Abstract

A large part of today's data exchange is done over the Internet and wireless networks are growing in importance. This makes it easy to make use of small handheld units, such as laptops and PDAs, to exchange data over the Internet. The sender may want to keep the transmitted data secret for a short or a long period, and the security requirements may vary for different data sets. This implies that it would be an advantage if the hosts could be able to decide how long time the data could be kept secret and point out which part of the data to encrypt, to save computer resources. There exist many ways to achieve these goals today. Weak and strong encryption algorithms give the ability to hold the data secure for a short or a long period, and situations where it is possible to point out certain parts of the data exists. In these solutions one has to decide which algorithm and which data parts to encrypt before establishing a connection between the hosts. In this thesis, we introduce the concept of dynamic encryption which offers variable levels of encryption during the session, and the ability to adapt this encryption level to performance and CPU resource availability constraints. A model to accomplish this concept is suggested and tested, and the results show that the dynamic concept could be implemented with a low overhead cost.