration at a minimal loss of efficiency. The theory of hybrid dynamical systems can be employed to develop closed-loop controllers that can be reconfigured to incorporate alerts from the attack diagnostic tools. We expect that this additional feature of operational strategies will make them more resilient to failures relative to the existing ones. Finally, to develop operational strategies that optimize the performance of transportation NCS in the presence of malicious actors, a game theoretic approach can be useful. Reflective of the networked nature of transportation systems, the transportation network can be represented as dynamic flow network. One can then consider incomplete information games on graphs, where security and reliability driven failures are modeled by attacker-defender and nature-defender games, respectively. To characterize the equilibria of these games, recent advances in the areas of discrete algorithms and combinatorial optimization will be useful. This will enable the transportation network planners to find the critical links, and also enable us to evaluate various IT- and control-specific enforcement solutions.

References Cited

[1] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *Proceedings of the 20th USENIX conference on Security*, SEC'11, pages 6–6, Berkeley, CA, USA, 2011. USENIX Association.

[2] A. H. F. Chow, G. Gomes, A. A. Kurzhanskiy, and P. Varaiya. Aurora RNM — A Macroscopic Tool for Arterial Traffic Modeling and Control. *89th Annual Meeting of the Transportation Research Board, Washington, D.C., USA*, 2010.

[3] ns-2 Homepage. http://www.isi.edu/nsnam/.

[4] The DETER Testbed. http://www.isi.deterlab.net/.