IRONSTACK

PERFORMANCE AND SECURITY FOR DEDICATED SYSTEMS USING OPENFLOW

Increasingly large numbers of critical infrastructure and enterprises employ dedicated, mission-critical networks. The performance and security of these networks are primary concerns that are difficult to address with retrofitting.

DEFICIENCIES IN NETWORKING

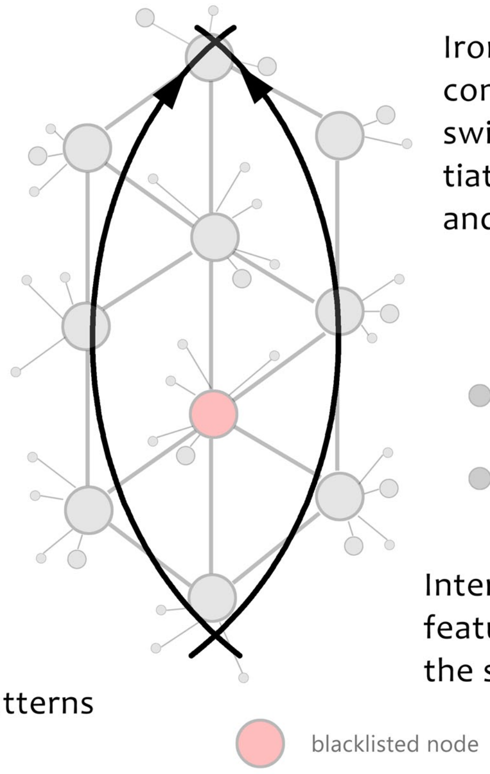
Mainstream switching hardware, although modern, are generally not highly configurable. Routing algorithms are standardized and is confined to what is natively available on the hardware.

1. Latencies and variances in latencies can be large, resulting in poor and choppy network performance.
2. Redundant networks links are underutilized, wasting potential bandwidth.
3. Network fault recovery can take several moments, during which communications may be disrupted.
4. Suitably positioned attackers can eavesdrop on network traffic, or otherwise gain signal intelligence from it.

MULTIPATH ROUTING

Route data along multiple disjoint paths for greater reliability and performance.

1. Replicate data across paths to minimize latency.
2. Maximize bandwidth by using all paths simultaneously.
3. Stripe data across paths to tune latency and bandwidth tradeoffs.



PHYSICAL ROUTE SECURITY

Alter choice of network paths or traffic patterns for data security.

1. Pick paths that avoid blacklisted nodes, or only use whitelisted nodes for routing.
2. Change or randomize upstream and downstream traffic to hinder signals intelligence gathering.

APPLICATIONS

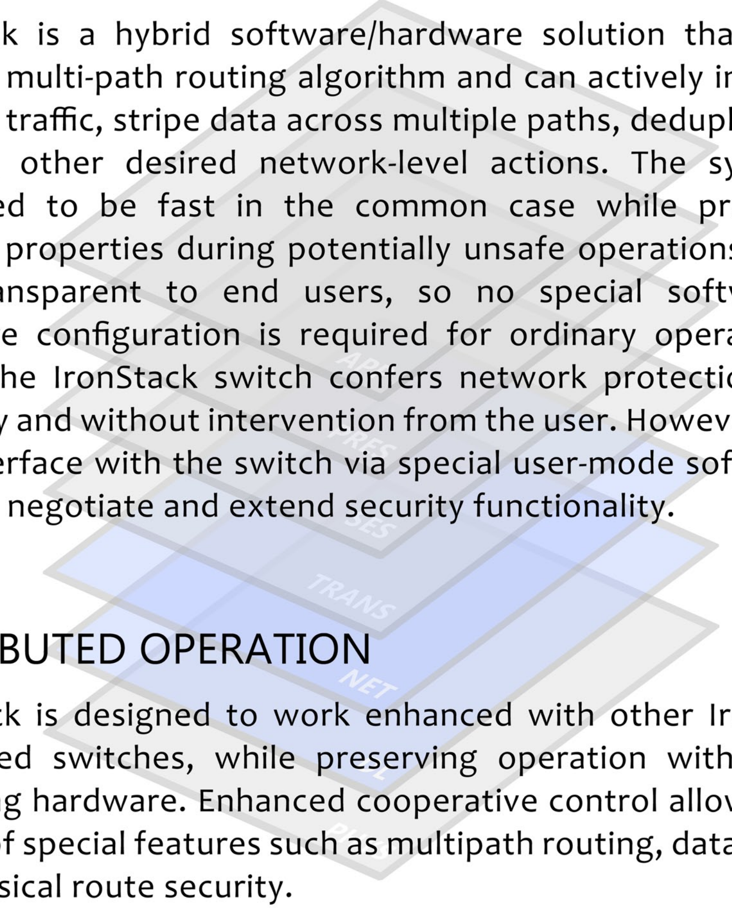
power monitoring | national grid | transportation | industrial processing | medicine

Mission-critical, dedicated enterprise networks.

WATCH THIS SPACE

Our full paper will present benchmarks about IronStack's resilience and performance under network duress. We will also discuss the implications of IronStack's security features.

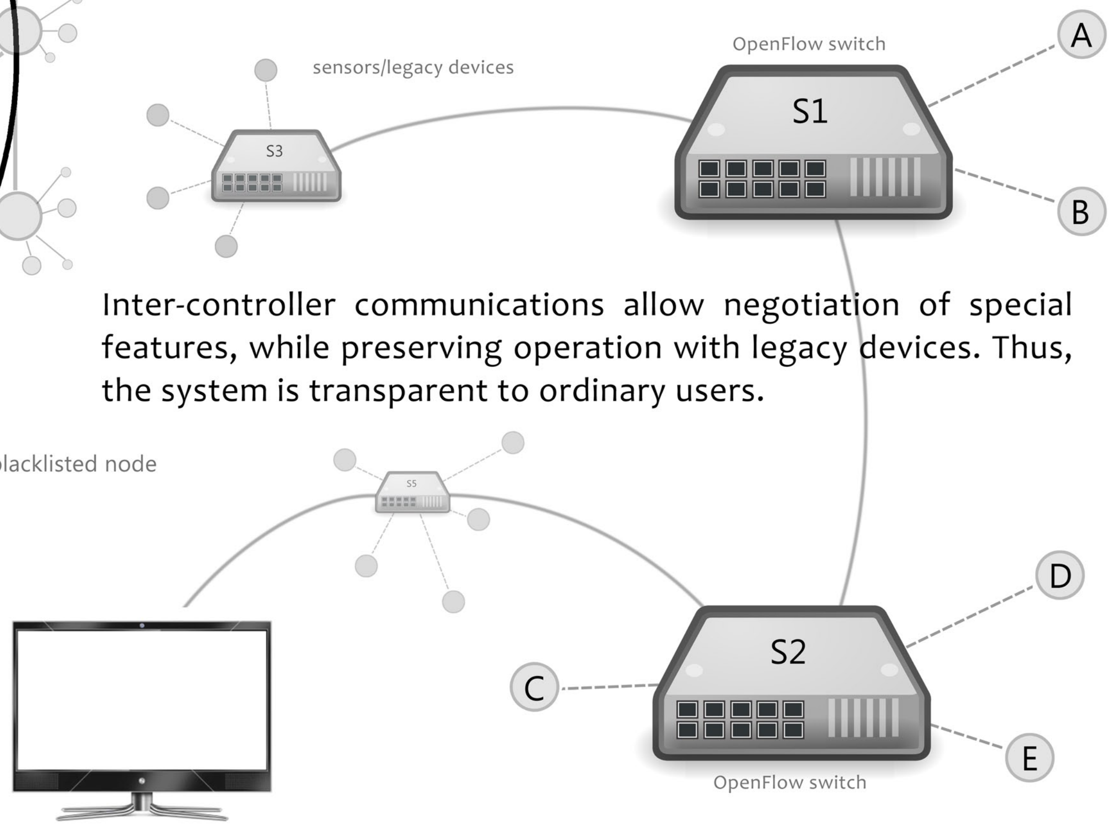
SYSTEM ARCHITECTURE



IronStack is a hybrid software/hardware solution that implements a multi-path routing algorithm and can actively intervene to block traffic, stripe data across multiple paths, deduplicate, or perform other desired network-level actions. The system is optimized to be fast in the common case while preserving security properties during potentially unsafe operations. This is fully transparent to end users, so no special software or hardware configuration is required for ordinary operation. In effect, the IronStack switch confers network protection automatically and without intervention from the user. However, users may interface with the switch via special user-mode software in order to negotiate and extend security functionality.

DISTRIBUTED OPERATION

IronStack is designed to work enhanced with other IronStack-controlled switches, while preserving operation with regular switching hardware. Enhanced cooperative control allows negotiation of special features such as multipath routing, data striping and physical route security.



Inter-controller communications allow negotiation of special features, while preserving operation with legacy devices. Thus, the system is transparent to ordinary users.

Management and monitoring interfaces can be attached remotely for greater convenience.

PEOPLE

zhiyuan teo

vera kutsenko

ken birman

robbert van renesse

cornell university