ABSTRACT

Distributed Denial of Service (DDOS) attacks are the major concern for security in the collaborative networks. Although non DDOS attacks are also make the network performances poor, the effect of DDOS attacks is severe. In DDOS attacks, flooding of the particular node as victim and jam it with massive traffic happens and the complete network performance is affected. In this paper, a novel Intrusion Detection and Prevention System is designed which detects the flooding DDOS attacks based on Firecol and prevents the attacks based on Dynamic Growing Self Organizing Tree (DGSOT) for collaborative networks. Simulation results in NS2 shows that DGSOT with Firecol (Firegroup) produces better intrusion detection and prevention system. Performance metrics based on the parameters delay, throughput, average path length, packet data ratio and energy conservation are better in Firegroup than the traditional Firecol system.

Keywords: Collaborative Networks, DDOS, Firegroup, Flooding, IDPS, Network Security

DOI: 10.4018/IJISP.2014040101
INTRODUCTION

A Collaborative network consists of various autonomous, heterogeneous and distributed entities with collaborative approach to achieve common goals and the interactions are supported by the computer network architecture. Lot of emphasis is being given related to security in the collaborative networks and the recent research in this domain highlights the various phenomena of the attack detection and prevention mechanisms. DDOS attacks and the defense mechanisms related to the classification are studied (Douligeris C & Mitrokotsa, A, 2003). The structural approach to the problem and the important features of each and every attack in the network with the described pros and cons are presented. DOS attacks on the web services, the vulnerability and inadequate defense mechanism with robustness is explained in (Zhijun Wu & Zhifeng Chen, 2006). Scalable mechanism of Distributed Denial of Service and the associated network architecture which address the problem of attack is presented with legitimate data sending procedures and their reception criteria (Wang, Fei, et al., 2012). The design decisions and their potential for denial of service attacks in the internet is studied. The state of art methods for defending the attacks, compare the counter measures are also discussed (Awad, M et al., 2004). The routing stability of the internet and the observed route changes over link metric and the analysis based on Principal Component Analysis (PCA) are reviewed as literature (Peng et al., 2007). The new direction in the routing stability measurement and the routing system performance are represented in the model. Network of compromised machines and their nodes controlled by attackers are dealt in Bot-nets which used peer to peer connectivity for remote control mechanisms. Also, the communication channel disruption and the mitigation possibilities are also explored (Yu Chen & Kai Hwang, 2006). A General Intrusion Detection Architecture Enhancing Trust Based Approaches is presented for the mobile adhoc networks. Examination of different intrusion detection systems and the adapted architecture for IDS are explained (Shui Yu & Wanlei Zhou, 2008). With respect to internet routing stability, a number of explanations for the anomalies and the evaluation of their potential impact on the Internet infrastructure is also analyzed (Holz, Thorsten, et al., 2008). The End-to-End Routing behavior in the Internet and their sequential results in the simulation is studied with the routing stability and the routing system parameters (Albers, Patrick, et al., 2002). Various researches related to botnets which describe the possible attacks performed by botnet communication technologies are also explored (Labovitz, Craig, G et al., 1999). To explore the possible vulnerability in the wireless networks against the probable attack, the classification of counter measure selection approaches are carried out and comprehensive prevention mechanism to address DDOS flooding problem is estimated (Saman Taghavi...
Information Security Awareness at Saudi Arabians’ Organizations: An Information Technology Employee’s Perspective
www.igi-global.com/article/information-security-awareness-saudi-arabians/72723?camid=4v1a