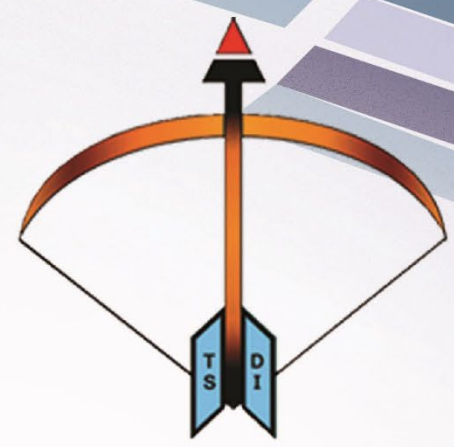




Temasek Defence Systems Institute

# Temasek Defence Systems Institute

## Resilience of Data Distribution Service (DDS) in the face of simulated cybersecurity threats in an Unmanned Systems Network

Author: Chee Xiang Sheng

Thesis advisor: Dr. Preetha Thulasiraman

Co-advisors: Dr. James Calusdian

### Background:

- Data Distribution Service (DDS) is a vital communication middleware used in unmanned systems networks.
- Growing reliance on unmanned systems increases cybersecurity risks.
- Adapted Network Architecture from previous student evaluating DDS performance of an unmanned system network

### Objectives:

- Assess DDS's ability to withstand simulated cyber attacks in a controlled environment.
- Identify potential vulnerabilities and weaknesses in DDS under attack scenarios.
- Contribute to the development of more robust and secure communication for unmanned networks.

### DDoS Attack Results:

- Throughput degradation: 6.67% to 46.67% decrease.
- Significant latency increase: 163.26% to 455k% increase.
- Loss rate increase for BEST EFFORT QoS: 1% increase.

### Data Extraction Attack Results:

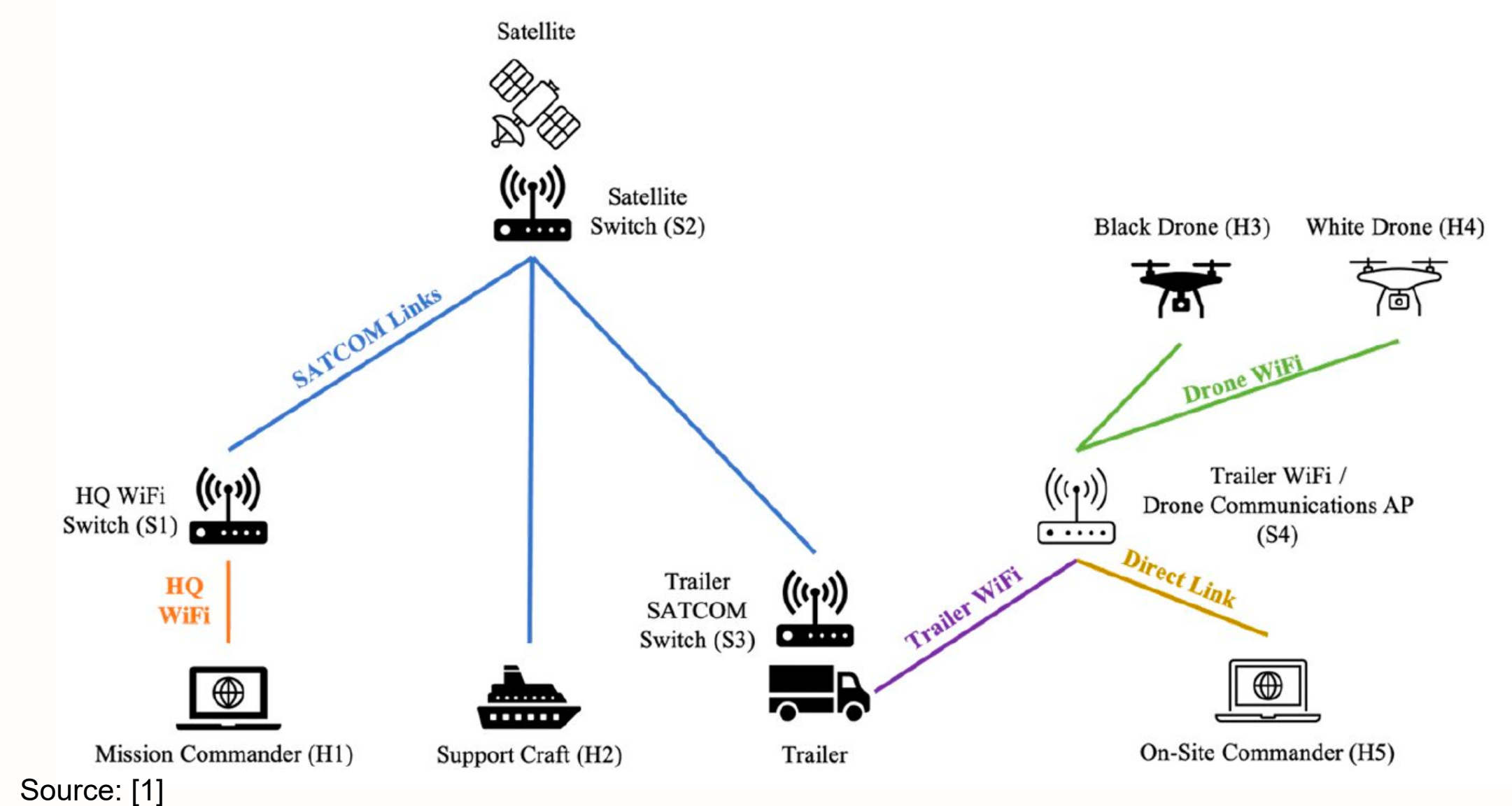
- Throughput degradation: Up to 50% decrease.
- Latency increase: Approximately 1.5 times the baseline.
- No packet loss due to RELIABLE QoS.

### Data Injection Attack Results:

- Latency increase:
  - WiFi links: Approximately 100% increase
  - Hybrid links: 6.61% to 7.73% increase
- Loss rate increase for BEST EFFORT QoS: 0.53% increase
- No packet loss for RELIABLE QoS

### Future work:

- Explore advanced anomaly detection systems tailored to DDS
- Investigate the impact of attacks on larger DDS networks,
- Explore security enhancements for DDS.



### Methodology:

- **DDoS Attack Simulation:** Implementation of UDP Flood to attack network.
- **Data Extraction Attack Simulation:** Implementation of data copying on active links.
- **Data Injection Attack Simulation:** Implementation of injecting malicious traffic to victims.
- **Data Collection and Analysis:** Monitoring and recording of DDS network performance metrics during attacks.
- **Security Enhancement Proposal:** Development of practical and ethical security solutions based on the results.

| Distributed Denial of Service (DDoS)                                                                                                                | Data Extraction                                                                                                                                          | Data Injection                                                                                                                                          |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                     |                                                                                                                                                          |                                                                                                                                                         |
| <ul style="list-style-type: none"><li>• Floods the network with malicious traffic to disrupt communication and overwhelm system resources</li></ul> | <ul style="list-style-type: none"><li>• Simulated unauthorized access and extraction of sensitive data to assess the impact on network quality</li></ul> | <ul style="list-style-type: none"><li>• Injected malicious traffic into network to disrupt operations to assess the impact on network quality</li></ul> |

**Recommendations:** Prioritizing the implementation of robust security measures, such as encryption, authentication, and access control, in DDS-based systems to mitigate the identified vulnerabilities and enhance the overall resilience of unmanned systems networks against cyber threats.