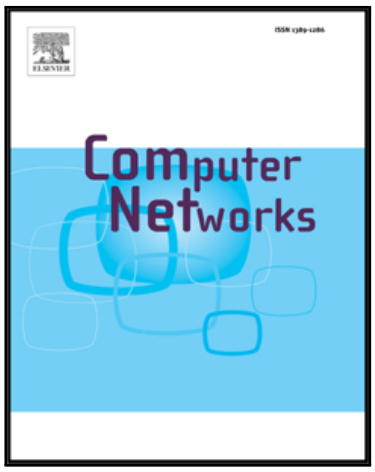

Analyzing, Quantifying, and Detecting the Blackhole attack in Infrastructure-less Networks

Christoforos Panos , Chirstoforos Ntantogian , Stefanos Malliaros , Christos Xenakis

PII: S1389-1286(16)30421-2
DOI: 10.1016/j.comnet.2016.12.006
Reference: COMPNW 6069

To appear in: *Computer Networks*

Received date: 3 January 2016
Revised date: 6 November 2016
Accepted date: 8 December 2016

Please cite this article as: Christoforos Panos , Chirstoforos Ntantogian , Stefanos Malliaros , Christos Xenakis , Analyzing, Quantifying, and Detecting the Blackhole attack in Infrastructure-less Networks, *Computer Networks* (2016), doi: 10.1016/j.comnet.2016.12.006

Analyzing, Quantifying, and Detecting the Blackhole attack in Infrastructure-less Networks

Christoforos Panos[1], *Chirstoforos Ntantogian*[2], *Stefanos Malliaros*[2], *Christos Xenakis*[2]

[1]*Department of Informatics & Telecommunications, University of Athens, Greece*

cpanos@di.uoa.gr

[2]*Department of Digital Systems, University of Piraeus, Greece*

{dadoyan, stefmal, xenakis}@unipi.gr

Abstract

The blackhole attack is one of the simplest yet effective attacks that target the AODV protocol. Blackhole attackers exploit AODV parameters in order to win route requests, and thus, attract traffic, which they subsequently capture and drop. However, the first part of the attack is often neglected in present literature, while the majority of attempts in detection focus only on the second part of the attack (i.e., packet drop). This paper provides a comprehensive analysis of the blackhole attack, focusing not only on the effects of the attack, but also on the exploitation of the route discovery process. As a result, a new critical attack parameter is identified (i.e., blackhole intensity), which quantifies the relation between AODV's sequence number parameter and the performance of blackhole attacks. In addition, a novel blackhole detection mechanism is also proposed. This mechanism utilizes a dynamic threshold cumulative sum (CUSUM) test in order to detect abrupt changes in the normal behavior of AODV's sequence number parameter. A key advantage of the proposed mechanism is its ability to accurately detect blackhole attacks with a minimal rate of false positives, even if the malicious node selectively drops packets.

Keywords: Blackhole attack, MANET, AODV, IDS, CUSUM.

1 Introduction

Infrastructure-less networks have gained considerable popularity due to the recent proliferation of mobile computing (i.e., smart phones, tablets, etc.). These networks comprise a wide range of networking paradigms such as mesh networks, mobile ad hoc networks (MANETs), vehicular ad hoc networks (VANETs), delay tolerant networks (DTN), opportunistic and sensor networks [1]. A common characteristic of these networks is the absence of any fixed architectural components such as routers, access points, etc., supporting and serving dynamic topologies and behaviors. To accommodate this characteristic, a variety of routing protocols have been proposed in the literature, however, the most widely adopted protocol is the ad hoc on demand distance vector (AODV) routing protocol [2]. AODV is a