eBPF FOUNDATION

Rakuten Mobile

RAKUTEN MOBILE ADOPTS EBPF TO STRENGTHEN ANOMALY DETECTION AND SECURITY IN CLOUD-NATIVE TELECOM NETWORKS

OVERVIEW

As mobile networks transition to virtualized and cloud-native architectures, traditional monitoring tools struggle to keep pace. To address this challenge, Rakuten Mobile adopted open source eBPF technology, originally designed for cloud and enterprise observability, and adapted it to the complex demands of telecom networks. The solution, Sauron eBPF, enables real-time telemetry, anomaly detection, security tracing, and observability across Rakuten's 5G infrastructure, enhancing both performance and security.

CHALLENGES

- Overwhelming Alert Volume: Static rules and thresholds triggered large volumes of false positives, exhausting operational resources and reducing system trust.
- Poor Adaptability: Legacy solutions lack the flexibility to adapt to evolving network topologies, routing paths, and zero-day attacks.
- Limited Real-Time Insight: Traditional passive monitoring tools couldn't provide granular visibility or timely feedback, especially across distributed, containerized environments.
- Performance Impact: Instrumenting the network without adding significant overhead remained a constant tradeoff.

SOLUTION

Rakuten Mobile developed Sauron eBPF, a lightweight, flexible framework integrated with AI/ML to address the visibility and security gaps in telecom networks. It provides:

- Network Performance (Transport): Active hop-by-hop testing and bottleneck prediction with eBPF. Real-time telemetry on latency, jitter, and packet loss.
- Observability (Traffic Mirroring and Energy): eBPF-powered 5G Cloud Native Network Function (CNF) traffic mirroring with dynamic filtering. Fine-grained CNF resource metrics and intelligent cluster optimization. Reduced overhead and energy consumption with real-time insights.
- Security: Linux-based tracing of cloud-native workloads. Real-time, policy-driven alerts on threats. Scalable detection and prevention of malicious activity.
- Enhanced AI/ML Capabilities: Data from eBPF provides near real-time threat detection from trained ML models. Continuous self-learning and adaptation to new behaviors. Integration with SIEM and SOAR platforms.

RESULTS

- Hop-by-Hop Visibility: Fine-grained insights into transport-layer performance enabled proactive issue resolution.
- Reduced False Positives: Alert noise dropped significantly, allowing teams to focus on critical issues and improving trust in automated monitoring.
- Improved Threat Detection: Enhanced ability to detect and respond to previously undetected anomalies and exploits, including zero-day threats.
- Increased Efficiency: Decreased need for manual investigation and intervention reduced operational cost and response time.

FUTURE PLANS

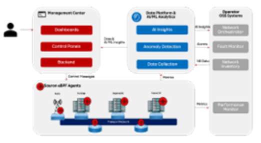
- Broader eBPF Use Cases: Extending capabilities to monitor control plane behavior and container orchestration layers.
- Advanced Threat Intelligence: Combining eBPF with GenAI technologies, Joint Embedding Predictive Architectures (JEPA), and reinforcement learning to enhance autonomous root cause analysis.
- Cross-Domain Correlation: Linking telemetry from multiple domains (compute, storage, network) for full-stack observability.

CONCLUSION

Rakuten Mobile's adaptation of eBPF for telecom use demonstrates the transformative power of combining real-time kernel-level telemetry with AI-driven analytics. By bridging the gap between static monitoring systems and dynamic, distributed mobile networks, Rakuten is not only improving performance and security, but also laying the foundation for intelligent, self-healing 5G and 6G networks.

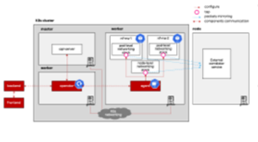
To learn more about their use of Sauron eBPF, check out the article on IEEE Access.

Network performance



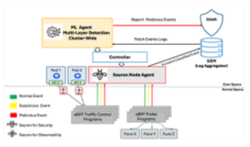
- **Features** – Domain: fronthaul, midhaul, backhaul and backbone networks. Devices: active testing on RIUD, STU, NGDU, RDC, CDC and router
- **Automation** – AI/ML automated prediction of bottlenecks (latency, jitter, packet loss, QoS)

Network observability



- **Features** – tapping pod-to-pod (NF-to-NF) 5GC SBI traffic, filtering out irrelevant packets, forwarding relevant packets to destination for further processing
- **Automation** – Integration with Kubernetes API to get notifications about new pods and programmatically tap them

Runtime security

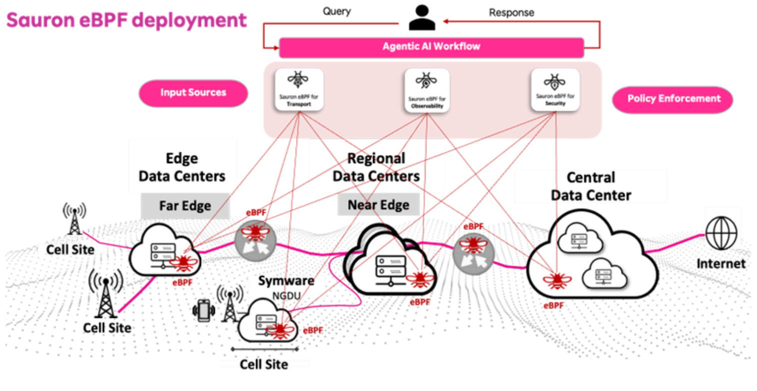


- **Features** – eBPF Traffic Control Module, ML Anomaly Detection and Mitigation Agent, Runtime Security Module, Plugins for Integration with any Orchestration Systems
- **Automation** – Analyze and improve the anomaly Detection Accuracy and False Positive Alarm

Energy telemetry

- **Features** – Energy consumption of any CNF (or microservice, interface) and capacity forecast in K8s clusters, providing consumption per Core CNFs & RAN components as well Container / Pod / Domain
- **Automation** – Estimating the unused capacity of the cluster in terms on the number of UEs, recommending worker nodes that can be put to sleep

Sauron eBPF deployment



- Proactive detection and remediation of both network and security anomalies
- Utilization of eBPF for data sourcing and enforcement