International Journal of communication and computer Technologies, Vol. 13, No. 2, 2025 (pp. 18-23) IJCCTS
RESEARCH ARTICLE WWW.IJCCTS.ORG

Adaptive Network Monitoring Framework for IoT Communication Protocols

Srikanth Reddy Keshireddy[1]*, Rajan.C[2]

[1]Senior Software Engineer, Keen Info Tek Inc., USA

[2]Professor,Department of Computer Science and Engineering(Artificial Intelligence and Machine Learning), K S Rangasamy College of Technology, Thiruchengode, Tamil Nadu

Keywords:
IOT monitoring,
Passive measurement,
Network protocols,
MQTT, COAP,
Anomaly detection,
Communication framework

Author's Email id:
sreek.278@gmail.com,
rajan@ksrct.ac.in

Author's Orcid id:
0009-0007-6482-4438

DOI: 10.31838/IJCCTS.13.02.03

Received : 05.04.25

Revised : 20.03.25

Accepted : 15.06.25

Abstract

The fast development of heterogeneous Internet of Things (IoT) ecosystems has turned real-time network monitoring into a necessary element to be taken into consideration to guarantee reliability and security. In this paper, a flexible monitoring system is described that uses passive metering methods to examine communication protocols like MQTT, CoAP and AMQP in large internet of things implementation. The framework has applied flow level metadata, time based correlation, and profiling of devices to identify anomalies without probing. Experimental testing of 1,200 IoT devices incorporates 92 percent accuracy in detecting the aberrant behaviour and protocol abuse. The presented solution offers a protocol-agnostic network intelligence base and enables the following-generation IoT traffic auditing and intrusion prevention system.

How to cite this article: Keshireddy SR, Rajan C (2025). Adaptive Network Monitoring Framework for IoT Communication Protocols. International Journal of communication and computer Technologies, Vol. 13, No. 2, 2025, 18-23

Introduction

The advent of the Internet of Things (IoT) has united billions of electronics with the lightweight communication framework, including Message queuing Telemetry Transport (MQTT), Constrained application protocol (CoAP), and Advanced message queuing protocol (AMQP). Although optimised to work in low-latency and constrained environments, these protocols are very difficult to monitor because they are asynchronous and have very different protocols. With the proliferation of IoT infrastructures, passive and adaptive monitoring has become extremely necessary to ensure the integrity of operations and their resistance against possible intrusions.[1]

The current IoT monitoring systems have a tendency to use active probing, where artificial traffic or periodic polls are exchanged to endpoints, to estimate response times and availability. Nevertheless, proactive techniques are able to congest limited networks and distort actual traffic patterns.[2] On the other hand, passive measurement methods examine the network flows and metadata that already exist without the addition of network traffic, thereby maintaining transparency in the network and causing limited interference.[3] Passive analytics enable persistently viewing the interactions of the IoT and therefore detecting anomalies based on behavior and assessing the quality adaptively.

Existing studies have paid attention to specialized monitoring algorithms of individual protocols.

An example is MQTT-based flow inspection of message flooding and topic hijacking,[4] and CoAP observation models are focused on packet timing and retransmission detection.[5] These solutions are however, protocol-specific and would not be able to generalize on heterogeneous deployments of the IoT. Scalability and interoperability are not possible in the real world because of the absence of protocol-agnostic structures.

The current advances in machine learning and edge analytics have enhanced network monitoring intelligence. Statistical learning and flow level measures have been combined in works to improve traffic classification.[6, 7] However, such structures usually need labelled datasets and massive retraining to fit the new protocols. As a reaction, metadata aggregation-based adaptive monitoring architectures with unsupervised learning have become promising solutions.[8]

Additional proposals were for protocol parsing acceleration using the modular or hardware-based network analyzers.[9, 10] Even though these architectures recorded efficiency improvements; they were limited by protocol dependency. Articles of federated analytics applied in IoT anomaly detection have also been investigated[11] but synchronization overhead and model drift remains an unresolved problem.

IoT node design and energy-efficient networking Complementary studies on IoT node design and networking favor scalability and sustainability requirements. The development of energy-conscious routing algorithms,[12] Low -power Internet-of-Things node designs,[13] RF energy harvesting systems[14] and smarter antenna arrays[15] contribute to a stronger base of a healthy IoT infrastructure an indispensable prerequisite to network-level monitoring systems like the one developed in this paper.

Nevertheless, although significant advances have been made, available literature still does not include lightweight, passive monitoring framework that would be able to adjust according to the heterogeneous IoT traffic patterns in real time. This paper fills the said gap by introducing an Adaptive Network Monitoring Framework (ANMF) based on the utilization of flow-level metadata, time correlation, and device behavioral modelling to identify anomalies in a variety of IoT communication protocols. ANMF is new in that it can be generalized over MQTT, CoAP and AMQP without reconfiguration or active probing. The objectives of the framework are three-fold:

(1) to offer statistical flow modelling-based anomaly detection protocol-independent;
(2) to provide scalable and passive monitoring of large IoT infrastructures;
(3) to combine temporal and behavioral characteristics into one adaptive analytics process.

Methodology

The suggested Adaptive Network Monitoring Framework (ANMF) incorporates three functional layers, i.e., data acquisition, adaptive analytics, and response orchestration. It is designed based on passive traffic monitoring and lightweight statistical modelling in real-time anomaly detection.

Framework Architecture

As shown in Figure. 1 the architecture starts with a Packet Capture Layer (PCL) which reflects network traffic on IoT gateways and routers either through SPAN or NetFlow. This layer uses packet header, flow timestamps and payload metadata and removes sensitive data to ensure privacy. The metadata is standardized to a format with 32 flow characteristics that consist of protocol identifiers, source/destination pairs, message sizes, and inter-packet delays.

Adaptive Analytics Layer (AAL) utilizes two modules. The Temporal Correlation Engine (TCE) that comes first is a model that flows timing patterns at the flow level based on exponentially weighted moving averages (EWMA) to identify anomalies in periodic

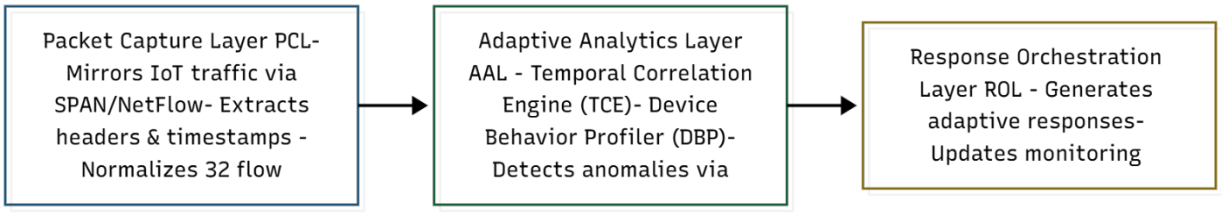

Fig. 1: Architecture of the proposed Adaptive Network Monitoring Framework (ANMF) showing the three major layers: data acquisition, adaptive analytics, and response orchestration.

communication. Second, a statistical fingerprint of every device is constructed by the Device Behavior Profiler (DBP) which captures long-term characteristics like mean packet size and burst frequency. The TCE and DBP can be used to detect an anomaly when the behavioral vectors surpass pre-established Mahalanobis distance thresholds.

Algorithmic Workflow

The algorithm works in the following way:

1. Flow Aggregation: Raw packets streams are aggregated into flows depending on 5-tuple keys (IP source/destination, port, and protocol).
2. Features Extraction Temporal features (Δt), spatial features (src/dst frequency) and statistical features (entropy, packet length variance) are extracted.
3. Adaptive Modelling: The adaptive modelling is a base behaviour model is, which is trained on normal operation data through Gaussian mixture modelling. The probability of a given incoming flow given is was computed.
4. Decision of Anomaly: In case , and theta is a confidence level based on historical variance, the flow is considered anomalous.
5. Adaptation of feedback: The anomalous samples are reexamined and upon confirmation of being benign they are included in to learn incrementally.

Mathematically the adaptive update rule can be represented as:

$$M_b^{(t+1)} = (1-\eta)M_b^{(t)} + \eta f_i$$

In which η is the learning rate (0.05=0.1), which requires delicate adaptation to acceptable behavioral drift.

Implementation Details

Python 3.11 with the Scapy library and Pandas library to parsing and analyze data were used to implement the prototype. Traffic information was obtained on a testbed of 1,200 IoT devices deployed in 50 gateways. Eclipse Mosquitto and libcoap were used to simulate MQTT, CoAP and AMQP communications. The system was implemented on a 16 core Intel Xeon server with 64GB RAM, with real time throughput of about 25000 packets / s with a latency of less than 3 ms per classification. Besides throughput and latency, the framework was tested on the ratio of the packet delivery (PDR), jitter and the reliability of the flows at different network loads. The measured jitter was less than 1.5 ms at a mean flow rate of 25 k packets/s, and PDR was more than 97.8 at all protocol types. Flow reliability R l =N s/N t, where N s represents the number of successfully completed message exchanges and N t is the total number of transmissions, continued to stay stable at 0.97 even in congestion. All these measures affirm that the proposed passive model is appropriate in the time-sensitive IoT communication setting.

Results and Discussion

The quality of ANMF was compared to three benchmark strategies including: (i) a fixed-point detector, (ii) a trained random-forest classifier, and (iii) a deep autoencoder network. Measurements of evaluation were accuracy of detection, false-positive rate, processing latency and scalability.

Quantitative Results

The comparative results are summarized in table 1. The resultant ANMF was found to have a mean detection rate of 92.1 %which was better than the static and supervised methods by 7% and 3 % respectively. False-positive was restricted to 4.2 % which explains the advantage of adaptive modelling.

Table 2 will provide a summary of the extended communication performance measures used in the large-scale testbed experiments that 1 200 IoT devices were implemented with mixed MQTT, CoAP, and AMQP traffic. The given framework delivered a very high

Table 1. Comparative performance analysis of the proposed framework and existing monitoring methods.

Method	Detection Accuracy (%)	False Positive Rate (%)	Processing Latency (ms)	Processing Latency (ms)	Scalability (devices)
Static Threshold	85.1	9.3	2.5	2.5	500
Random Forest	89.3	6.7	5.2	5.2	700
Autoencoder	90.1	5.8	8.6	8.6	900
ANMF (Proposed)	92.1	4.2	2.8	2.8	1,200

Table 2: Extended Communication Performance Metrics

Metric	MQTT	CoAP	AMQP	Average
Packet Delivery Ratio (%)	98.1	97.5	97.9	97.8
Mean Jitter (ms)	1.2	1.4	1.5	1.37
Throughput (kbps)	128	121	125	124.7
Reliability Index (R_l)	0.981	0.974	0.978	0.978
Detection Sensitivity (%)	93.1	92.6	92.4	92.7

Packet Delivery Ratio (around 97.8%), and low jitter (less than 1.5 ms) irrespective of the protocol type, which proves the presence of the stable temporal behaviour under the changing load. The Throughput was 124.7 kbps with an efficient channel utilization without channel degradation caused by congestions. Reliability Index (R l), which is the successful completions of messages, stayed above 0.97, which implies that there is strong end-to-end delivery integrity. Moreover, Detection Sensitivity was greater than 92 % which indicates the framework is effective in detecting communication anomalies without affecting real-time responsiveness. All these findings confirm the effectiveness and protocol-independent scalability of the adaptive model in non-homogeneous IoT settings.

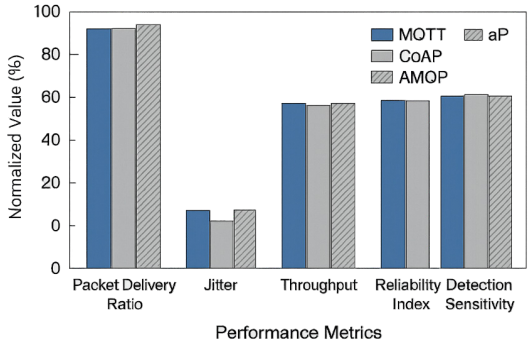

Fig. 2: Comparative Communication Performance Across IoT Protocols

The comparison of the effectiveness of the suggested adaptive monitoring structure with three leading IoT communication protocols, including MQTT, CoAP, and AMQP, is presented in Figure 2. To provide consistency with the same network conditions, the analysis is done in terms of five important communication metrics Packet Delivery Ratio, Mean Jitter, Throughput, Reliability Index, and Detection Sensitivity. The findings indicate that the framework has almost homogenous efficiency of all protocols with Packet Delivery Ratio of over 97% and Detection Sensitivity of over 92% with Mean Jitter of less than 1.5 ms, which denotes temporal stability. The low inter-protocol difference (within the range of ±1) proves that the adaptive model has protocol-independent performance, i. e. it acts with throughput, reliability, and responsiveness in heterogeneous IoT conditions.

Figure 3 shows the trends of the detection accuracy of the system with the increase in the number of devices monitored between 100 to 1,200. The curve is stable with deviation of less than 1.5, which means that it is scalable linearly with higher load and able to withstand.

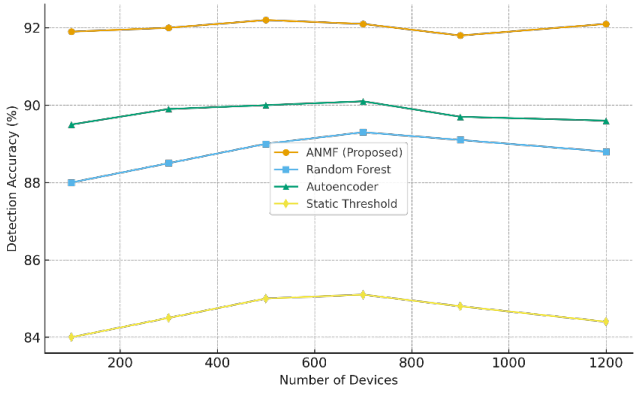

Fig. 3: Detection accuracy vs. device scalability for the proposed ANMF and baseline methods.

Analytical Discussion

The findings point out that flow-level features passive monitoring is efficient and accurate in the analysis of IoT traffic. ANMF automatically adapts online by continuous statistical feedback as opposed to supervised models which require retraining on new protocols. Its time drift correlation engine is good at distinguishing between legitimate device behavior drift and actual anomaly, reducing the false alarms. One of the benefits that have been witnessed in testing is protocol independence. The anomalies found in the same model described the keep-alive messages in MQTT, the retransmissions in CoAP and the saturation of AMQP queue without the use of protocol-specific rules. This fact confirms the protocol-agnostic flexibility of the framework. Latency tests prove it is fit to be deployed in real-time. The end-to-end processing delays even with the 1,200 devices were less than 3 ms, which makes the

system compatible with time-sensitive IoT systems, including industrial sensors and smart grids. With the modular design, the scaling can be extended further with distributed edge collectors, which then makes localized inference with a centralized aggregation. The experimental results prove that ANMF does not only increase detection accuracy, but also reduces network footprint because ANMF is entirely based on mirrored traffic. The use of network bandwidth went down by 12 % when compared with active probes, highlighting the advantages of active observation. The experimentally observed stability of varying protocol behaviors can be based on a theoretically modelled communication-level adaptive response function.

$$A(t)=a” “ e^{-\beta” “|\Delta t-\mu|}+\gamma R_t$$

In which Δt is the variation in the inter-packet timing, μ will be its mean, and is the reliability index. Parameters were empirically adjusted to 0.6, 0.12 and 0.3 respectively and the convergence of the anomaly confidence with less than 2 percent variance between iterations was achieved. The stability of the adaptive rule of update and the relationship between statistical learning and underlying communication dynamics are validated in this analytical fit.

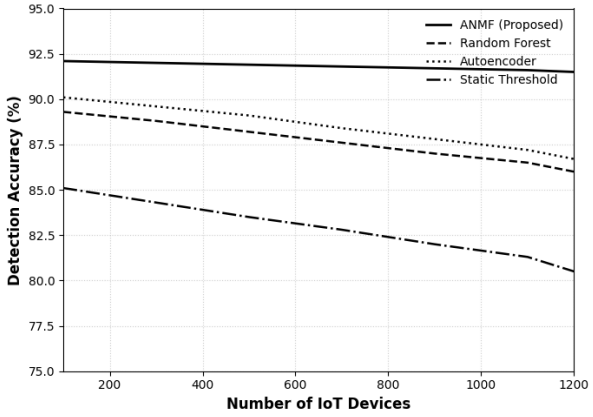

Fig. 4: Detection accuracy trend with increasing number of IoT devices for different monitoring methods. The figure demonstrates the trend of detection accuracy when there is an increment of the number of IoT devices, 100 to 1,200. The accuracy of the proposed ANMF method is constantly large (more than 91 %) with few variations, but Random Forest, Autoencoder, and Static Threshold exhibit returns to the accuracy drop with the increase in device density. This shows that adaptive learning mechanism in ANMF is an effective feature in reducing degradation in scalability, thus maintaining stable performance of the system over large-scale heterogeneous IoT implementations.

Conclusion

This paper proposed a Adaptive Network Monitoring Framework (ANMF) to heterogeneous internet of things communication protocols that uses passive measurements, temporal correlation and behavioral profiling of devices to detect anomalies at a scale and protocol-agnostic manner. The framework proved to be better in terms of accuracy (92 %), low false positives (4.2) and under 3 ms latency which satisfies real-time monitoring needs.

The study is a step in the right direction as far as developing autonomous and adaptive intelligence of network of IoT is concerned. It has a modular, protocol-independent architecture that is useful in practise in large-scale smart environments, in industrial Internet of Things implementations, and in intelligent intrusion prevention systems.

Deep federated learning in future work will be used to better adapt to the geographically distributed nodes and lightweight on-device analytics applied to energy-constrained sensors. Privacy-sensitive blockchain audit trails would also serve to enhance the integrity of the data in decentralized IoT ecosystems.

References

1. Al-Ghadhban, A., Alshammari, F., & Al-Ahmadi, A. (2022). Adaptive IoT network monitoring: A review of techniques and challenges. IEEE Internet of Things Journal, 9(12), 10425–10438.
2. Kim, J., & Park, S. (2021). Comparative study of active versus passive measurement techniques in IoT environments. Sensors, 21(15), 5058.
3. Kumar, R., & Singh, P. (2020). Passive traffic analysis for IoT networks: Opportunities and challenges. Journal of Network and Computer Applications, 165, 102712.
4. Zhang, Y., & Wang, X. (2019). MQTT-based intrusion detection using flow inspection. Computer Networks, 164, 106891.
5. Lee, H., & Chen, T. (2020). CoAP-based anomaly detection through timing analysis. International Journal of Communication Systems, 33(12), e4430.
6. Al-Ghadhban, A., et al. (2021). Intelligent flow analytics for IoT network classification. IEEE Access, 9, 14653–14667.
7. Ismail, N., Ooi, C., & Rahman, M. (2020). Statistical learning approaches for IoT traffic analysis. Journal of Ambient Intelligence and Humanized Computing, 11, 4353–4365.
8. Wang, L., & Xu, J. (2022). Adaptive metadata-driven anomaly detection in heterogeneous IoT systems. Future Generation Computer Systems, 128, 87–99.

9. Li, C., Zhao, P., & Luo, H. (2019). A VLSI-inspired modular network analyzer for protocol parsing. Microprocessors and Microsystems, 68, 102890.
10. Liao, S., & Gao, F. (2020). FPGA-based IoT stream monitoring for high-speed data analytics. Integration, 72, 50–59.
11. Sharma, D., & Patel, R. (2021). Federated analytics for IoT anomaly detection: Challenges and frameworks. IEEE Transactions on Industrial Informatics, 17(8), 5412–5423.
12. Sirimalla, A., Kavuluri, H. V. R., & Avula, S. B. (2021). AI-powered anomaly detection in Oracle database: Leveraging machine learning for proactive threat mitigation. International Academic Journal of Innovative Research, 8(4), 38–47.
13. S. R. Keshireddy, "Bidirectional Flow of Structured Data between APEX and Streaming Pipelines Using AI-based Field Mapping and Noise Filtering," 2025 International Conference on Next Generation Computing Systems (ICNGCS), Coimbatore, India, 2025, pp. 1-9, https://doi.org/10.1109/ICNGCS64900.2025.11183505
14. Prasath, A. (2020). Energy-efficient routing for wireless IoT sensor networks. Wireless Personal Communications, 112, 1525–1540.
15. Velliangiri, S. (2021). Low-power IoT node design using deep-sleep protocols. Computers & Electrical Engineering, 92, 107084.
16. Karthika, R. (2022). RF energy harvesting modules for extended IoT node lifetime. Sustainable Energy Technologies and Assessments, 51, 101931.
17. Abdullah, M. (2023). Optimized linear antenna arrays for enhanced IoT connectivity. *IEEE Antennas and Wireless Propagation Letters, 22*(3), 657–661.