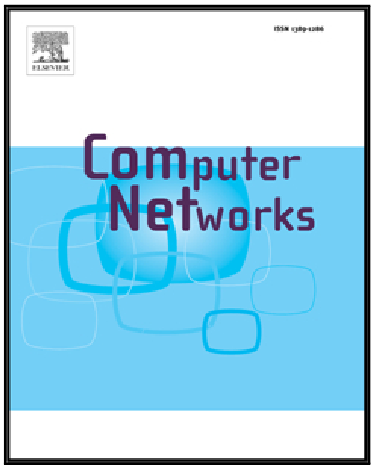
Accepted Manuscript



An Intelligent Cyber Security System Against DDoS Attacks in SIP Networks

Murat Semerci, Ali Taylan Cemgil, Bulent Sankur

PII: S1389-1286(18)30098-7
DOI: 10.1016/j.comnet.2018.02.025
Reference: COMPNW 6423

To appear in: *Computer Networks*

Received date: 26 September 2017
Revised date: 11 January 2018
Accepted date: 25 February 2018

Please cite this article as: Murat Semerci, Ali Taylan Cemgil, Bulent Sankur, An Intelligent Cyber Security System Against DDoS Attacks in SIP Networks, *Computer Networks* (2018), doi: 10.1016/j.comnet.2018.02.025

An Intelligent Cyber Security System Against DDoS Attacks in SIP Networks

Murat Semerci[a,*], Ali Taylan Cemgil[a], Bulent Sankur[b]

[a]*Department of Computer Engineering, Bogazici University, 34342, Bebek, Istanbul, Turkey*
[b]*Department of Electrical and Electronics Engineering, Bogazici University, 34342, Bebek, Istanbul, Turkey*

Abstract

Distributed Denial of Services (DDoS) attacks are among the most encountered cyber criminal activities in communication networks that can result in considerable financial and prestige losses for the corporations or governmental organizations. Therefore, autonomous detection of a DDoS attack and identification of its sources is essential for taking counter-measures. This study proposes an intelligent security system against DDoS attacks in communication networks that is composed of two components: A monitor for detection of DDoS attacks and a discriminator for detection of users in the system with malicious intents. A novel adaptive real time change-point model that tracks the changes in Mahalanobis distances between sampled feature vectors in the monitored system accounts for possible DDoS attacks. A clustering model that runs over the similarity scores of behavioral patterns between the users is used to segregate the malicious from the innocent. The proposed model is deployed over a simulated telephone network that uses a Session Initiation

*Corresponding author
Email address: murat.semerci@boun.edu.tr (Murat Semerci)