European
Commission

Agriculture and global food security
Economic and monetary union
Low-carbon economy and resource efficiency
Single market, growth, jobs and innovation
Public health, safety and security
Joint Research Centre
the European Commission's
in-house science service

Building a hybrid experimental platform for mobile botnet research

Apostolos Malatras
EC JRC, Institute for the Protection and Security of the Citizen
apostolos.malatras@jrc.ec.europa.eu

Laurent Beslay
EC JRC, Institute for the Protection and Security of the Citizen
laurent.beslay@jrc.ec.europa.eu

BotConf 2015
December 3, 2015

Joint Research Centre

Outline

- Motivation
- Mobile botnets
  - Definition & components
  - Taxonomy
- Hybrid experimental platform
  - Functionality
  - Design
  - Limitations
- Implementation
  - Software and hardware elements
  - Configuration
- Mobile botnet experiments
  - Counting active bots
- Conclusions

Outline

- Motivation
- Mobile botnets
  - Definition & components
  - Taxonomy
- Hybrid experimental platform
  - Functionality
  - Design
  - Limitations
- Implementation
  - Software and hardware elements
  - Configuration
- Mobile botnet experiments
  - Counting active bots
- Conclusions

Motivation

- Current status
  - Limited support for repeating experiments
  - Limited validity due to ad hoc testing
  - Not possible to compare results

- Common experimentation platform
  - Well-defined, established way for experimentation
  - Exchange of results and experimentation settings
  - Scalable and flexible experiments in contained environment
  - Facilitates development efforts
  - Promotes uniformity and common practices
    - E.g. network simulators/emulators

Outline

- Motivation
- Mobile botnets
    - Definition & components
    - Taxonomy
- Hybrid experimental platform
    - Functionality
    - Design
    - Limitations
- Implementation
    - Software and hardware elements
    - Configuration
- Mobile botnet experiments
    - Counting active bots
- Conclusions

Mobile botnets

- A collection of compromised mobile machines that aims to perform certain activities envisaged by the botmaster

- Exploit security vulnerabilities of mobile systems and OSs
  - Pervasive and always-on
  - Plethora of OS versions
  - Apps with varying levels of permissions
  - Convergence with traditional computing systems

- Tightly linked to user accounts
  - Rich set of information that can be eavesdropped
  - Lucrative gains

Botnets: components

Botmaster

C&C Server

Servant bot

Client bot

Particularities of mobile botnets

- Contextualization
  - Onboard sensors and tight connection to user account/profile
  - Context inference
    - Location
    - User condition/state
    - Proximity
    - Preferences
  - Possibility to contextualize the targets of attacks

- Financial gains
  - Phones acting as mobile wallets
  - SMS and premium numbers

European Commission

Particularities of mobile botnets

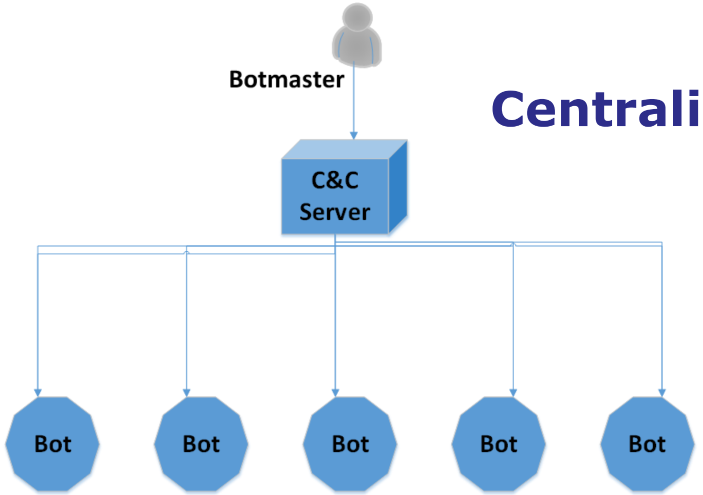
- Dynamic IP addressing
- Constraints imposed by cellular networks
- Great number of OS versions and a lot of vulnerabilities
- Size of screen is in itself a vulnerability
- Sensors can be used as side channel for communication
- Not tightly controlled ecosystem
  - Off market installations a risk

Taxonomy of mobile botnets features

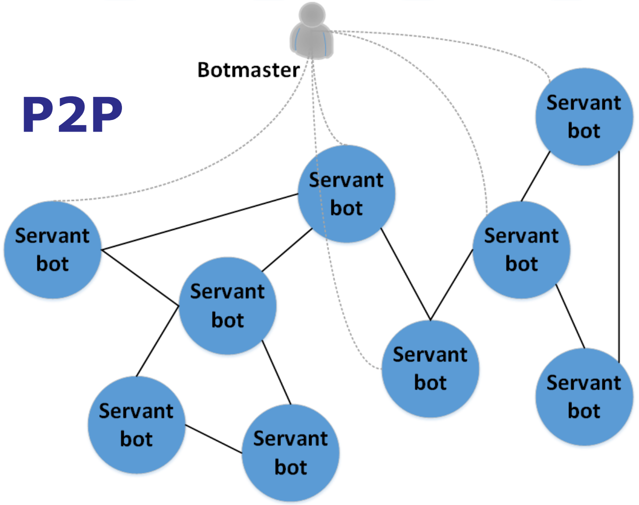
1. Network/connectivity
2. Platform
3. Architecture
4. Propagation of infection
5. Means of infection
6. Motivation/impact
7. Target
8. Detection

Architecture

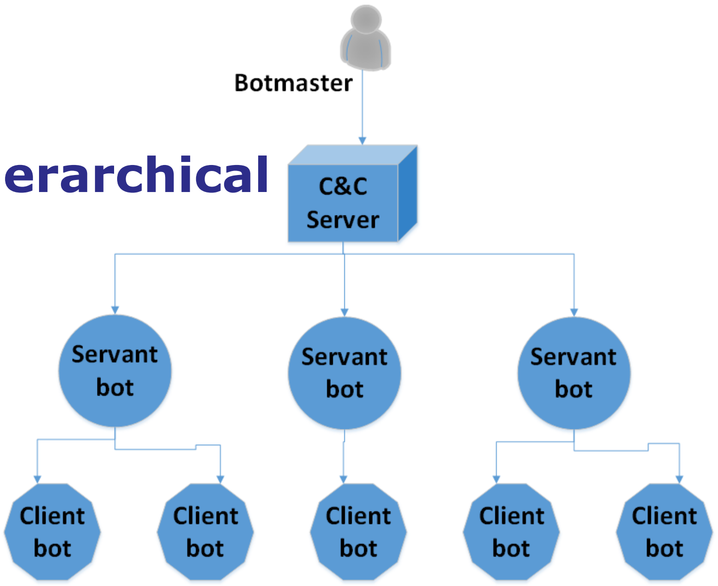
Centralized



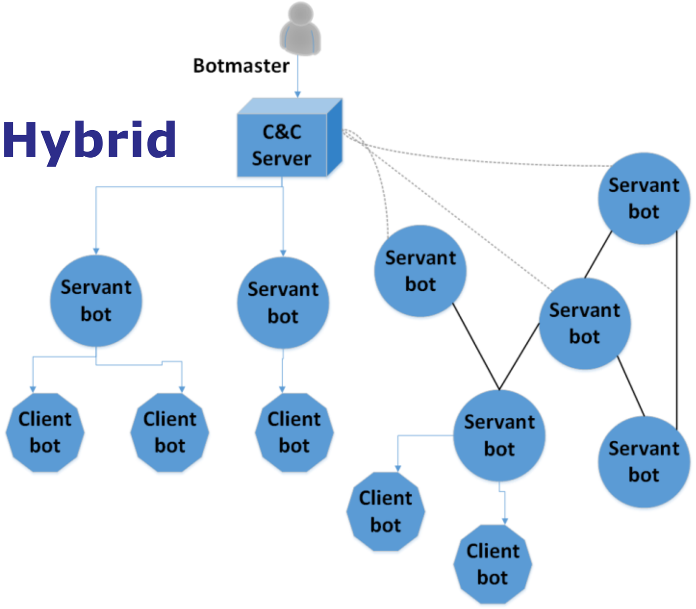
P2P



Hierarchical



Hybrid



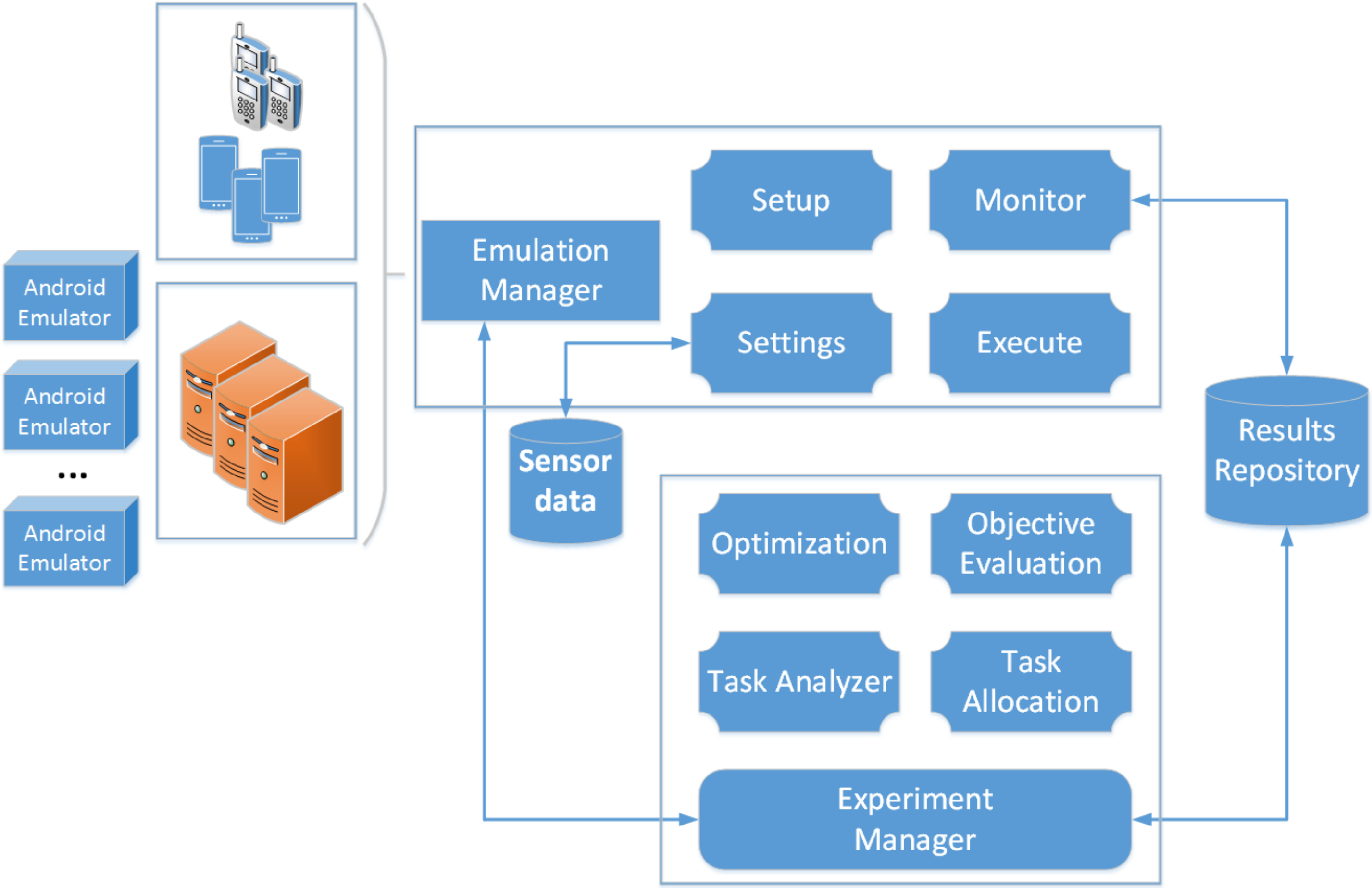
Outline

- Motivation
- Mobile botnets
  - Definition & components
  - Taxonomy
- Hybrid experimental platform
  - Functionality
  - Design
  - Limitations
- Implementation
  - Software and hardware elements
  - Configuration
- Mobile botnet experiments
  - Counting active bots
- Conclusions

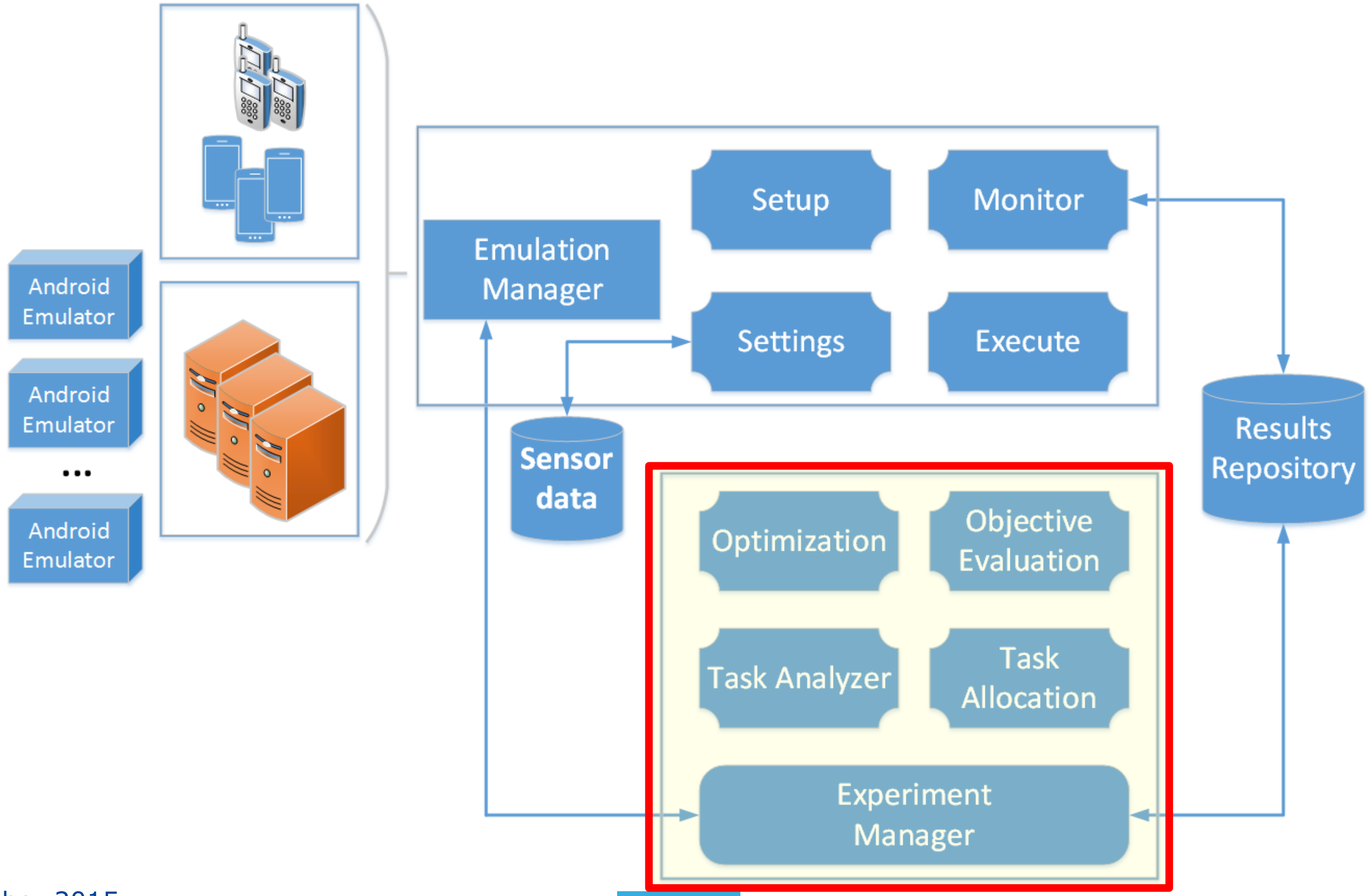
Design goals

- Generic to support variety of experiments
  - Different types and architectures
  - Various OS configurations
  - Heterogeneous networking
- Scalable
  - Large number of infected bots
  - Possibility to run experiments for more than one botnet
- Extensible
  - Allow for dynamic (re-)configuration
- Usability
  - Definition of the experiments
  - Interacting with the execution and the collection of results

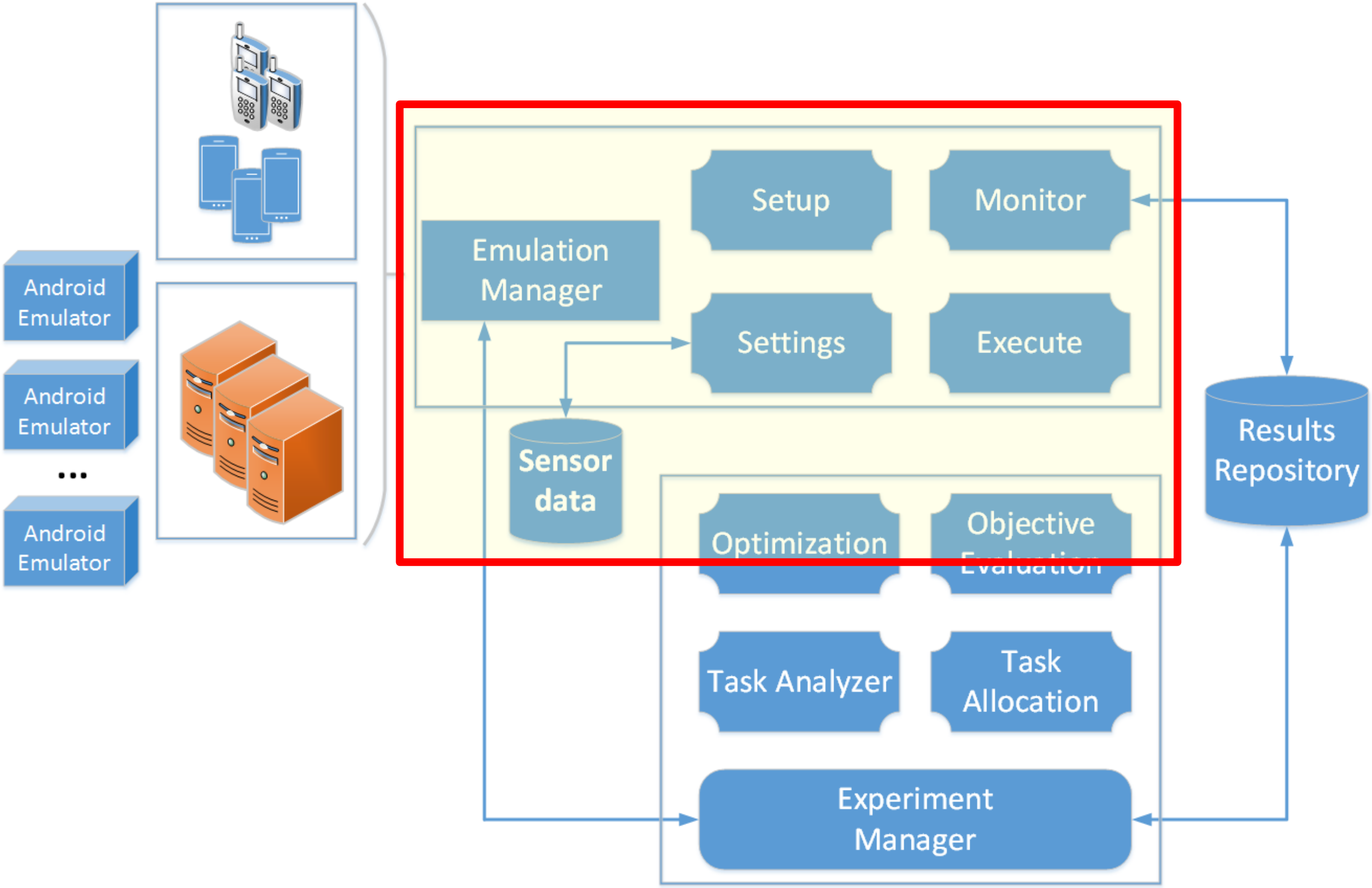
Architecture



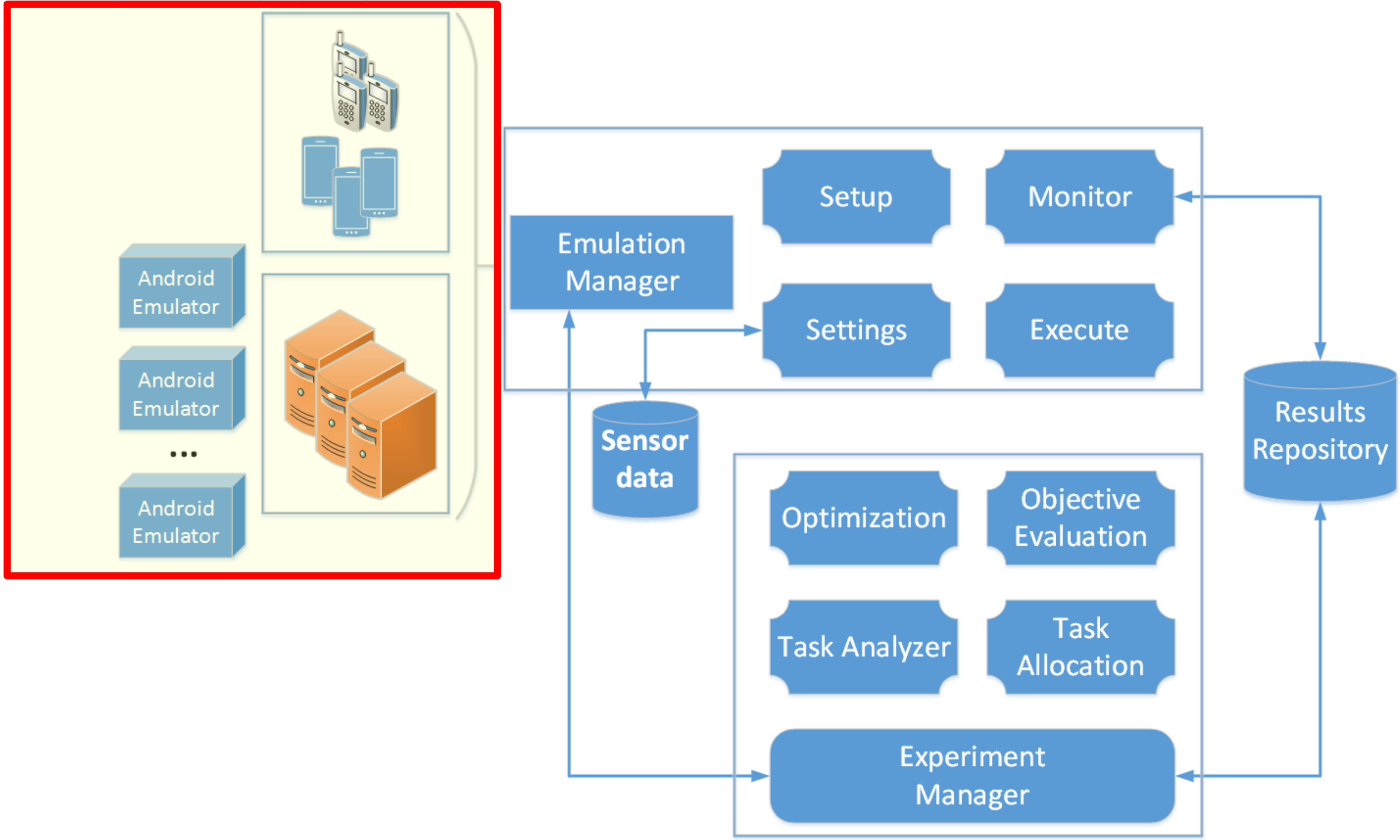
Architecture



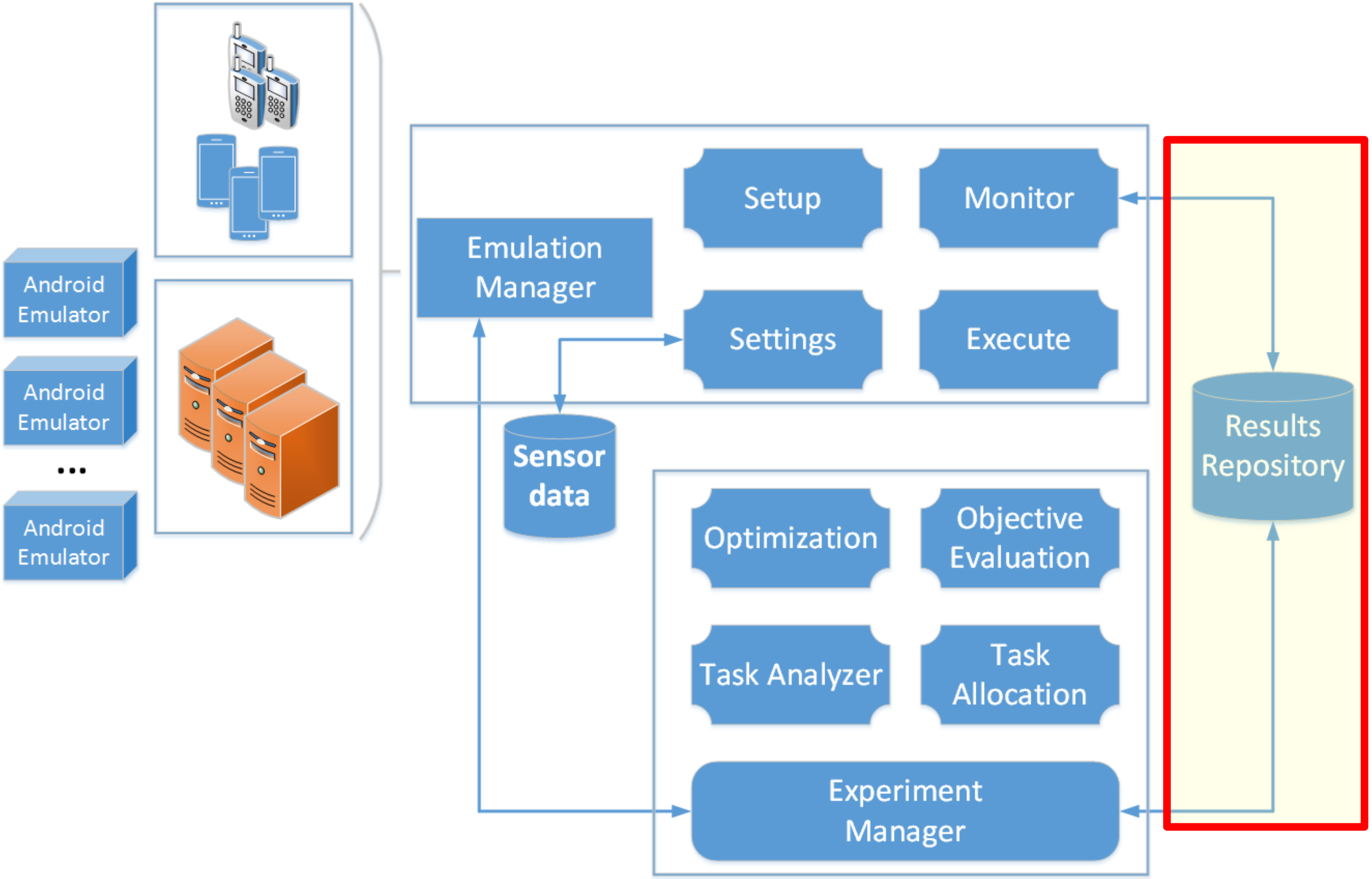
Architecture



Architecture



Architecture



What can it do?

- Test mobile botnets
  - Infection, distribution, detection
  - Diverse parameter configurations
- Observation of mobile botnets operation
  - Real and emulated devices
- Scenario-based execution of events
  - Simple and advanced scenarios
- Remote configuration of real and emulated devices
- Collection of results and runtime measurements
- Integration of realistic sensor data
- Parallel execution of multiple experiments
  - Subject to availability of resources

Outline

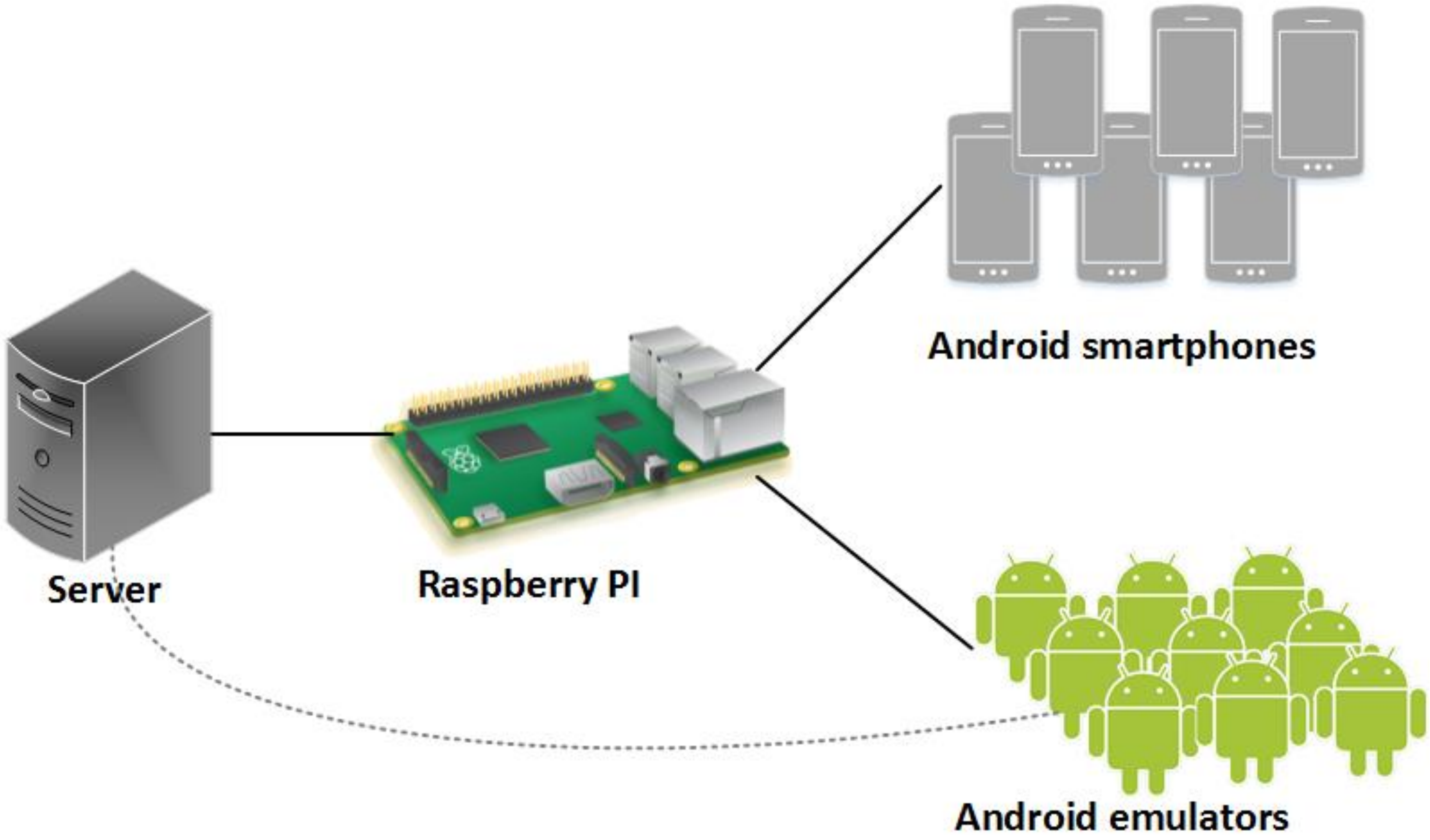
- Motivation
- Mobile botnets
  - Definition & components
  - Taxonomy
- Hybrid experimental platform
  - Functionality
  - Design
  - Limitations
- Implementation
  - Software and hardware elements
  - Configuration
- Mobile botnet experiments
  - Counting active bots
- Conclusions

Implementation

- Using
  - Java technologies
  - Android Emulator
  - Android Debug Bridge
  - XML for configuration
  - SensorSimulator to create “realistic” “fake” sensor data

European Commission

Infrastructure



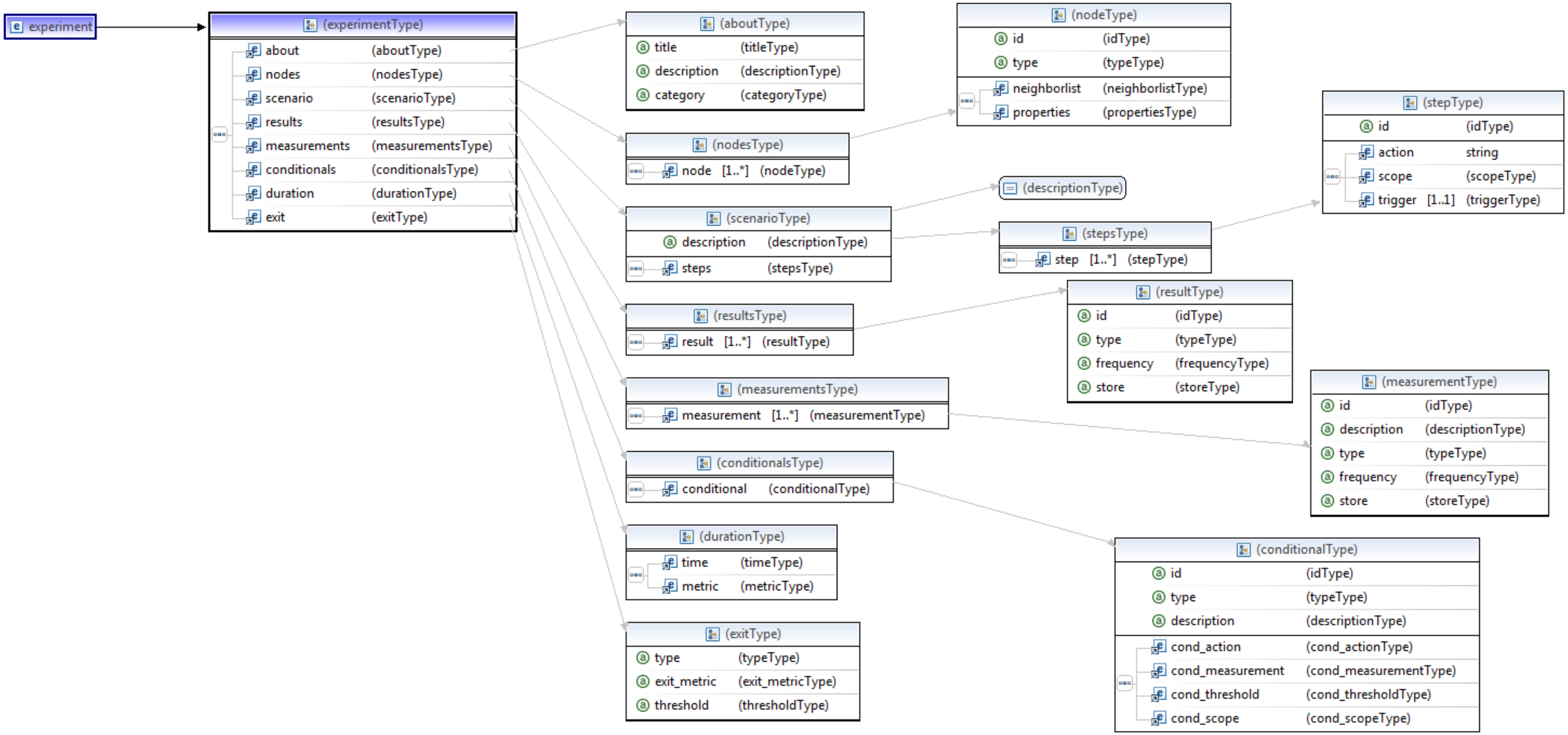
Networking

- WiFi network
  - No wide Internet access
  - Plan to use traffic shaping to emulate cellular networks
- IP addressing
  - Real devices: DHCP
  - Emulated devices: via the virtual router of the Android emulator
  - Port redirection used on emulated devices to connect them to real ones (based on topology definition)
- All devices need to be on the same network
  - Allows for full interaction with all devices
  - Could be relaxed subject to all Android platforms having a telnet daemon installed

Configuration

- Scenarios defined using XML Schema
  - XML SAX parser
  - Steps define scenario execution
  - Conditional triggering of steps or time-based
  - Exit conditions or duration of experiment
  - Definition of topology
  - Setting up of measurements and results monitors

Configuration – XML Schema



e experiment

(experimentType)
about (aboutType)
nodes (nodesType)
scenario (scenarioType)
results (resultsType)
measurements (measurementsType)
conditionals (conditionalsType)
duration (durationType)
exit (exitType)

(aboutType)
title (titleType)
description (descriptionType)
category (categoryType)

(nodesType)
node [1..*] (nodeType)

(nodeType)
id (idType)
type (typeType)
neighborlist (neighborlistType)
properties (propertiesType)

(scenarioType)
description (descriptionType)
steps (stepsType)

(descriptionType)

(stepsType)
step [1..*] (stepType)

(stepType)
id (idType)
action string
scope (scopeType)
trigger [1..1] (triggerType)

(resultsType)
result [1..*] (resultType)

(resultType)
id (idType)
type (typeType)
frequency (frequencyType)
store (storeType)

(measurementsType)
measurement [1..*] (measurementType)

(measurementType)
id (idType)
description (descriptionType)
type (typeType)
frequency (frequencyType)
store (storeType)

(conditionalsType)
conditional (conditionalType)

(conditionalType)
id (idType)
type (typeType)
description (descriptionType)
cond_action (cond_actionType)
cond_measurement (cond_measurementType)
cond_threshold (cond_thresholdType)
cond_scope (cond_scopeType)

(durationType)
time (timeType)
metric (metricType)

(exitType)
type (typeType)
exit_metric (exit_metricType)
threshold (thresholdType)

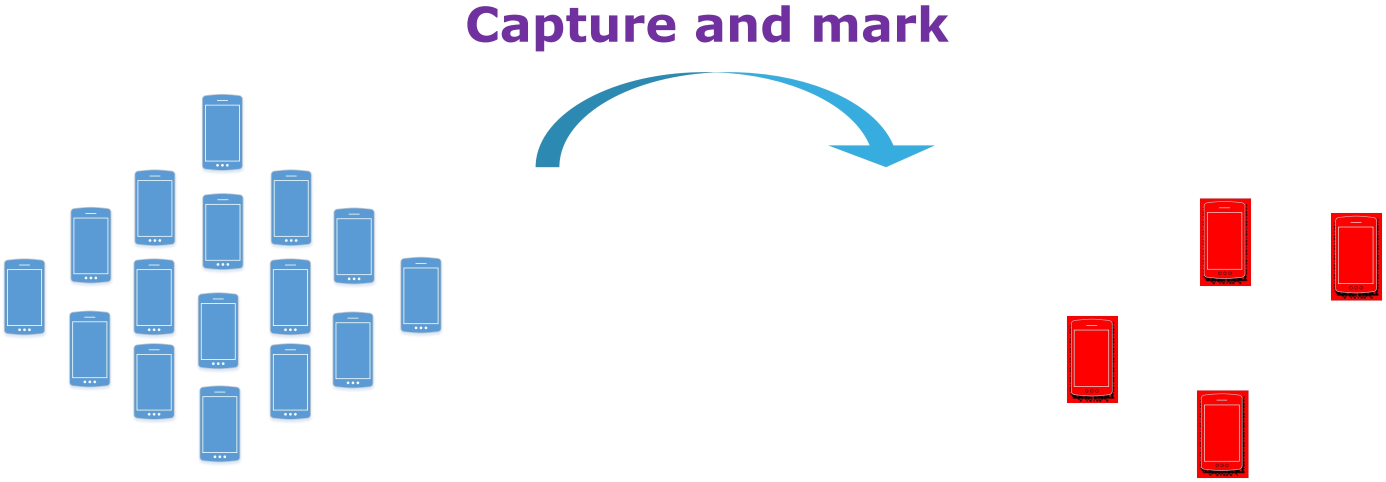
Outline

- Motivation
- Mobile botnets
  - Definition & components
  - Taxonomy
- Hybrid experimental platform
  - Functionality
  - Design
  - Limitations
- Implementation
  - Software and hardware elements
  - Configuration
- Mobile botnet experiments
  - Counting active bots
- Conclusions

Counting bots in a botnet

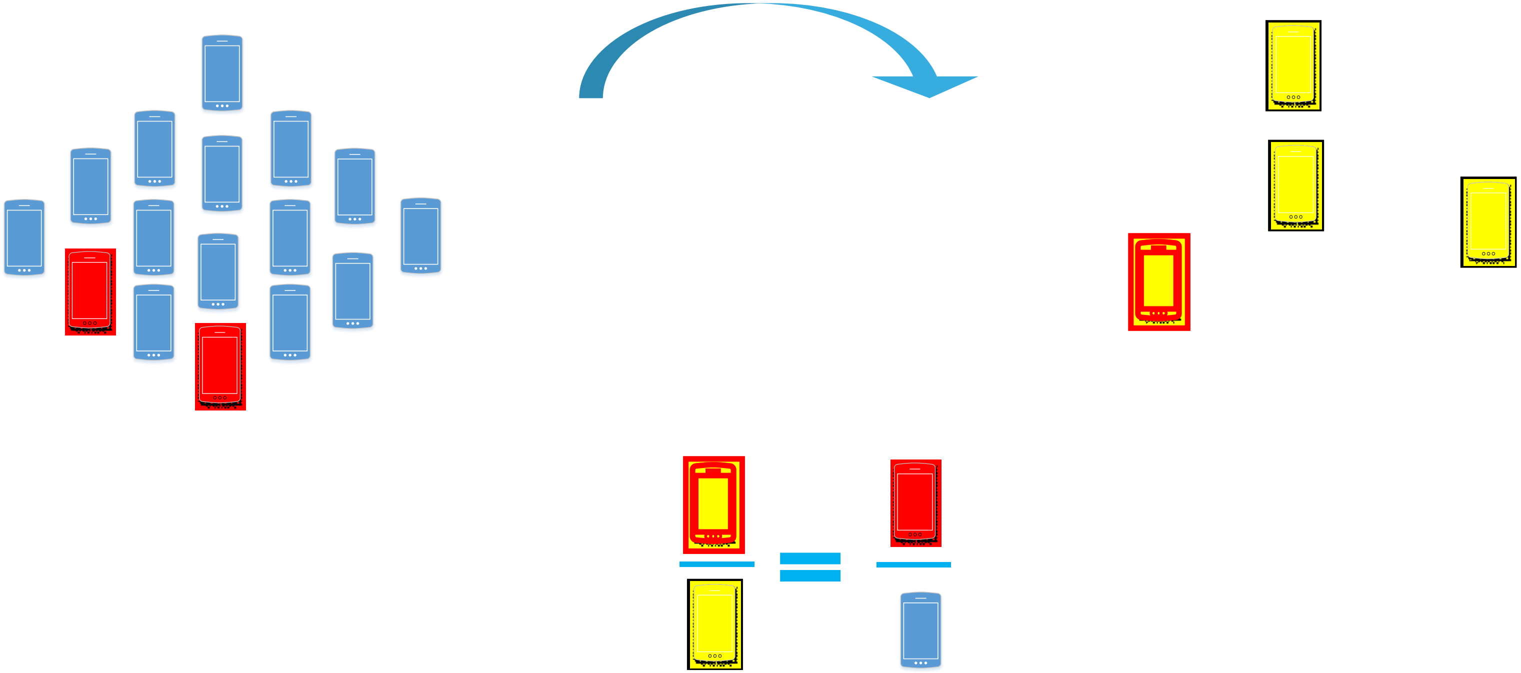
- Variant of Jolly-Seber capture-recapture method
  - Used in biology to calculate size of animal populations
  - Statistical method based on a stochastic model
  - Yields good results in relative short time

Counting bots in a botnet



Counting bots in a botnet

Recapture and count



Using the hybrid experimental platform

- Centralized/hybrid mobile botnets
  - Operate honeypot to monitor infected instances
  - Periodically mark observed instances

- P2P mobile botnets
  - Real devices infiltrate botnet
  - Periodically collect identifiers of nodes in peer list
  - Reset network settings
  - Repeat process with all nodes

Outline

- Motivation
- Mobile botnets
  - Definition & components
  - Taxonomy
- Hybrid experimental platform
  - Functionality
  - Design
  - Limitations
- Implementation
  - Software and hardware elements
  - Configuration
- Mobile botnet experiments
  - Counting active bots
- Conclusions

Conclusions

- Mobile botnets are emerging into the scene
  - Convergence of traditional and mobile ecosystems
  - Pervasive nature of mobile phones

- Need for systematic research efforts
  - Organize and classify existing work and botnets
  - Numerous particularities and distinguishing characteristics
  - Research has been quite dispersed so far

- We proposed a hybrid experimental platform to study mobile botnets
  - Highlight challenges and opportunities
  - Allows for systematic, comparable research works

Feedback/Discussion