Abstract

Steganography is the process of hiding message in another cover medium such that it is difficult to detect. Cover medium is used as a carrier. this carrier can be Image, video, text or IP packet. Covert Channel is implemented in different header Fields of IPv4 header to send secret message. A covert channel is the medium that is used to transmit the information such as message, image or file. The fields flow label, traffic class and IPV6 source address of IPV6 header are selected as covert channel in this project. The more security in IPV6 header steganography can be achieved by applying cryptography i.e. Encryption. Public key algorithm i.e. RSA is selected for cryptography. Message is at first encrypted using RSA algorithm. The ciphertext is embedded in selected fields. Theses covert channels could be used for a Exploiting the Security rules so hidden Communication can be possible. this can be used for purpose such as pinching encryption key, login information or other secrets from in a way that should not easily detectable, but it could also be used for a good reason such as secret message can be passed under the watchful eyes of passive attacker. The demonstration of covert channel increases information security.
- Request for Comments: 6437 IPv6 Flow Label Specification
- Wojciech Mazurczyk, Miosz Smolarczyk, Retransmission steganography applied 2010 International Conference on Multimedia Information Networking and Security
- Miller, Steganography in IPv6 If Eva determine what Alice sent. Then all probabilities are 0 or 1

Index Terms

Computer Science
Communication Systems

Keywords
IPv6 Covert Channel Steganography