A

Project Report

On

SECURITY EVALUTION OF PATTERN CLASSIFIERS UNDER ATTACK

Submitted to

Department of
Computer Science and Engineering

By

ADUPA VARSHITHA	(206Y1A6701)
UPPULA PRAVALIKA	(216Y5A6704)
KATAKAM SHREEMAYI	(206Y1A6713)
KASARLA SADHASRI	(206Y1A6712)

Under the guidance

Of

Ms.V.PRANATHI
Asst.Professor

Department of Computer Science & Engineering

SUMATHI REDDY INSTITUTE OF TECHNOLOGY for WOMEN

(Approved by AICTE, New Delhi; Affiliated to JNTU, Hyderabad)

Ananthasagar(Vill), Hasanparthy(M), Warangal – 506 371 (A.P.), Website : www.sritw.org

2022-2023

S.R.I.T. FOR WOMEN * WARANGAL *

PRINCIPAL
Sumathi Reddy Institute of Technology for Women
Ananthasagar (V), Hasanparthy (M)
WARANGAL - 506 371 (T.S.)

SUMATHI REDDY INSTITUTE OF TECHNOLOGY for WOMEN

(Approved by AICTE, New Delhi; Affiliated to JNTU, Hyderabad)

Ananthasagar(Vill), Hasanparthy(M), Warangal – 506 371 (A.P.), Website : www.sritw.org

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the project entitled **"SECURITY EVALUTION OF PATTERN CLASSIFIERS UNDER ATTACK"** is submitted by ADUPA VARSHITHA(206Y1A6701), UPPULA PRAVALIKA(216Y5A6704), KATAKAM SHREEMAYI(206Y1A6713) and KASARLA SADHASRI(206Y1A6712) to the department of Computer Science and Engineering during academic year 2022-23.

Ms.V.PRANATHI
Project Guide

Dr.E.SUDARSHAN
Head of the Department

PRINCIPAL
Sumathi Reddy Institute of Technology for Women
Ananthasagar (V), Hasanparthy (M)
WARANGAL - 506 371 (T.S.)

R.I.T. FOR WOMEN * WARANGAL *

ABSTRACT

Networks are getting larger and more complex, yet administrators rely on rudimentary tools such as and to debug problems. We propose an automated and systematic approach for testing and debugging networks called "Automatic Test Packet Generation" (ATPG). ATPG reads router configurations and generates a device-independent model. The model is used to generate a minimum set of test packets to (minimally) exercise every link in the network or (maximally) exercise every rule in the network. Test packets are sent periodically, and detected failures trigger a separate mechanism to localize the fault. ATPG can detect both functional (e.g., incorrect firewall rule) and performance problems (e.g., congested queue). ATPG complements but goes beyond earlier work in static checking (which cannot detect liveness or performance faults) or fault localization (which only localize faults given liveness results). We describe our prototype ATPG implementation and results on two real-world data sets: Stanford University's backbone network and Internet2. We find that a small number of test packets suffice to test all rules in these networks: For example, 4000 packets can cover all rules in Stanford backbone network, while 54 are enough to cover all links. A sending 4000 test packet 10 times per second consumes less than 1% of link capacity. ATPG code and the datasets are publicly available.

Principal
Sumathi Reddy Institute of Technology for Women
Ananthasagar (V), Hasanparthy (M)
WARANGAL - 506 371 (TS)