A Measure and Design Method of Security Protocol *

Wang Tao, Guo Heqing, Yao Songtao
Computer Science and Engineering Department,
South China University of Technology
Guangzhou, Guangdong Province 510642, P.R. China
Email: filion@163.net **Tel.:** 0086-020-85285432

ABSTRACT

In this paper we introduce a method for security protocol measurement and redundancy measurement. We formally give the definition of protocol security property (goal) satisfaction measurement and discuss the relating factors of it. By this we give a method to measure the redundancy of the protocol and propose the method of reduction. We then give two application of the method both using reverse inference: analysis method of implicit assumptions and improper assumptions involved in modal logic based protocol analysis, protocol design and generation.

Keywords: security protocol; measure; redundancy; protocol generation; reverse inference;