N.T. Nguyen et al. (Eds.): ACIIDS 2017, Part II, LNAI 10192, pp. 14–22, 2017.

A Fuzzy Logic Based Network Intrusion Detection System for Predicting the TCP SYN Flooding Attack

Nenekazi Nokuthala Penelope Mkuzangwe
Fulufhelo Vincent Nelwamondo

Abstract. Fuzzy logic is one of the powerful tools for reasoning under uncertainty and since uncertainty is an intrinsic characteristic of intrusion analysis, Fuzzy logic is therefore an appropriate tool to use to analyse intrusions in a Network. This paper presents a fuzzy logic based network intrusion detection system to predict neptune which is a type of a Transmission Control Protocol Synchronized (TCP SYN) flooding attack. The performance of the proposed fuzzy logic based system is compared to that of a decision tree which is one of the well-known machine learning techniques. The results indicate that the performance difference, in terms of predicting the proportion of attacks in the data, of the proposed system with respect to the decision tree is negligible.