Cyber-Physical Approaches for Designing Trustworthy Intelligent Transportation Systems

Sriram Chellappan - chellaps@mst.edu

I. Overview

Organizations across the world are heavily investing in Intelligent Transportation Systems (ITS) for many services including smarter vehicle routing, pollution minimization, accident avoidance infotainment etc. However, a critical aspect that will decide success of these services is how trustworthy ITS technologies turn out to be. Since many upcoming ITS service have significant economic, societal and technological impacts, attackers have increased incentives for compromising them. Unlike traditional communication networks, ITS are characterized by tight integration of Cyber and Physical components. The vulnerability set in ITS can hence be much higher. Also, an attack in one component can cascade into other components. For example, a cyber message that fakes superior route advertisements may increase vehicle congestion in the physical (road) component, which may cause drivers to aggressively communicate, hence increasing cyber congestion. A natural outcome of such challenges necessitates cyber-physical designs for trustworthy operation of ITS under attacks. What we argue is that - A technique may be designed by Cyber engineers, but their evaluation and deployment has to be executed by Transportation engineers, and ultimately utilized by Society. Unless solutions are designed by bridging stakeholders from the cyber and physical disciplines together, their practical deployment and utility will be impeded.

In this position paper, we introduce a vision for cohesive and integrated cyber-physical techniques for designing trustworthy ITS. Should this vision be feasible in practice, ensuing technologies will bridge disparities between Cyber and Transportation Engineers, hence providing a common platform to integrate them during ITS design, deployment and validation. The premise for this vision stems from answers to two questions: a). With decades on research in Transportation Engineering modeling physical (road) and social (driver) components, do they lend themselves for designing trustworthy ITS; b). If yes, is it feasible to integrate such theories with existing theories from Cyber components for designing solutions that effective, efficient and practically deployable. In this position paper we argue that the answer to the above questions is a "Yes". Specifically, we demonstrate a case for how existing theories in *Vehicle Flow* - specifically *Vehicle Platooning* can be integrated with machine learning and information theory to protect communicating vehicles against Sybil attacks, and preserving their Location Privacy. We also present some insights on the superiority of our approaches over current ones that are overtly cyber-centric. Finally, we present some open issues and avenues for future research in cyber-physical design for trustworthy ITS.

II. The Formation and Dispersion of Vehicle Platoons

In simple terms, a platoon is a group of vehicles traveling together in close proximity over a length of time. Ideally, consistent vehicle platooning is preferable and improves critical transportation parameters like signal optimization, congestion avoidance, improved road safety and capacity. Practically though, vehicle platooning under normal traffic is not long-term. Clearly, if all vehicles in an existing platoon maintain their speeds, a platoon never breaks up. However, due to physical factors like road friction, vehicle characteristics and signalling, along with human factors like car following pattern, lane changes and fatigue, there is inherent *randomness* in driver behavior, and platoons tend to disperse over time. Intuitively, longer the travel time between points, greater is the dispersion, since there is more time for drivers to deviate from current speeds. This phenomena is called *Platoon Dispersion*, a simple illustration of which is shown in Figure 1.

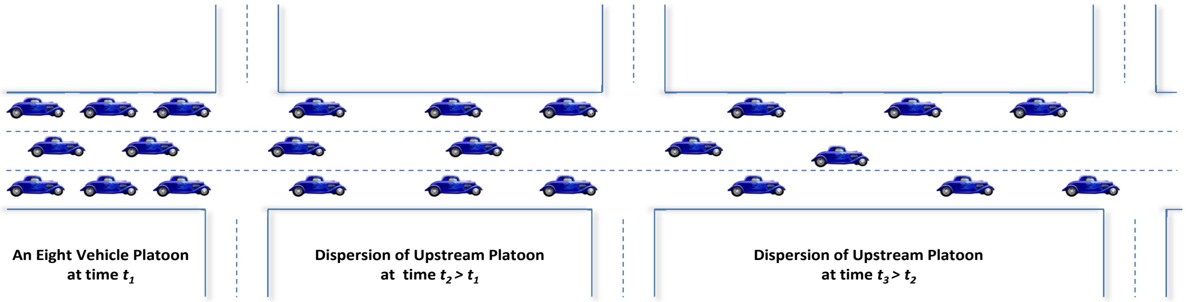
An Eight Vehicle Platoon at time t_1
Dispersion of Upstream Platoon at time $t_2 > t_1$
Dispersion of Upstream Platoon at time $t_3 > t_2$

Fig. 1. An Illustration of Platoon Dispersion

Platoon Dispersion has been well studied in transportation engineering via two mathematical models. One is the Pacey's normal distribution model [6], and the other is the Robertson's geometric distribution model [7]. Both models assume that travel times along a road segment fits some probability distributions. The Robertson platoon dispersion model, which is more widely adopted follows a shifted geometric series and takes a recursive mathematical formulation:

$$q'_t = F_n \cdot q_{t-T} + (1 - F_n) \cdot q'_{t-n}. \tag{1}$$

A numerical procedure was developed for the Robertson model in [8] by rewriting Equation 1 as,

$$q'_t = \sum_{i=T}^{\infty} F_n \cdot (1 - F_n)^{i-T} \cdot q_{t-i}. \tag{2}$$

where,
q'_t: arrival flow at the downstream location at time t (veh/hr);
q_t: departure flow at the upstream location at time t (veh/hr);
n: time step duration;
T: minimum travel time on the roadway;
$F_n = n\frac{\sqrt{n^2+4\sigma^2}-n}{2\sigma^2}$: smoothing factor governing dispersion;
σ: the standard deviation of link travel time.

III. Integrating Platoon Dispersion with Machine Learning and Information Theory for Designing Trustworthy ITS

A. Cyber-Physical Designs for Mitigating Sybil Attacks in ITS

A Sybil attack is one where an adversary assumes multiple identities to defeat trust of an existing reputation system. When Sybil attacks are launched in vehicular networks, an added challenge in detecting malicious nodes is mobility that makes it difficult to tie a node to the location of attacks. Existing approaches that detect Sybil attacks in vehicular networks are overtly Cyber-centric in that they either require additional hardware like directional antennas or RSSI measuring devices, or they employ complex cryptographic operations to securely tie a vehicle to a location. Naturally, the physical, communication and computational cost of existing techniques is quite high.

In [5], [1], we address the Sybil threat in ITS by designing techniques that integrate Clustering ideas (in the Cyber domain) with Platoon Dispersion theory (in the Physical domain). Our technique employs a number of road side units (RSUs) that periodically collect reports from communicating vehicles regarding their neighborhood. In the event of a Sybil node, clearly the geographic proximity of the node and all its Sybil identities will be long-term and repeating, while the geographical proximity of other benign nodes will not be long-term. To put it in terms of transportation engineering, Sybil identities will appear to platoon together, while identities of other benign nodes will eventually disperse. We subsequently design fuzzy time-series based clustering protocol to detect vehicles that *abnormally* cluster over time, where the degree of dispersion (captured as a notion of speed variance of vehicles from historic information) is a critical parameter to the clustering algorithm. To the best of our knowledge, these are the first works integrating a well established theory in transportation engineering for detecting cyber space attacks in vehicular networks. The resulting protocol is naturally simple, efficient and performs very well.

B. Cyber-Physical Designs for Providing Location Privacy in ITS

A critical component of emerging ITS is vehicles communicating wirelessly to realize a number of services. Unfortunately, the vision of vehicles communicating over the wireless medium will neve gain traction unless privacy guarantees are made. Needless to say, when a Vehicle V_x communicates to an external Location Based Server (LBS) periodically, it is entirely likely that the LBS tracks the trajectory of V_x and could use the information later with malicious intent. How to enable vehicular communication while also simultaneously providing location privacy is a major challenge today.

Broadly speaking, there are two classes of approaches in the literature currently to provide location privacy in ITS. The first one employs local communication and coordination among geographically close peer vehicles, wherein a particular node is chosen as a cluster-head to act as a proxy for other vehicles that wish to communicate. In combination with assigning temporally varying pseudonyms, and with new cluster-heads chosen periodically, a certain degree of confusion is present for an LBS that aims to track the messages and hence locations emanating from a particular vehicle. The downsides of this approach are increased communication overhead, constant need for refreshing pseudonyms, and the exposing of a vehicles location to its peers. The second approach to provide location privacy in ITS employs a trusted central server that acts as an intermediary between vehicles and the LBS. By collecting messages from several vehicles, the central server appropriately delays them before sending to the LBS in such a manner that when the LBS attempts to tie a message and location to a vehicle, multiple vehicles appear as candidate choices and hence there is confusion for the LBS. Given a sufficient amount of vehicles, the similarity of traces at a time are inherently indistinguishable and inherently protect the privacy of vehicles. Unfortunately, there is a non-trivial delay in service provisioning, and also the central server needs to be completely trusted.

We are currently investigating the degree of location privacy that is *inherent* in urban vehicular networks as a results of vehicle platoons and their dispersion. Recall from Figure 1 that while vehicles for platoons at intersections, they start dispersing eventually until they reach the next intersection at which newer platoons emerge. Clearly, there is randomness (and hence unpredictability) in how individual vehicles chooses it speed between intersection. We can hence envisage a simple protocol where vehicles send messages to an LBS only at intersections. In urban vehicular networks, distance between intersections are relatively short and density of vehicles tends to be high as well. As such, there are two sources of inherent confusion for an LBS attempting to track a vehicle - the first due to unpredictability in dispersion of platoons, and the second due to other peer vehicles. Our preliminary results are highly encouraging, and we are observing high quality of location privacy (computed as a means of Shannon Entropy) in realistic urban vehicular networks, with the Entropy increasing as a vehicle travels longer. Clearly, in this approach, there is absolutely no increase in communication overhead and there is also no need for any infrastructure support. Once again, we are not aware of platoon dispersion being used as a leverage to provide location privacy in ITS.

IV. Future Research Directions

There are a number of future research directions for cyber-physical designs for Trustworthy ITS.

- **Modeling trade-offs among multiple trust requirements:** We believe that there are some fundamental trade-offs between Integrity and Privacy in ITS. For instance, consider free flowing traffic. In such cases, dispersion among peer vehicles in quite high, which means that detecting a Sybil node (whose identities cluster) is faster and more accurate. But on the other hand, in free flow traffic, the diminishing degree of peer neighbors over space and time means that predictability of an individual vehicle's speed is more accurate, which means it is easier for an LBS to predict vehicle trajectories more accurately. To the best of our knowledge, such inherent trust trade-offs in the cyber domain in ITS are not identified before, especially from the perspective of existing vehicle flow theories in the physical domain.
- **Trustworthy Peer-to-Peer based Traffic Management System:** It is a fact that in the US, less than 1% of intersections are equipped with traffic lights. That is around $260,000$ out of $50,000,000$, and that is primarily because of the cost of deploying traffic lights. We are aware of some recent studies that attempt to design peer-to-peer based approaches for traffic management, where vehicles coordinate using cyber message exchanges to regulate traffic flow over intersections [10], [9]. Needless to say, trust becomes a critical component of such designs and services. There are a number of theories in transportation engineering that we believe can significantly improve traffic flow across intersections with fairness, safety and trust. We believe that such approaches need to deeply investigate and integrate models of car following (particularly those can model driver reaction time under upstream stoppages) [3], degree of platooning (to decide when vehicles from a lane start and stop moving through the intersection), and finally stability of platoons under dynamics [2] and how cyber communications and delays impact stability properties of the physical road network [4].

References

[1] N. Dutta and S. Chellappan. A time-series clustering approach for sybil attack detection in vehicular ad hoc networks. In *Proceedings of Intl. Conf. on Advances in Vehicular Systems, Technologies and Applications (Vehicular)*, Nice, June 2013.

[2] M. E. Khatir and E. J. Davison. Decentralized control of a large platoon of vehicles using non-identical controllers. In *American Control Conference, 2004. Proceedings of the 2004*, volume 3, pages 2769–2776. IEEE, 2004.

[3] H. Lenz, C. Wagner, and R. Sollacher. Multi-anticipative car-following model. *The European Physical Journal B-Condensed Matter and Complex Systems*, 7(2):331–335, 1999.

[4] X. Liu, A. Goldsmith, S. Mahal, and J. K. Hedrick. Effects of communication delay on string stability in vehicle platoons. In *Intelligent Transportation Systems, 2001. Proceedings. 2001 IEEE*, pages 625–630. IEEE, 2001.

[5] M. A. Mutaz, L. Malott, and S. Chellappan. Leveraging platoon dispersion for sybil detection in vehicular networks. In *Proceedings of IEEE Intl. Conf. on Privacy, Security and Trust (PST)*, Tarragona, July 2013.

[6] G. Pacey. The progress of a bunch of vehicles released from a traffic signal. *Research note No. Rn/2665/GMP. Road Research Laboratory, London*, 1956.

[7] D. Robertson. Transyt-a traffic network study tool. rrl report lr 253. *London: TRRL*, 1969.

[8] P. Seddon. Another look at platoon dispersion: 3. the recurrence relationship. *Traffic Engineering and Control*, 13(10):442–444, 1972.

[9] O. K. Tonguz. Biologically inspired solutions to fundamental transportation problems. *Communications Magazine, IEEE*, 49(11):106–115, 2011.

[10] W. Viriyasitavat and O. K. Tonguz. Priority management of emergency vehicles at intersections using self-organized traffic control. In *Vehicular Technology Conference (VTC Fall), 2012 IEEE*, pages 1–4. IEEE, 2012.

Bio

Sriram Chellappan is an Assistant Professor in the Dept. of Computer Science at Missouri University of Science and Technology-Rolla. His research interests are in Social Computing, Cyber Security and Cyber-Physical Systems. Sriram received the PhD Degree in Computer Science and Engineering from The Ohio-State University in December 2007. He received the NSF CAREER Award in 2013.