A Game-Theoretic Analysis of Adversarial Classification

ABSTRACT

Classification is one of the most used tools from machine learning. In its simplest instance, a classification algorithm trains a model from a set of labeled data samples of two different classes (class 0 and class 1) and then uses this model to predict the class of new data samples. Many classification algorithms (Support Vector Machines, Logistic Regression, Naive Bayes, etc.) were developed over the past decades and successfully used in applications ranging from computer vision to biology or marketing One of the most prominent applications of classification is security where a defender typically aims to classify a system's usage into normal/non-attack (class 0) or malicious/ attack (class 1).

EXISTING SYSTEM

In Existing System, Attack detection is usually approached as a classification problem. However, standard classification tools often perform poorly because an adaptive attacker can shape his attacks in response to the algorithm. This has led to the recent interest in developing methods for adversarial classification, but to the best of our knowledge, there have been very few prior studies that take into account the attacker's tradeoff between adapting to the classifier being used against him with his desire to maintain the efficacy of his attack.

DIS ADVANTAGES

- Apps are classified as malicious and not removed from the stores.
- The detection cost is the more for the attacker.

PROPOSED SYSTEM

In Proposed System, we model the interaction as a game between a defender who chooses a classifier to distinguish between attacks and normal behavior based on a set of observed features and an attacker who chooses his attack features (class 1 data). Normal behavior (class 0 data) is random and exogenous. The attacker's objective balances the benefit from attacks and the cost of being detected while the defender's objective balances the benefit of

correct attack detection and the cost of false alarm. We provide an efficient algorithm to compute all Nash equilibrium and a compact characterization of the possible forms of a Nash equilibrium that reveals intuitive messages on how to perform classification in the presence of an attacker.

ADVANTAGES

- It recognizes the inefficiency of deterministic classifiers in this context.
- Detecting an attacker using game models.

SYSTEM REQUIREMENTS

H/W System Configuration:-

Processor	-	Pentium –III
RAM	-	256 MB (min)
Hard Disk	-	20 GB
Key Board	-	Standard Windows Keyboard
Mouse	-	Two or Three Button Mouse
Monitor	-	SVGA

S/W System Configuration:-

Operating System	:	Windows95/98/2000/XP
Application Server	:	Tomcat5.0/6.X
Front End	:	HTML, Jsp
Scripts	:	JavaScript.
Server side Script	:	Java Server Pages.
Database	:	MySQL 5.0

Database Connectivity : JDBC