ANGELE HAMEL, Wilfrid Laurier University

A Generalized Anonymity Metric for Probabilistic Attacks

In theory, an anonymity network allows two participants, Alice and Bob, to communicate without an adversary being aware that the message Alice sends is the same one that Bob receives. However, in practice, a statistical attack on such a system is possible through observation of the patterns of sending and receiving. How anonymous is the communication really, and how can this anonymity be measured? In 2007 Edman et al. proposed a combinatorial model for this problem. In this talk we show how, by interpreting the problem in terms of contingency tables, we can define a new measure of the anonymity provided by the system. This measure generalizes two existing measures, and provides a new framework for future results. (Joint work with Jean-Charles Grégoire).