Available online at www.sciencedirect.com

ScienceDirect

Procedia Engineering 174 (2017) 1309 – 1314

Procedia Engineering

www.elsevier.com/locate/procedia

13th Global Congress on Manufacturing and Management, GCMM 2016

DPI & DFI: a Malicious Behavior Detection Method Combining Deep Packet Inspection and Deep Flow Inspection

Yu-tong Guo[&], Yang Gao[&], Yan Wang*, Meng-yuan Qin, Yu-jie Pu, Zeng Wang, Dan-dan Liu, Xiang-jun Chen, Tian-feng Gao, Ting-ting Lv, Zhong-chuan Fu

Department of Computer Science and Technology, Harbin Institue of Technology, Harbin 150001, P.R. China

Abstract

A malicious behavior detection approach which combines both the DPI (Deep Packet Inspection) and DFI (Deep Flow Inspection) is proposed, namely DPI & DFI. For the DPI & DFI method an outlier data mining method is employed. The fine-grained DPI is suitable for plaintext traffic, while DFI is a complementary for encrypted or emerging traffic. The collaborative detection approach includes three phases: DPI detection, DFI detection & comparison, and feedback. In present work, the C4.5 data-mining decision tree is adopted as classifier. The KDD Cup'99 benchmark is used and representative attack categories such as Probing, DOS, R2L (Remote to User) and U2R (User to Root) are evaluated. In-depth analysis demonstrates that the U2R and R2L attack categories lead to lower detection rate, and in particular the attack types contribute most are put forward. In future work, some other types of classifiers suitable to R2L and U2R attack categories should be investigated.

Peer-review under responsibility of the organizing committee of the 13th Global Congress on Manufacturing and Management

Keywords: DPI; DFI; Probing; DOS; R2L; U2R

1. Introduction

The malicious behavior detection is of vital importance to internet security. The following attack categories such as Probing, DOS (Denial Of Service), R2L (Remote to User) and U2R (User to Root) remain a serious threat to internet. Malicious behavior detection is generally classified into two levels: packet level and flow level, for which DPI (Deep Packet Inspection) and DFI (Deep Flow Detection) are representatives. DPI is a fine-grained detection

& Authors contribute equally to this work and should be considered as co-first authors.
* Corresponding author. Tel.:13009871730, 15124585561
E-mail address: wang_yan@hit.edu.cn, 15124585561@163.com

approach, by resolving headers and sometimes the payload of protocols, the fingerprints of application-layer content of network packets are recognized. It is very suitable for unencrypted traffic and known protocols. However the low detection rate and high false positive made it unaffordable [1]. DFI is a coarse-grained approach aiming at macroscopic traffic behavior with a statistical or AI analysis, which is very effective for the encrypted traffic and unknown protocols [2]. In recent years, the fine-grained DPI is coupled with a coarse-grained flow level DFI analysis, and a classifier is employed to overcome the low detection rate of DPI [3]. In this paper, a malicious behavior detection method namely DPI & DFI is proposed, which combines the fine-grained DPI with a coarse-grained DFI, and an outlier data mining analysis is conducted to overcome the false positives of DPI. The proposed approach includes three phases: DPI detection, DFI detection & comparison, and a feedback. The efficacy of the proposed method and the underlying factors that cause false positive detections are investigated in great details.

2. The Proposed Method

2.1. Framework

The proposed DPI & DFI collaborative detection approach is depicted in Fig. 1. It includes three phases: Phase I DPI detection, phase II DFI detection & comparison, phase III feedback and DPI restarts.

Phase I. DPI detection.

In this phase, A fine-grained packet level inspection, e.g. DPI, is conducted. By resolving the protocol headers, fingerprints of application-layer content of network packets are recognized, e.g. the IP address, port number, the name of application protocol and etc. The DPI is effective for unencrypted traffic and known protocols. After that a result is accquired.

Phase II. DFI detection & Comparison.

DPI is not suitable for the encrypted traffic and unknown protocols, besides the high false-positive detection rate is unfordable. Accordingly, in this work it is coupled with a coarse-grained DFI engine and a data-mining analysis is employed. In this work, an outlier data mining method is adopted for deep flow inspection. The data-mining includes the following processes, e.g. mapping symbolic attributes to numeric attributes, dataset fragmentation, feature reduction, and data-mining, etc. In fact, the coarse-grained DFI and the data minging classifier are not only effective for encrypted traffic and unknown protocols, but also aiming at false-positive detections of DPI [4].

Phase III. Feedback

When an encrypted traffic and an unknown protocol is resolved, the detection result of DFI is the final result. Otherwise, a comparison is made for DFI and DPI deteciton. When the fingerprints of DFI detection is the same with that of the DPI, the final result is accauired. Otherwise, a false-positive sample is signaled and a feedback is forwarded to the Phase I and the DPI is restarted.

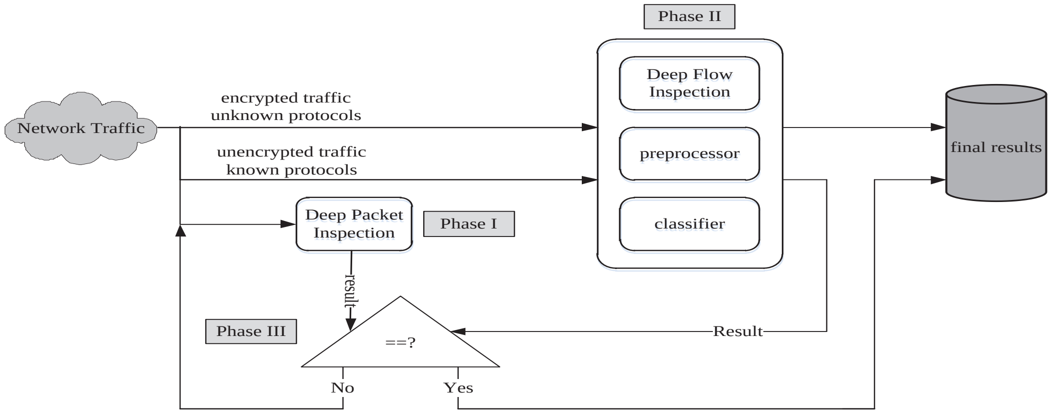

Fig. 1. The overall framework of DPI & DFI

2.2. Experimental Setup

Intrusion detection mainly focuses on four attack categories, including DOS (Denial Of Service), probing, U2R (User2Root) and R2L (Remote2Local) attacks. Owing to the nature of IDS, DoS attack category accounts for the major of the attacks. Denial of Service (Dos) is the primary attack category for which an attacker tries to prevent legitimate users from using a service. DOS includes the following attack types: apache, back, land, mailbomb, neptune, pod, processtable, smurf, teardrop, and udpstorm, etc.

Probing is one of the attack categories that an attacker tries to gain information about the target, typical attack types are ipsweep, mscan, nmap, portsweep, saint, and satan attack, etc.

R2L (Remote to Local) is the attack category that an attacker does not have an account of the victim, hence he tries to gain a privilege. The representative attack types include ftp_write, guess_password, imap, multihop, named, phf, sendmail, snmpgetattack, snmpguess, warezmaster, worm, xlock, xsnoop, and httptunnel etc.

U2R (User to Root) is the attack category that an attacker uses normal user account to gain a super-user privilege by taking the measures such as password sniffing, dictionary attacking, and social engineering etc. The typical attack types for U2R include: buffer_overflow, loadmodule, perl, rootkit, ps, sqlattack, and xterm etc.

KDD Cup '99 is adopted to evaluate the proposed method in this work. KDD Cup'99 is a representative benchmark in the field of intrusion detection system. There are altogether thirty-three attack types in KDD Cup'99. KDD has three kinds of datasets, e.g. "10% KDD", "Whole KDD" and "Corrected KDD". "Corrected KDD" dataset contains fourteen additional attack types with different distributions rather than the "10% KDD" and "Whole KDD" dataset [5].

In this work, the "10% KDD" dataset is adopted as training set, e.g. kddcup.data_10_percent.gz file, while "KDD Corrected" is used for testing set. The KDD Cup'99 data set includes a set of records of connections, while each connection consists of a set of packets flowing from a specific source IP to a target IP for a specified protocol in a short time interval. The training set and testing set are made up of both normal connections and attack connections. Normal connections are composed of various protocols such as TCP, UDP, ICMP and etc., besides different kinds of services should be included as well, e.g. FTP, Telnet, and etc. Different attack types are randomly synthesized into normal connection streams according to a probability. The detailed distribution of the training and testing set for four attack categories are described in Table.1.

Table 1. Distribution of Training Set and Testing Set.

Attack Types	Training Set (10%KDD)	Testing Set (corrected KDD)
Probe	4,107	4,166
DOS	391,458	229,853
U2R	52	228
R2L	1,126	16,189

2.3. Experimental Method

There are altogether forty-one features for the KDD Cup'99. The features are grouped into four categories: basic features, content features, time-based traffic features, and host-based traffic features. The name and corresponding number (#) for each feature is listed in Table.2.

The basic features are resolved by packet headers without the need of inspecting the content of the payload. In contrast, content features are acquired by inspecting the contents of payload in TCP packets, e.g. the number of failed login attempts, the knowledge of domain information and etc. Time-based traffic features describe the properties in a two second temporal window, e.g. the number of connections to the same host, etc. The Host-based traffic features are used to depict the attacks in an estimated window over the number of connections instead of in a time interval, e.g. in number of destination host services count. In present work, a preliminary feature reduction experiment is conducted and the features adopted are listed in Table.3.

Table 2. Description of Features of KDD CUP'99 Benchmark.

Categories	Name of Features (# of Features)
Basic Features	Duration(1), Protocol_type(2), Service(3), Flag(4), Src_bytes(5), Dst_bytes(6), Land(7), Wrong_fragment(8), Urgent(9)
Content Features	Hot(10), Num_failed_logins(11), Logged_in(12), Num_compromised(13), Root_shell(14), Su_attempted(15), Num_root(16), Num_file_creations(17), Num_shells(18), Num_access_files(19), Num_outbound_cmds(20), Is_hot_login(21), Is_guest_login(22)
Time Based Traffic Features	Count(23), Srv_count(24), error_rate(25), Srv_error_rate(26), Rerror_rate(27), Srv_rerror_rate(28), Same_srv_rate(29), Diff_srv_rate(30), Srv_diff_host_rate(31)
Host-Based Traffic Features	Dst_host_count(32), Dst_host_srv_count(33), Dst_host_same_srv_rate(34), Dst_host_diff_srv_rate(35), Dst_host_same_src_port_rate(36), Dst_host_srv_diff_host_rate(37), Dst_host_error_rate(38), Dst_host_srv_error_rate(39), Dst_host_rerror_rate(40), Dst_host_srv_rerror_rate(41)

Table 3. Features Selected

Classifier	Features Selected (#)
C4.5 Decision Tree	Duration (1), Protocol_type(2), Service(3), Src_bytes(4), Dst_bytes(5), Num_failed_logins(11), Logged_in(12), Root_shell(14), Num_root(16), Num_file_creations(17), Num_shells(18), Num_access_files(19), Num_outbound_cmds(20), Count(23), Serror_rate(25), Srv_rerror_rate(28), Same_srv_rate(29), Dest_host_srv_count(33), Dest_host_same_src_port_rate(36), Dest_host_rerror_rate(40)

In this work, the evaluation includes the following steps, including preprocessing, profiling, detection, threshold adjustment, and statistics. In the preprocessing step, the symbolic valued attributes of a feature are mapped into numeric valued attributes.

3. Evaluations

In this work, the C4.5 Decision tree classifier is adopted for deep flow inspection. Experimental result shows that with the DPI & DFI method the detection rate is improved, and false postive and detection failure rate is decreased. However, the overall detection rate is unaffordable with only 46% and 49% for DPI and DPI & DFI respectively. An in-depth analysis is made, and the experimental results are listed in Table.4. The detection rate of DPI & DFI reaches 72.1%, 92.4% for Probing and DOS catogories, while it is only of 3.5% and 6.5% for the U2R and R2L attack categories. This demonstrates that it is the U2R and R2L attack categories that lead to low detection rate.

The following factor contributes the reason. The DoS and Probe attack categories exhibit a continuous attributes of connections in a short time interval. R2L (Remote to Local) is the attack category that an attacker does not have an account of the victim and thus he tries to gain priority.

Table 4. Detection Efficacy of C4.5 Decision Tree

Attack Categories	Overall PPC (Percent of Correct Classification) (%)	False Positive (%)	Failure Rate (%)
Probe	72.1	18.89	9.01
DOS	92.4	0.86	6.74
U2R	3.5	85.74	10.77
R2L	6.48	73.09	20.43

Table 5. False Positive Analysis of R2L Attack Category (% of Scattered Attack Patterns)

Attack Type	Number of Connections (#)	Continues Patters (%)	Scattered Patterns (%)
ftp_write	11	-	-
guess_passwd	4420	25%	75%
imap	13	-	-
multihop	25	-	-
named	17	-	-
phf	6	-	-
sendmail	17	-	-
snmpgetattack	7741	32%	68%
snmpguess	2406	42%	58%
spy	2	-	-
warezclient	1020	50%	50%
warezmaster	1622	39%	61%
worm	2	-	-
xlock	9	-	-
xsnoop	4	-	-

The typical attack types of R2L include: ftp_write, guess_password, imap, multihop, named, phf, sendmail, snmpgetattack, snmpguess, warezmaster, worm, xlock, xsnoop, and httptunne. This means that the attacks R2L are intermingled into data packets of normal traffic flows. This makes its traffic exhibit a scattering pattern, thus the samples in both the training set and testing set manifest a deviating behavior which leads to a high false positive. As the U2R attack category is in a similar way with R2L, its explanation of R2L is omitted.

Taking the R2L attack category as an example, a breakdown of scattered attack pattern is illustrated in Table.5. In this work, the percent only accounts for the size of records greater than 1,000 connections. Analysis reveals that for R2L attack category the following attack types attributes most to false positives, including guess_passwd, snmpgetattack, snmpguess, warezclient, and warezmaster. The work shows that the outlier data mining classifier is not suitable for the R2L and U2R attack categories, and some other type of classifier should be investigated in our furture work[6][7].

4. Conclusions

In this paper, a malicious behavior detection approach combining DPI and DFI, namely DPI & DFI is investigated. The fine-grained DPI is suitable for plaintext traffic, while DFI is suitable for the encrypted and unknown traffic. In this work, an outlier data mining method is employed to overcome the false-positives of DPI. The collaborative detection approach includes three phases: Phase I DPI detection, phase II DFI detection & comparison, phase III feedback and DPI restarts. Experimental results show that the detection rate is improved and the false positive is reduced. An in-depth analysis is made, demonstrating that it is the U2R and R2L attack category that lead to load detection rate. Taking the R2L as an example, the following attack types contributes most, including guess_passwd, snmpgetattack, snmpguess, warezclient, and warezmaster. Some other type of classifier suitable to the U2R and R2L attack categories should be investigated in the future.

References

[1] Ntop.org. nDPI. http://www.ntop.org/products/deeppacket-inspection/ndpi/. 2015

[2] M Alsabah, K Bauer, I Goldberg. Enhancing Tor's performance using real-time traffic classification. ACM Conference on Computer & Communications Security, 2012:73-84.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.