



## **University of Bradford eThesis**

This thesis is hosted in [Bradford Scholars](#) – The University of Bradford Open Access repository. Visit the repository for full metadata or to contact the repository team



© University of Bradford. This work is licenced for reuse under a [Creative Commons Licence](#).

IMPROVED PERFORMANCE HIGH SPEED  
NETWORK INTRUSION DETECTION SYSTEMS (NIDS)

A high speed NIDS architectures to address limitations of  
Packet Loss and Low Detection Rate by adoption of  
Dynamic Cluster Architecture and Traffic Anomaly Filtration (IADF)

Monis Akhlaq

Submitted for the Degree  
of Doctor of Philosophy

School of Computing, Informatics and Media  
University of Bradford

2011

Dedicated to my beloved father, **Mr Akhlaq Ahmed**  
who was the major source of inspiration to me, I miss him a lot.....

# Acknowledgments

I pray and thank Almighty Allah for giving me the strength and the wisdom to complete this research, I have a firm belief that without His help this work would have not been completed.

First and foremost, I am indebted to my advisors, Mr John Mellor and Professor Irfan Ullah Awan, for the outstanding motivation, guidance, support, and knowledge that they have provided throughout the course of this work. They kindly took me into the Network Security Research Group and provided me with a great amount of freedom to work. Their confidence and trust on my abilities were the major motivating factors for this achievement.

I am also grateful to my research colleague Faeiz Alserhani for helping me throughout this long journey. His punctuality and capacity to attend the lab for long hours were the source of encouragement. His support to review my research papers and attend the presentation rehearsals cannot be forgotten. Collectively, we have made quite a few reputable publications and have also arranged conferences/ workshops.

My sincere thanks to my sponsors, National University of Sciences & Technology (NUST), Pakistan for giving me this opportunity to study abroad for this coveted qualification. My employers Pakistan Army also deserve recognition for allowing me to study abroad.

The major contributor in this achievement is my family - my lovely wife Erum, I thank you for your support and encouragement. I really appreciate your patience for accepting my absence for long hours, this must have spoiled some precious moments of our life. My naughty kids, Duaa, Manahil and Chiya also deserves pats on their back, they really supported me in this journey. I am sure my son Umar bin Monis must be celebrating these moments in his true home.

Last, but not the least I thank my parents, my mother in law, my family and friends back home in Pakistan. It has been their prayers, encouragement and support that enabled me to reach at this point.

# Abstract

Intrusion Detection Systems (IDS) are considered as a vital component in network security architecture. The system allows the administrator to detect unauthorized use of, or attack upon a computer, network or telecommunication infrastructure. There is no second thought on the necessity of these systems however; their performance remains a critical question.

This research has focussed on designing a high performance Network Intrusion Detection Systems (NIDS) model. The work begins with the evaluation of Snort, an open source NIDS considered as a de-facto IDS standard. The motive behind the evaluation strategy is to analyze the performance of Snort and ascertain the causes of limited performance. Design and implementation of high performance techniques are considered as the final objective of this research.

Snort has been evaluated on highly sophisticated test bench by employing evasive and avoidance strategies to simulate real-life normal and attack-like traffic. The test-methodology is based on the concept of stressing the system and degrading its performance in terms of its packet handling capacity. This has been achieved by normal traffic generation; fussing; traffic saturation; parallel dissimilar attacks; manipulation of background traffic, e.g. fragmentation, packet sequence disturbance and illegal packet insertion. The evaluation phase has lead us to two high performance designs, first distributed hardware architecture using cluster-based adoption and second cascaded phenomena of anomaly-based filtration and signature-based detection.

The first high performance mechanism is based on Dynamic Cluster adoption using refined policy routing and Comparator Logic. The design is a two tier mechanism where front end of the cluster is the load-balancer which distributes traffic on pre-defined policy routing ensuring maximum utilization of cluster resources. The traffic load sharing mechanism reduces the packet drop by exchanging state information between load-balancer and cluster nodes and implementing switchovers between nodes in case the traffic exceeds pre-defined threshold limit. Finally, the recovery evaluation concept using Comparator Logic also enhance the overall efficiency by recovering lost data in switchovers, the retrieved data is then analyzed by the recovery NIDS to identify any leftover threats.

Intelligent Anomaly Detection Filtration (IADF) using cascaded architecture of anomaly-based filtration and signature-based detection process is the second high performance design. The IADF design is used to preserve resources of NIDS by eliminating large portion of the traffic on well defined logics. In addition, the filtration concept augment the detection process by eliminating the part of malicious traffic which otherwise can go undetected by most of signature-based mechanisms. We have evaluated the mechanism to detect Denial of Service (DoS) and Probe attempts based by analyzing its performance on Defence Advanced Research Projects Agency (DARPA) dataset. The concept has also been supported by time-based normalized sampling mechanisms to incorporate normal traffic variations to reduce false alarms. Finally, we have observed that the IADF has augmented the overall detection process by reducing false alarms, increasing detection rate and incurring lesser data loss.

# Contents

|   |           |
|---|-----------|
| <b>Chapter 1: Introduction</b>                                | <b>1</b>  |
| 1.1 Motivation.....   | 1         |
| 1.2 Research Contribution.....                                | 3         |
| 1.2.1 Dynamic Cluster and Comparator Logic.....               | 5         |
| 1.2.2 Intelligent Anomaly Detection Filter (IADF).....        | 6         |
| 1.3 Thesis Outline.....                                       | 7         |
| 1.4 Publications.....   | 9         |
| <br>  |           |
| <b>Chapter 2: Network Intrusion Detection Systems</b>         | <b>12</b> |
| 2.1 Network Intrusion Detection – Historical Perspective..... | 12        |
| 2.2 Concept of Network Intrusion Detection.....               | 13        |
| 2.2.1 How an IDS Works?.....                                  | 14        |
| 2.2.2 NIDS Architecture.....                                  | 15        |
| 2.3 Types of Network Intrusion Detection Systems.....         | 16        |
| 2.3.1 Anomaly-based IDS.....                                  | 16        |
| 2.3.1.1 Protocol Anomaly.....                                 | 18        |
| 2.3.1.2 Application Payload Anomaly.....                      | 19        |
| 2.3.1.3 Statistical Anomaly.....                              | 19        |
| 2.3.2 Signature-based IDS.....                                | 19        |
| 2.4 NIDS Deployment Scenario.....                             | 21        |
| 2.4.1 NIDS with a Screening Router.....                       | 21        |
| 2.4.2 NIDS with a Firewalled Architecture.....                | 22        |
| 2.4.3 NIDS with Firewalled Network and DMZ.....               | 22        |
| 2.4.4 NIDS in Switched Network.....                           | 23        |
| 2.5 Characteristics of NIDS.....                              | 23        |
| 2.5.1 Scalability.....  | 24        |
| 2.5.2 Accuracy.....   | 25        |
| 2.5.3 Real-time Detection.....                                | 26        |
| 2.5.4 Versatility.....  | 26        |
| 2.5.5 Distributed Architecture.....                           | 27        |
| 2.6 Contemporary Open Source and Commercial NIDS.....         | 27        |
| 2.6.1 Snort.....  | 28        |

|       |                              |    |
|-------|------------------------------|----|
| 2.6.2 | Bro.....                     | 31 |
| 2.6.3 | Cisco IDS.....               | 33 |
| 2.6.4 | Astaro Security Gateway..... | 33 |
| 2.6.5 | Tipping Point 3Com.....      | 34 |
| 2.6.6 | Defense Pro-Radware.....     | 34 |
| 2.6.7 | McAfee-Intrushield.....      | 35 |
| 2.7   | Summary.....                 | 35 |

**Chapter 3: Performance Debate - Network Intrusion Detection Systems 38**

|         |   |    |
|---------|---|----|
| 3.1     | Network Speed.....  | 39 |
| 3.2     | Hardware Resources.....   | 40 |
| 3.3     | Sophistication in Evasion Techniques.....                         | 43 |
| 3.4     | Packet Capturing.....   | 44 |
| 3.5     | State Analysis.....   | 46 |
| 3.6     | Evaluation Strategy.....  | 47 |
| 3.7     | Generation of False Positives.....                                | 48 |
| 3.8     | Performance Crashed – Case Study of Denial of Service Attack..... | 49 |
| 3.8.1   | Denial of Service (DoS).....                                      | 49 |
| 3.8.2   | DoS Working Phenomena.....  | 51 |
| 3.8.3   | Impact of DoS – Resource Exhaustion.....                          | 52 |
| 3.8.3.1 | CPU Exhaustion.....   | 53 |
| 3.8.3.2 | Memory Exhaustion.....  | 54 |
| 3.8.3.3 | Bandwidth Exhaustion.....   | 55 |
| 3.9     | Summary.....  | 56 |

**Chapter 4 : Evaluating Performance of NIDS – Snort 58**

|       |                          |    |
|-------|--------------------------|----|
| 4.1   | Test-Bench I.....        | 61 |
| 4.1.1 | Traffic Generators.....  | 61 |
| 4.1.2 | Attacking Host.....      | 62 |
| 4.1.3 | IDS Machine (Snort)..... | 62 |
| 4.2   | Results.....             | 62 |
| 4.2.1 | Scenario Alpha.....      | 63 |
| 4.2.2 | Scenario Bravo.....      | 64 |
| 4.2.3 | Scenario Charlie.....    | 65 |



|                                     |  |           |
|-------------------------------------|--|-----------|
| 4.2.4                               | Scenario Delta.....                                      | 65        |
| 4.2.5                               | Scenario Echo.....                                       | 65        |
| 4.3                                 | Test-Bench II.....                                       | 66        |
| 4.3.1                               | Evaluation Methodology.....                              | 67        |
| 4.3.1.1                             | UDP Traffic.....   | 68        |
| 4.3.1.2                             | Mixed Traffic.....                                       | 68        |
| 4.4                                 | Results.....   | 69        |
| 4.4.1                               | UDP Traffic.....   | 69        |
| 4.4.1.1                             | UDP Traffic – 750 Mbps.....                              | 70        |
| 4.4.1.2                             | UDP Traffic – 1.0 Gbps.....                              | 70        |
| 4.4.1.3                             | UDP Traffic – 1.5 Gbps.....                              | 71        |
| 4.4.1.4                             | UDP Traffic – 2.0 Gbps.....                              | 71        |
| 4.4.2                               | Mixed Traffic.....                                       | 72        |
| 4.5                                 | Test-Bench III.....                                      | 72        |
| 4.5.1                               | Evaluation Methodology.....                              | 74        |
| 4.6                                 | Results.....   | 75        |
| 4.6.1                               | UDP Traffic.....   | 76        |
| 4.6.1.1                             | Snort Response for packet Sizes – 128 and 256 Bytes..... | 76        |
| 4.6.1.2                             | Snort Response for packet Sizes – 512 and 1024Bytes..... | 77        |
| 4.6.1.3                             | Snort Response for packet Sizes – 1460 Bytes.....        | 78        |
| 4.6.2                               | TCP Traffic.....   | 78        |
| 4.6.2.1                             | Snort Response for 50 Connections – 512 Bytes.....       | 79        |
| 4.6.2.2                             | Snort Response for 100/200 Connections – 512 Bytes.....  | 79        |
| 4.7                                 | Analysis.....  | 80        |
| 4.7.1                               | Test-Bench I.....  | 80        |
| 4.7.2                               | Test-Bench II.....                                       | 83        |
| 4.7.3                               | Test-Bench III.....                                      | 84        |
| 4.8                                 | Recommendations.....                                     | 86        |
| 4.8.1                               | Protocol Oriented Analysis.....                          | 86        |
| 4.8.2                               | Serialization Concept.....                               | 87        |
| 4.8.3                               | Dynamic Configuration.....                               | 88        |
| 4.9                                 | Summary.....   | 89        |
| <b>Chapter 5: Literature Review</b> |  | <b>91</b> |
| 5.1                                 | Dynamic Cluster and Comparator Logic.....                | 91        |

|   |   |            |
|---|---|------------|
| 5.2   | Intelligent Anomaly Detection and Filtration.....                   | 93         |
| 5.3   | Summary.....  | 96         |
| <b>Chapter 6: Dynamic Cluster and Comparator Logic</b>          |   | <b>99</b>  |
| 6.1   | Integrated System Architecture.....                                 | 99         |
| 6.1.1   | Cluster Overview.....   | 99         |
| 6.1.2   | Network load-balancer.....  | 101        |
| 6.1.3   | Plug Ins.....   | 103        |
| 6.2   | Test-Bench.....   | 104        |
| 6.3   | Results and Analysis.....   | 105        |
| 6.3.1   | Load-balancer CPU Usage.....  | 105        |
| 6.3.2   | MAC Translation – Response Time.....                                | 105        |
| 6.3.3   | Cluster nodes Performance on Variable Traffic load.....             | 107        |
| 6.3.4   | Comparison of IDS Performance – Single VS Cluster Architecture..... | 108        |
| 6.4   | Summary.....  | 111        |
| <b>Chapter 7 : Intelligent Anomaly Detection and Filtration</b> |   | <b>112</b> |
| 7.1   | Evaluation Parameter – DARPA Dataset.....                           | 114        |
| 7.2   | Intelligent Anomaly Detection filter (IADF).....                    | 117        |
| 7.2.1   | Process Flow.....   | 117        |
| 7.2.2   | IADF - Mechanism.....   | 118        |
| 7.2.2.1   | Normal Data Sample Generation.....                                  | 118        |
| 7.2.2.2   | Adaptive Threshold Generation.....                                  | 121        |
| 7.2.3   | IADF Architecture.....  | 125        |
| 7.3   | Test-Bench.....   | 129        |
| 7.4   | Training Data for Normalized Behaviour.....                         | 131        |
| 7.5   | Results and Analysis.....   | 132        |
| 7.5.1   | Verifying Threshold Adoption.....                                   | 132        |
| 7.5.2   | IDS (Snort) Performance without IADF Mechanism.....                 | 133        |
| 7.5.3   | IADF Implementation In Support to Snort.....                        | 134        |
| 7.6   | Summary.....  | 137        |
| <b>Chapter 8 : Conclusion and Future Work</b>                   |   | <b>138</b> |
| 8.1   | Conclusion.....   | 138        |

|       |  |            |
|-------|--|------------|
| 8.1.1 | Dynamic Cluster-based adoption for High Performance.....       | 139        |
| 8.1.2 | Intelligent Anomaly-based filtration for High Performance..... | 140        |
| 8.2   | Future Work.....   | 141        |
| 8.2.1 | High Performance NIDS Interface.....                           | 142        |
| 8.2.2 | Determine Hardware Scalability and Performance.....            | 142        |
| 8.2.3 | Amplify the scope of IADF.....                                 | 143        |
| 8.2.4 | Fusion of Filtration and Detection concepts.....               | 144        |
| 8.2.5 | Modern day Evasion Detection.....                              | 144        |
|       | <b><i>Bibliography</i></b> .....                               | <b>146</b> |
|       | <b><i>Acronyms</i></b> .....                                   | <b>156</b> |

# Figures

|      |  |    |
|------|--|----|
| 2.1  | Common NIDS Architecture.....  | 15 |
| 2.2  | Anomaly-based Detection Model of NIDS.....   | 17 |
| 2.3  | Signature-based Detection Model of NIDS.....   | 20 |
| 2.4  | Deployment Scenario - NIDS with Screening Router.....  | 21 |
| 2.5  | Deployment Scenario - NIDS with Firewalled Architecture.....   | 22 |
| 2.6  | Deployment Scenario - NIDS with Firewalled Network & DMZ.....  | 23 |
| 2.7  | Deployment Scenario - NIDS in Switched Network.....  | 24 |
| 2.8  | Snort Architecture.....  | 29 |
| 2.9  | Bro Architecture.....  | 31 |
| 3.1  | Alert Log – DDoS Attack on WikiLeaks.....  | 51 |
| 4.1  | Test-bench I – Performance Evaluation of Snort on mid range hardware.....                                      | 61 |
| 4.2  | Results – Scenario Alpha (Attacker on Host Linux 2.6 and Snort on Virtual Platform.....<br>built on Windows)   | 64 |
| 4.3  | Results – Scenario Bravo (Attacker on Host Linux 2.6 and Snort on Virtual Platform.....<br>built on Linux 2.6) | 64 |
| 4.4  | Results – Scenario Charlie (Attacker on Host Linux 2.6 and Snort on Host Platform.....<br>built on Windows)    | 65 |
| 4.5  | Results – Scenario Delta (Attacker on Host Linux 2.6 and Snort on Host Platform .....<br>built on Linux 2.6)   | 66 |
| 4.6  | Results – Scenario Echo (Attacker on Host Windows and Snort on Host Platform.....<br>built on Linux 2.6)       | 66 |
| 4.7  | Test-bench II – Performance Evaluation of Snort on high range Commodity.....<br>hardware (Host Configuration)  | 68 |
| 4.8  | Results: Packet Dropped, UDP Traffic – 750 Mbps.....   | 70 |
| 4.9  | Results: Packets Dropped, UDP Traffic – 1.0 Gbps.....  | 70 |
| 4.10 | Results: Packets Dropped, UDP Traffic – 1.5 Gbps.....  | 71 |
| 4.11 | Results: Packets Dropped, UDP Traffic – 2.0 Gbps.....  | 71 |

|      |  |     |
|------|--|-----|
| 4.12 | Test-bench III – Performance Evaluation of Snort on high range Commodity hardware (Virtual Configuration)..... | 73  |
| 4.13 | Snort Packets Received (%) - UDP Traffic (128 Bytes & 256 Bytes).....  | 76  |
| 4.14 | Snort Packets Received (%) - UDP Traffic (512 Bytes & 1024 Bytes).....   | 77  |
| 4.15 | Snort Packets Rx (%) - UDP (1460 Bytes) & TCP (50 Connections).....  | 78  |
| 4.16 | Snort Packets Received (%) - TCP Traffic (100 & 200 Connections).....  | 79  |
| 4.17 | <i>Test-bench I</i> - Analysis - Packets Dropped.....  | 81  |
| 4.18 | <i>Test-bench I</i> - Analysis - Alerts & Log (Success Rate) .....   | 82  |
| 4.19 | <i>Test-bench I</i> - Comparison - Snort on Linux & Win.....   | 83  |
| 4.20 | <i>Test-bench III</i> - Virtualization Concept.....  | 85  |
| 4.21 | <i>Test-bench III</i> - Statistics I/O System (SATA 300) Hard Drive.....                                       | 86  |
| 4.22 | <i>Recommendations</i> - Protocol Oriented Analysis.....   | 87  |
| 4.23 | <i>Recommendations</i> - Serialization Concept.....  | 88  |
| 6.1  | Dynamic Cluster Architecture.....  | 100 |
| 6.2  | Flow Chart – Policy-based loadbalancer.....  | 101 |
| 6.3  | Listing – Threshold Monitor Listing –CPU Usage Monitor.....  | 102 |
| 6.4  | Listing – Comparator Logic.....  | 103 |
| 6.5  | Test-bench – Dynamic Cluster-based adoption.....   | 104 |
| 6.6  | Results & Analysis - Loadbalancer – CPU Usage.....   | 106 |
| 6.7  | Results & Analysis - Response Time – MAC Translation.....  | 106 |
| 6.8  | Results & Analysis - CPU Usage – Variable injected load on cluster nodes.....                                  | 108 |
| 6.9  | Results & Analysis - CPU Usage – Equivalent load on cluster nodes.....   | 109 |
| 6.10 | Results & Analysis - NIDS Performance – Single Node.....   | 109 |
| 6.11 | Results & Analysis - Performance of Dynamic NIDS Cluster without Comparator Logic Connections.....             | 110 |
| 6.12 | Performance of Dynamic NIDS Cluster with Comparator Logic.....   | 111 |
| 7.1  | IADF - The Process Flow.....   | 118 |
| 7.2  | Normalized Sample Generation.....  | 120 |

|      |  |     |
|------|--|-----|
| 7.3  | Average variation in normal traffic in different times of the day describing variation.....<br>in network activity | 123 |
| 7.4  | Adaptive Threshold Generation during Linear Phase of Traffic Variation .....                                       | 124 |
| 7.5  | Adaptive Threshold Generation during Increasing Phase of Traffic Variation .....                                   | 124 |
| 7.6  | Adaptive Threshold Generation during Decreasing Phase of Traffic Variation .....                                   | 125 |
| 7.7  | IADF Implementation.....   | 126 |
| 7.8  | IADF Listing.....  | 129 |
| 7.9  | Test-bench - IADF Implementation and Evaluation.....   | 130 |
| 7.10 | Results - Random injection of attack DoS traffic to analyse the performance.....                                   | 132 |
| 7.11 | Results - IDS (Snort) Performance without IADF Implementation.....   | 134 |
| 7.12 | Alert and IADF Matcher.....  | 135 |
| 7.13 | Results - System Performance with IADF Implementation.....   | 135 |

# Tables

|     |   |     |
|-----|---|-----|
| 2.1 | Performance Results – Pattern Matching Algorithm.....                     | 30  |
| 2.2 | Comparison – Contemporary Open Source and Commercial NIDS.....            | 36  |
| 3.1 | Results - Host-based Configuration for Mixed Traffic.....                 | 46  |
| 3.2 | Types - Denial of Service (DoS) Attacks.....                              | 52  |
| 4.1 | Hardware Description- Test-bench I.....                                   | 60  |
| 4.2 | Performance Evaluation Scenario - Test-Bench I.....                       | 63  |
| 4.3 | Hardware Description- Test-bench II and III.....                          | 67  |
| 4.4 | Results - Host-based Configuration (UDP Traffic) .....                    | 69  |
| 4.5 | Results - Host-based Configuration Results (Mixed Traffic) .....          | 72  |
| 4.6 | Results – Test-bench III, Packets Received at Host Operating Systems..... | 75  |
| 7.1 | Considered Exploits and their influence in DARPA dataset.....             | 116 |
| 7.2 | Attack distribution in DARPA dataset.....                                 | 116 |
| 7.3 | Detection approaches and anomalies.....                                   | 126 |
| 7.4 | System Performance – Attack types.....                                    | 136 |