विश्वजीवनामृतं ज्ञानम्

ATAL BIHARI VAJPAYEE-INDIAN INSTITUTE OF INFORMATION TECHNOLOGY AND MANAGEMENT (ABV-IIITM), GWALIOR

Energy-Efficient Lightweight Defense for DDoS Attacks in IoT Networks Using Identity–Behavior Mismatch

PRESENTED BY:

Sidhant Kapoor : 2021IMT-100

SUBMITTED TO:

Prof. Shashikala Tapaswi

Dr. W Wilfred Godfrey

Base research paper :
IoTDevID: A Behavior-Based Device Identification Method for the IoT by Kahraman Kosta, Mike Just and Michael A. Lones
https://ieeexplore.ieee.org/document/9832419/

IEEE Internet of Things Journal
2022

CONTENTS

1. Background of the Problem
2. Motivation
3. Literature Survey
4. Research Gaps
5. Problem Statement
6. Objective
7. Proposed Methodology
8. References

BACKGROUND OF THE PROBLEM

- **Rapid Growth:** The number of IoT devices is growing exponentially, expected to exceed 80 billion by 2026, increasing network complexity.
- **Increased Attack Surface:** The heterogeneous and always-connected nature of IoT makes it highly vulnerable to large-scale cyberattacks, especially DDoS.
- **Current Device Identification Approaches**: Existing methods primarily rely on IP based features extraction from network packets to identify devices.
- **Diverse Protocols**: Many IoT devices operate on low-resource, non-IP protocols such as bluetooth, ZigBee making them invisible to IP-based methods.
- **Limitations of Traditional Defenses**: Conventional IDS and firewall-based systems are too heavy for low-power IoT devices and often fail to detect early-stage attacks.
- **Behavioral Inconsistency in Compromised Devices**: Compromised IoT nodes often deviate from their normal communication patterns a potential behavioral indicator of DDoS activity.

MOTIVATION

- **Energy Constraints in IoT Devices**: IoT nodes have limited battery and processing power, making lightweight defense mechanisms essential.
- **Ineffectiveness of Traffic-Based Detection:** Traditional DDoS detection relies on heavy traffic analytics rather than smart behavioral modeling.
- **Potential of Identity–Behavior Correlation**: Leveraging behavioral identity models (like IoTDevID) can help detect when a legitimate device starts behaving abnormally.
- **Preventing Botnet-Based DDoS Attacks**: Early detection of identity–behavior mismatch can stop IoT devices from being hijacked into DDoS botnets.
- **Aim for Real-Time and Scalable Protection:** To create a system that ensures real-time DDoS defense while maintaining minimal latency and energy usage.

LITERATURE SURVEY

Categorization of Reviewed Papers

1. IoT Device Identification & Behavioral Fingerprinting:
   - Kostas et al. (2022) – IoTDevID: A Behavior-Based Device Identification Method for the IoT
   - Wang (2024) – Classifying IoT Devices Before and After Compromise

2. DDoS Detection and Mitigation Frameworks
   - Gavrić et al. (2024) – Towards Resource-Efficient DDoS Detection in IoT
   - Nawaz & Tahira (2025) – Lightweight ML Framework for DDoS Detection in IoT Networks

3. Behavior-Aware DDoS Defense and Edge-Based Solutions
   - Bhardwaj & Singh (2018) – Towards IoT-DDoS Prevention Using Edge Computing

LITERATURE SURVEY

Author(s)	Year	Paper Title	Key Contribution	Major Limitation
Kostas et al.	2022	*IoTDevID: A Behavior-Based Device Identification Method for the IoT*	Introduces ML-based behavioral identity models for device identification.	Does not address DDoS or compromised device behavior.
Celdrán et al.	2023	*Intelligent Behavioral Fingerprinting to Detect Attacks in IoT Sensors*	Uses behavioral fingerprints for attack and anomaly detection.	Limited focus on energy efficiency and DDoS-specific defense.
Wang	2024	*Classifying IoT Devices Before and After Compromise*	Compares device behavior pre- and post-compromise to identify malicious activity.	Lacks a real-time defense or mitigation mechanism.
Gavrić et al.	2024	*Towards Resource-Efficient DDoS Detection in IoT*	Proposes lightweight, energy-efficient DDoS detection models.	Does not leverage device behavior or identity modeling.

LITERATURE SURVEY

Nawaz & Tahira	2025	*Lightweight ML Framework for DDoS Detection in IoT Networks*	Introduces optimized ML models for DDoS detection on constrained devices.	Relies mainly on traffic-level features; lacks adaptive behavior analysis.
Khedr et al.	2023	*FMDADM: Multi-Layer DDoS Mitigation in SDN-Based IoT Networks*	Uses SDN controllers for distributed detection and mitigation.	High controller load; unsuitable for ultra-lightweight IoT nodes.
Feraudo et al.	2024	*Mitigating IoT Botnet DDoS Attacks through MUD and Behavioral Fingerprints*	Combines MUD policy and fingerprinting for device-level defense.	Energy overhead and scalability challenges in large networks.
Bhardwaj & Singh	2018	*Towards IoT-DDoS Prevention Using Edge Computing*	Introduces edge-layer early DDoS prevention to reduce traffic impact.	Does not include behavior-based or identity-driven detection logic.

RESEARCH GAPS

- **Integration of Behavioral Identity**: Extends IoTDevID for real-time DDoS detection using behavior–identity correlation.
- **Lightweight Computation**: Uses low-overhead ML models ensuring minimal energy and resource use.
- **Early Detection:** Employs Behavior Deviation Score (BDS) for proactive anomaly identification.
- **Energy-Efficient Mitigation:** Offloads defense actions to edge/SDN controllers to save device power.
- **Scalability:** Works across diverse IoT devices and protocols for real-world deployment.

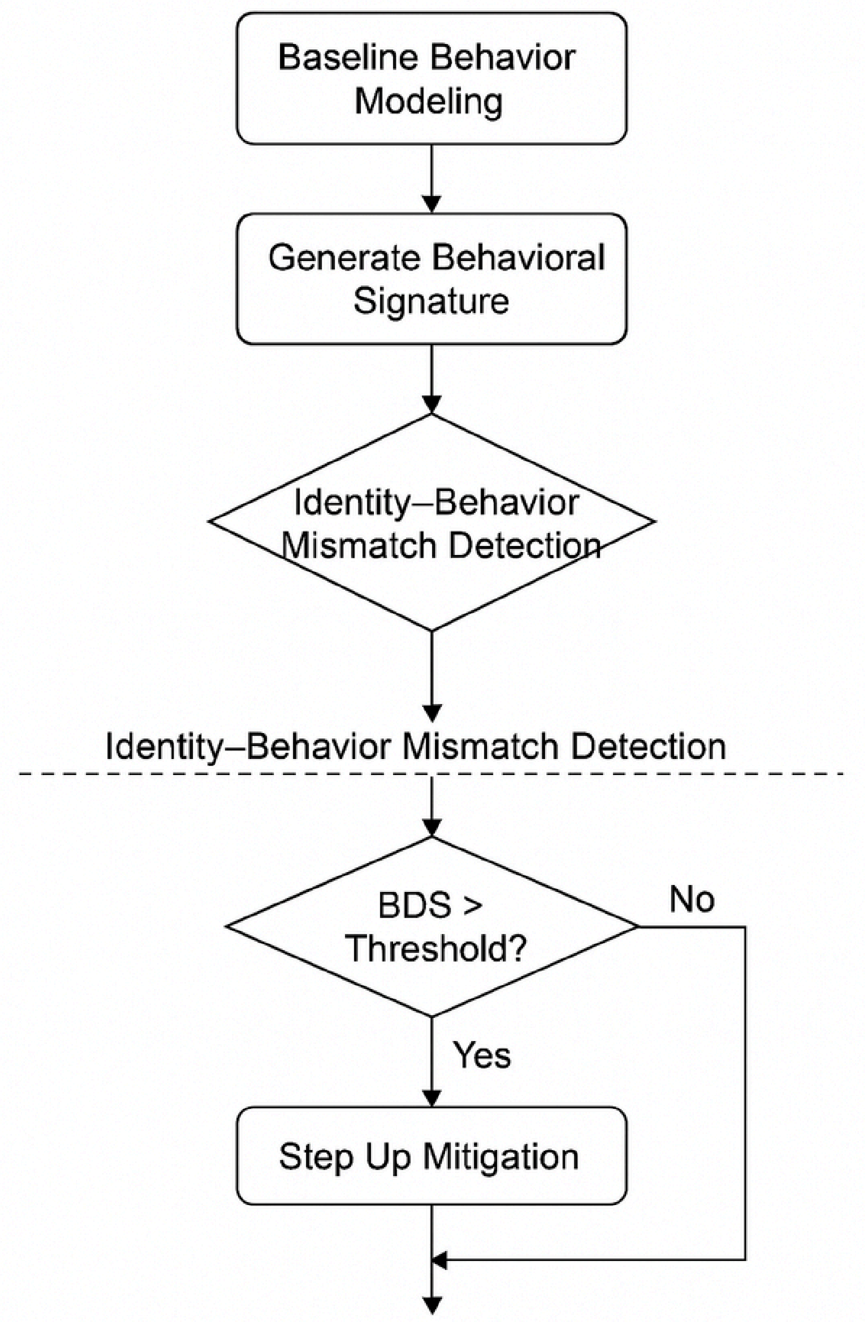
PROBLEM STATEMENT

- The growing number of IoT devices has increased vulnerability to DDoS attacks due to limited power and processing capacity.
- Existing detection systems rely on heavy traffic analysis, making them unsuitable for lightweight IoT environments.
- Current methods ignore a device’s behavioral identity, missing early signs of compromise.
- There is a need for an energy-efficient lightweight defense mechanism that uses identity–behavior mismatch detection to identify and mitigate DDoS attacks in real time.

OBJECTIVE

- Extend the IoTDevID framework beyond device identification to include real-time DDoS defense by monitoring deviations between device identity and behavioral patterns.
- Integrate a Behavior Deviation Scoring (BDS) module that quantifies identity–behavior mismatch to detect compromised or abnormal device activity before large-scale flooding occurs.
- Optimize defense decision-making using lightweight ML classifiers (Decision Tree / Random Forest) trained on behavioral baselines for accurate yet low-power operation.
- Introduce a behavior-based trust evaluation mechanism to dynamically adjust device reliability scores and trigger selective mitigation actions.
- Evaluate system performance using benchmark IoT DDoS datasets (e.g., BoT-IoT, CIC-IoT, or custom synthetic traces) and metrics such as detection accuracy, latency, and energy consumption.

PROPOSED METHODOLGY



Identity-Behavior Mismatch DDoS Defence for IOT devices

Key Components

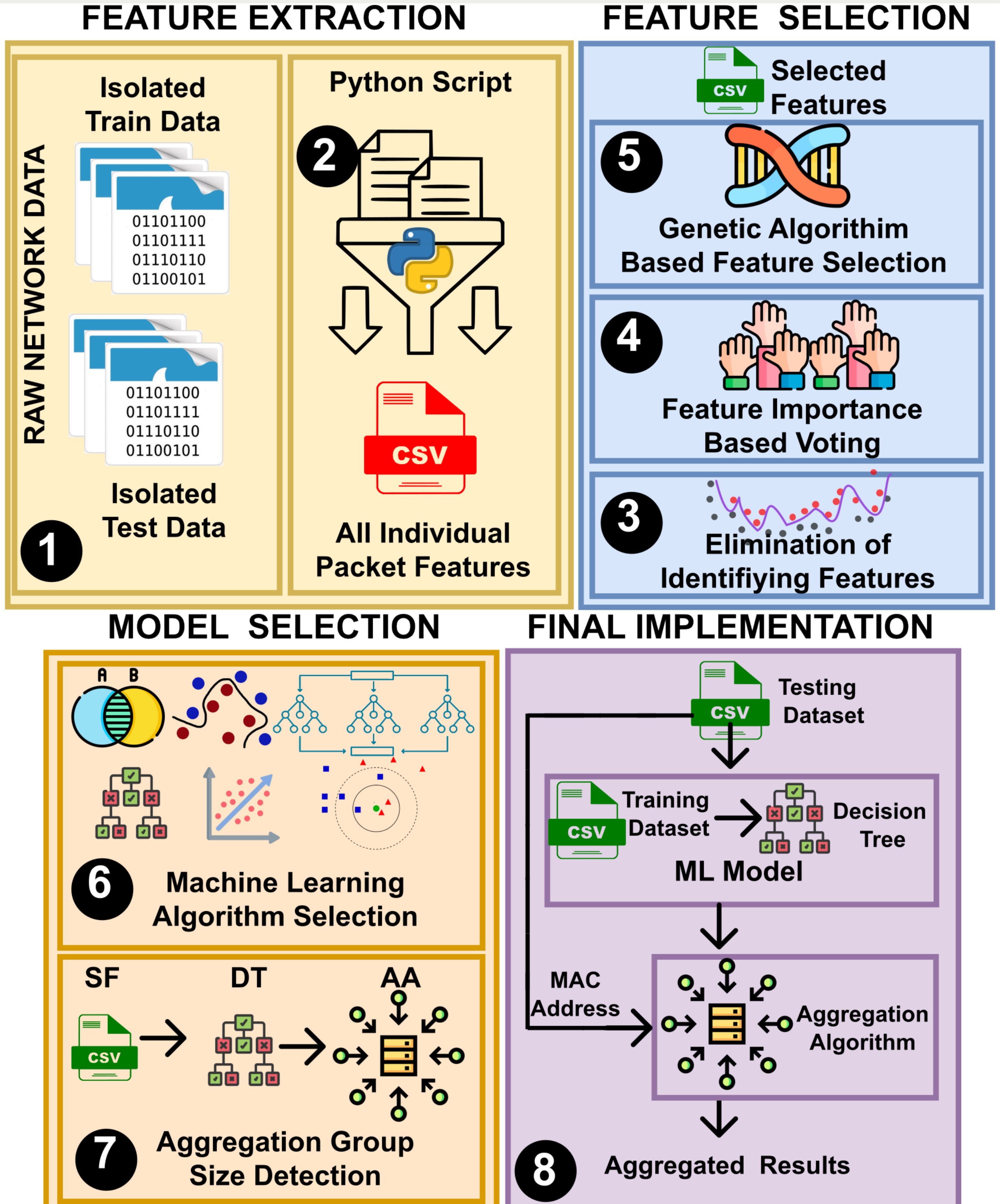
- Behavior Baseline Modeling
- Real-Time Monitoring & Deviation Detection
- Lightweight Mitigation & Energy Optimization

PROPOSED METHODOLGY

Step-by-Step Operation:

1. **Device Enrollment**: Capture each IoT device’s normal traffic during non-attack periods.
2. **Feature Extraction**: compute compact statistical features.
3. **Model Training**: create behavioral identity model.
4. **Real-Time Monitoring**: Continuously capture live traffic at the edge or SDN controller.
5. **BDS Computation**: Compute similarity/distance between live and baseline behavior vectors.
6. **Anomaly Decision**: if BDS > threshold → mark as suspicious.
7. **Mitigation**: rate-limit or isolate device at edge controller.
8. **Post-Mitigation Check**: restore connectivity if behavior normalizes.
9. **Continuous Learning**: update baseline when legitimate changes occur.

CURRENT APPROACH



IoTDevID Workflow

Packet Capture (Aalto & UNSW dataset)

⬇

Feature Extraction

⬇

Feature Selection (Voting based selection & GA)

⬇

Model Training (DT)

⬇

Packet Classification (Using DT)

⬇

Aggregation

⬇

Final Device Identification

REFERENCES

- Kostas et al., IoTDevID: Behavior-Based Device Identification, IEEE IoT Journal, 2022.
- Nguyen et al., DÏoT: Federated Self-Learning Anomaly Detection, ICDCS, 2019.
- Meidan et al., N-BaIoT, Elsevier, 2018.
- Xu et al., Addressing Concept Drift in IoT Anomaly Detection, IEEE TNSM, 2024.
- Mirjalili & Lewis, Whale Optimization Algorithm, Elsevier, 2016.
- Shan et al., Hybrid WOA–GWO for IDS, Nature Sci. Rep., 2025.
- Bezawada et al., IoTSense, IEEE CNS, 2018.
- Xu et al., Detecting Compromised IoT Devices, Elsevier, 2023.

THANK YOU!