

CAREER: Collaborative Optimization with Limited Information Disclosure

Jaideep Vaidya, Rutgers University Management Science & Information Systems

With the rapid increase in computing, storage and networking resources, data is not only collected and stored but also analyzed. This creates a serious privacy problem which often inhibits the use of this data. In this proposal, we explore the problem of performing optimization analysis over distributed data without conflicting with privacy and security concerns. Optimization is a fundamental problem found in almost every aspect of real life. With resource constraints, optimization is necessary to ensure the best possible usage of scarce resources. Research in optimization methods has generated many successes; the ubiquitous collection of data opens even greater opportunities. Much of this data is constrained by privacy and security concerns, preventing the sharing and access to data needed to apply optimization techniques. This proposal tackles the challenge of developing privacy-preserving distributed optimization techniques. This is especially challenging due to the complexity and iterative nature of the solutions. An inherent aim is to also solve some of the fundamental problems underlying privacy-preserving analysis / secure computation and make it more accessible and applicable.

The proposed project will advance this state of the art by developing a suite of distributed privacy-preserving optimization techniques using secure computation tools and methodologies. In particular, we will develop privacy-preserving variants of several specific optimization techniques as well as more general solutions. This may involve finding new definitions that are more relaxed than the standard SMC definitions, yet still accurately model the real security concerns. This is a very challenging research task due to the subtle nature of security and security definitions. By integrating developed protocols into existing toolkits, we will foster real use of this technology. With the integrative education activities, we will foster actual use of the technology and open up its acceptance into the real world.

Intellectual Merit: The proposed research will advance the state of the art in methods and techniques for privacy-preserving distributed optimization, and improve our scientific understanding of secure computation. Some of the innovative expected results include: (1) novel formulations of security definitions that are more relaxed than the traditional definitions yet still model the real security concerns; (2) new algorithms, computational complexity results, and tools for specific widely used optimization problems; (3) a more generalized view of privacy; (4) game theoretic interpretations and modeling of the multi-party computation; and (5) result analysis – a quantification of privacy loss through results.

Significant further development and understanding of privacy may be necessary. The overall contribution in this area will have far reaching impact in terms of real effectiveness of the research developed. The PI believes the proposed research will result in significant contributions, both theoretical as well as practical, in enabling distributed optimization. Achieving the goals of this project requires a deep understanding of secure computation and data analysis, as well as a solid background in optimization methods. The PI has expertise and extensive experience in applying secure computation techniques to data mining analysis and is well situated in a operations research environment to perform the necessary research.

Broader impacts: Direct outcomes of the research will support the ability to efficiently perform optimization analysis over distributed data while protecting the privacy of individuals and establishments. This can significantly help in widening co-operation between organizations and prevent loss through data isolation. Overall, this would result in cost savings and new income realization potentially worth billions of dollars through joint resource usage. Successful translation of the research to real use has the potential to revolutionize the mediator/consolidator industry. The technology will also lead to a de facto “defense in depth” for networked systems, since the minimal disclosure of information automatically limits the possible ill effects of compromise. Broader impact will also result from a range of education and dissemination activities, including course development and student mentoring both at the undergraduate and graduate levels. The PI will also prepare lectures and tutorials to introduce the discovered concepts to a wider audience, in operations research as well as computer science, thus sparking a multidisciplinary effort. The emphasis on privacy will attract individuals who might otherwise view information systems as a threat, broadening participation in computer science research. Rutgers-Newark is especially well situated to attract such participation. The unique opportunity to collaborate with colleagues from the Business School and with industry through the Customer Relationship Management center at Rutgers will focus the project on relevant problems.