ΔΙΑΛΕΞΗ

" Reliable communication using minimal knowledge against powerful adversaries"

Αριστείδης Παγουρτζής
Αναπληρωτής Καθηγητής
Σχολή Ηλεκτρολόγων Μηχανικών και
Μηχανικών Υπολογιστών, ΕΜΠ

Περίληψη – Abstract

A fundamental communication primitive in distributed computing is Reliable Message Transmission (RMT), which refers to the task of correctly sending a message from a party to another, despite the presence of Byzantine corruptions. In this work we address the problem in the general adversary model of Hirt and Maurer, which subsumes earlier models such as the global or local threshold adversaries. Regarding the topology knowledge, we introduce and discuss the Partial Knowledge Model, which encompasses both the full knowledge and the ad hoc model; the latter assumes knowledge of the local neighborhood only.

Our main contributions are: (a) A necessary and sufficient condition for achieving RMT in the partial knowledge model with a general adversary, yielding a characterization of the minimal level of knowledge which renders the problem solvable for a given network and adversary structure. In order to show the sufficiency of the condition, we propose the RMT-Partial Knowledge Algorithm (RMT-PKA), an algorithm that solves RMT whenever the condition is met. This implies that RMT-PKA achieves reliable message transmission in every instance where this is possible, therefore it is a so called 'unique' protocol. To the best of our knowledge, this is the first unique protocol for RMT against general adversaries in the partial knowledge model. (b) A study of efficiency in the case of the ad hoc network model: we show that either the recently proposed Z-CPA protocol is fully polynomial or no unique fully polynomial protocol for RMT exists, thus introducing a new notion of uniqueness with respect to efficiency that we call 'poly-time uniqueness'.

To obtain our results we introduce, among others, a 'joint view' operation on adversary structures, allowing participants to combine their local knowledge in a sound manner, a new notion of separator (RMT-cut), appropriate for RMT in unreliable networks, and a self-reducibility property of the RMT problem, which we show by means of a protocol composition. The latter plays a crucial role in proving the poly-time uniqueness of Z-CPA.

Παρασκευή 15/12/2017 – 12:00
Αίθουσα Σεμιναρίων,
Κτίριο Μηχανικών Η/Υ & Πληροφορικής
Πανεπιστήμιο Ιωαννίνων