Abstract

The firewall ensures the protection of a network by falling on some number of defined rules set by the administrator of the computer network. Managing these rules to be optimum without errors is very difficult and sometimes leads to the formation of anomalies such as redundant, correlation, and shadowing rules. This defined problem has received the attention of both the academic and industry players in finding a pragmatic solution. A lot of reasonable attempts has been made by researchers of which many resorted to the automation of the firewall rule management process. The automation is to aid determine and resolve the conflicting rules and also to reduce the load that will be on the network administrator, which almost always leads to the creation of contradictory rules. The existing literature has not focused much on the amount of time it takes to determine and resolve these anomalies. Most of the conflicting rules are as a result of the wrongful position a rule may occupy in the rule list. The research proposes a contextual design of an improved firewall framework, that rest on the heuristic approach of the Particle Swarm Optimization (PSO) Algorithm to determine and assign the best position
to a rule and thereby improving the search and resolution of identified anomalies in a firewall rules list. Three (3) lightweight algorithms are designed for anomaly detection and resolution using PSO as the backbone.

References

10. Sethuram, J., and Sankareeswari, G. “Redundancy Management a nd Anomaly Detection o n Firewall Ruleset u sing Fame”, in International Journal of Science Technology & Engineering, Volume 1, Issue 10, April 2015. ISSN(online): 2349-784X.

Index Terms

Computer Science       Algorithms

Keywords

Firewall rule management, Network Security, Particle Swarm Optimization Algorithm