DOCTORAL CANDIDATE:	Hung Quoc Vo
DEGREE:	Philosophiae Doctor
FACULTY:	Det matematisk-naturvitenskapelige fakultet
DEPARTMENT:	Institutt for informatikk
AREA OF EXPERTISE:	Datanett
SUPERVISORS:	Amund Kvalbein, Olav Lysne, Paal Engelstad
DATE OF DISPUTATION:	14th of February 2014

DISSERTATION TITLE: *Permutation Based Routing for Increased Robustness in IP Networks*

The reliability of the Internet is an important factor to guarantee the quality of many online services of critical importance for business and individuals. However, the reliability is often threatened by frequent network failures due to a wide range of reasons such as networking component faults, operational errors, natural disasters, and malicious attacks. Unfortunately, most of the outages are sudden and hardly predicted in large networks. We propose a new routing protocol to increase the robustness of the Internet against the failures while requiring barely change of the current architecture of the Internet. Our method is theoretically proved to offer nearly optimal network protection against any random single failure and increased robustness under multiple fault conditions in the network.

IP networks are employing the Internet protocol suite and have evolved to be the backbone of the Internet. Due to the long history of its development, IP networks are complicated systems and therefore are reluctant to change although they now expose severe limitations in assuring the service availability to many modern Internet applications under failure situations. Our routing protocol is designed to work with the current Internet without any change, promising that the idea can be quickly deployable. However, our protocol can be easily extended to work with general interconnection networks.

The thesis work defines a new routing concept, proposes a mathematical model for the new routing protocol, followed by the design and the implementation of various algorithms to realize the model in specific types of IP networks. The evaluation results on ISP networks show that our protocol outperforms the current deployed methods in terms of network protection at the expenses of only small increases of path lengths and computational complexity.