The primary goal of my research is to model and analyze user behavior in distributed information systems and control networks, with a focus on the users’ network of influences and interdependencies, and to develop tools for shaping autonomous and strategic users’ behavior, so as to enhance the network’s performance. I combine tools from several disciplines, including mathematical economics, control and optimization theory, and machine learning, to address problems in these areas.

Specifically, my main research interests are in network economics, game theory, economics of cyber-security, crowdsourcing, optimization, and data analytics. A rough breakdown of the main areas of my past and current research is as follows: (1) the study of public good provision on networks using optimization and graph theory, (2) information aggregation from distributed and strategic agents using crowdsourcing and peer-prediction methods, (3) designing incentive mechanisms for improving cyber-security, and (4) machine learning and large-scale data analytics for quantifying cyber security and predicting cyber incidents. I will briefly explain my contributions in each area, and conclude with a summary of ongoing and future research.

Public good provision games on networks: Networks of connections shape our social and economic interactions. In particular, they play a central role in the provision of public goods, where they determine the externalities and spill-overs of public goods among agents, and consequently, the level of public good provided through individual agents' private contributions.

In [8, 13], we have derived several fundamental results about the outcomes of agents’ interactions over networks when providing public goods. At the network level, we have found a necessary and sufficient condition under which the Nash equilibrium of the public good provision game exists and is unique, by using a parallel between these games and linear complementarity problems (LCP). This result extends previous known conditions; existing results in the literature can be recovered as special cases of our condition for uniqueness. At the node level, we show how an agent’s effort towards providing the public good can be determined by her position in the network, and specifically, by her centrality in the interaction graph. This finding can help us identify the most important agent(s) in the network to target in policy design.

This work is of importance for policy and network design in a wide range of applications, including the spread of research and innovation within an industry, security decisions of interdependent agents, propagation of shocks in financial markets, and emotional contagion over social networks.

Information aggregation from distributed and strategic agents: Crowdsourcing is the process of obtaining data/beliefs that are critical to a system’s operation from autonomous, distributed agents. Despite the versatility and potential benefits of crowdsourcing, there exist significant challenges including scenarios where (1) the crowd does not put in high effort, and (2) the crowd may give misleading information that changes the outcome to their benefit. My research has included work on both challenges.

In [1] I have worked on addressing the first challenge, using a combination of external verification and history dependent payments to elicit high effort. This work provides guidelines for operating a distributed and autonomous sensor network based on verification costs and accuracy requirements. In [4, 6], I have worked on the second problem of mitigating misleading or malicious input. We have proposed a new crowdsourcing mechanism for estimating the true qualities/types of agents interacting over a network, which elicits both self-assessments and cross-assessments from agents. We show that even without invoking monetary taxes/rewards, the elicitation of both self and cross assessments can improve estimates of the true underlying types, over using only cross-assessments.

Designing incentive mechanisms for improving cyber-security: The increasing number and cost of cyber-attacks over the past years call for incentive mechanisms and policy interventions that can motivate better security decisions by end-users and organizations. I have worked on the design of such incentive mechanisms, with a focus on capturing two key features of security: the interdependent nature of users’ security decisions, and its non-excludability. I have focused mainly on two applications: cyber-insurance contracts and security information sharing agreements. Specifically, we have shown that the design of cyber-insurance contracts is different from contract design for other types of risks, due to users’ risk interdependency. This is because in addition to risk transfer,
there is a profit opportunity for the insurer, created by the users’ security interdependency and the insurer’s ability to reduce the risk spillovers among his clients. I have also analyzed the implications of the non-excludable nature of security on the feasibility of using cyber-insurance as an incentive mechanism. My research in this area appears in [2, 5, 7, 9, 12].

I have also worked on the design of incentive mechanisms for voluntary disclosure in security information agreements in [10, 11]. We take a repeated game approach to these agreements, and propose the design of inter-temporal incentives, i.e., conditioning future cooperation on the history of past interactions.

**Machine learning and data analytics for cyber-security:** Our contribution is this area is to show that it is possible to quantify and predict the security risks of an entity, based on only externally collected, and often publicly available, data; see [3, 14, 15].

In particular, by training and testing a random forest classifier on externally observable data, we were able to predict cyber-incidents with a 90% true positive with 10% false positive rate [3]. In addition, in [14, 15] we showed that it is possible to use only publicly available data to predict the type of incident (such as hacking, error, malware, etc) that a given organization is most likely to experience. These fine-grained predictions leverage a wide array of data, making them more accurate than existing methods that focus on limited indicators such as business type alone.

**Ongoing and future research:** I am currently active in the following main directions of research. First, I am greatly interested in network economics, and the use of optimization theory in the study of games on networks. I am currently working on generalizing our existing work by expanding our model using techniques from non-linear optimization. A main theoretical contributions of this work will be establishing a unified framework for the study of network games and complementarity problems in optimization theory. A second direction is addressing the challenges that arise in a joint study of data aggregation and learning techniques, when there is a partial, yet not full alignment, between the agents and the system operator’s goals. This leads to questions such as how to effectively incorporate biased yet useful information through new or modified versions of existing learning techniques. I have recently started working on multi-agent reinforcement learning problems, in the presence of other strategic learners. This line of research will be at the intersection of machine learning, information economics, and stochastic control. Lastly, I am continuing my research on cyber-insurance contracts and markets from both theoretical and empirical perspectives, where I am currently focusing on the effects of correlated risks on policy and contract design.

**References**


