"Multi-path Based Avoidance Routing in Wireless Networks"

Title	"Multi-path Based Avoidance Routing in Wireless Networks"
Publication Type	Conference Paper
Year of Publication	2015
Authors	K. Sakai, M. T. Sun, W. S. Ku, J. Wu, T. H. Lai
Conference Name	2015 IEEE 35th International Conference on Distributed Computing Systems
Date Published	June
Publisher	IEEE
ISBN Number	978-1-4673-7214-5
Accession Number	15310480
Keywords	coding scheme, computer hardware, cryptographic protocols, data encryption, electronic messaging, encoding, Encryption, MPAR protocol, multipath channels, multipath message avoidance routing protocol, network coding, pubcrawl170102, radio networks, Routing, Routing protocols, secure communication, speedy advancement, wireless network

Abstract

The speedy advancement in computer hardware has caused data encryption to no longer be a 100% safe solution for secure communications. To battle with adversaries, a countermeasure is to avoid message routing through certain insecure areas, e.g., Malicious countries and nodes. To this end, avoidance routing has been proposed over the past few years. However, the existing avoidance protocols are single-path-based, which means that there must be a safe path such that no adversary is in the proximity of the whole path. This condition is difficult to satisfy. As a result, routing opportunities based on the existing avoidance schemes are limited. To tackle this issue, we propose an avoidance routing framework, namely Multi-Path Avoidance Routing (MPAR). In our approach, a source node first encodes a message into k different pieces, and each piece is sent via k different paths. The destination can assemble the original message easily, while an adversary cannot recover the original message unless she obtains all the pieces. We prove that the coding scheme achieves perfect secrecy against eavesdropping under the condition that an adversary has incomplete information regarding the message. The simulation results validate that the proposed MPAR protocol achieves its design goals.

URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7164955&isnumber=7164877

DOI 10.1109/ICDCS.2015.77

Citation Key 7164955

coding scheme computer hardware Cryptographic Protocols data encryption electronic messaging encoding encryption MPAR protocol multipath channels multipath message avoidance routing protocol network coding pubcrawl170102 radio networks Routing Routing protocols secure communication speedy advancement wireless network