Chapter 3
Building Recommender Systems for Network Intrusion Detection Using Intelligent Decision Technologies

Mrutyunjaya Panda  
Gandhi Institute for Technological Advancement (GITA), India

Manas Ranjan Patra  
Berhampur University, India

Sachidananda Dehuri  
Fakir Mohan University, India

ABSTRACT

This chapter presents an overview of the field of recommender systems and describes the current generation of recommendation methods with their limitations and possible extensions that can improve the capabilities of the recommendations made suitable for a wide range of applications. In recent years, machine learning algorithms have been considered to be an important part of the recommendation process to take intelligent decisions. The chapter will explore the application of such techniques in the field of network intrusion detection in order to examine the vulnerabilities of different recommendation techniques. Finally, the authors outline some of the major issues in building secure recommendation systems in identifying possible network intrusions.

INTRODUCTION

Recommendation systems produce a ranked list of items on which a user might be interested, in the context of choosing a current item. Recommendation systems are built for movies, books, communities, news, articles, electronic commerce and other information access systems. Users have come to trust the recommendation software to reduce the burden of navigating large information spaces and product catalogues. The preservation of this trust is important both for the users and site owners, and is dependent upon the perception of
the recommender systems as objectives, unbiased and accurate. However, because recommendation systems are dependent on external sources of information, such as user profiles, they are vulnerable to attack. If a system generates recommendations collaboratively that is by user-to-user comparison, hostile users can generate bogus profiles for the purpose of biasing the systems’ recommendations for or against certain products.

There are two main approaches to build a recommendation system—collaborative filtering and content based (Melville, Mooney & Nagarajan, 2002). Collaborative filtering computes similarity between two users based on their rating profile, and recommends items which are highly rated by similar users. However, quality of collaborative filtering suffers in case of sparse preference databases. Content based system on the other hand does not use any preference data and provides recommendation directly based on similarity of items. Similarity is computed based on item attributes using appropriate distance measures.

Some previous attempts at integrating collaborative filtering and content based approach include content boosted collaborative filtering (Melville, Mooney & Nagarajan, 2002), weighted, mixed, switching and feature combination of different types of recommender system (Bruke, 2002). But, none of them discuss about producing recommendation to a user without getting preferences. The authors conducted a pioneering study on the problem of the robustness of collaborative recommendations in (O’Mahoney, Silvestre & Hurley, 2004), where they use kNN-based collaborative filtering for vulnerability analysis. Lam and Riedl (2004) use some empirical studies of attacks against collaborative algorithms.

Intrusion detection is defined as the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions (Power, 2002). The need for effective intrusion detection mechanism for computer systems was recommended by Denning and Neumann (1985) in order to find reasons for intrusion detection within a secure computing framework. The first major work in the area of intrusion detection was discussed by Anderson (1985) with an insight to the fact that certain types of intrusions to the computer system security could be identified through a detailed analysis of information contained in the system’s audit trial. Three threats are identified by Anderson which could be: External Penetrations, as unauthorized users of the system; internal penetrations, as authorized system users who uses the system in an unauthorized manner; and finally Misfeasors, an authorized user who try to exploit their access privileges. But, it is Denning (1987), who proposed an intrusion detection model which is considered to be the fundamental core of most intrusion detection research in use today.

Approaches for intrusion detection can be broadly divided into two types: misuse detection and anomaly detection. In misuse detection system, all known types of attacks (intrusions) can be detected by looking into the predefined intrusion patterns in system audit traffic. In case of anomaly detection, the system first learns a normal activity profile and then flags all system events that do not match with the already established profile. The main advantage of the misuse detection is its capability for high detection rate with a difficulty in finding the new or unforeseen attacks. The advantage of anomaly detection lies in the ability to identify the novel (or unforeseen) attacks at the expense of high false positive rate.

In fact, intrusion detection is considered as a classification problem, namely, to identify the behaviour of the network traffic to fall either in normal or any one out of the four attack categories (i.e. Probing, Denial of Service, User to Root and Root to Local). Hence, the main motivation is to develop accurate classifiers that can effectively classify the intrusive behaviour than the normal one.

Despite number of approaches based on different soft computing paradigms have been proposed for intrusion detection, the possibilities of using the techniques are still considered to be under uti-
Related Content

Pattern Discovery as Event Association
[www.igi-global.com/chapter/pattern-discovery-event-association/56234?camid=4v1a](www.igi-global.com/chapter/pattern-discovery-event-association/56234?camid=4v1a)

Balance Modelling and Implementation of Flow Balance for Application in Air Traffic Management
[www.igi-global.com/chapter/balance-modelling-implementation-flow-balance/56215?camid=4v1a](www.igi-global.com/chapter/balance-modelling-implementation-flow-balance/56215?camid=4v1a)

On Localities of Knowledge Inconsistency
[www.igi-global.com/article/localities-knowledge-inconsistency/53163?camid=4v1a](www.igi-global.com/article/localities-knowledge-inconsistency/53163?camid=4v1a)

Granular Computing and Human-Centricity in Computational Intelligence
[www.igi-global.com/article/granular-computing-human-centricity-computational/49129?camid=4v1a](www.igi-global.com/article/granular-computing-human-centricity-computational/49129?camid=4v1a)