UNIVERSITY OF SCIENCE AND TECHNOLOGY

COLLEGE OF GRADUATE STUDIES AND ACADEMIC ADVANCEMENT

Faculty of Computer Science and Information Technology

A Thesis Submitted in Fulfillment of the Requirement for the

Degree of Master in Computer Science

Accuracy of Machine Learning Algorithms in Detecting DoS/DDoS Attacks Types

By:

Izzeldin M.B.Yusuf

Supervisor:

Prof. Dr. Noureldien Abdalrhman Noureldien

March 2016

Abstract

Today, computers are most useful if they are networked together to take some simple protection to reduce the risk of unauthorized access. Every year, corporations, governments, and other organizations spend billions of dollars on expenditures related to network security. The rates at which these organizations are expending funds seem to be increasing. The main purpose of this work is to find the detection accuracy of a set of selected machine learning algorithms in detecting different DoS attack class types.

Denial of service attack(DoS)’s main purpose is to degrade an application or computer system, or denial the legal user from accessing the resources, it can be accomplished in various ways ,this can be achieved by depleting various resources like CPU , memory, disk space, network bandwidth etc. Denial of service attack can be of many forms, SYN flooding, UDP flooding, ICMP flooding etc.

This work had been divided in two sections theoretical in which we discussed the matters of detection, prevention after a literature review of DoS attack, then in practical section we exam the detection accuracy of a set of selected machine learning algorithms in detecting different DoS attack class types. The algorithms are belonging to different supervised techniques, namely, PART, BayesNet, IBK, Logistic, J48, Random Committee and Input Mapped.

The experimental work is carried out using NSLKDD dataset and WEKA as a data mining tool. The results show that the best algorithm in detecting the Smurf attack is the Random Committee with an accuracy of 98.6161%, and the best algorithm in detecting The Neptune attack is the PART algorithm with an accuracy of 98.5539, and on the average PART algorithm is the best algorithm in detecting DoS attacks while Input Mapped algorithm is the worst.

المستخلص

تأتي اهمية وفائدة الحواسيب هذه الأيام عندما تكون مرتبطة ببعضها البعض مع زيادة نظم الحماية لتقليل مخاطر الوصول الغير مصرح به. يوميا تقوم الحكومات والهيئات بانفاق البلاين من الدولارات في مجال أمن الشبكات وهذا الانفاق في تزايد مستمر ممايدل علي أهمية أمن الشبكات في بيئة نظم المعلوات.الهدف الأساسي من هجوم اعاقة الخدمة هوتدمير التطبيقات ونظم تشغيل الحواسيب واعاقة وصول الخدمة الي المستخدم الشرعي،وهذا الامريتم بتعطيل موارد الحاسوب المختلفة مثل(وحدة المعالجة المركزية،الذاكرة.مساحة القرص الصلب،ومعدل تدفق البيانات في الشبكة وغيره).هجوم اعاقة الخدمة يأتي في صور متعددة منهاهجوم الاغراق حيث يقوم باغراق بعض البروتوكولات و والاجهزة وخاصةعند تعارف الاجهزة اثناء الارتباط الاولي وغيرها من الطرق المختلفة.

هذا العمل تم تقسيمه الي قسمين القسم النظري وقد تمثل في مناقشة مواضيع اكتشاف الهجوم بأنواعها المختلفة وكذلك طرق منع الهجوم وقد سبق ذلك بحث عام عن موضوع هجوم اعاقة الخدمة. في الجانب العملي قمنا بفحص كفائة مجموعة مختارة من خوارزميات تعلم الآلة في اكتشاف هجوم اعاقة الخدمة، و كل هذه الخوارزميات متعلقة بمحموعات ذات تقنيات مختلفة بالاسم مثل:
Part,ByesNet,ABK,Logistic,J48,RandomCommity,InputMap

في اكتشاف انواع مختلفة من هجوم اعاقة الخدمة مثل:

Smurf, Neptune, Teardrop, Land, Back.

وقد اجريت التجربة باستخدام قاعدة البيانات نيلسون وهي قاعدة بيانات معدة سلفا للأبحاث العلمية وبرنامج ويكاوهو عبارة عن سوفتوير معد من جامعة ويكاتو وقد تم استخدامها جميعا كأدوات لتنقية البيانات.

وقد أظهرت النتائج أن أفضل الخوارزميات لإكتشاف (Smurf)هي الخوارزمية (RandomCommity)

بكفائة تصل الي١٦١٦١. ٩٨% وNeptune هي الخوارزمية(PART)بكفائة تصل الي٥٥٥٣٩. ٩٨%

ولكن في المتوسط وجدنا ان الخوارزمية (PART) هي الأفضل في اكتشاف هجوم إعاقة الخدمة بينما الخوارزمية(

(Input Map هي الأسوأ

١-١Introduction .

The computer network security is a very big challenge in the network security and information security researchers community, because everyday a new type of attack will be discover and one of the famous and dangerous attack is DoS/DDoS Distributed denial-of-service attacks (DDoS) attacks consist of an overwhelming quantity of .packets being sent from multiple attack sites to a victim site

Distributed denial-of-service attacks are widely regarded as a major threat to the Internet. They have adversely affected service to individual machines, major Internet .[commerce sites, and even core Internet infrastructure services [1

Denial of Service (DoS) is the degradation or prevention of legitimate use of network. :DoS attacks that target resources can be grouped into three broad scenarios namely as

- Attacks targeting energy resources, specifically the power source(battery) of the service provider(In such these attacks a malicious node may be continuously send a bogus packet to a node with the intention of consuming the victim's battery and .preventing other nodes from communicating with it

- Those attacks aimed at targeting storage and processing resources (these attacks are .carried out mainly to target memory, storage space, or CPU of the service provider

- The third attack scenario targets bandwidth, where an attacker located between multiple communicating nodes wants to waste the network bandwidth and disrupt .connectivity

The first large-scale appearance of distributed denial-of-service (DDoS) attacks had .[occurred in mid-1999. [2

DDoS traffic is highly similar to legitimate traffic. The attack usually consists of legitimate packets, generated in high quantity. They blend completely with the small amount of legitimate client traffic, so no differentiation can be made on a packet-by-.[packet basis [3

DDoS traffic is distributed, attack streams are generated from numerous attack machines spread all over the Internet and converge only in the proximity of the victim. The detection system must control a large portion of the total attack to alleviate the denial-of-service effect on the victim. Single-point system located near the victim or a distributed system whose defense nodes cover a significant portion of the Internet [4].

1-2 Research Problem .

The main problem of this thesis is the detection of denial of serves attacks (DoS) .which is presently a very serious threat for the network security

Because of seriousness of the problem many defense mechanisms have been proposed to encounter the attack, but no studies have been performed for measuring the accuracy of machine learning algorithms in detecting of DoS attack types

1-3 Research Objective .

The Main Objective of this thesis is to measure the accuracy of different machine .learning algorithms in Detecting DoS/DDoS attacks Types

1-4 Research Scope .

This research is limited to the DoS attack types namely, Smurf, Neptune, Land, Teardrop and Back. And the tested machine learning algorithms are: Part, BayesNet, .IBK, Logistic, J48, RandomCommity and InputMappedClassifer

1-5 Research Limitations .

In this work the accuracy of machine learning algorithms is measure only in terms of corrected instances, but a more sophisticated accuracy measures may give a better .accurate results

1-6 Research Methodology .

:In this work we applied the experimental methodology as following steps

all experiments were performed using a laptop with windows7 ultimate operating -١ .system, Intel Atom tm Cpun2700 processor, and 1.00 GB

we use NLS-KDD which consists of only selected records from the complete KDD -٢ .data sets

The experiments was carried out using train+20percent for training and test-21 for -٣ testing

To test and evaluate the algorithms we use 10-fold cross validation to ensure that -٤ .algorithms will perform on unseen data

We use WEKA-3.6 as a data mining tool to select and evaluate accuracy of -٥ .algorithms

Lstly we get our results from the correctly and in correctly instances in the -٦ algorithms detections performance

.

1-7 Thesis Organization .

This thesis is organized in the follows, chapter two discusses the background and literature and literature review, chapter three focuses on DDoS/Dos detections techniques, chapter four discusses the preventions mechanisms for DDoS/DoS attacks .and vies a classification of DDoS/DoS prevention

Chapter five is dedicated for examining the performance of machine learning algorithm in detection of DDoS/DoS attack, chapter six provides conclusions and .recommendations for future work