AI-driven Cyber Defense for Drone Mission Recovery at the Tactical Warfighting Edge

Presenter: Prasad Calyam

Curators' Distinguished Professor & Greg L. Gilliom Professor of Cybersecurity

University of Missouri-Columbia

Other Team Members: Rohit Chadha (University of Missouri-Columbia), Vijay Anand (University of Missouri-St. Louis), Reshmi Mitra (Southeast Missouri State University)

CAE IN CYBERSECURITY COMMUNITY

University of Missouri

Mizzou CERI

Center for Cyber Education, Research & Infrastructure

Agenda

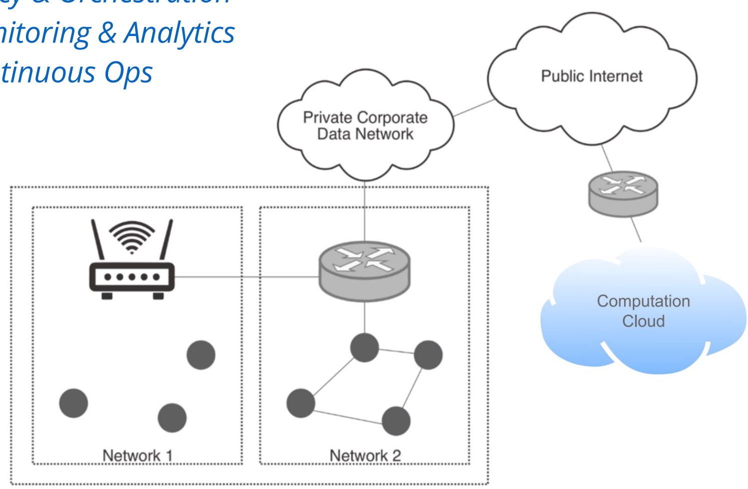
- Research Motivation
  - Tactical Warfighting Edge
  - Zero Trust
  - Problem Statement
- Arculus: Low-overhead Zero Trust Security Architecture
- AI-driven Predictive Model Technologies
  - RL-based Intelligent Drone Trajectory Management
  - Bayesian Network for Risk Quantification
- Arculus Evaluation
  - TBAC vs RBAC results
  - Predictive models results
  - Hardware experimentation results for TWE threat scenarios
- Conclusion and Future Directions

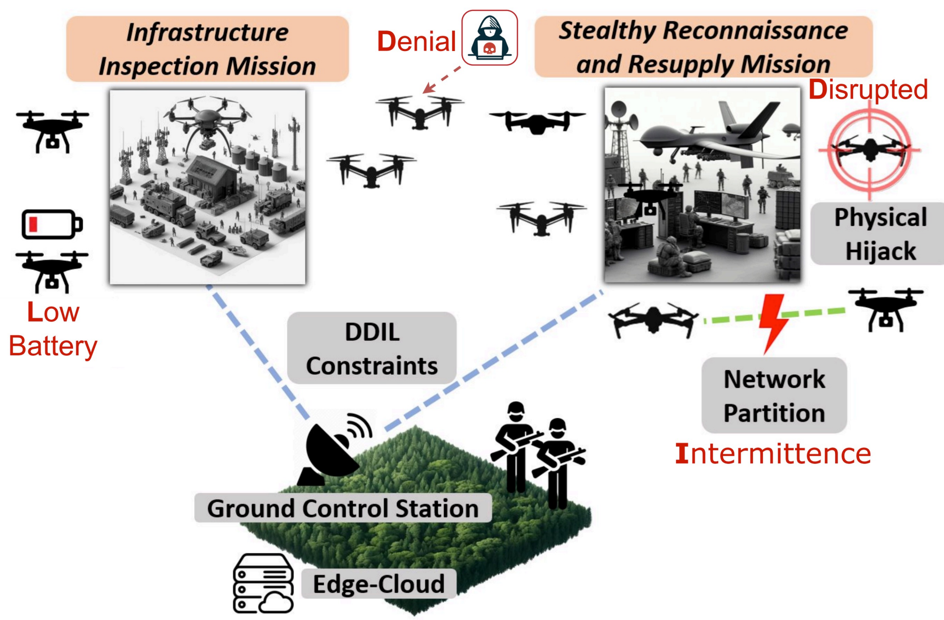
Enterprise Network vs TWE Network

Capabilities:
Identity Verification
Access Control
Resource Protection
Policy & Orchestration
Monitoring & Analytics
Continuous Ops

Enterprise Network Vs. Tactical Warfighting Edge

High Availability | *Intermittent / Low Availability*



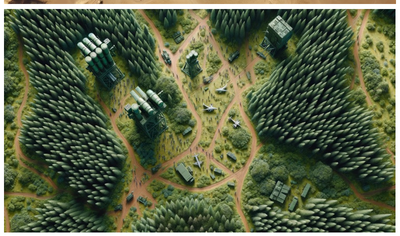


ZT Enterprise capabilities **are not effective at the tactical warfighting edge** due to operational impacts from denied, disrupted, intermittent, and limited **(DDIL) environments**, including limited bandwidth, and other constrained resources.

Exemplar TWE Mission Types and Tasks

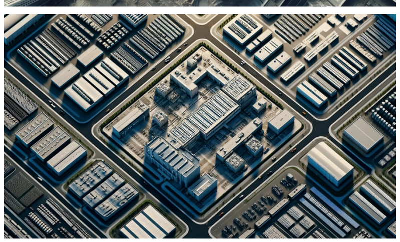
Stealthy Reconnaissance and Resupply

Mine-Aware Search and Rescue



Disaster Assessment and Recovery

Infrastructure Inspection

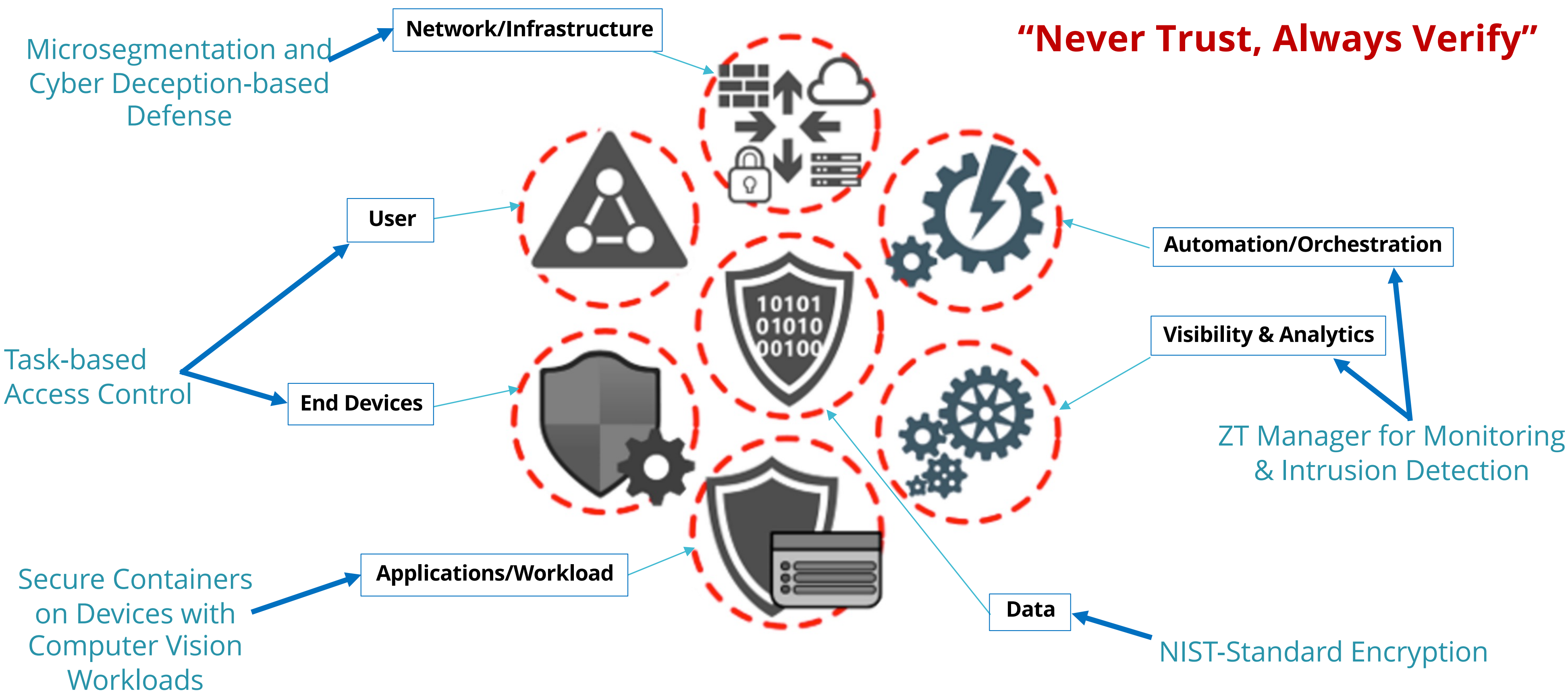


Mission Tasks Carried out by TWE devices in the Internet of Battlefield Things (IoBT) - Stakeholder Scenarios

- **Video data collection, transmission and processing** for real-time situational awareness, decision-making, and strategic intelligence *(highly sensitive task)*
- **Sensor data processing** for surveillance on environmental conditions, target movements, and potential threats, guiding actions, and ensuring operational success
- **Chemical, Biological, Radiological, & Nuclear (CBRN) threat detection** to safeguard civilians, prevent catastrophic incidents, and execute effective response measures in hazardous situations
- **Tracking casualties, injuries, and medical help requirement** ensuring optimal resource allocation, and swiftly delivering life-saving care during missions *(lower sensitive task)*

Liu, Dongxin, et al. "Iobt-os: Optimizing the sensing-to-decision loop for the internet of battlefield things." *2022 International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 2022.
Stocchero, Jorgito Matiuzzi, et al. "Secure command and control for internet of battle things using novel network paradigms." *IEEE Communications Magazine* 61.5 (2022): 166-172.

DoD Seven Pillars of Zero Trust: Requirements



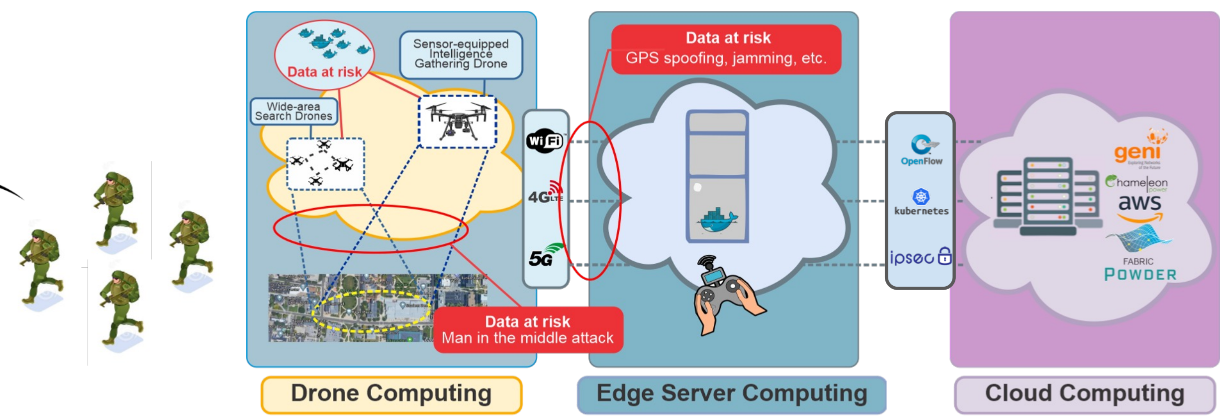
Problem Statement - Use Case

Network-edge Connectivity and Computation Security in Drone Video Analytics

- **Drone operations in FANETS are inherently insecure** but need to aid warfighters in scenes of interest
- **Limited resources on UAVs brings additional constraints** on any security scheme that can be applied to the common protocols in the UAV systems
- **Malicious communications, jams or spoofs in Ground Control Station (GCS) signals, or Denial of Service (DoS) attacks or malware that corrupts containerized data collection/processing** - all these disrupt the drones operations (e.g., cause data integrity or loss of privacy issues)

DISA

U.S.NAVAL RESEARCH LABORATORY



Cyber attacks can target UAV flight networks, GCS communication, or containerized data processing tasks

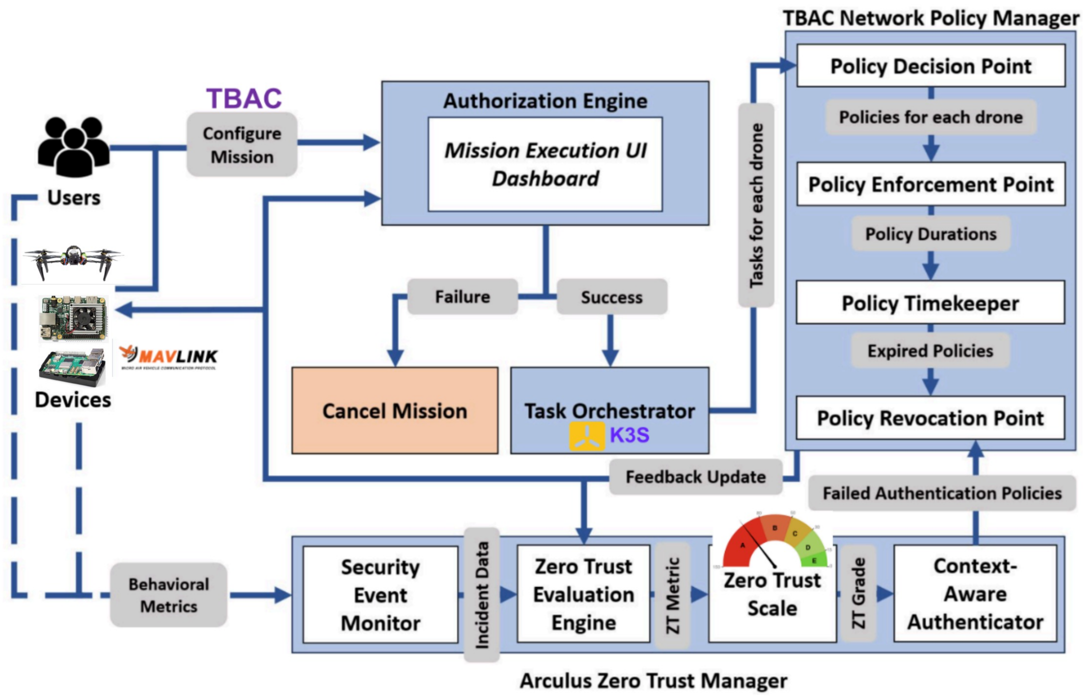
C. Qu, F. Sorbelli, R. Singh, P. Calyam, S. Das, “Environmentally-Aware and Energy-Efficient Multi-Drone Coordination and Networking for Disaster Response”, IEEE Transactions on Network and Service Management (TNSM), 2023.

Low-Overhead ZT Architecture of Arculus

with Task-based Access Control at the TWE

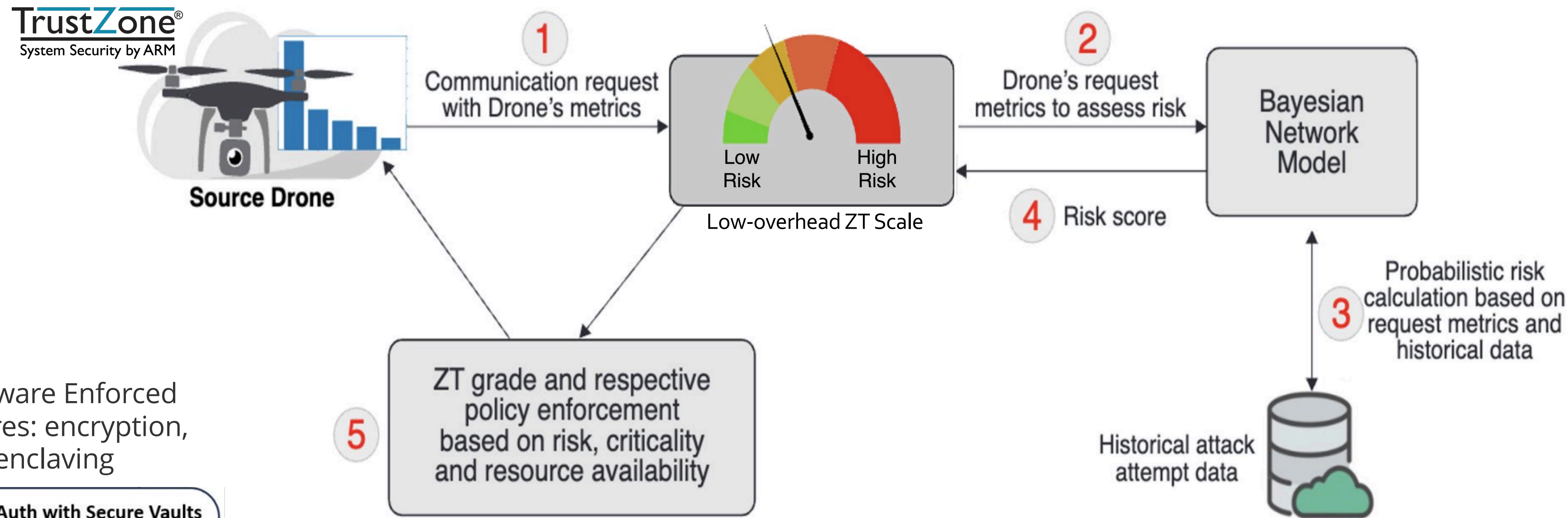
- Reference Architecture
  - Adheres to NIST ZT model guidelines SP 800-207 and SP 800-201
- Low Overhead features
  - Sliding-scale ZT
  - Task-based Access Control
  - K3s Lightweight Kubernetes
  - MAVLink protocol
- Threat agent handling using predictive modeling
  - RL-based drone guidance for safe mission recovery
  - Bayesian network-based risk quantification
  - FedML-based threat detection

Towards implementation for automation of control policies
Listen → Record → Detect → Defend



ARCULUS

Risk Quantification-based Zero Trust Scale
for Tactical Edge Network Environments [*]



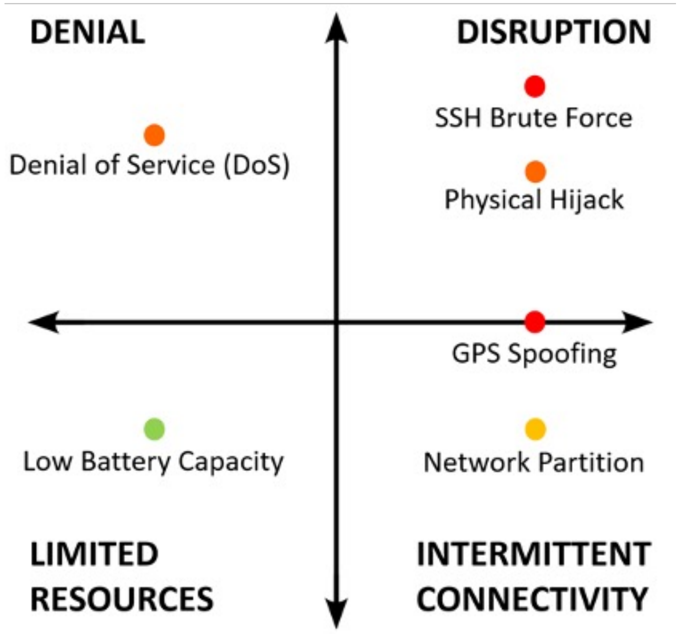
Hardware Enforced Features: encryption, enclaving

- **Mutual Auth with Secure Vaults**
- **Basic Mutual Authentication**
- **Higher Authentication Rate**
- **Token-based Authentication**
- **Basic Lightweight Authentication**

[*] S. Poduvu, S. Saghaian N. E., E. Ufuktepe, A. Esquivel Morel, P. Calyam, "Risk-based Zero Trust Scale for Tactical Edge Network Environments", *ACM Trustworthy Edge Computing Workshop, 2023.*

Classification of threats based on DDIL constraints

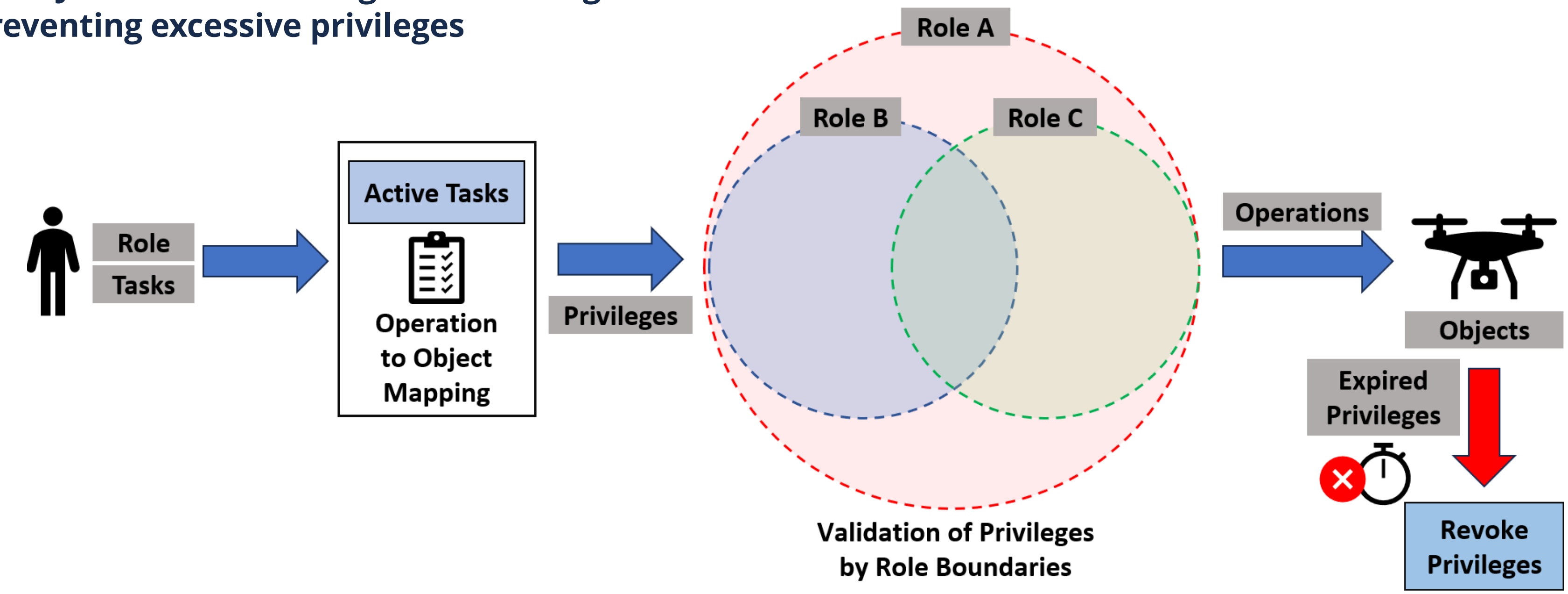
Classifying the modeled threats based on the attack impact they cause on the Tactical Warfighting Edge and mapping them onto the **DDIL Quadrants** can help better understand their quantifiable impact.



An attack like GPS Spoofing can have impact in multiple ways like disrupting the mission execution as well as causing the drone to lose connectivity to the ground control station.

Task-based Access Control for DDIL Cases

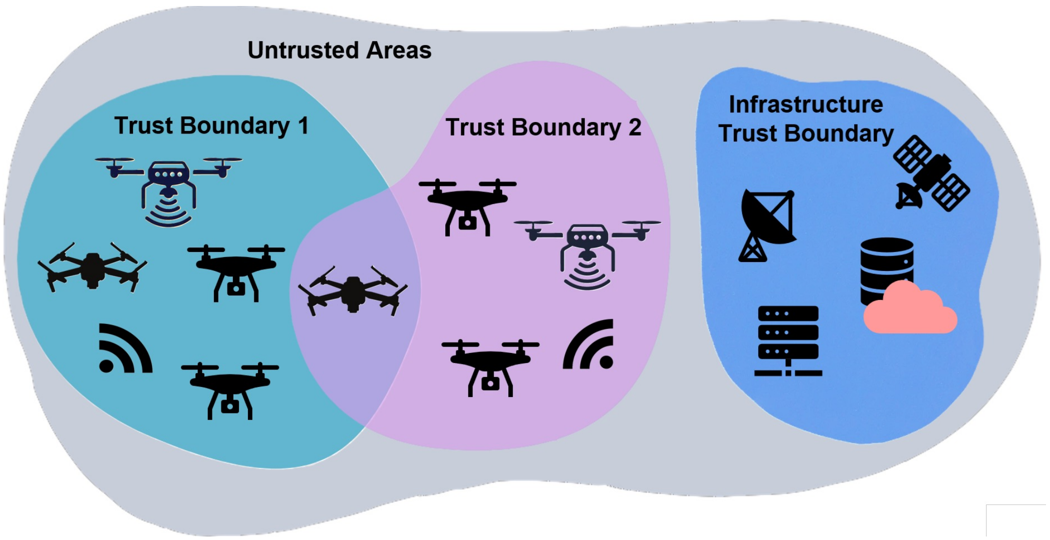
TBAC Just-in-Time Privilege Provisioning preventing excessive privileges



- TBAC on the other hand, considers the **necessity of privileges based on tasks** and the provision of these privileges are **validated by the trust boundary of RBAC** configuration
- Through TBAC configuration, network policies are assigned **Just-in-Time (JIT) access**, ensuring that communication channels remain open only for the duration they are needed, mitigating the causes for excessive privileges

S. Poduvu, R. L. Neupane, A. E. Morel, R. Mitra, V. Anand, R. Chadha, P. Calyam, "Task-Based Access Control for Computation and Communication in the Tactical Warfighting Edge". IEEE Military Communications Conference (MILCOM) 2024.

Trust Boundaries in DDIL Environments



Trust boundary is an imaginary perimeter in a DDIL environment where a set of devices tasked to complete a mission have been vetted, authenticated and provisioned. As devices move between trust boundary's role hierarchies change. Tasks are determined within highly fluid trust boundaries (1 and 2)

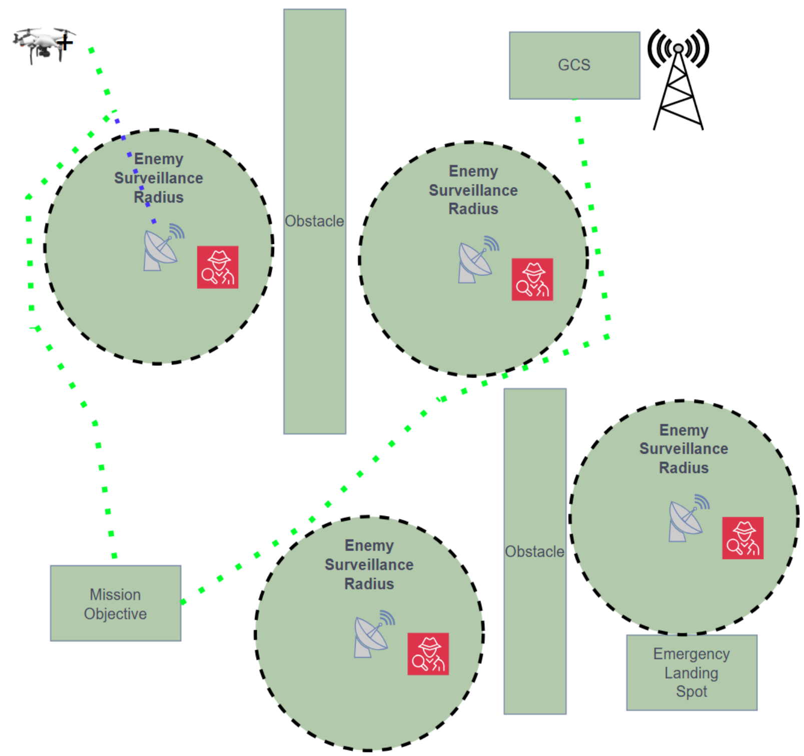
Each trust boundary can implement

- Its own policy of device authentication
- Role hierarchy
- Policy for seeking support from Infrastructure
- Policies of data movement within the boundary, with another trusted boundary and untrusted region

Reinforcement Learning for Drone Guidance

- A novel Intelligent Drone Trajectory Management (IDTM) model to ensure optimal drone trajectory planning in scenarios of lost network connectivity with the GCS
- The drone may choose to:
  - Proceed to complete Mission Objective or,
  - Divert to an emergency landing spot or, Return to the GCS
- IDTM model uses a Reinforcement Learning with a focus on Q-learning to leverage state representations to adapt to uncertain conditions; uses:
  - Drone's position
  - Mission completion status
  - Drone proximity to Enemy Surveillance Zones
  - General drone direction
  - GCS/drone network status

Predictive Model Technologies

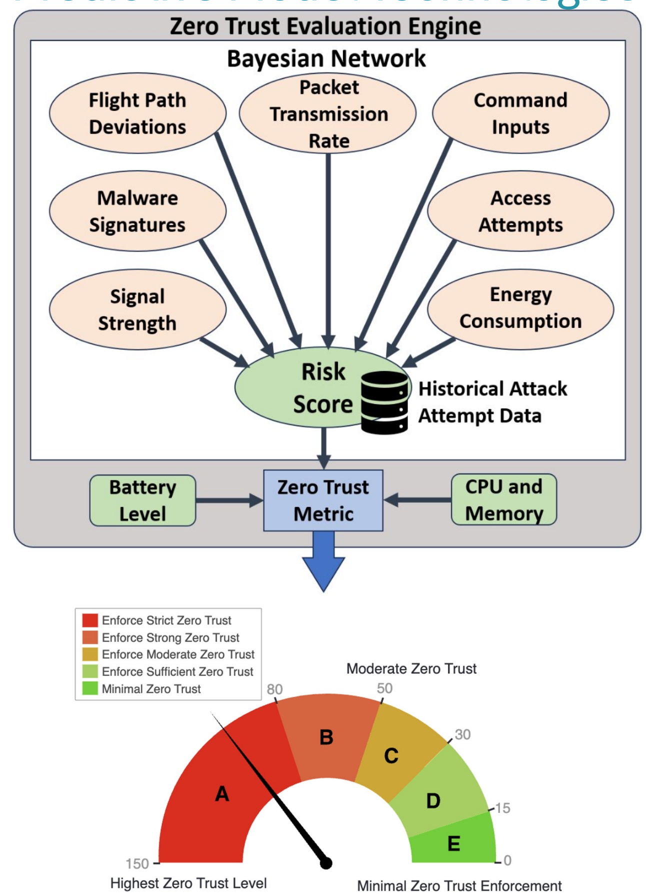


C. Bhamidipati, A. Maxwell, E. Pham, J. Zhang, Z. Murry, A. Morel, C. Qu, S. Srinivas, P. Calyam, "Q-Learning-Based Dynamic Drone Trajectory Planning in Uncertain Environments", IEEE International Conf. on Computing, Networking and Communications (ICNC), 2025.

Bayesian network for Risk Quantification

- Bayesian network for probabilistic risk scoring that assesses behavioral metrics
- Risk score, onboard battery, TWE resources, etc.
- These values help generate ZT metric to define appropriate security level
(A: Most stringent, E: Most lenient)
- Risk score is computed by considering all possible combinations of states across the input signals
  - such as flight path deviation, packet transmission rate, etc.

Predictive Model Technologies

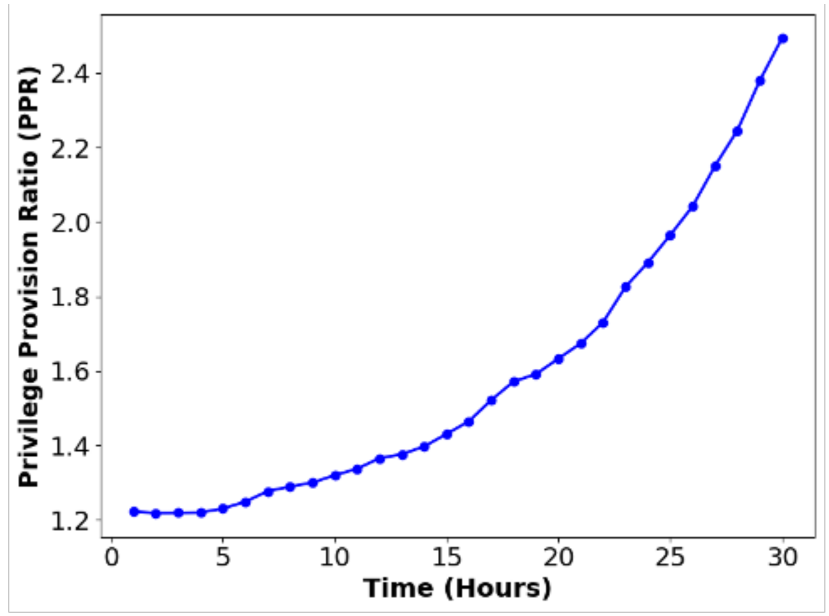


RBAC vs. TBAC Performance Evaluation

- Evaluation of TBAC's efficiency in comparison with RBAC in preventing provisioning of unnecessary privileges under the same device and mission circumstances.

- We introduce Over-provisioned Privilege Percentage (OPP) that calculates the percentage of over-provisioned privileges (RBAC vs TBAC)

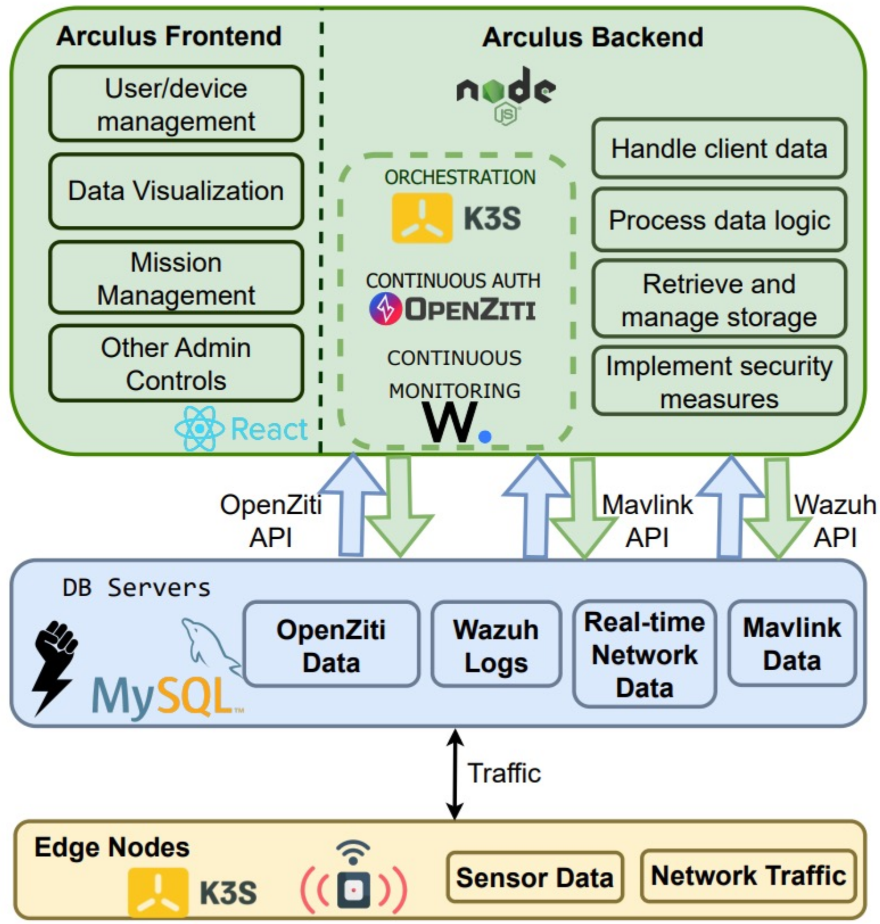
$$OPP = \frac{\sum_{t=0}^{60} P_{RBAC}(t) - \sum_{t=0}^{60} P_{TBAC}(t)}{\sum_{t=0}^{60} P_{TBAC}(t)} \times 100\%$$



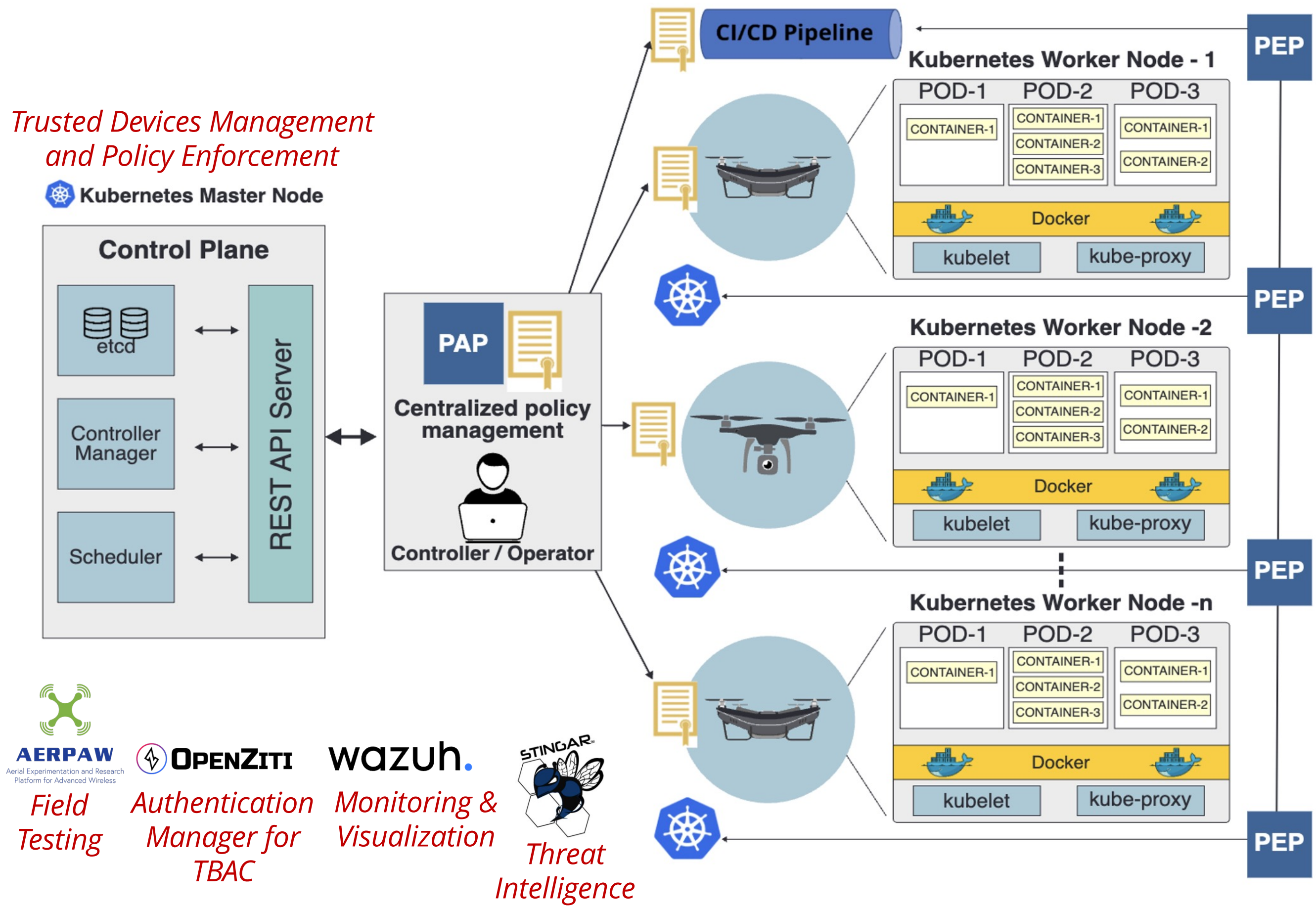
Privilege Provision Ratio (PPR) of RBAC to TBAC over a 30-hour period with gradual addition of new drones.

Technology Stack

- **Integrated Architecture**: Combines frontend user interfaces, backend processing, and edge nodes for seamless data flow
- **Lightweight Orchestration**: Uses K3s for efficient container management and scalability
- **Secure Data Handling**: Implements OpenZiti for authentication, Wazuh for monitoring, and end-to-end encryption
- **Edge and Centralized Systems**: Real-time data processing at edge nodes with centralized logging and analytics
- **APIs**: Facilitates secure communication and integration across components

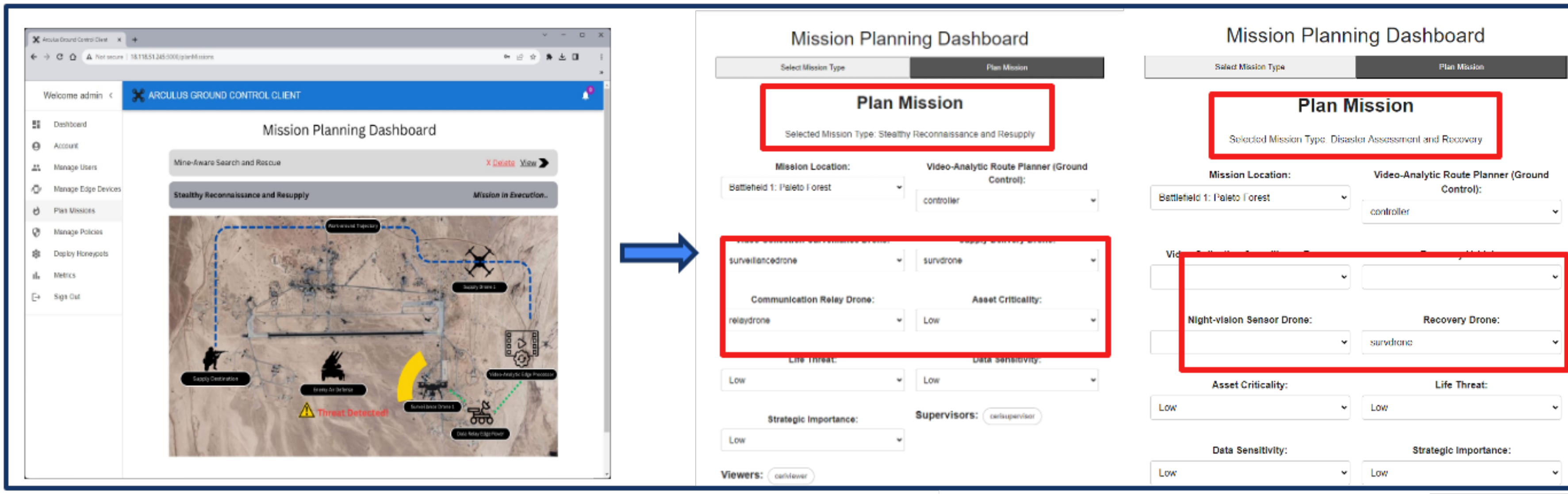


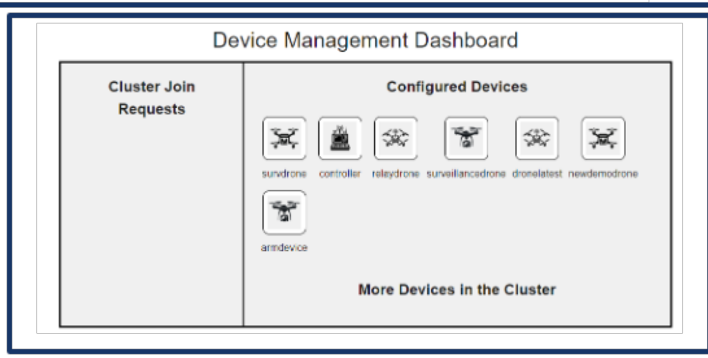
Arculus Cloud/Hardware Testbed

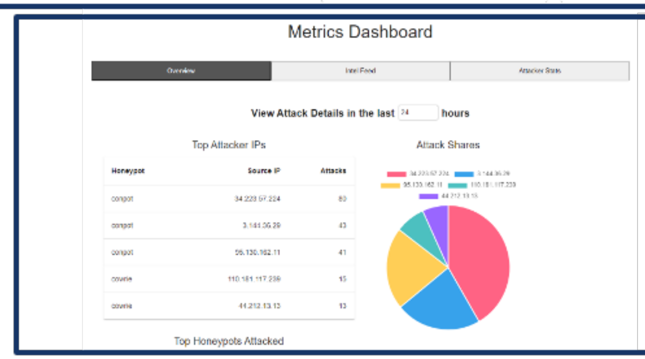


- Used for **Simulation, Field Testing, Hardware-based Experiments**
- **Monitoring methodologies** adapted for programmable network services deployment and their management, including credentials/commands used on edge devices (e.g., Raspberry pi)
- **Enforcing low overhead security controls** by using TBAC, MAVLink, & micro-segmentation using Kubernetes (k3s)
- **Integrating Defense by Pretense methodologies** with distributed honeypots that can report intrusion attempts, verify legitimate or misconfiguration actions

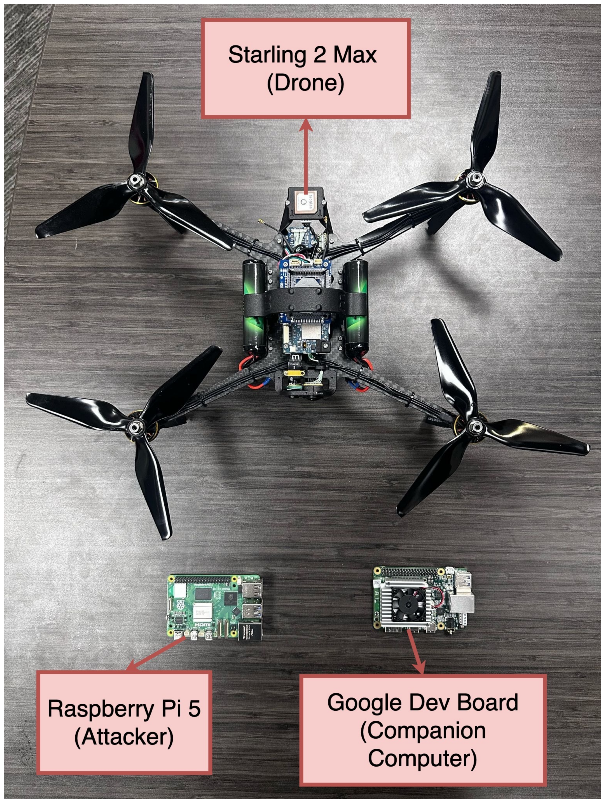
Arculus Simulation Testbed

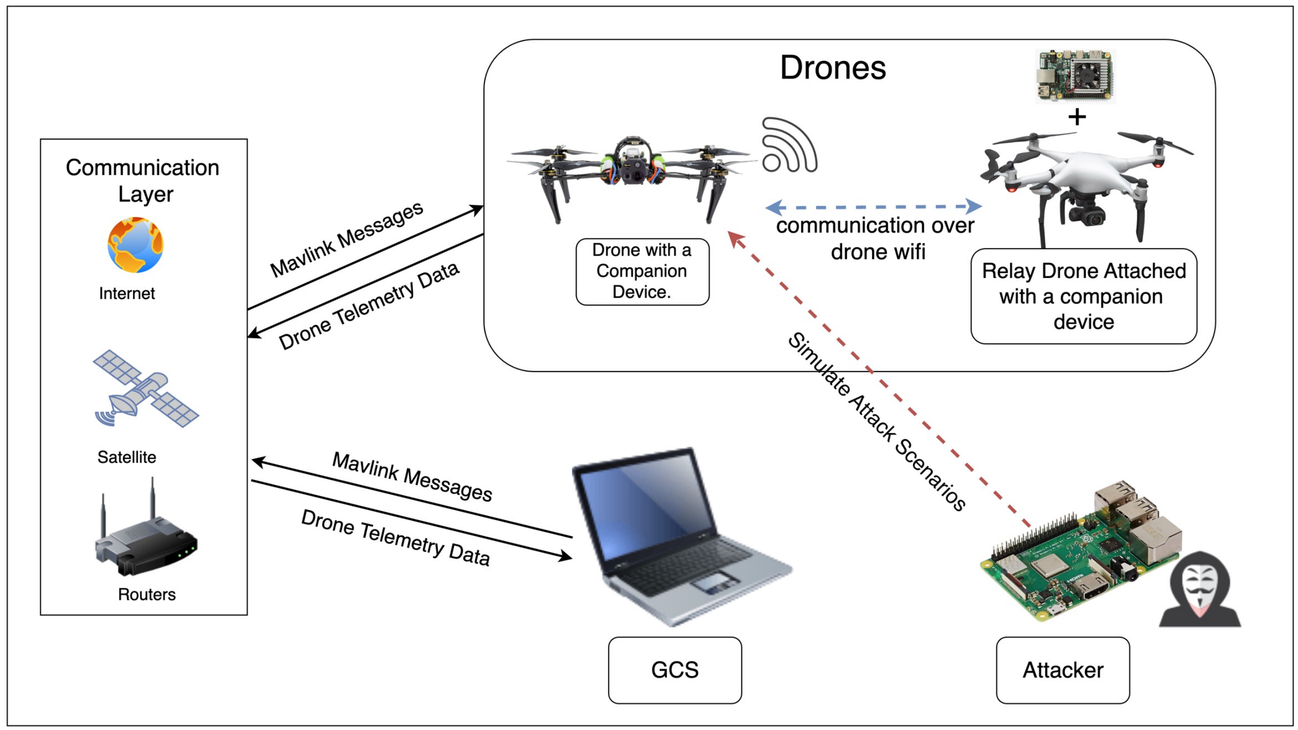




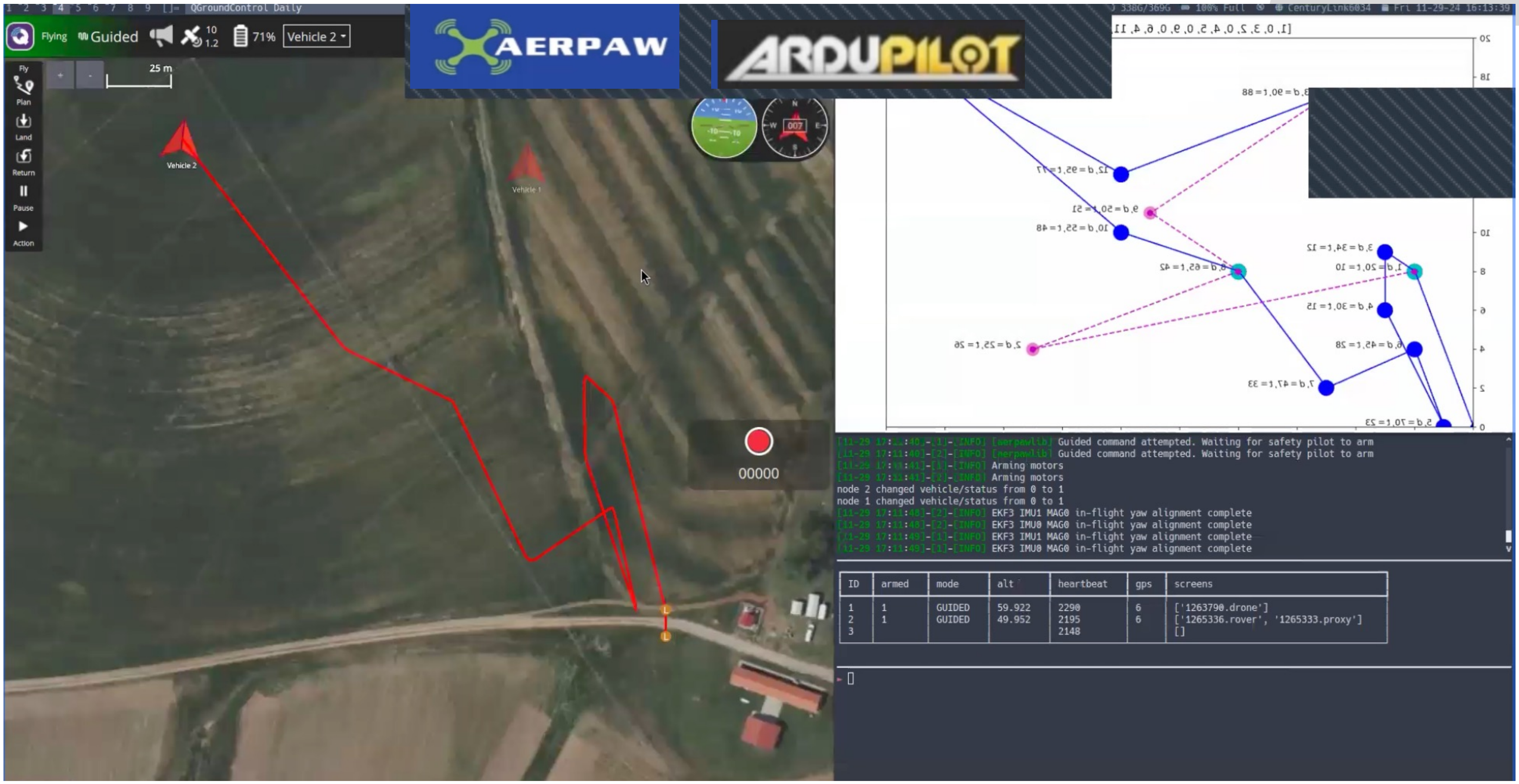


Arculus Physical Hardware Testbed

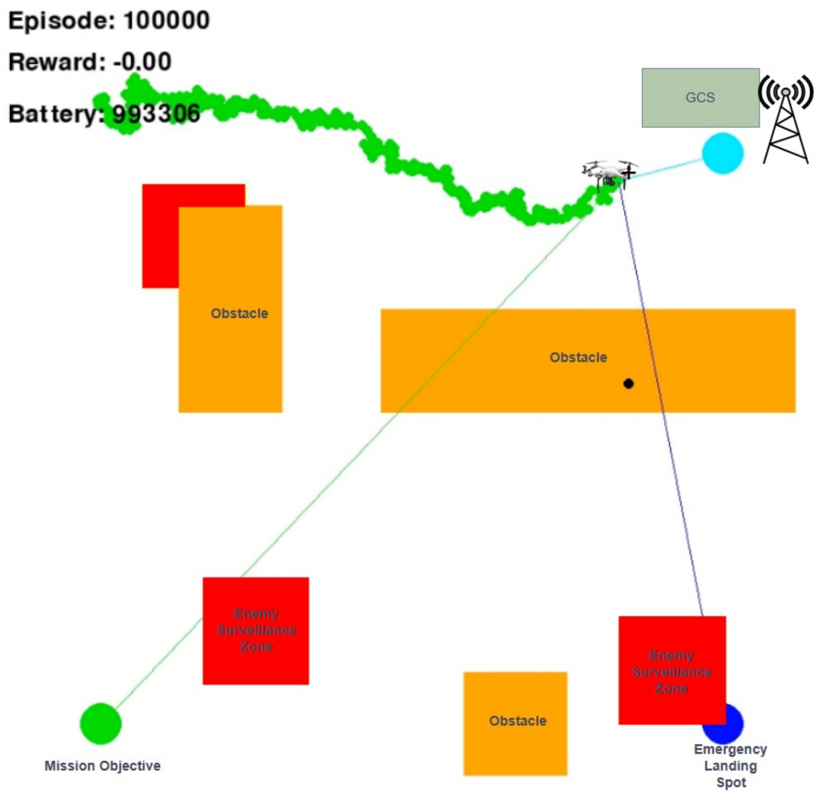




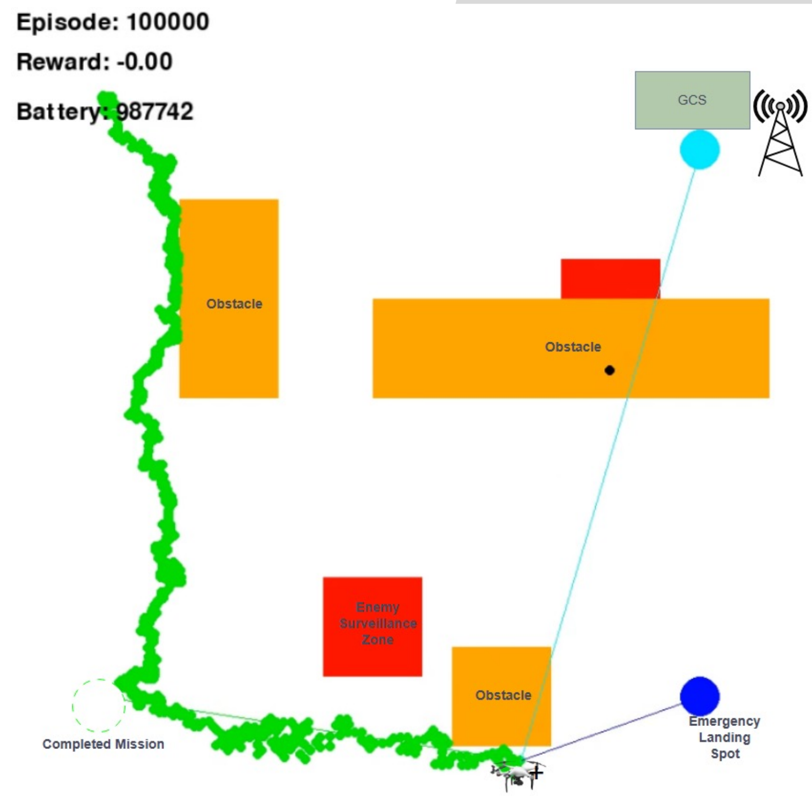
Mission Adaptation to ensure Data Integrity



IDTM: Safety First vs Mission First with Reward Tuning



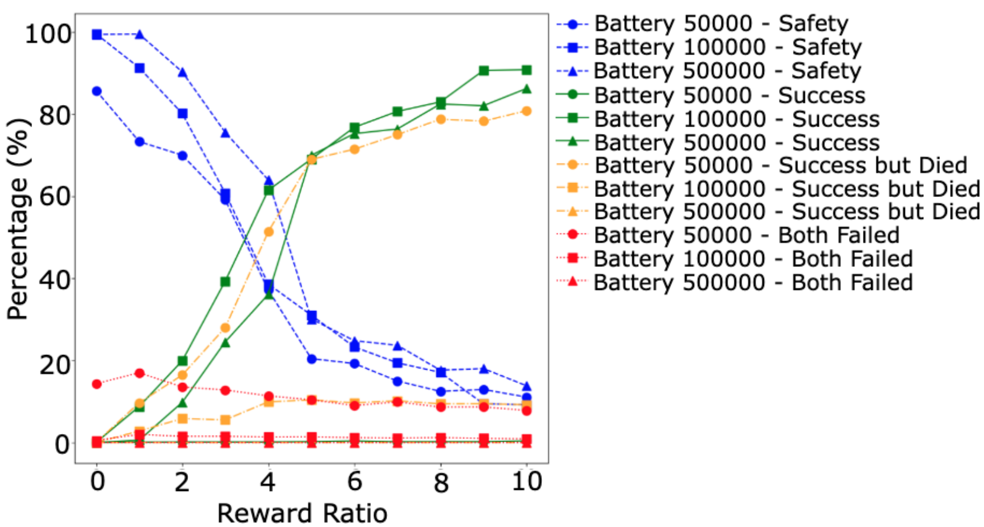
Safety First *approach, where the drone decides to land safely abandoning the mission*



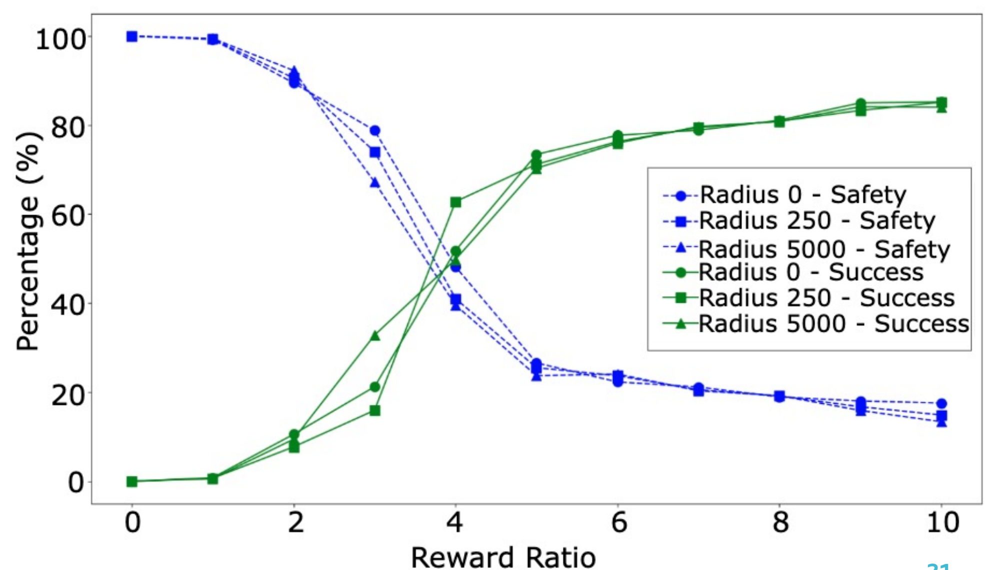
Mission First *approach, where the drone decides to complete mission and then head for Emergency Landing Spot*

Evaluation of IDTM Model

- *Mission Success Rate* and *Survivability* under different battery levels and trust zone radii
- Higher reward ratios incentivize drone to prioritize mission success, potentially at the expense of safety
- Categorize mission outcomes into *Safety, Success, Success but Died, Both Failed*
- Observation –
  - Increasing battery capacity and trust zone radii enhances mission performance and survivability.
  - Lower Configurations force trade offs between safety and mission success

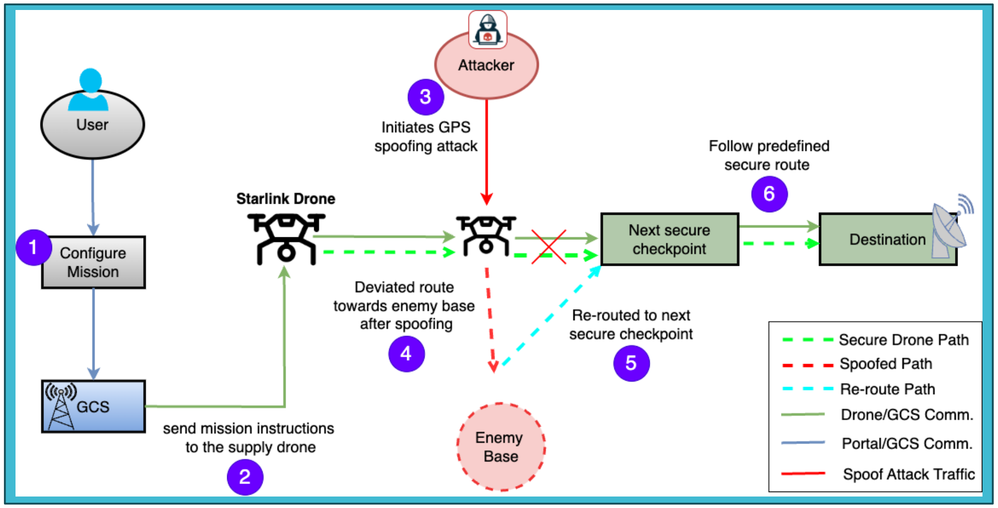


Impact of battery levels on drone success and safety.



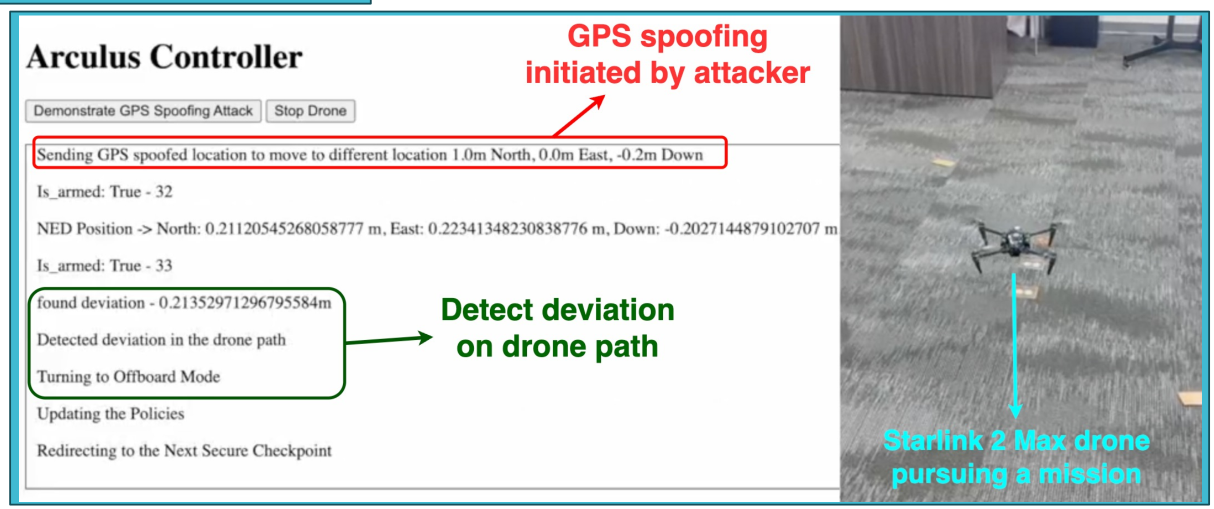
Impact of trust zone radii on drone success and safety.

TWE Attack Scenario: Drone under GPS Spoofing

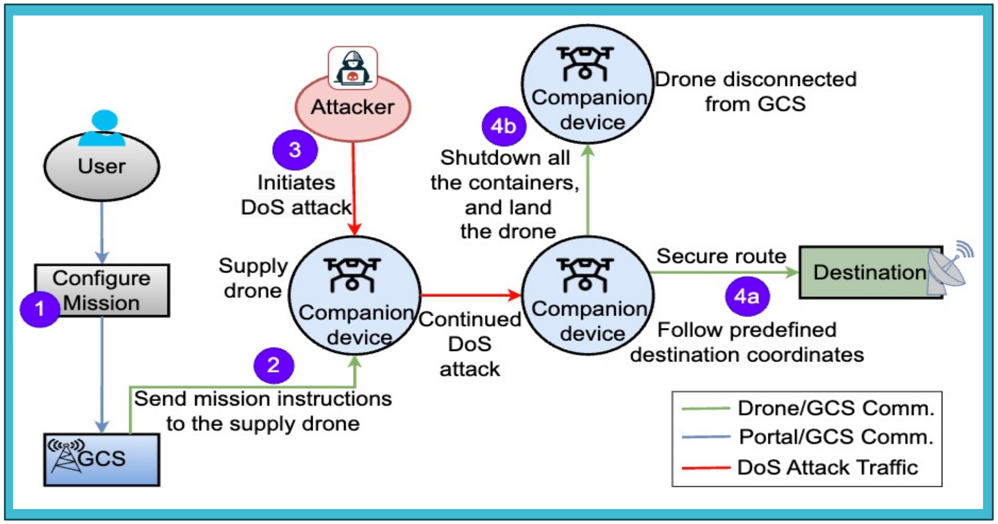


Drone mission scenario flow under GPS spoofing

Hardware Experimentation using Starlink 2 Max Drone for GPS Spoofing Detection and Mitigation via Drone Path Adaptation

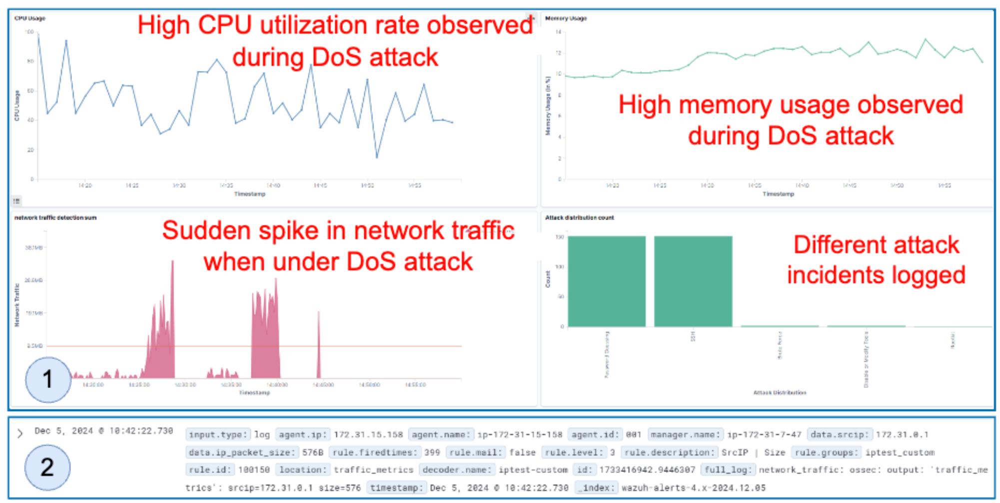


TWE Attack Scenario: Drone under DDOS



Drone mission scenario flow under DDoS attack

SIEM agent monitoring anomaly events for using mitigative measures to block attacker's IP using OpenZiti (1: visualization; 2: raw logs)



Conclusion

- Presented a novel low-overhead zero trust reference architecture to move defense strategies away from static network perimeters, and focus on users, assets, and resources at the TWE
- Presented an AI-driven predictive model featuring Reinforcement learning-based Intelligent Drone Trajectory Planning (IDTM) for safe mission recovery under adversarial threat related incidents
- Discussed software stack developed following the ZT reference architecture and hardware testbed configuration for showcasing mission under normal operation and under attack scenarios

Future directions

- Automating ZT with seamless control - Design effective feedback based on dynamic ZT score calculation as per battlefield situation, mission goals and device resource constraints
- Standardize the mission planning framework to make it adaptable to other critical mission types with heterogeneous devices (x86, ARM) and develop user guides for training and operations

University of Missouri

Mizzou CERI

Center for Cyber Education, Research & Infrastructure

Thanks for your attention!

Any questions?

Contact: Prof. Prasad Calyam (PI)
(calyamp@missouri.edu)
Department of Electrical Engineering and Computer Science,
University of Missouri-Columbia