The 22nd International Symposium on Network Computing and Applications (NCA 2024)

Enhancing Network Intrusion Detection Systems: A Real-time Adaptive Machine Learning Approach for Adversarial Packet-Mutation Mitigation

Presenter
Md Mehedi Hasan
PhD Researcher
School of Computing, Mathematics and Engineering
Charles Sturt University
New South Wales, Australia

Authors
Md Mehedi Hasan
A/Prof. Rafiqul Islam, PhD
Quazi Mamun, PhD
Prof. Md Zahidul Islam, PhD
Prof. Junbin Gao, PhD

Introduction

Research Context

Network Intrusion Detection Systems (NIDS) serve as the primary defense mechanism against malicious network activities. However, they face unprecedented challenges from sophisticated attack methods, particularly adversarial packet mutations that can bypass traditional detection approaches.

Growing Threats

Increasing sophistication of cyber-attacks, particularly packet-mutation techniques

Detection Limitations

Traditional NIDS struggle with advanced evasion methods

Rapid Evolution

Continuous development of new attack patterns and techniques

Research Problem

Why traditional NIDS need enhancement in today's threat landscape

Vulnerability of Traditional NIDS

Current Network Intrusion Detection Systems are increasingly vulnerable to sophisticated packet-mutation attacks***

Impact: Up to 80% misclassification rate in some cases

Advanced Evasion Techniques

Attackers use subtle packet modifications to maintain malicious intent while evading detection systems

Impact: Continuous evolution of attack patterns

Rapid Threat Evolution

Traditional solutions struggle to adapt to the rapid development of new attack patterns and adversarial mutations

Impact: Growing security gap

Real-time Detection Challenges

Current systems lack real-time adaptation capabilities needed to respond to emerging threats effectively

Impact: Delayed response to new attacks

Critical Statistics

80%
Potential misclassification rate

30%
Annual increase in evasion techniques

24/7
Required monitoring capability

Research Objectives

Enhance Detection
Develop advanced detection mechanisms for mutated packets

Real-time Adaptation
Create adaptive learning framework for immediate response

Practical Implementation
Design solution suitable for high-speed networks

Our Solution

Adaptive Layered Mutation Algorithm (ALMA)

- Advanced adversarial example generation
- Multi-layer packet modification
- Dynamic mutation rate adjustment
- Intelligent attack pattern synthesis

Runtime Adaptive ML Framework

- Real-time threat detection
- Continuous learning capability
- Ensemble Model Architecture
- Automated Response Architecture

System Integration

Real-time Detection

98% detection accuracy

Rapid Adaptation

2-3 update cycles for new threats

Enhanced Security

50% reduction in false positives

Precision

90%+ accuracy for novel attacks

ALMA Architecture

Input Phase
- Original packet ingestion
- Initial mutation rate ($\propto$) setting
- Parameter initialization

Processing Phase
- Mutation type selection
- Adaptive rate adjustment
- Packet modification execution

Output Phase
- Mutation validation
- Fitness evaluation
- Modified packet generation

Mutation Types and Techniques

IP Header
Source Address Modification
- IP randomization
- Address masking
- Subnet alterations

Port Numbers
Dynamic port manipulation
- Port randomization
- Service port shifting
- Range modifications

Protocol Fields
Protocol-specific alterations
- Header field mutation
- Payload segmentation
- Protocol switching

TTL Values
Time-to-Live adjustments
- Value randomization
- Path length simulation
- Hop count modification

TCP Flags
Flag state modifications
- Flag bit flipping
- State manipulation
- Connection spoofing

Adaptive Rate Adjustment

Success Case:
$\propto = \min(\propto + \delta, 1.0)$

Failure Case:
$\propto = \min(\propto - \delta, 0.1)$

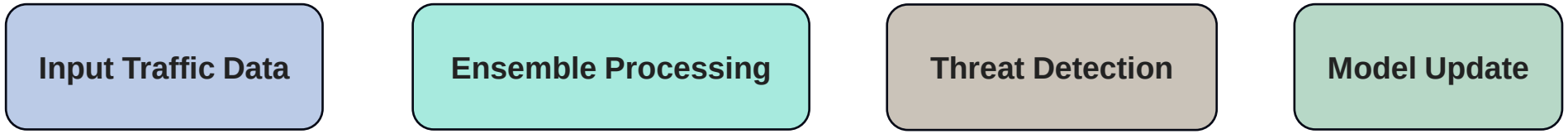
Adaptive ML Framework

Ensemble Model Architecture
- Multiple ML models integration
- Weighted voting mechanism
- Model diversity optimization
- Dynamic weight adjustment

Real-time Detection System
- Continuous traffic monitoring
- Rapid threat assessment
- Pattern matching engine
- Instant alert generation

Adaptive Learning Component
- Continuous model updating
- New pattern recognition
- Performance optimization
- Auto-tuning mechanisms

Framework Workflow



Key Performance Metrics

Detection Accuracy 98%	**False Positive Rate** < 2%
Response Time < 100ms	**Model Update Time** 2-3 cycles

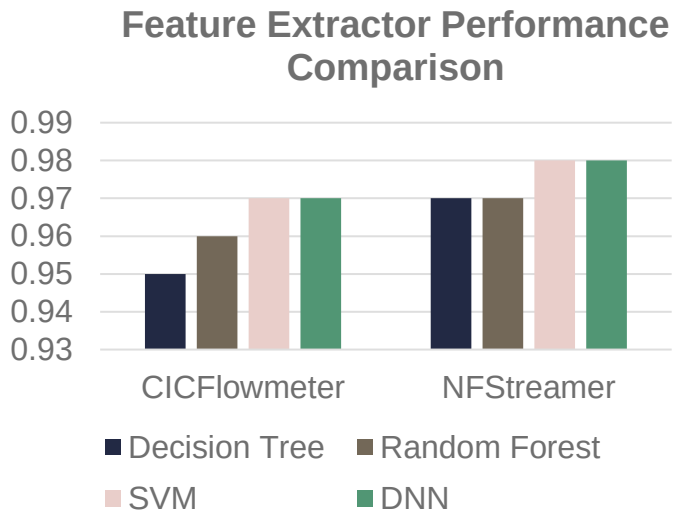
Experimental Results

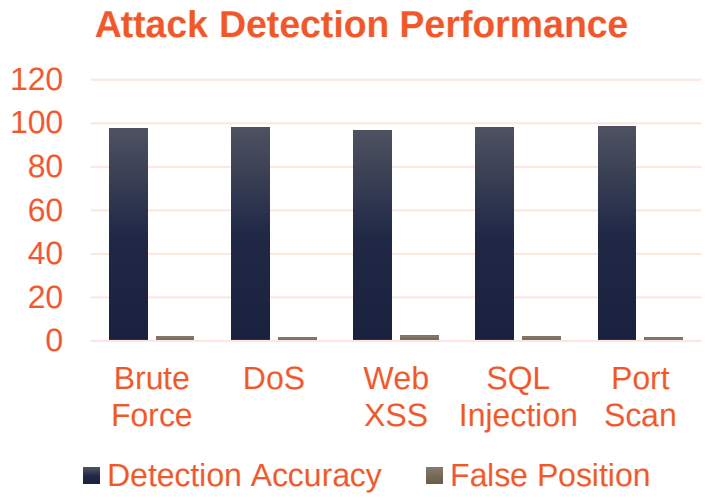
Overall Accuracy
98%

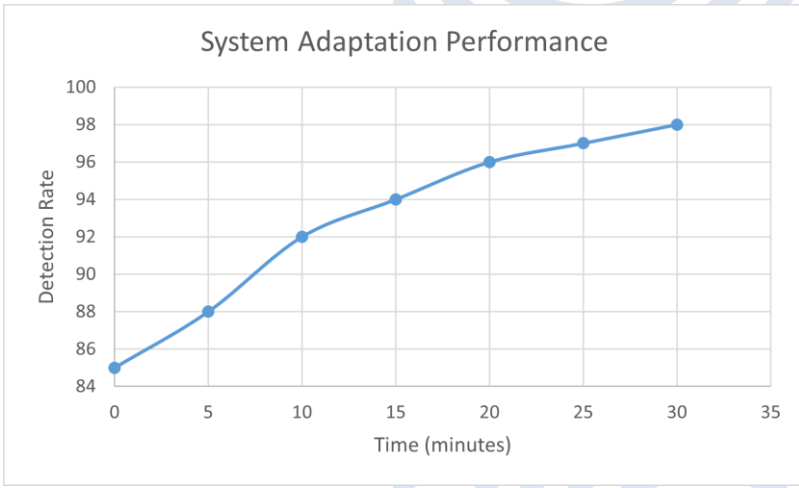
False Positive Rate
1.9%

Adaptation Speed
2-3 cycles

Processing Time
<100ms







Key Findings

Superior Detection Performance
Achieved 98% detection accuracy across diverse attack patterns
Significant improvement over traditional NIDS: **98% accuracy**

Reduced False Positives
Significant reduction in false positive rates
Improved operational efficient: **50% reduction**

Rapid Adaptation
System adapts to new attack patterns within 2-3 update cycles
Enhanced protection against zero-day threats : **90% + accuracy for novel attacks**

Real-time Processing
Sub-100ms response time for threat detection
Immediate threat mitigation: **<100ms**

Comparative Analysis with Traditional NIDS

Category	Proposed System	Traditional NIDS	Improvement
Detection Capability	98% accuracy	85% accuracy	**+13%**
False Positive Rate	1.9%	4.2%	**-55%**
Adaptation Time	2-3 cycles	Manual updates	**Automatic**
Processing Speed	< 100ms	250 ms	**2.5x faster**

Research Implications

Technical Impact
Demonstrates viability of adaptive ML for real-time network security

Practical Applications
Immediate applicability in high-speed network environments

Future Research
Opens new avenues for adaptive security systems

Industry Impact
Potential for significant improvement in cybersecurity tools

Future Work & Conclusion

Key Achievements

Enhanced Detection
98% detection accuracy with reduced false positives

Rapid Adaptation
2-3 cycles for new attack pattern recognition

Innovative Architecture
Integration of ALMA with adaptive ML framework

Future Research Directions

Advanced Mutation Techniques
- Exploring quantum-inspired mutation algorithms
- Enhanced payload-level modifications
- Context-aware mutation strategies

Extended Security Domains
- Applications to IoT security
- Cloud infrastructure protection
- 5G/6G network security

Performance Optimization
- Hardware acceleration
- Distributed processing
- Resource optimization

Concluding Remarks

Research Impact
Significant advancement in NIDS technology with demonstrated improvements in detection accuracy and adaptation speed

Practical Significance
Immediate applicability in real-world network security scenarios with proven performance benefits

Thanks