# A Novel Method for Information Hiding in AODV

## The Case of Mobile Ad-hoc Networks

Mehrdad Khosravi
Shahed University
Tehran, Iran
mh.khosravi@shahed.ac.ir

Maryam Hasanzadeh
Shahed University
Tehran, Iran
hasanzadeh@shahed.ac.ir

Vahid Khodabakhshi
Sharif University of Technology
Tehran, Iran
vkhodabakhshi@ce.sharif.edu

*Abstract*—**Steganography is one of the most important fields of security which has attracted various research attempts recently. The goal of steganography is to hide the entire transmission process of hidden data. Steganography is done in various contexts including network protocols.**

**In this study, a new method for information hiding in AODV routing protocol is presented; which is intended to improve the level of security in the expanding area of wireless networks. We use ID field of RReq packet headers as a place for hiding information; RReq is one kind of routing control packets used in AODV. Regarding the fact that the steganography operations are solely managed in higher layers, in this method the traffics under steganography is not visible to higher layers. Simulation's results of implementing this method shows the good throughput of this method regarding performance and hiding capacity, comparing similar methods.**

***Keywords-Steganography; Information Hiding; Ad-hoc on demand distanse vector; Mobile Ad-hoc Networks;***

## I. INTRODUCTION

Security is one of the oldest challenges in communications. In the past, security concepts such as confidentiality, integrity and availability were provided mostly by mechanisms like cryptography. But today by communications in critical sites, new aspects of security is considered. In recent year's steganography has gained increasing importance, and have attracted lots of researchers' attention [1, 2].

Steganography is intended to hide any sort of secret communications between sender and receiver. The importance of covering secret communications is because of the fact that critical communication areas are more likely to be target of intrusions [3-5]. This concept for providing message security is alongside conventional methods like cryptography [1-3, 6].

In cryptography it is assumed that the intruder knowing the encrypted message attempts to reveal its contents. But in steganography the main goal is to hide all the hidden information traffic from the intruder in order to protect message security. In this research we intend to present a new method for information cryptography in context of network protocols [1, 6].

## II. RELATED WORKS

History of using steganography backs long ago, but in the context of network steganography has developed by emerging the new generation of network communications. It is one of interesting study fields for security researchers. In a general categorization in [4] studies on this field are categorized to 3 groups:

- **Steganography methods that modify packets:** These methods hide data mostly by changing available bits in different parts of packets, including main data, packet header or some combinations of these two. So they can send the intended information in a covered way based on the communication context.

- **Steganography methods that modify the structure of packet streams:** In these methods instead of changing packet contents, the hidden data is transmitted by changing traffic flows. Modifying inter-packet delay, making some special patterns in dropping packets, or making some changes in communication parameters are some examples of common methods in this category.

- **Hybrid Steganography methods:** Some methods are based on combination of last two methods, like the method presented in namely RSTEG. This method, besides changing contents of packet headers, also manipulates the traffic flow in order to send hidden data.

In this research a new method for steganography of data in wireless area networks is presented which uses AODV routing protocol. This method is placed in the third category, as a hybrid method. Here the first priority is to develop a new method for steganography in local area wireless networks and the next goal is to increase the hiding capacity of this method.

After reviewing research needs and motivations in section III, we introduce the proposed method in section IV. After that, in section V as simulations, we explain details and conditions of implementation of proposed method in OPNET network simulation environment.

At last the conclusion section is presented which discuss advantages and disadvantages of the presented method.