Zero Trust-based Collaborative Drone System with Intelligence-driven Edge Routing

*Cameron Grant, **Samuel Elfrink, †Alicia Esquivel, †Ekincan Ufuktepe, †Kannappan Palaniappan, †Prasad Calyam

* University of Georgia, ** Southeast Missouri State University, †University of Missouri-Columbia

Problem and Motivation

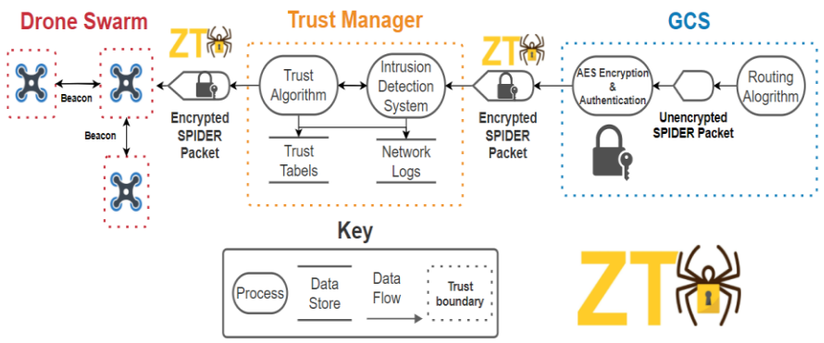
- Drone swarms provide efficient and reliable packet data transmission (e.g., disaster incident response)
- It is important to have reliable security that works in spite of limited energy and computational resources on drones

Problem: Create a security framework for collaborative drone systems with intelligence-driven edge routing

Solution and Novelty

- We propose a novel security architecture that is energy efficient featuring a trust manager in a ground control station

- **Novelty**: Trust is never granted implicitly but must be continually evaluated via the concept of **"Zero Trust"** [2]
  >> All device communication in the network is encrypted and authenticated to ensure confidentiality and integrity

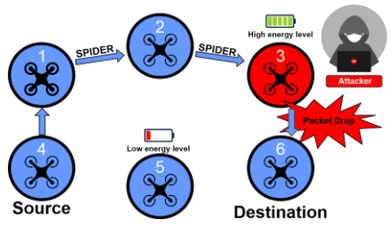


- Our work builds on SPIDER [1] geographic routing, and our simulations are performed in the Network Simulator (NS-3)

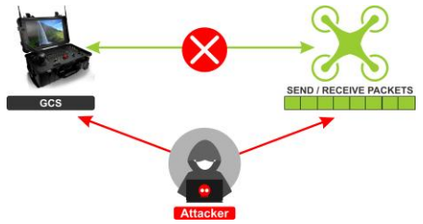
- We formulate a threat model based on SPIDER communications and handle overheads in Zero Trust implementation

Vulnerability Analysis

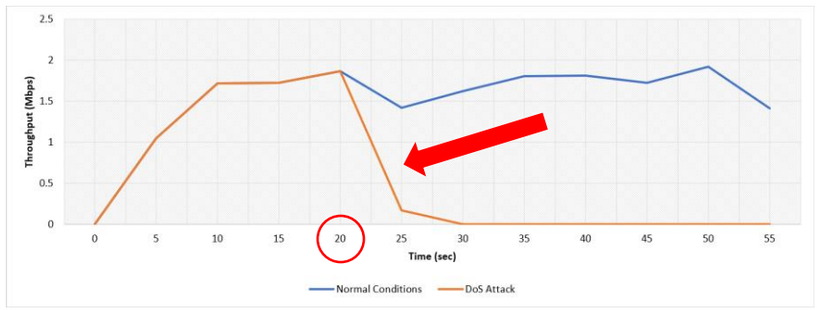
Blackhole Attack: malicious node claims to have high energy to attract packets from other nodes and then drops packets that are received



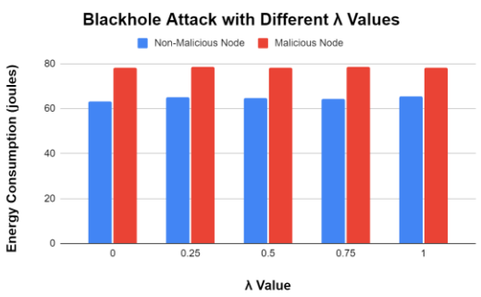
Man-in-the-Middle: packets being sent are intercepted and modified by an attacker in order to change packet data such as drone location or images/footage



DoS Attack: The figure below shows a comparison of the simulation's throughput during normal conditions vs a DoS attack starting at 20 seconds with no security implementation



- The λ value determines different routing policies in the SPIDER algorithm



- The simulation shows that malicious nodes in a blackhole attack expend more energy than non-malicious nodes, indicating that the routing protocol prefers to send packets through the blackhole node over the non-malicious nodes.

Threat Model

We identified network level vulnerabilities of geographic routing protocols and implemented various cyber-attacks as follows:

Threat	Property Violated	Threat Definition	Typical Victims	Detection	Prevention
Tampering	**Integrity** Ex: Changing the contents of a packet to misinform a drone	Modifying something on a drive, network, or memory	Packets in transmission, system logs, data storage	Message Authentication Code	Trace packet route to identify which node changed the packet and blacklist it
Denial of Service	**Availability** Ex: Flooding the ground station with UDP packets	Absorbing resources needed to provide service	Ports on drones, trust manager, and control station	Intrusion detection system with packet threshold limit	Identify the offending node and blacklist it

Conclusion & Future work

- We demonstrated vulnerabilities within geographic routing protocols for multi-drone systems and developed a security framework that handles resource constraints

- **Future Work:** Experiments can be conducted to test the overheads of zero-trust implementation and design defense for attacks outside of the network level, such as GPS jamming and spoofing attacks as well as probing attacks

References

[1] H. Trinh et al. "Energy-Aware Mobile Edge Computing and Routing for Low-Latency Visual Data Processing," in IEEE Transactions on Multimedia, vol. 20, no. 10, pp. 2562-2577, Oct. 2018.

[2] Kerman, Alper, Oliver Borchert, Scott Rose, and Allen Tan. Implementing a Zero Trust Architecture. National Institute of Standards and Technology, 2020.

Special thanks to our mentors Alicia Esquivel, Ekincan Ufuktepe, Kannappan Palaniappan and Prasad Calyam. This material is based upon work supported by the National Science Foundation under Award Number: CNS-1950873. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.