DIAT: Data Integrity Attestation for Resilient Collaboration of Autonomous Systems

Tigist Abera, Raad Bahmani, Ferdinand Brasser, Ahmad Ibrahim, Ahmad-Reza Sadeghi, and Matthias Schunter

Introduction

- Autonomous collaborative embedded systems are increasing every year
  - Ad-hoc networks including: vehicles, factory robots, drones, etc
  - Networks working together to perform a task
  - Networks are homogeneous devices
  - Devices form meshed network
- Hard to secure ad-hoc collaborative networks from attacks
  - Data received from compromised device in network may be malicious
  - No central authority to coordinate actions or security
- Security questions DIAT attempts to answer for autonomous collaboration:
  - How were the data generated?
  - How were the data processed?
- Collaboration requires data integrity
  - Sensor data, status information, commands exchanged between devices must be trusted

Concepts

- Remote attestation
  - Verifier, remote entity, verifies integrity of software running on untrusted device
  - Untrusted device called prover
- Conventional control flow attestation
  - Allows verifier to detect attacks that do not conform to program’s control-flow graph
    - Like return-oriented programming (ROP)
    - Also unintended program execution meaning non-control data attacks
  - Needs huge database of execution paths to compare prover attestation against
    - Very expensive
  - Tracks each loop iteration

DIAT Claims/Contributions

- Secure collaborative data-flow integrity through run-time attestation
  - Operations on data and variables conform to program’s data-flow graph
  - Data shared across devices attestable
- Efficiency gains
  - Software decomposed into small interacting modules
  - Control flow of the small modules attestable
  - Smaller size reduces control-flow graph size thus reducing search costs and total overhead
  - Control-flow attestation has linear overhead

Assumptions

- Adversary is stealthy
  - Denial-of-service, physical attacks, non-control data attacks are not considered
    - DIAT could potentially be adapted to prevent non-control data attacks
  - Adversary wants to affect collaborative task by manipulating data on a compromised device
- Trusted Computing Base
  - Hardware attacks are out of scope
  - All software, including OS, is considered potentially compromised
  - Sensors are trusted
    - Attacks like spoofed GPS signals are not considered
  - Attestor is part of TCB
    - Attestor is composed of DFMonitor and CFMonitors
- DIAT works in conjunction with data execution prevention (DEP)
  - DEP prevents code injections

Example Task

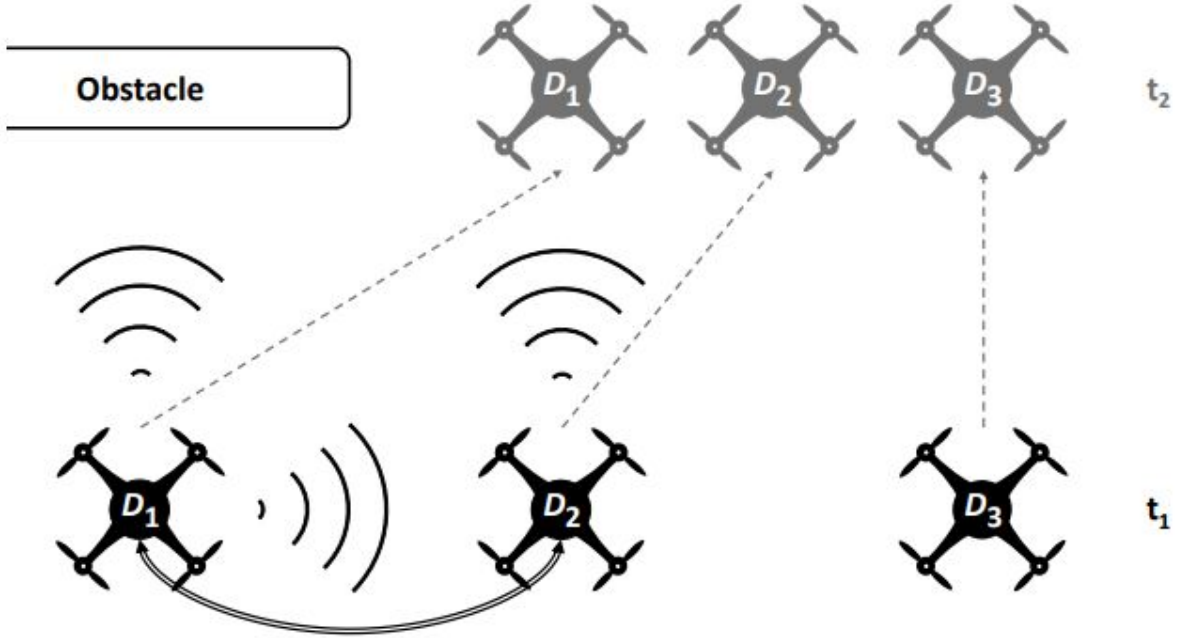


Figure 2: Example of collaborative drones.

Design

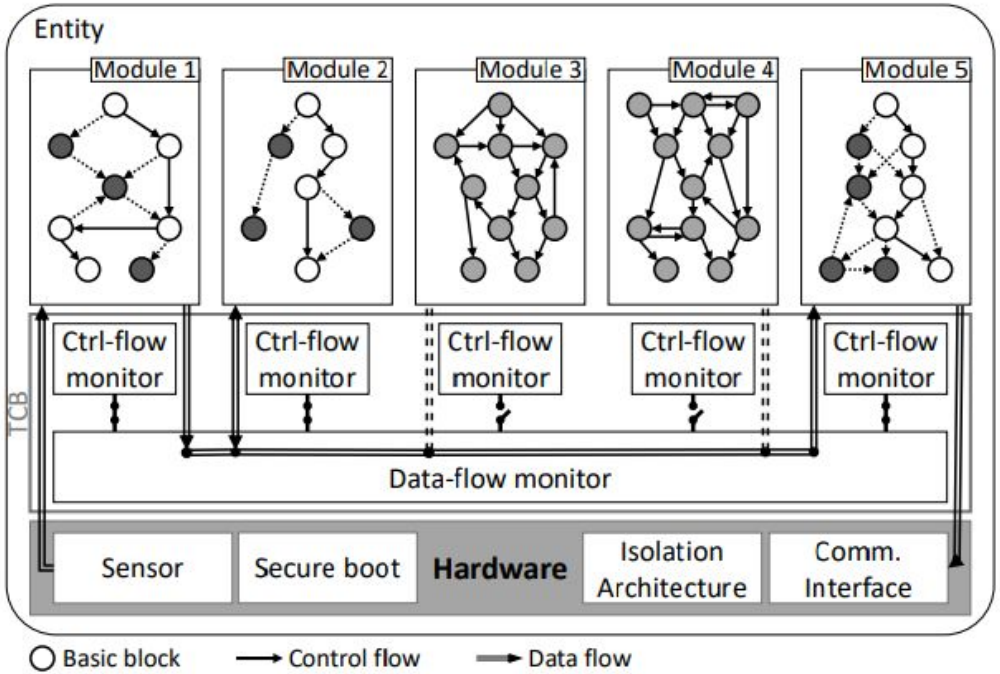


Figure 3: DIAT system architecture. Closed switches symbolize activation of control-flow monitoring.

Design

- Only protect what has be explicitly selected
  - Only critical modules and data
    - Critical modules determined at runtime and are task dependant
    - Determined by DFMoniter
  - Protection is expensive
- Software modules are isolated from all other software components
  - Reduces control-flow complexity
- Communication between modules only allowed through DFMoniter
- Multiset hash represents execution path
  - Under-approximation of path
  - More expensive than traditional hash but worth it
    - Small size for impressive network communication overhead

Interaction

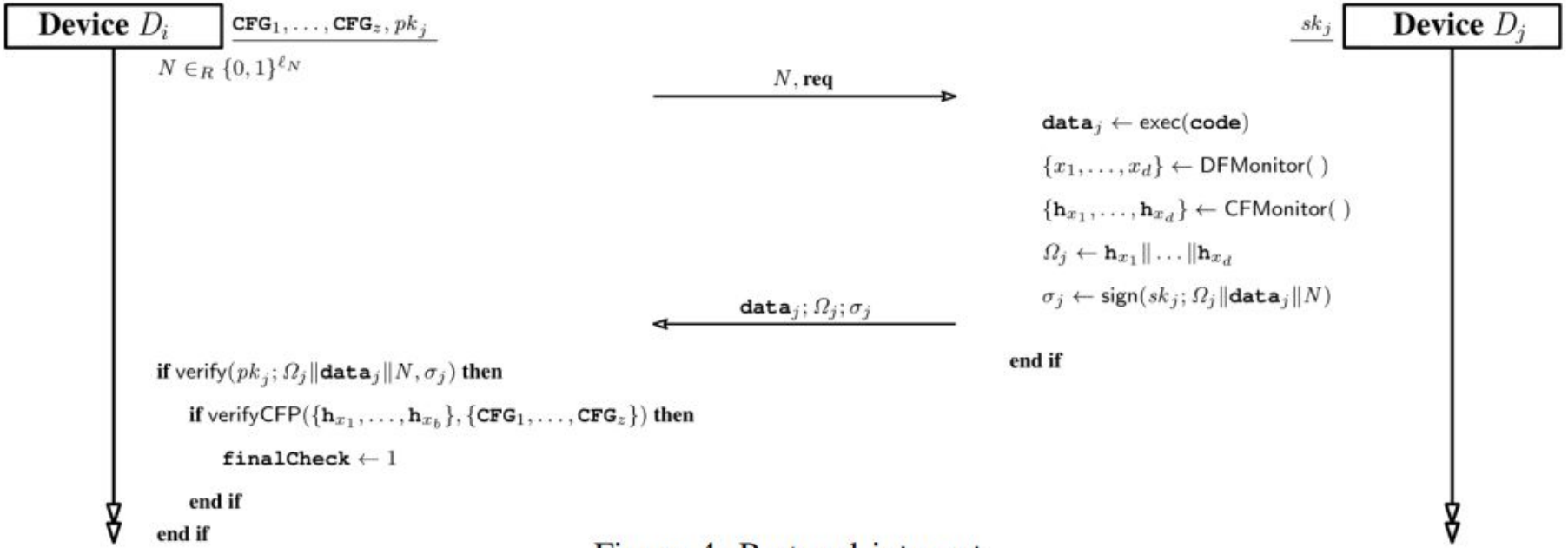


Figure 4: Protocol interact

Implementation

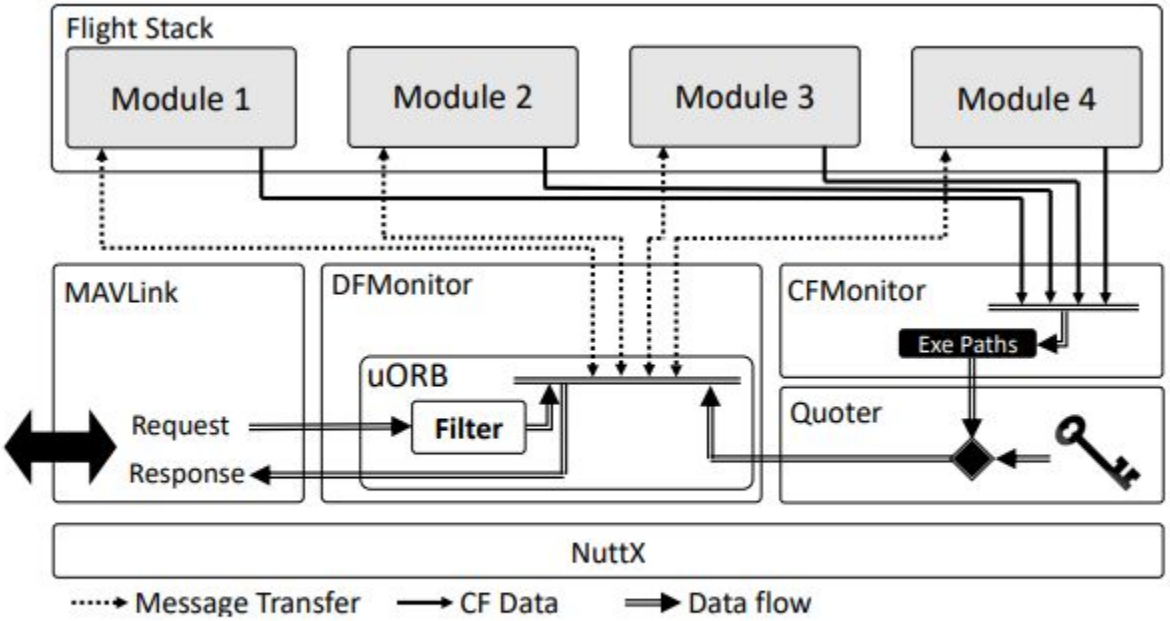


Figure 7: DIAT Implementation

Implementation

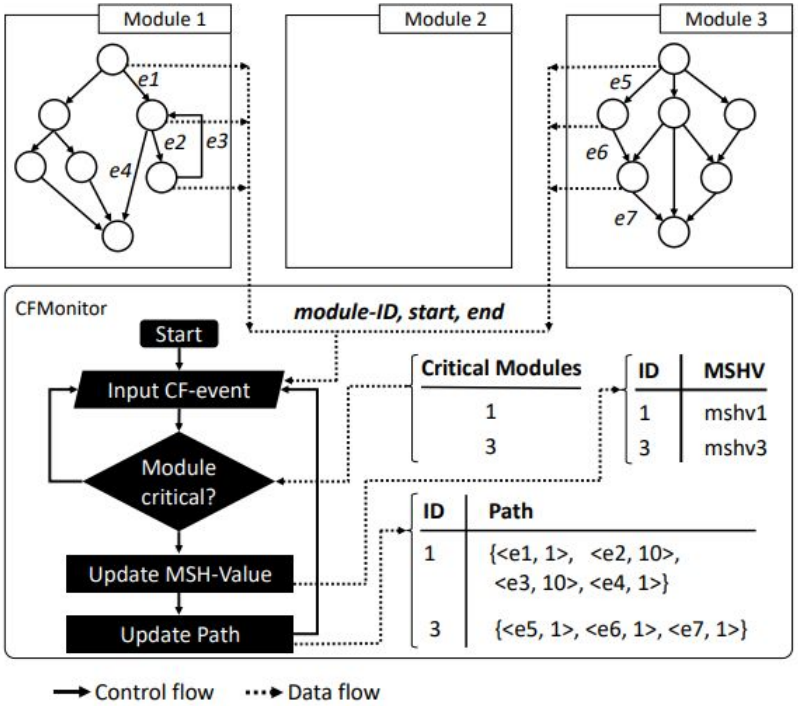
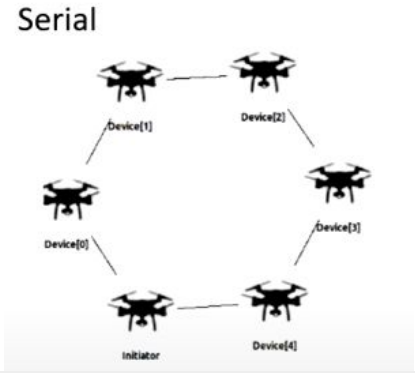
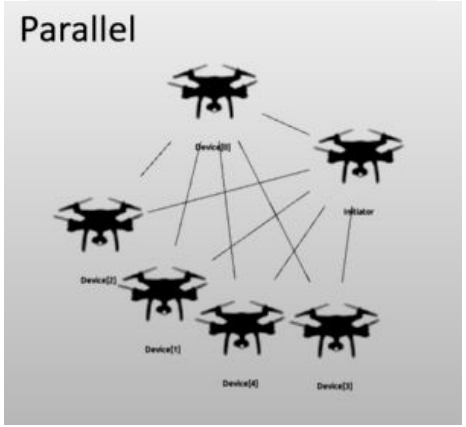
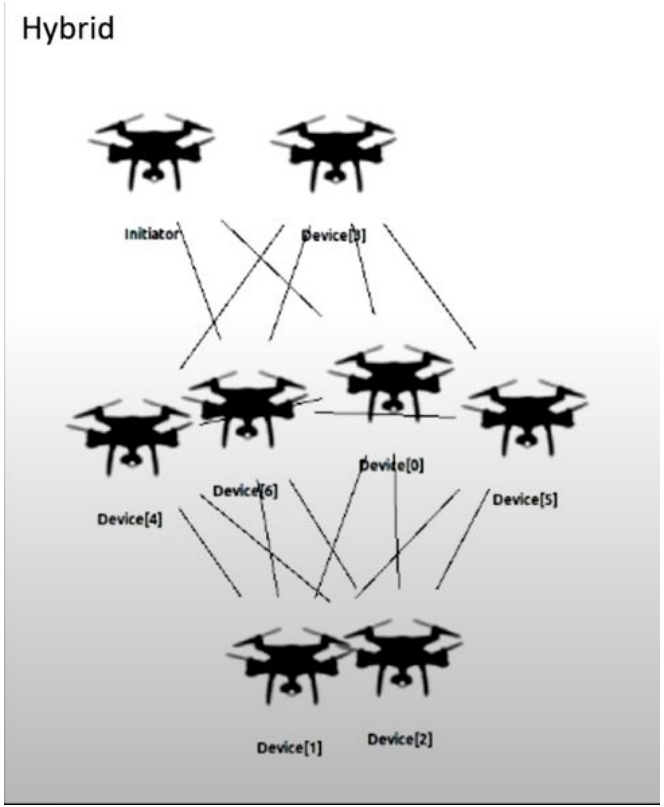


Figure 6: CFMonitor Logic

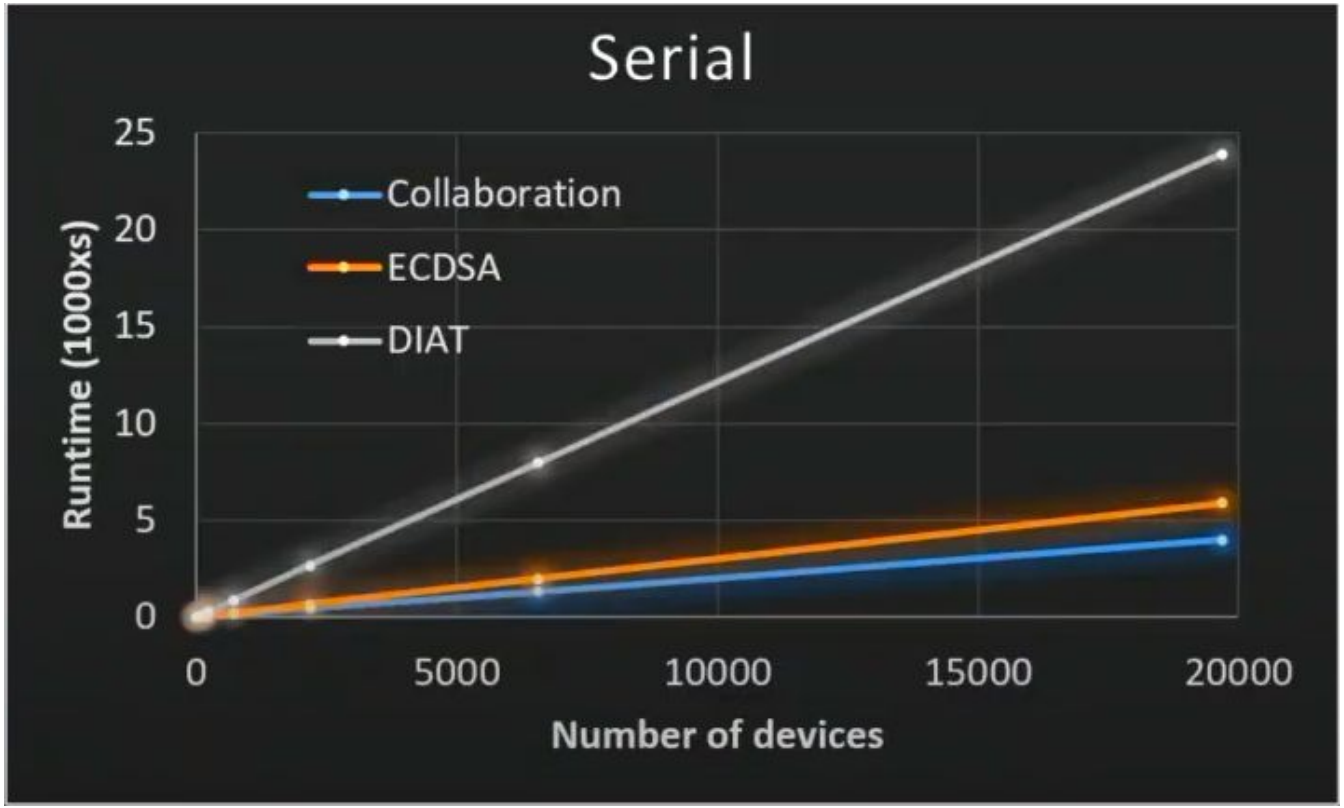
Simulation


Serial
Device[1]
Device[2]
Device[0]
Device[3]
Initiator
Device[4]

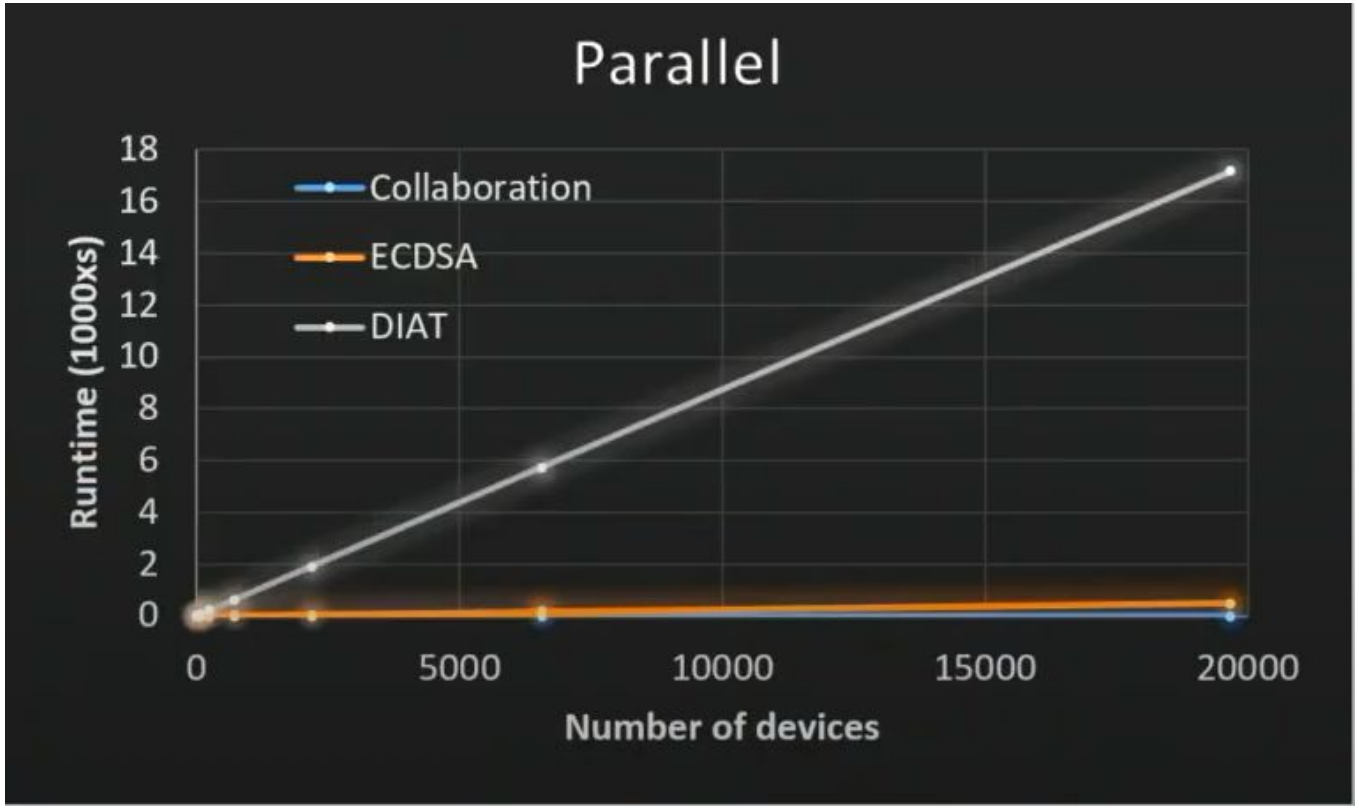

Parallel
Initiator


Hybrid
Initiator
Device[3]
Device[0]
Device[6]
Device[4]
Device[5]
Device[1]
Device[2]

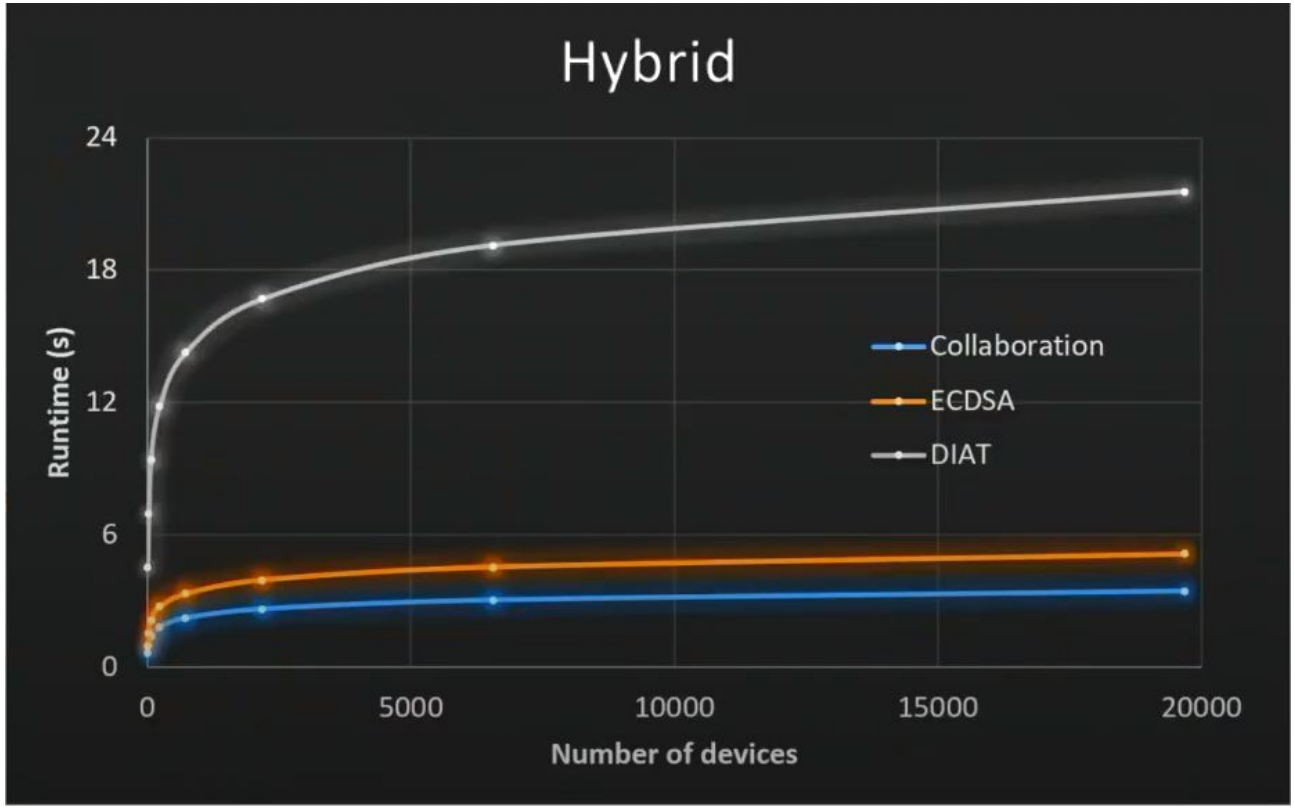
Simulation


Serial
Runtime (1000xs)
25
20
15
10
5
0
Collaboration
ECDSA
DIAT
0
5000
10000
15000
20000
Number of devices

Simulation


Parallel
Runtime (1000xs)
18
16
14
12
10
8
6
4
2
0
Collaboration
ECDSA
DIAT
0
5000
10000
15000
20000
Number of devices

Simulation


Hybrid
24
18
12
6
0
Runtime (s)
0
5000
10000
15000
20000
Number of devices
Collaboration
ECDSA
DIAT

Weaknesses

- Does not protect against interrupts or traps
  - These do not affect control flow
  - Disabled by setting, but hard to verify
    - Relevant to future work
- No demonstration of attack detection or prevention
- ‘TCB’ is used nine times before being defined twice on pg. 12
  - And again on pg. 13

Future Thoughts

- Military drone swarms
  - Air Force F-35 costs $148,000,000 (plus inflation)
    - Only 760 produced to date
  - Hypothetical: future military component drone of swarm costs $50,000
    - The cost of a single F-35 could buy 2,960 drones
      - Why is this important? Even inexpensive missiles normally cost $100k+
- Civilian drone fleets
  - How many millions will operate world wide?
- IoT
  - Collaborative networks don’t have to be vehicles
- Collaboration integrity is an absolute necessity