Adaptive Network Intrusion Detection and Mitigation Model using Clustering and bayesian Algorithm in a Dynamic Environment

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 181
Number 20

Year of Publication: 2018

Authors:
Musyimi S. Muthama, Waweru Mwangi, Otieno Calvin

Abstract

Today, there is a serious challenge facing Network Security, especially Networking Intrusion Detection and prevention attacks of Denial of Service. Denial of Service (DoS) has the most devastating effects on Networking and Information security. It has also put tremendous pressure over the security experts lately, in bringing out effective defense solutions. The adversary methods are ever changing day night, the complexity and sophistication of attacks and vulnerability methods continue to rise yearly, and the potential impact to the bottom line is significant organization information systems. These attacks could be implemented diversely with a variety of tools and techniques. Since there is no single solution for DoS, this attack has managed to prevail on internet for nearly a decade. The task of uncovering previous unseen DOS attacks and new attacks in dynamic Intranet networks quickly becomes unmanageable. Network Intrusion Detection Systems (NIDS) have become a necessity in information security model because of the increase DOS and malicious activities. Therefore, the research proposes a Data mining technique enhanced with Artificial intelligent that is classification, clustering, and Behavior profiling networks algorithm to categorize a network process as either normal or
abnormal. Prevention of DOS attacks using techniques as Quarantine IP address, Blackholing, Sinkholing. The proposed model Adaptive Network Intrusion Detection Model (ANIDM) based on the combination of techniques artificial intelligent and anomaly detection. Which is self-learning and adaptive in presence of DOS attacks and malicious activities under minimal human intervention. The proposed model is based on clustering and classification through K-NN algorithm. The results show that these mitigation approaches improve the ability to separate between unknown abnormalities in the dataset and the legitimate traffic structure. The ANIDM can effectively detects existing and new attacks focusing on Denial of service attack (DOS), while providing continuous service even under attacks. The model is based on speed, crypt-isolation, log-audit and preemptively restored on a regular basis. The model can be applied to Dynamic environment learning institution and business enterprise. Finding the primary challenges to Network intrusion detection are the problem of misjudgment, previous unseen attacks, overwhelming volume of false alarms, misdetection, new attacks tactics. Therefore, the paper concludes that variation ANIDM can be considered for detection and mitigate of DoS and DDOS attacks.

References


**Index Terms**

Computer Science  
Security

**Keywords**

Network Security Smurf, Neptune, Ping-Of-Death (POD), ICMP, Back, LAND (Local Area Network Denial &KDD Cup 99 Dataset, Dedicate to my family and all A.I, Datamining, Hackathons and knowledge discovery all of me for all of us.