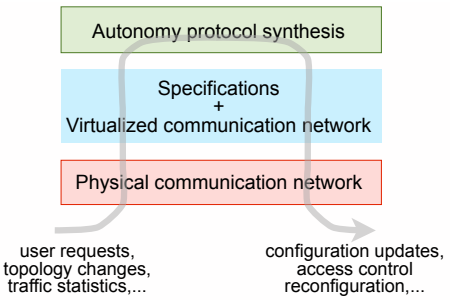
Position Paper
Synthesis of Provably Correct, Integrated Protocols for Autonomy and Networking

Ufuk Topcu and Jie Fu
University of Pennsylvania
December 4, 2013

A problem: Concepts based on onboard processing of data acquired through communication with the infrastructure and the other vehicles, and autonomous decision-making are often discussed for constructing safer, more reliable and efficient operation of transportation systems. Such a transition calls for new protocol-based controllers. These protocols will go beyond the traditional feedback loops in the sense that it needs to blend continuous decisions with discrete, logic-based, network-wide decisions. They will be built on layered architectures enabled by software running on unconventional platforms. The wide situational awareness required by these protocols is certainly beyond the local sensing and perception capabilities of any single vehicle. Moreover, it depends on the information flow patterns formed by each vehicle with the rest of the dynamic assets and infrastructure. That is, the underlying possibly dynamically evolving communication networks constrain the execution of these control protocols. On the flip side, in dynamic environments, the actions by the control protocols and other uncontrolled assets also affect and constrain the availability, bandwidth, and quality of the underlying communication networks and the resulting information flow patterns. Consequently, securely extracting and routing actionable information, and transforming this information into safe and trustworthy decisions are two inseparable capabilities which are desired.

Current state: Despite isolated progress in both autonomy and networking, neither side is equipped to serve the needs in the development of autonomous, connected vehicles/assets whose operation is heavily contingent on the information that is propagated and processed over networks. Indeed, we almost entirely lack suitable languages and tools to systematically reason about design questions at the interface of these two domains. One core reason is due to their differences in the models, specifications and primary design concerns. For example, autonomy protocols do not explicitly account for the utility of information or the quality of service specifications used in networking. Recent attempts toward incorporating communication constraints into control design focused either on very low-level control loops or on enterprise-level task assignments with a narrow set of specifications on the evolution of the underlying communication network. Furthermore, the diverse operating conditions put unconventional requirements on the control protocols for autonomy as well as networking. For example, the latter should be able to migrate the network from one configuration to another one without causing violation of mission, safety, or performance requirements. Our current limited set of tools are far from supporting such flexibility and run-time adaptation of network management controllers.

A potential approach: The method we envision should allow us to specify the relevant properties and constraints from both autonomy and networking. With respects to the specifications, it can automatically synthesize control protocols for both sides such that, when they are implemented together, their execution guarantees the correctness of the entire networked system. Such a development may leverage and extend a number of emerging concepts and opportunities in formal methods, controls, and networking. Recent advances in two-player, temporal-logic games provide algorithmic and efficient solutions for the synthesis of reactive, discrete strategies. These reactive strategies serve as



core building blocks both in autonomy and network management. They have already been utilized for formalizing and (partly) automating the construction of hierarchical autonomy protocol stacks from formal specifications in relatively rich languages, for example, temporal logic. Furthermore, trends toward software-defined networking and network virtualization introduce a separation between the network services and the physical hardware delivering these services, which makes it possible to update and reconfigure the networks through changes in/by software. With this separation between the control and data planes, analysis and design of controllers for network management is becoming increasingly amenable to formalization and specification languages used in autonomy protocols. Finally, note that the increased flexibility for updating the network services is indeed much needed in multi-vehicle/multi-asset environments with dynamically changing requirements and heterogenous sensing and communication capabilities for the vehicles and the infrastructure.

Preliminary results: Two-player, temporal logic games with incomplete information are suitable for modeling, symbolically simulating and analyzing systems in which the availability of information is constrained by the underlying communication networks. On the other hand, the effect of control actions may causes topology changes and reconfigurations of the network. In our preliminary work, the synthesis method for control protocols with partial observations has been developed. We envision this synthesis method can be accommodated to the protocol design with incomplete information caused by dynamical network. As an initial step, it is crucial to establish a formal model which correctly captures the behavior of the underlying communication network, the dependence between control protocols and the information flow pattern, and the effects of control execution on the availability of current and future information.