

## International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology



ISSN 2320-088X

International Conference on Mobility in Computing- ICMiC13, Organized by Mar Baselios College of Engineering and Technology during December 17-18, 2013 at Trivandrum, Kerala, India, pg.166 – 172

### **SURVEY ARTICLE**

# Feasibility of Machine Learning Techniques to Reduce False Alarm in Intrusion Detection

Anne Dickson, Ciza Thomas

Dept. of Electronics & Communication Engineering, College of Engineering, Trivandrum , Kerala, India  
ansalins2010@gmail.com, ciza\_thomas@yahoo.com

---

*Abstract- The sophisticated recent advances in networking increased the dependability of humans in Network technology everyday life. Now-a-days the number of attacks on networks got increased drastically. With the development of large open networks, security threats have increased significantly in the past two decades. So mitigating those attacks is one of the significant interests of researchers in the network security. The goal of an intrusion detection system is to provide a wall of defence to confront the attacks of computer systems on internet. Machine Learning algorithms have been successfully applied to intrusion detection; however the true positive and false positive trade-offs is always a major challenge in the choice of the algorithms. This paper explores the wide variety of machine learning algorithms focusing on the feasibility of these algorithms for the purpose of reducing false positives.*

*Keywords- : Artificial Neural Network; Adaptive Learner for Alert Classification; K Nearest Neighbour ; Data Mining; Genetic Algorithm; Particle Swarm Optimization; Multilayer Perception; Detection Rate; False Positive; Support Vector Machine .*

---

Full Text: <http://www.ijcsmc.com/docs/papers/ICMIC13/ICMIC13S19.pdf>