Contents

Preface ix

Introduction xi

Chapter 1. State of the Art on Network Troubleshooting 1

1.1. Network troubleshooting 1
1.1.1. State of the art 2
1.1.2. Traditional troubleshooting architecture 9
1.2. Background on encryption protocols 10
1.2.1. QUIC 11
1.2.2. Other protocols 16
1.3. Drawbacks of troubleshooting with encrypted traffic 18
1.3.1. Network performance monitoring 18
1.3.2. Intrusion detection system 20
1.4. Conclusion 22

Chapter 2. Novel Global Troubleshooting Framework for Encrypted Traffic 25

2.1. Novel network troubleshooting architecture for encrypted traffic 25
2.2. Proof of concept of novel troubleshooting architecture in SDN 28
2.3. Data collection 32
2.3.1. Data classification 32
2.3.2. Monitoring tools 34

2.3.3. Parameter measurement 37
2.4. Troubleshooting dataset 40
2.4.1. Datasets for root cause analysis 40
2.4.2. Dataset for traffic classification 42
2.5. Conclusion 43

Chapter 3. Traffic Classification: Novel QUIC Traffic Classifier Based on Convolutional Neural Network 45

3.1. Introduction 45
3.2. Background 48
3.2.1. Convolutional network 48
3.2.2. Characteristics of QUIC-based applications 49
3.3. Traffic classification approaches 50
3.3.1. Port-based approaches 50
3.3.2. Payload-based approaches 51
3.3.3. Statistic-based approaches 51
3.3.4. DL-based approaches 52
3.4. Novel traffic classification method for QUIC traffic 53
3.4.1. Traffic collection 55
3.4.2. Flow-based features 55
3.4.3. Preprocessing 56
3.4.4. Novel traffic classification method 56
3.5. Experimental results 59
3.5.1. Dataset specification 59
3.5.2. Performance metrics 60
3.5.3. Performance analysis 61
3.6. Conclusion 65

Chapter 4. Anomaly Detection 67

4.1. Introduction 67
4.2. Anomaly detection approaches 68
4.2.1. Knowledge-based mechanisms 68
4.2.2. Rule inductions 69
4.2.3. Information theory 70
4.2.4. ML-based mechanisms 70
4.3. Anomaly detection approach using machine learning 71
4.3.1. ML-based anomaly detection method 72
4.3.2. Data collection and processing 74

4.4. Experimental results 75
4.4.1. Experimental setup 75
4.4.2. Performance analysis 76
4.5. Conclusion 79

Chapter 5. Temporary Remediation: SDN-based Application-aware Segment Routing for Large-scale Networks 81

5.1. Introduction 81
5.2. Application-aware routing mechanisms 84
5.2.1. Application-aware routing 84
5.2.2. Application-aware MPLS 86
5.2.3. Application-aware SR 86
5.3. Adaptive segment routing mechanism for encrypted traffic . . . 87
5.3.1. Overview of the SDN-based adaptive segment routing framework 87
5.3.2. Network monitoring 89
5.3.3. Anomaly detection 90
5.3.4. Application-aware remediation 91
5.4. Experimental results 95
5.4.1. Experiment setup 95
5.4.2. Benchmark 97
5.4.3. Performance analysis 97
5.5. Conclusion 104

Chapter 6. Root Cause Analysis and Definitive Remediation . 107

6.1. Root cause analysis: machine learning based root cause analysis for SDN network 107
6.1.1. Introduction 107
6.1.2. Root cause analysis mechanisms 109
6.1.3. ML-based RCA mechanism 111
6.1.4. Experimental results 114
6.1.5. Conclusion 119
6.2. Definitive remediation: adaptive QUIC BBR algorithm using reinforcement learning for dynamic networks 121
6.2.1. Introduction 121
6.2.2. Congestion control mechanisms 123
6.2.3. Adaptive BBR algorithm 126

6.2.4. Experimental results 128
6.2.5. Conclusion 133

Conclusions and Prospects 135

References 141

Index 159