

## **263. A STOCHASTIC APPROACH FOR MALWARE DETECTION IN MOBILE NETWORK**

Lakshmi S (lakshmis2401@gmail.com)

Hemalatha R (Assistant Professor) (hemesau\_03@yahoo.com)

Department of Computer Science & Engineering

St. Joseph's College of Engineering, OMR, Chennai.

Wireless mobile devices have turned out to be the integral part of all human communication. As a result, the computer malware is now drifting from computers to mobile phones. The problem of optimal distribution of the content-based signatures of malware helps to detect the corresponding malware and disable further propagation, in order to minimize the number of infected nodes. But in some cases, the malicious nodes may inject some dummy signatures targeting no malware into the network and induce denial-of-service attacks to the defence system. Enhancement of the system is done by developing an attack detection system that uses Multivariate Correlation Analysis (MCA) for accurate network traffic characterization by extracting the geometrical correlations between network and traffic features. MCA-based attack detection system employs the principle of anomaly-based detection in attack recognition. This makes the solution capable of detecting known and unknown attacks effectively by learning the patterns of legitimate network traffic only. Furthermore, a triangle-area-based technique is proposed to enhance and to speed up the process of MCA. The effectiveness of proposed detection system is evaluated, and the influences of both non-normalized data and normalized data on the performance of the proposed detection system are examined.

Index Terms- MCA, triangle area based, correlation, traffic features.

*Journal of Science and Innovative Engineering & Technology*