POLITECNICO DI TORINO

Corso di Laurea in Ingegneria Informatica

Tesi di Laurea Magistrale

Sistemi anti-DDoS distribuiti

Relatore
prof. Guido Marchetto

Studente
Stefano Loscalzo
matricola: s267614

Supervisore aziendale
Centro Ricerche FIAT
dott. ing. Giovanni Giacosa

Anno accademico 2020-2021

Abstract

This short abstract, is typeset with the `abstract` environment (from the `report` document class) just to test if it works. or what concerns working, it works, but in Italian ist title turns out to be “Sommario” in bold face series and normal size; its apperance looks like a bad copy of what one obtains with the `\summary` command. In English, though, its title is “Abstract”, as it should be, since at the beginning of this template a suitable `\ExtendCapions` command was issued.

Please, read the documentation in Italian (file `toptesi-it.pdf` in order to fully understand the difference beteesn “abstract” and “summary” in the context of this bundle.

Abstract

Gli attacchi di denial of Service distribuiti (DDoS) sono uno dei maggiori problemi di sicurezza delle reti. Hanno lo scopo di impedire ad utenti legittimi l'accesso a dei servizi o degradare loro le prestazioni. In questa tesi proveremo a identificare anomalie riconducibili ad attacchi DDoS, in un contesto di una rete aziendale con più sedi, usando un riconoscimento delle anomalie effettuato tramite rete neurale allenata su dati provenienti dai router di più sedi aziendali e una successiva mitigazione degli attacchi tramite un agent sugli stessi.

Indice

Capitolo 1

Introduzione

1.1 Motivazione

Prova

1.2 Gli attacchi DDoS

Prova prova

1.2.1 Tipologia di attacchi DDoS

1.2.2 Vittime attacchi DDoS

1.2.3 Diffusione attacchi DDoS

1.3 Organizzazione della tesi

Capitolo 2

Riconoscimento anomalie

2.1 Motivazione

Prova

2.2 Reti neurali e funzionamento

Prova prova

2.2.1 Autoencoders

2.2.2 Modello della rete

2.3 Selezione features

2.3.1 Collectd

2.3.2 NDPI

2.4 Test sulle anomalie

2.4.1 Tool utilizzati

2.4.2 Risultati

Capitolo 3

Mitigazione degli attacchi

3.1 Introduzione

Prova

3.2 Funzionamento

Prova prova

3.2.1 eBPF

3.2.2 BCC

3.3 Test sulle anomalie

3.3.1 Tool utilizzati

3.3.2 Risultati

Capitolo 4

Lavoro futuro

Capitolo 5

Conclusioni

Capitolo 6

Stato dell'arte

6.1 Gli attacchi DDoS

Prova prova

6.2 I satelliti medicei

Prova prova

Capitolo 7

Il barometro

7.1 Generalità

Il barometro, come dice il nome, serve per misurare la pesantezza; più precisamente la pesantezza dell'aria riferita all'unità di superficie.

Studiando il fenomeno fisico si può concludere che in un dato punto grava il peso della colonna d'aria che lo sovrasta, e che tale colonna è tanto più grave quanto maggiore è la superficie della sua base; il rapporto fra il peso e la base della colonna si chiama pressione e si misura in once toscane al cubito quadrato, [2]; nel Ducato di Savoia la misura in once al piede quadrato è quasi uguale, perché colà usano un piede molto grande, che è simile al nostro cubito.

7.1.1 Forma del barometro

Il barometro consta di un tubo di vetro chiuso ad una estremità e ripieno di mercurio, capovolto su di un vaso anch'esso ripieno di mercurio; mediante un'asta graduata si può misurare la distanza fra il menisco del mercurio dentro il tubo e la superficie del mercurio dentro il vaso; tale distanza è normalmente di 10 pollici toscani, [2, 3], ma la misura può variare se si usano dei pollici diversi; è noto infatti che gl'huomini sogliono avere mani di diverse grandezze, talché anche li pollici non sono egualmente lunghi.

7.2 Del mercurio

Il mercurio è un a sostanza che si presenta come un liquido, ma ha il colore del metallo. Esso è pesantissimo, tanto che un bicchiere, che se fosse pieno d'acqua, sarebbe assai leggiero, quando invece fosse ripieno di mercurio, sarebbe tanto pesante che con entrambe le mani esso necessiterebbe di essere levato in suso.

Esso mercurio non trovasi in natura nello stato nel quale è d'uopo che sia per la costruzione dei barometri, almeno non trovasi così abbondante come sarebbe necessario.

Il Monte Amiata, che è locato nel territorio del Ducato[26] del nostro Eccellentissimo et Illustrissimo Signore Granduca di Toscana[27], è uno dei luoghi della terra dove può rinvenirsi in gran copia un sale rosso, che nomasi *cinabro*, dal quale con artifizi alchemici, si estrae il mercurio nella forma e nella consistenza che occorre per la costruzione del barometro terrestre.

La densità del mercurio è molto alta e varia con la temperatura come può desumersi dalla tabella 7.1.

Il mercurio gode della sorprendente qualità et proprietà, cioè che esso diventa tanto solido da potersene fare una testa di martello et infiggere chiodi aguzzi nel legname.

Temperatura °C	Densità t/m^3
0	13,8
10	13,6
50	13,5
100	13,3

Tabella 7.1. Densità del mercurio. Si può fare molto meglio usando il pacchetto booktabs.

Osservazione 1 Questa proprietà si manifesta quando esso è estremamente freddo, come quando lo si immerge nella salamoia di sale e ghiaccio che usano li maestri siciliani per confetionare li sorbetti, dei quali sono insuperabili artisti.

Per nostra fortuna, questo grande freddo, che necessita per la confetione de li sorbetti, molto raramente, se non mai, viene a formarsi nelle terre del Granduca Eccellentissimo, sicché non vi ha tema che il barometro di mercurio possa essere

[26] Naturalmente stiamo parlando del Granducato di Toscana.

[27] Cosimo IV de' Medici.

ruinato dal grande gelo e non indichi la pressione giusta, come invece deve sempre fare uno strumento di misura, quale è quello che è descritto costì.[4]

Conlusioni

E con questo si conclude la tesi d'esempio per una tesi magistrale con un capitolo non numerato che si trova ancora nella main matter.

Dovrebbe essere evidente che il comando `\chapter*` non dovrebbe mai essere usato nella main matter, tranne eventualmente un capitoletto conclusivo e riassuntivo *non strutturato*. Infatti se esso contenesse al suo interno paragrafi, sottoparagrafi e affini, questi verrebbero numerati erroneamente con il numero del capitolo precedente.

Il listato del pacchetto `topcoman.sty`

```
%%
%% This is file ‘topcoman.sty’,
%% generated with the docstrip utility.
%%
%% The original source files were:
%%
%% toptesi.dtx  (with options: ‘topcmn’)
%%   ------------------------------------------------------
%%   The TOPtesi bundle
%%   Copyright (C) 2015-2019 Claudio Beccari
%%   All rights reserved
%%
%%   License information appended
%%
\NeedsTeXFormat{LaTeX2e}[2018/01/01]
\ProvidesPackage{topcoman}[%
2019-07-26 v.6.3.06
Additional commands for the TOPtesi bundle]



\RequirePackage{iftex}
\ifPDFTeX
\newcommand*\DeclareSlantedCapitalGreekLetters{%
   \mathchardef\Gamma="7100
   \mathchardef\Delta="7101
   \mathchardef\Theta="7102
   \mathchardef\Lambda="7103
   \mathchardef\Xi="7104
   \mathchardef\Pi="7105
   \mathchardef\Sigma="7106
   \mathchardef\Upsilon="7107
   \mathchardef\Phi="7108
```

```
   \mathchardef\Psi="7109
   \mathchardef\Omega="710A
}\else
\newcommand*\DeclareSlantedCapitalGreekLetters{%
\PackageWarning{toptesi}{%
   When using LuaLaTeX or XeLaTeX specify\MessageBreak
   option math-style=ISO to package unicode-math\MessageBreak}
}
\fi
\providecommand*\ensuremath[1]{\ifmmode#1\else$#1$\fi}%
\providecommand*\textormath{}
\renewcommand*\textormath{\ifmmode\expandafter\@secondoftwo\else
    \expandafter\@firstoftwo\fi}
\providecommand*\textsubscript{\raisebox{-0.5ex}}

\ifPDFTeX
\@ifpackageloaded{textcomp}{}{\RequirePackage{textcomp}}
\fi
\providecommand{\ohm}{\textormath{\textohm}{\mathrm{\Omega}}}
\@ifpackageloaded{toptesi}{%
\providecommand\ped{}\providecommand\ap{}%
\renewcommand*{\ped}[1]{\textormath{\textsubscript{#1}}{_{\mathrm{#1}}}}%
\renewcommand*{\ap}[1]{\textormath{\textsuperscript{#1}}{^{\mathrm{#1}}}}}%
{\providecommand*{\ped}[1]{\textormath{\textsubscript{#1}}%
  {_{\mathrm{#1}}}}%
\providecommand*{\ap}[1]{\textormath{\textsuperscript{#1}}%
  {^{\mathrm{#1}}}}}
\@ifpackageloaded{siunitx}{\def\unit#1{\si{\,#1}}}%
  {\providecommand\unit{}%
   \renewcommand\unit[1]{\ensuremath{{\mathrm{\,#1}}}}%
  }
\providecommand{\gei}{\ensuremath{\mathop{\mathrm{\mathstrut j}\nolimits}}}
\providecommand{\eu}{\ensuremath{\mathop{\mathrm{e}}\nolimits}}
\providecommand{\micro}{\textormath{\textmu}{%
  \ifPDFTeX
    \ifdefined\muup\muup\else\mbox{\textmu}\fi
  \else
    \mathup{\mu}%
  \fi
}}
\providecommand{\gradi}{\textormath{\textdegree}{^\circ}}
\RequirePackage{fancyvrb}
\fvset{fontsize=\small}
\let\listing\VerbatimInput
\DeclareRobustCommand*{\fakeSC}[1]{%
{\dimen@=\f@size\p@\dimen@=0.75\dimen@
```

```
\fontsize{\dimen@}{\f@baselineskip}\selectfont
\expandafter{\uppercase{#1}}}}%
\ifPDFTeX\let\simulatedSC\fakeSC\else\let\simulatedSC\textsc\fi
\def\ft@figure{\iflanguage{italian}{\MakeLowercase{\figurename}}%
            {\figurename}~}
\def\ft@table{\iflanguage{italian}{\MakeLowercase{\tablename}}%
            {\tablename}~}
\newcommand*\EnableFigTabNames{%
            \let\p@figure\ft@figure\let\p@table\ft@table}
\newcommand*\DisableFigTabNames{%
            \let\p@figure\empty\let\p@table\empty}
\DisableFigTabNames
%%
%% Copyright 2005-2019 Claudio Beccari
%%
%% Distributable under the LaTeX Project Public License,
%% version 1.3c or higher (your choice). The latest version of
%% this license is at: http://www.latex-project.org/lppl.txt
%%
%% For important further details see the English or the Italian
%% documentation.
%%
%% This work is "author-maintained"
%%
%% This work consists of this file toptesi.dtx, a README file
%% the manifest.txt file, and the derived files:
%%     toptesi.cls,
%%     toptesi.sty,
%%     topfront.sty,
%%     topcommand.sty,
%%     toptesi-scudo.sty,
%%     toptesi.cfg,
%%     toptesi-monografia.sty,
%%     toptesi-sss.sty,
%%     toptesi-magistrale.sty,
%%     toptesi-dottorale.sty,
%% and the English documentation toptesi.pdf.
%%
%% Furthermore the bundle contains the documentation source
%% file toptesi-it.tex and the derived file
%% toptesi-it.pdf.
%%
%% The toptesi-example.tex source file is just an example
%% that shows how to use the various commands; by commenting
%% or uncommenting certain source lines it is possible to
%% typeset different kind of theses and their front pages.
```

```
%%
%% The topfront-example.tex source file is an example of how
%% to produce just the title page with TOPtesi and the external
%% package frontespizio.
%%
%% The toptesi-scudo-example.tex source file is an example
%% that shows the particular features available with TOPtesi,
%% when a doctoral thesis is produced for the Scuola di
%% Dottorato (ScuDo) of Politecnico di Torino.
%%
%% The toptesi.cfg file is a sample of a local configuration
%% file that can be copied to another file and its copy freely
%% edited and customised.
%%
%% The other toptesi-*.sty files are extension modules for
%% typesetting the specific thesis kinds described by the
%% suffix that replaces the asterisk.
%%
%% By running pdflatex on toptesi.dtx the user gets the class,
%% sty and cfg files and the English documentation file in
%% PDF format.
%%
%% The source file of the Italian documentation file
%% toptesi-it.pdf is another example of how to use TOPtesi.
%% This file toptesi-it.tex may be typeset with pdfLaTeX,
%% XeLaTeX, and LuaLateX; see the first comment lines of
%% the file for how-to information. In spite of being mainly
%% written in Italian, it contains several sections in English
%% for the benefit of foreign students attending the Doctoral
%% School of Turin.
%%
%% End of file ‘topcoman.sty’.
```

Seconda appendice

Questa è la seconda appendice numerata con una lettera perché questo comando `\chapter` viene dopo il comando `\appendix`.

Le appendici vanno numerate se sono più di una e devono quindi stare nella main matter, perché nella back matter nulla viene numerato.

La bibliografia che segue non è numerata perché l'ambiente `thebibliography` compone il suo titolo con il comando `\chapter*` e ne manda il titolo nell'indice generale con i suoi propri comandi interni. La definizione di questo ambiente è specifica di questo macro-pacchetto `TOPtesi`.

Sarebbe meglio inserire la bibliografia dopo un comando `\backmatter` esplicito. La back matter è destina espressamente a una sola appendice non numerata (ci pensa da sola a non numerare le sue sezioni); alla bibliografia, a uno o più indici analitici, a glossari o nomenclature, liste di acronimi, e simili. Nulla è obbligatorio in una back matter, ma una tesi senza bibliografia non sarebbe appropriata, tanto meno una tesi magistrale priva di una bibliografia.

Bibliografia

[1] G. Galilei, *Nuovi studii sugli astri medicei*, Manuzio, Venetia, 1612.

[2] E. Torricelli, in "La pressione barometrica", *Strumenti Moderni*, Il Porcellino, Firenze, 1606.

[3] E. Torricelli e A. Vasari, in "Delle misure", *Atti Nuovo Cimento*, vol. III, n. 2 (feb. 1607), p. 27–31.

[4] Duane J.T., *Learning Curve Approach To Reliability Monitoring*, IEEE Transactions on Aerospace, Vol. 2, pp. 563-566, 1994

[5] Chiesa S., *Affidabilità, sicurezza e manutenzione nel progetto dei sistemi*, CLUT, gennaio 2008

[6] Chiesa S., Fioriti M., Fusaro R., *On Board System Technological Level Improvement Effect on UAV MALE*

[7] Bigliano M., *Sicurezza nell'installazione di un velivolo senza pilota MALE; applicazione di metodologia di Zonal Safety Analysis al velivolo del Progetto SAvE*, Politecnico di Torino, maggio 2010

[8] Chiesa S., Di Meo G.A., Fioriti M., Medici G., Viola N., *ASTRID - Aircraft on board Systems sizing and TRade-off analysis in Initial Design*, Research Bulletin, Warsaw University of Technology, Institute of Aeronautics and Applied Mechanics, p. 1-28, 17-19, ottobre 2012