Reliable Environment for Secure Police Operations and NetworkS

Dirk.Grunwald@Colorado.edu [†◊]
Sangtae.Ha@Colorado.edu [†◆]
Eric.Wustrow@Colorado.edu [◊]

† Dept. of Computer Science
◊ Electrical, Computer & Energy Eng.
◆ Interdisciplinary Telecom Program

University of Colorado
Boulder

In many first-response scenarios, it is common for multiple departments and jurisdictions to need to cooperate with one another, introducing complex communication challenges:

- **Reliable**: Communications must be robust against network fragmentation and disruption

- **Distributed**: The decentralized nature of operations requires devices to directly communicate with one another in the temporary absence of a central controller

- **Secure**: Communications must be protected from eavesdropping and active interference

The Problem

Image: Hartlepool College, Creative Commons

Example: "Active shooter" scenario requires **reliable**, **distributed**, and **secure communication** between police, fire & medical first responders.

Responders must be able to temporarily share information such as maps, photos and messages without significant pre-planning

Objectives

The goals of **Respons** are to build a robust and reliable software framework that simplifies the construction of advanced public safety applications in disconnected or intermittently connected environments.

Our approach builds on emerging *Information Centric Network* and *Fog Computing* concepts while using proven technologies adopted in data center applications to minimize risk.

Milestones

Impacts

The **Respons** software environment should simplify agency-specific software development for information gathering & dissemination in field operations.

Approach

We plan to use existing commodity software where possible, and leverage technology that already tackles similar reliability and decentralized challenges in a different context.

We propose to use technology widely deployed in **modern datacenters,** and apply them to disconnected mobile communication.

Technologies such as **etcd** offer distributed consensus, while remaining robust in the face of intermittent disconnection
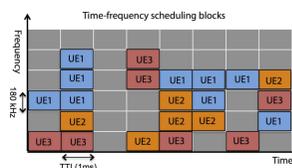
Proven **machine learning techniques for network occupancy** will infer LTE, WiFi performance, allowing informed selection of multiple wireless links
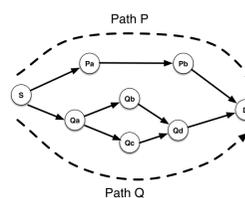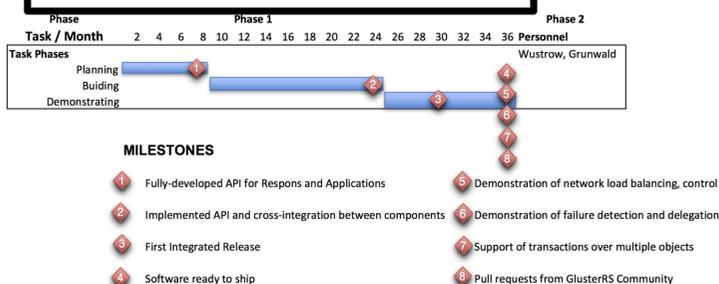
We will use standard network tools like **multipath TCP** for robust communication over multiple links.

We plan to use **opportunistic encryption** between devices to protect against passive eavesdroppers, and an optional certificate authority.