INTELLIGENT NETWORK SNIFFER USING DATA MINING

MITESH JAIN & ARUNA GAWADE

Department of Computer Engineering, Dwarkadas J. Sanghvi College of Engineering,
University of Mumbai, Mumbai, Maharashtra, India

ABSTRACT

A packet sniffer is a computer program or a piece of computer that can intercept and log traffic passing over a digital network or part of a network. The goal of a network sniffer is to detect malicious traffic over the network. The sniffer monitors all the incoming and outgoing traffic. However, the flaw with the traditional Intrusion Detection Systems (IDS) [1] is that they can’t detect the newly emerging cyber threats. In this paper, we propose a novel technique of an Intelligent Network Sniffer (INS) [1] using the data mining algorithms for measuring the deviation of malicious traffic from normal profile. We use the Iterative Dichotomizer-3 (ID3) [3] algorithm for this purpose.

KEYWORDS: Data Mining, Entropy, IDS, INS, IDS, Network Sniffing