CERIAS

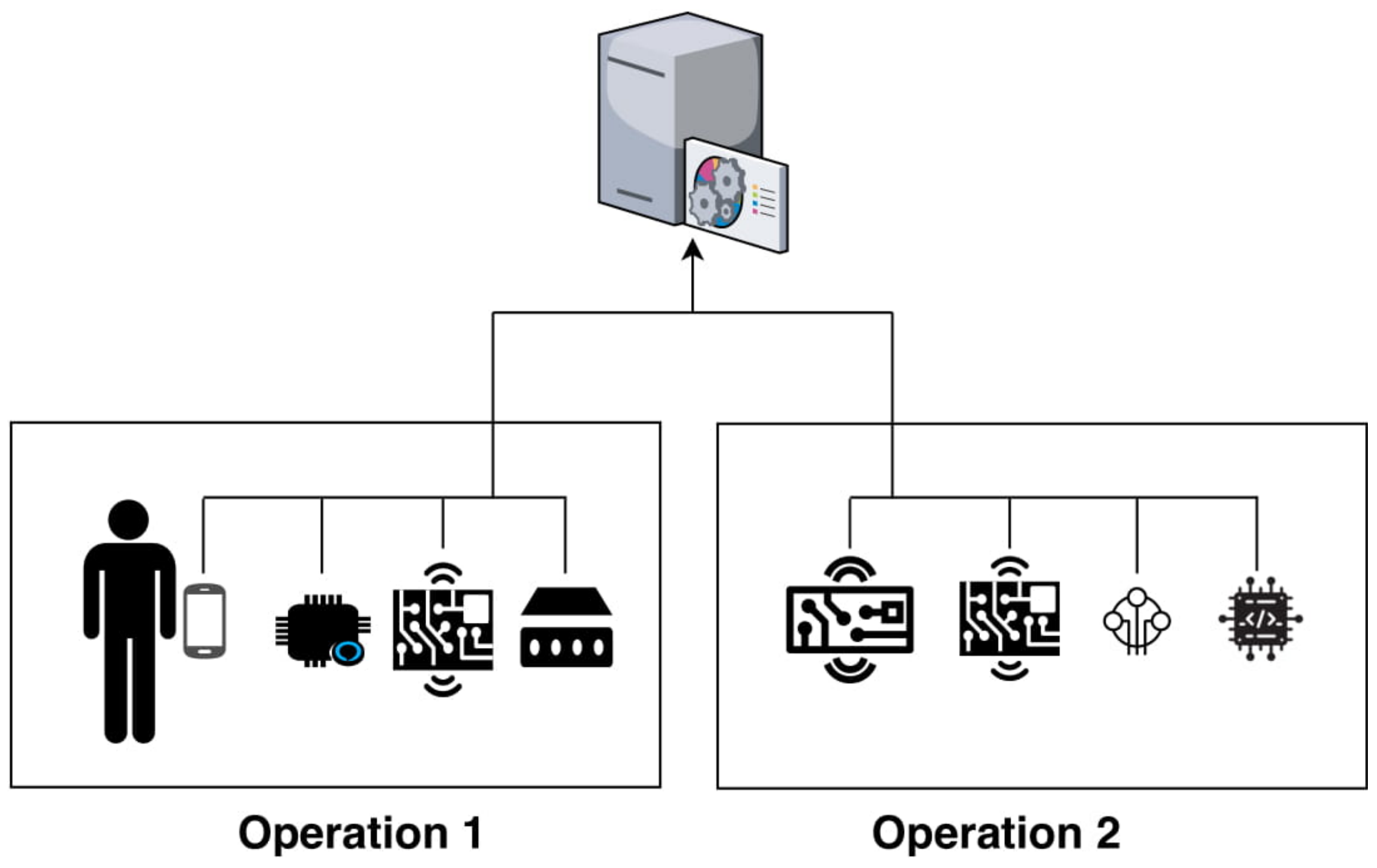
E2C - Energy Efficient Consensus*

Adithya Bhat   Manish Nagaraj   Akhil Bandarupalli   Saurabh Bagchi   Michael K. Reiter   Aniket Kate

The Center for Education and Research in Information Assurance and Security

*This project is funded by the Army Research Lab (ARL)

1. Cyber Physical Systems (CPS)

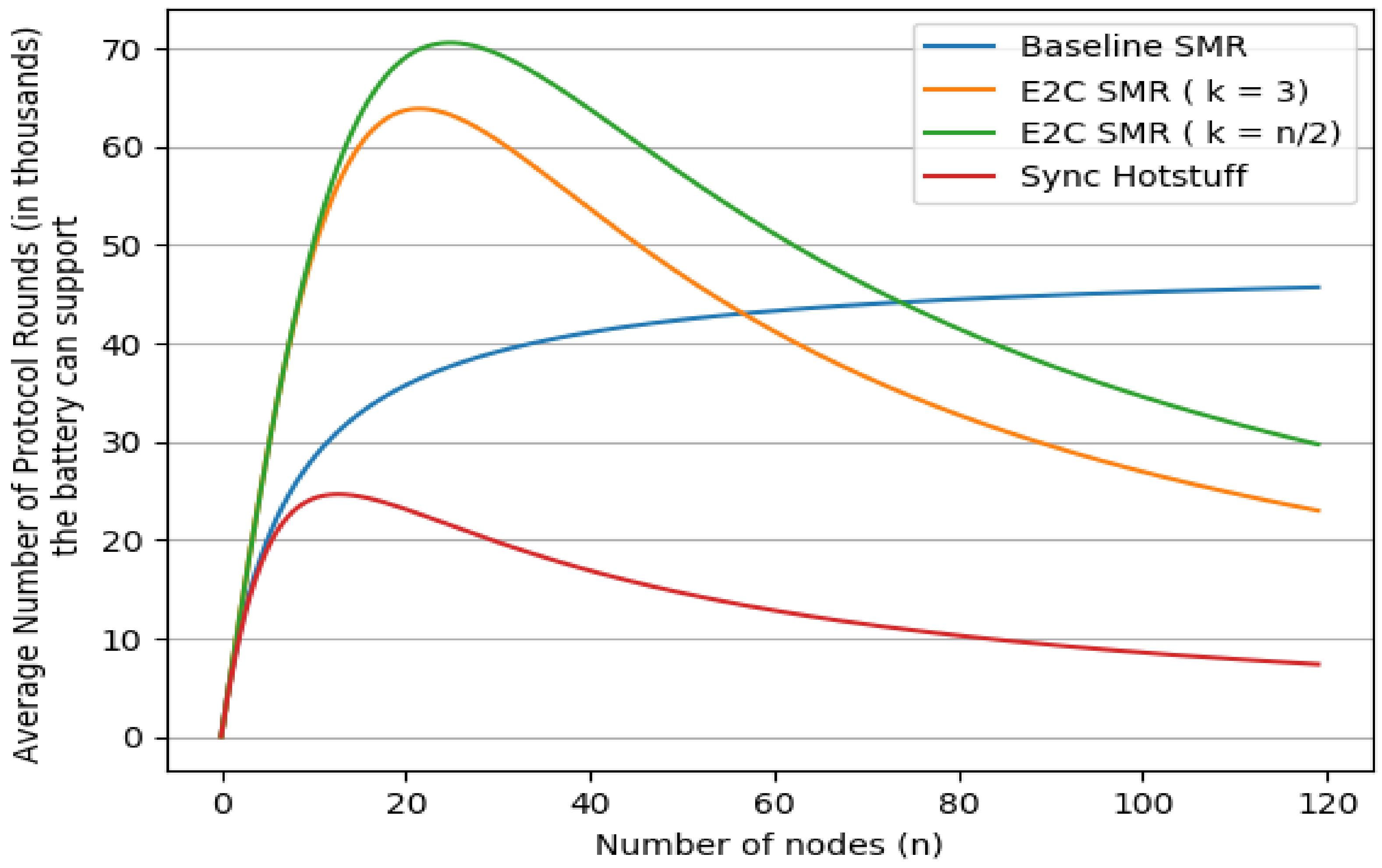


- Often deployed in large-scale defense applications
- Devices need achieve consensus by tolerating byzantine faults
- An energy efficient and optimally resilient state machine replication protocol is necessary in this scenario.

3. Current Protocols do not

- Address energy overheads and fairness
- Assume that adversaries have limited energy resources
- Assume nodes to be heterogenous, have partial network connectivity and have limited computational or energy resources
- Consider network bandwidth limitations
- Address synchronization of sensors/lower tier devices
- Consider the availability of k –cast/local reliable broadcast channels for State Machine Replication

5. Benchmarks



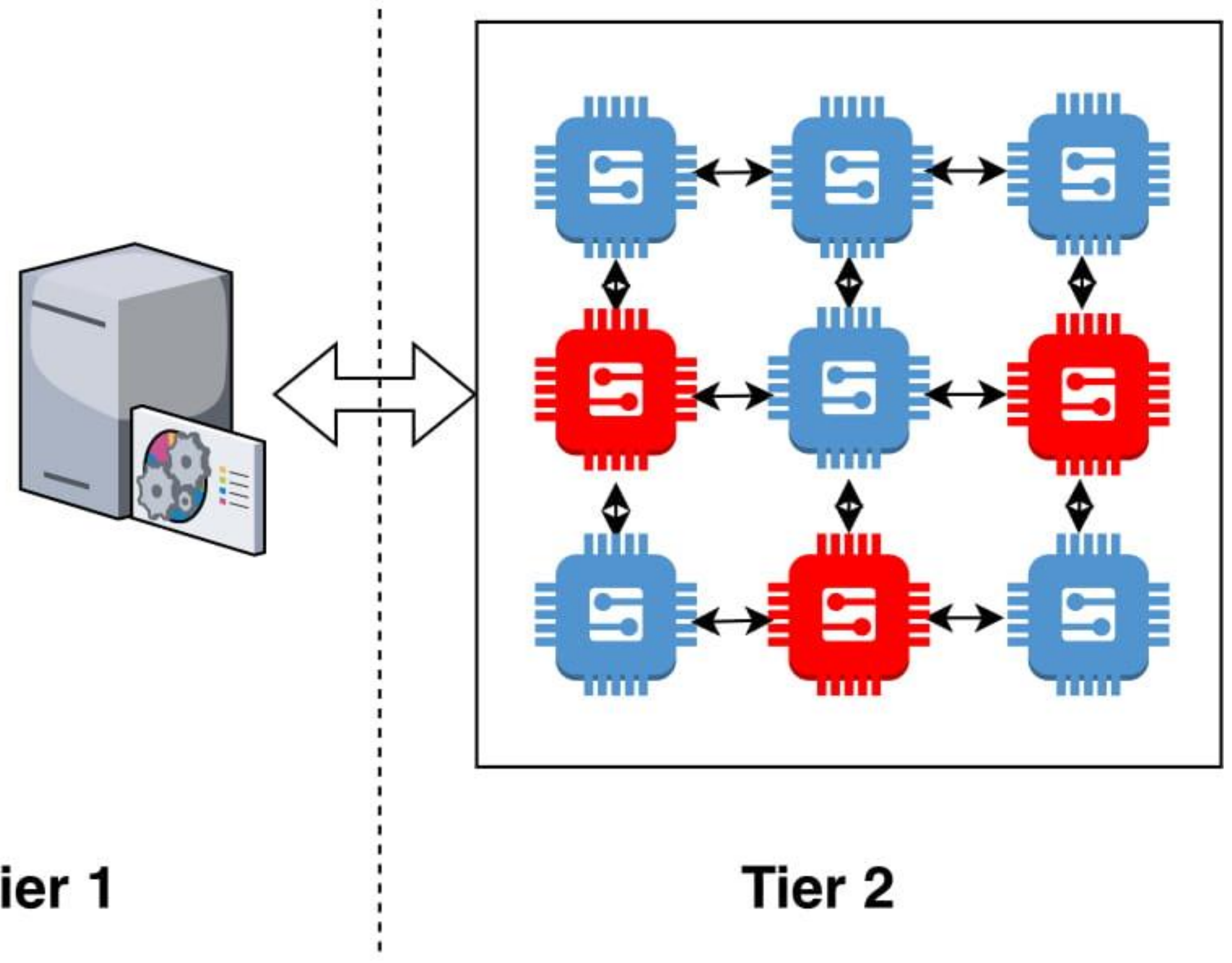
- Bluetooth LE consumes less power than WiFi (approx. 700x)
- Cost of ECDSA (339mJ,540mJ to sign and verify resp.) is nearly $\mathbf{10^3}$ **times greater** than HMAC(0.139mJ)

2. CPS State Machine Replication

Ideal CPS SMR

- ***Byzantine Fault Tolerance*****:** In a system of n nodes, tolerate up to f faults
- ***Liveness***: Each client request is eventually committed by all correct nodes
- ***Energy Efficiency***: The overall cost of performing the agreement must be optimal for non-faulty nodes
- ***Fairness***: Energy expenditure for any node is the same over multiple nodes

4. Two-Tiered System Model



- *No resource and network constraints* for Tier 1 nodes
- Tier 2 nodes are embedded nodes with *limited computational and energy resources*
- Some k-cast links available for nodes in Tier 2 providing *local reliable broadcast*
- Nodes in Tier 2 *possess energy efficient k –cast links* (such as BLE) and have *partial network connectivity*
- Up to f faulty nodes in Tier 2
- All Tier 2 nodes are connected to Tier 1 nodes via an expensive link (such as WiFi/4G)

6. Contributions

- Leverage *k-cast* and *resource bounded adversary* to optimize energy efficiency of the protocol
- Protocols must be optimal when all nodes are correct to be energy efficient
- E2C is the *most energy efficient* leader based SMR protocol and is based on best-case optimality
- E2C generates *certificates on-demand* (when the leader is bad)
- E2C uses *O(1) signatures and O(n) verification* operations per round, as opposed to *O(n) and O(n^2)* by the state-of-the-art protocol Sync-HotStuff

I. Abraham, D. Malkhi, K. Nayak, L. Ren and M. Yin, "Sync HotStuff: Simple and Practical Synchronous State Machine Replication

PURDUE UNIVERSITY Discovery Park

CERIAS