Anomalous Packets Handling for DetNet

draft-han-detnet-anomalous-packets-handling-01

Z. Han, R. Pang, C. Liu (China Unicom)
J. Yan, X. Zhu (ZTE Corporation)

IETF 124 - DetNet

October 2025

Overview

- DetNet provides deterministic guarantees through **resource allocation** at control plane (bounded latency, low jitter, low packet loss)
- **Aggregation nodes** face challenges when multiple flows converge and share reserved resources at outgoing ports
- **Anomalous forwarding behaviors** can occur in the data plane due to various factors
- **Enhanced handling mechanisms** are needed to preserve deterministic guarantees under anomalous conditions

Problems — Why Anomalies Occur

1. Diversity of Flows

Deterministic flows exhibit **microbursts** and **packet size fluctuations** that deviate from control plane assumptions

2. Software/Hardware Limitations

Algorithmic flows in control plane scheduling and hardware constraints lead to imperfect resource allocation

3. High-Priority Protocol Messages

ARP packets and other protocol messages under abnormal conditions can **preempt service packets** and disrupt scheduling

4. Resource Conflicts at Aggregation

Multiple flows converging at aggregation nodes cause **allocated resources to be exceeded** despite control plane planning

Result:

Anomalous packets detected when queue depth exceeds allocated capacity for current scheduling cycle

Problems — Why Handling is Needed

Current Approaches and Their Inadequacies

Direct Discard

Data loss, violates deterministic guarantees

Buffer and Wait

Unbounded delays, potential queue overflow

Best-Effort Treatment

Loses deterministic scheduling and priority

PREOF (Control Plane)

Excessive resource reservation, poor utilization

Core Issue:

These existing approaches result in **QoS degradation worse than traditional QoS approaches**, undermining DetNet's value

Need:

Data plane mechanism to preserve deterministic guarantees for traffic within allocated capacity while handling anomalous packets appropriately

Handling Policy — Considerations

Policy-based approach: Flexible handling of anomalous packets based on network conditions and operator preferences

Squeezing Policy

Temporary deferral to next timeslot while **preserving original scheduling information** for downstream processing

Degrading Policy

Redirect to **lower-priority queue** when anomaly accumulation exceeds predefined threshold

Key Characteristics

Configurable by control plane based on network conditions

Flexible deployment: Individual or combined policy activation

Compatible with various queuing mechanisms

Safeguard mechanisms to prevent unbounded delays

Squeezing Policy

- **Threshold-based activation**: Configured squeezing threshold determines when policy is applied
- **Mechanism**: Anomalous packets are enqueued and squeezed into the next available timeslot
- **Preservation**: Original scheduling information (timeslot labels) is retained for downstream processing
- **Recording**: System tracks the number of squeezed bits for monitoring and control
- **Benefit**: Provides temporary capacity expansion to avoid data loss during transient anomalies

Squeezing Example

```
|<---Timeslot1--->|<---Timeslot2--->|<---Timeslot3--->|
+---------+-------+-----------------+-------------------+
|/////////|       |                 |                   |
+---------+-------+-----------------+-------------------+

Packet sequence: P1  P2  P3  P4
Target timeslot: TS1 TS1 TS1 TS1

Queue 1 (TS1): | P1 | P2 |  (Capacity: 2000 bits)

Anomaly detected! P3, P4 exceed threshold
                  ↓
Queue 1 (TS1): | P1 | P2 |
Queue 2 (TS2): | P3 | P4 |  (Squeezed, retain TS1 label)
```

Packets P3 and P4 squeezed to Timeslot 2
while preserving original Timeslot 1 scheduling

Single-packet scheduling across time slots should be supported

Degrading Policy

Activation: Triggered when anomalous packet accumulation exceeds predefined threshold, or when squeezing safeguard limits are reached.

Two Deployment Modes

Mode 1: Combined with Squeezing

Processes anomalous traffic that exceeds the squeezing threshold. Acts as a secondary mechanism when squeezing capacity is exhausted.

Mode 2: Independent Operation

Applied directly to anomalous packets that exceed allocated buffer capacity. Functions as the primary anomaly handling mechanism.

Implementation by Queuing Solutions

Time Bounds Queuing Solutions

Packets processed by adjusting target sending time. The resultant delay time can be flexibly configured based on congestion level at the outgoing port.

Periodicity Queuing Solutions

Packets redirected to lower-priority queue and scheduling parameters modified accordingly. Maintains network stability under extreme conditions.

Handling Policy — Information Reporting

Report to Controller

Enable **re-orchestration, flow entry reconfiguration, and resource expansion** decisions based on detected anomalies

Report to Downstream Nodes

Allow downstream nodes to **adjust forwarding behavior or restore original packet parameters**

Reported Information

Basic information: Node ID, port ID, timestamp

Packet information: Flow ID, sequence number, original parameters

Policy information: Policy type applied, squeezed bits/packets, priority changes, degraded packet count

Benefit:

Provides visibility and enables proactive network-wide anomaly management

Thank You

Questions?

draft-han-detnet-anomalous-packets-handling-01

Contact

hanzx21@chinaunicom.cn
yan.jinjie@zte.com.cn