Cyber Physical Security (CPS) Extension to Air Traffic Management (ATM) Testbed

Koushik Datta

NASA Ames Research Center

Gano Chatterji

Crown Consulting, Inc.

Daniel Zeng, Asif Mahmud and Nathan Wendt

NASA Student Interns

Outline

- The Problem
- Motivation
- Cyber Physical System Attack Avenues
- ATM System Attack Examples
- Study Approach
- Emulation & Study Environment - NASA’s ATM Testbed
- Cyber Physical System Attack Types
- Attack Methods Developed
- Attack Emulation Procedure
  - Traffic Scenario Creation
  - Visualization of Simulated Traffic
- Future Work

The Problem

Truck driver with GPS jammer accidentally jams Newark airport
CNET, August 2013

Hackers ground 1,400 passengers at Warsaw in attack on airline's computers
The Guardian, June 2015

French fighter planes grounded by computer virus
The Telegraph, February 2009

"The cyber world of interconnected and interdependent systems has increased the vulnerability of aircraft and systems and therefore the potential impact that breaches in security can have."
Cyber Security in Civil Aviation, August 2012

At the Hack-In-The-Box conference in Amsterdam, security consultant Hugo Teso demonstrated PlaneSploit, that he claims can take control of airplane systems and cause it to change direction or crash into the ground
Bloomberg, April 2013

Malware implicated in fatal Spanair plane crash. Computer monitoring system was infected with Trojan horse, authorities say
NBC News, August 2010

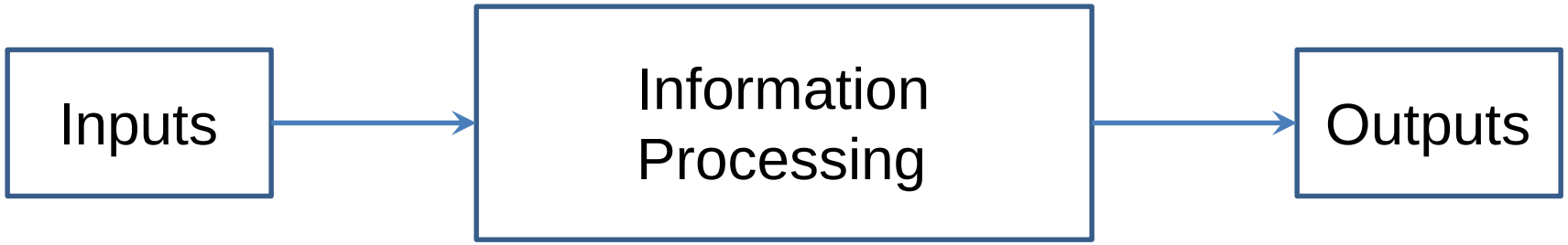
Researchers use GPS spoofing to hack into a flying drone
BBC, June 2012

Motivation

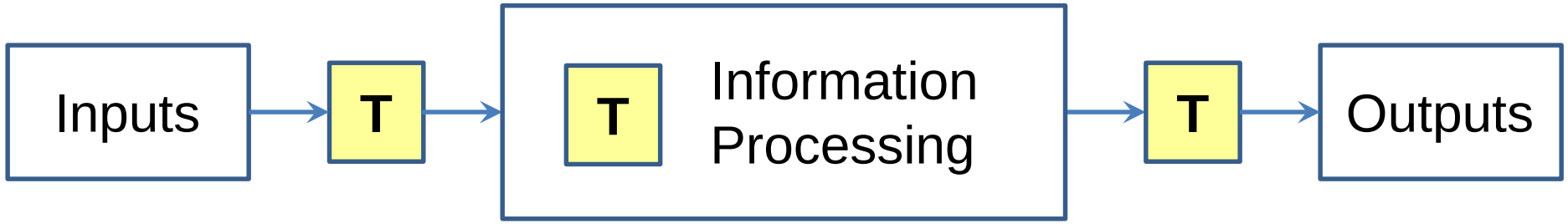
We do not currently have a way to study the effects of cyber-attacks on future ATM concepts and decision support tools that are being developed by NASA and the FAA, and to support the development of detection and mitigation strategies in response to cyber-attacks

Cyber Physical System (CPS) Attack Avenues

Normal CPS

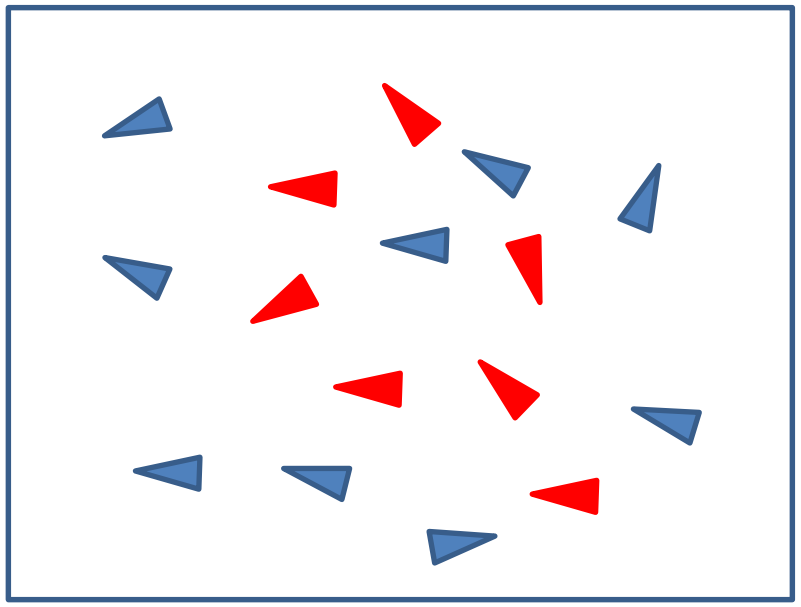


Compromised CPS

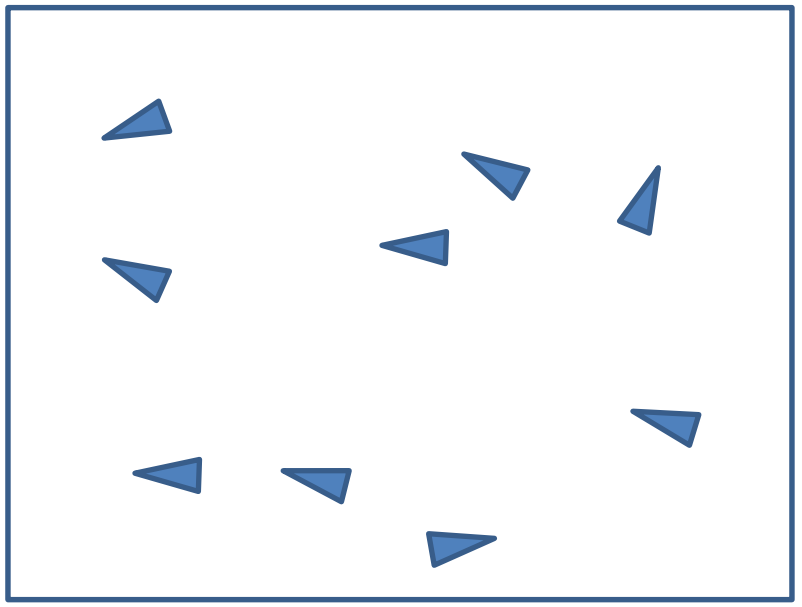


T CPS attack attempts to transform Inputs, processing and outputs

Example Attack 1: Fake Aircraft



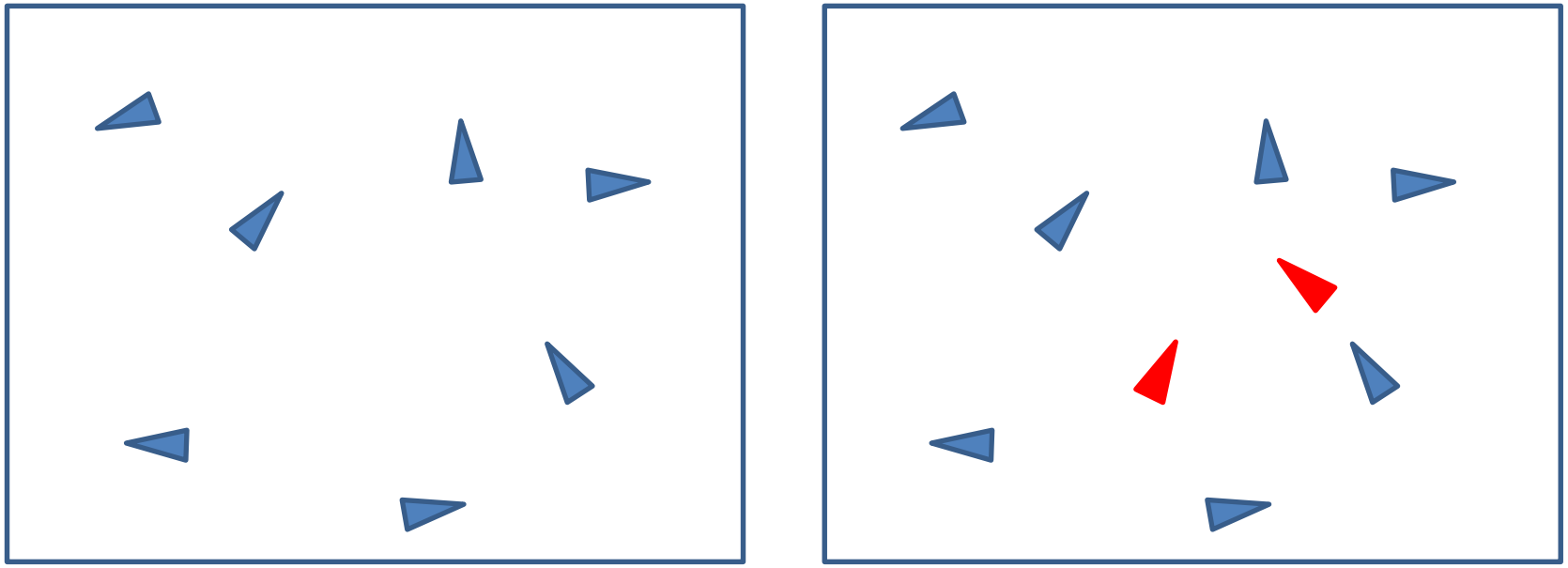
ATC Display



Reality

Fake aircraft that do not exist in reality appear on Air Traffic Control (ATC) display to overwhelm the air traffic controller

Example Attack 2: Invisible UAS

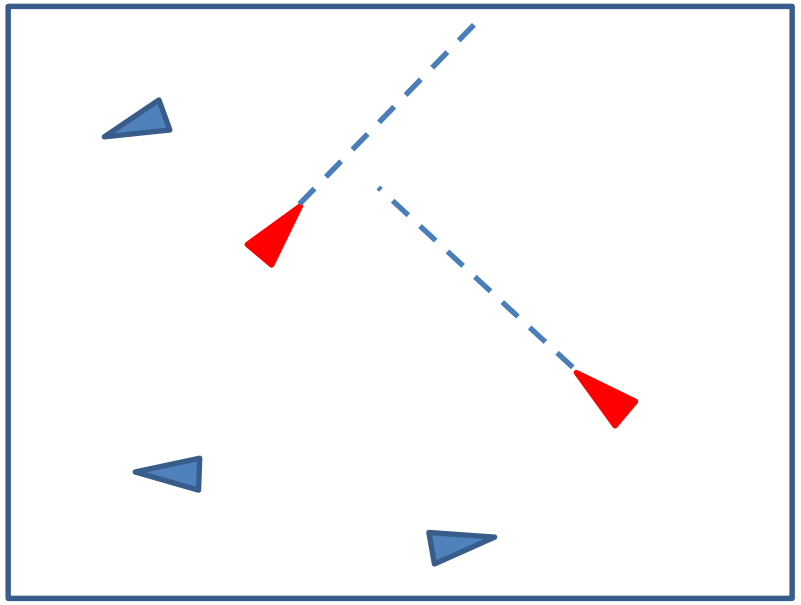


Observed via Surveillance

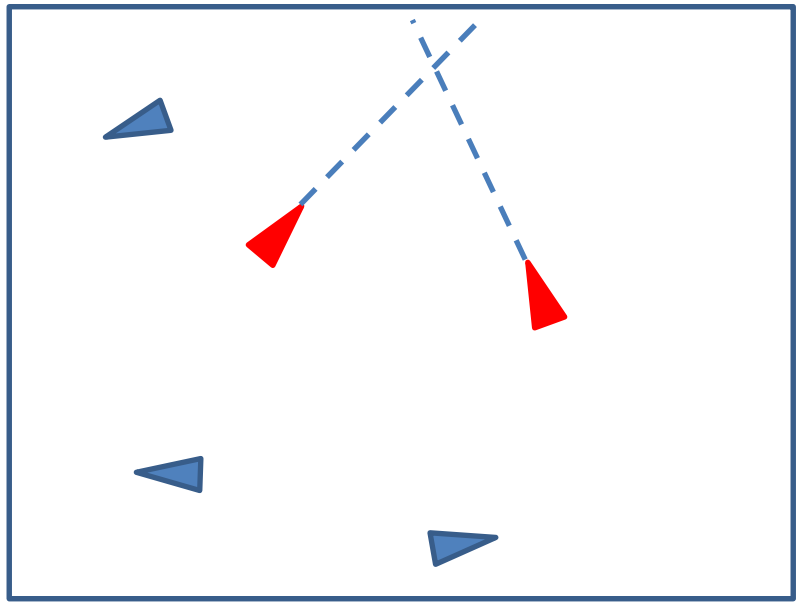
Reality

Two rogue UASs, shown in red, are flying undetected; they are not transmitting their position information to the UAS Service Supplier

Example Attack 3: Incorrect State Reported on ATC Display



No conflict on ATC Display



Conflict in Reality

Position and heading of one aircraft reported incorrectly in ATC system to mask an impending conflict

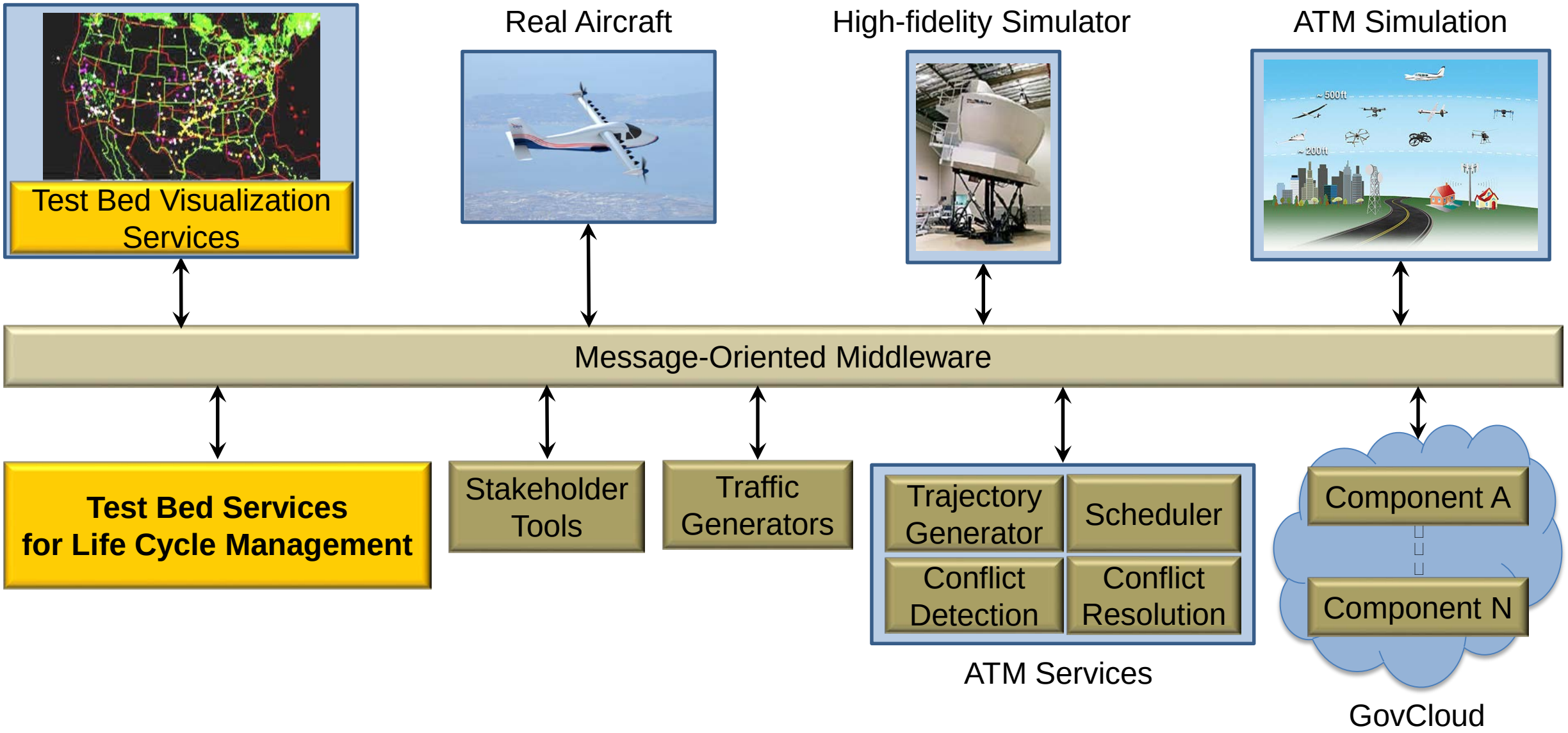
Study Approach

- Emulate attack scenarios in a modeling and simulation environment to explore Air Traffic Management (ATM) system cybersecurity vulnerabilities
- Develop methods for detecting and analyzing the impact on the ATM system based on emulated security events
- Develop mitigation strategies, including prevention, containment and recovery, for uninterrupted operation of the ATM system

Emulation & Analysis Environment – NASA's ATM Testbed

- Platform-as-a-Service for creating, configuring and running real-time and fast-time simulations with large-scale simulators, mathematical models and operational systems
- Provides a service-oriented-architecture in which components are autonomous; they interact with each other via data exchange using message-oriented middleware
- Provides configuration driven automated simulation life cycle management including deployment, initialization, run, shutdown and data archival
- Provides user friendly utilities & tools
  - GUI-based tool for simulation configuration
  - Code generation widget to build adapters for connecting components to Testbed
  - Adapters for connecting legacy systems

Emulation & Analysis Environment – ATM Testbed Architecture



Cyber Physical Security (CPS) Attack Types

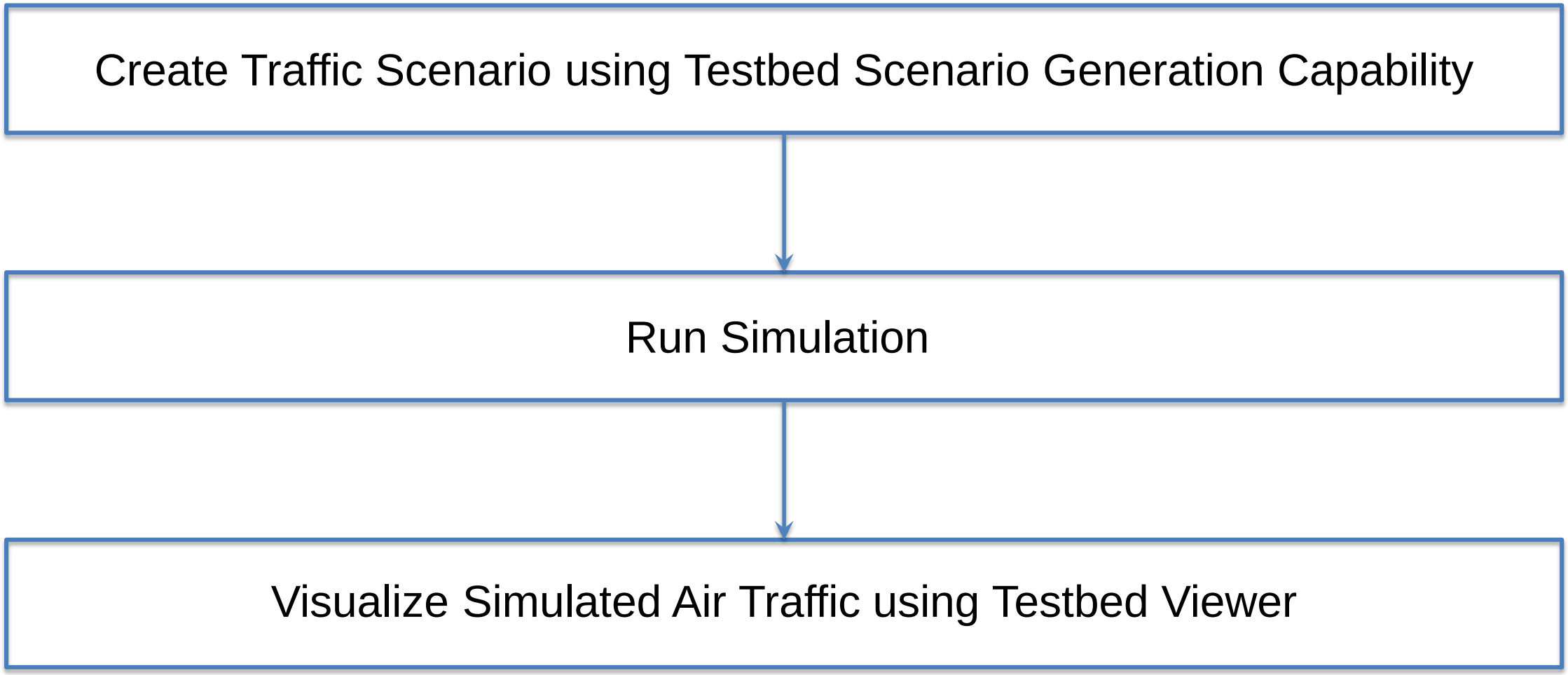
Attack Type	Action
Denial of Service	Overwhelming or removing values
Spoofing	Tampering with values
Exploiting	Taking advantage of a vulnerability
Counterfeiting	Passing fake information as legitimate
Man in the Middle	Adversary intercepts and broadcasts own signal

Violating the Confidentiality, Integrity, and Availability of the System

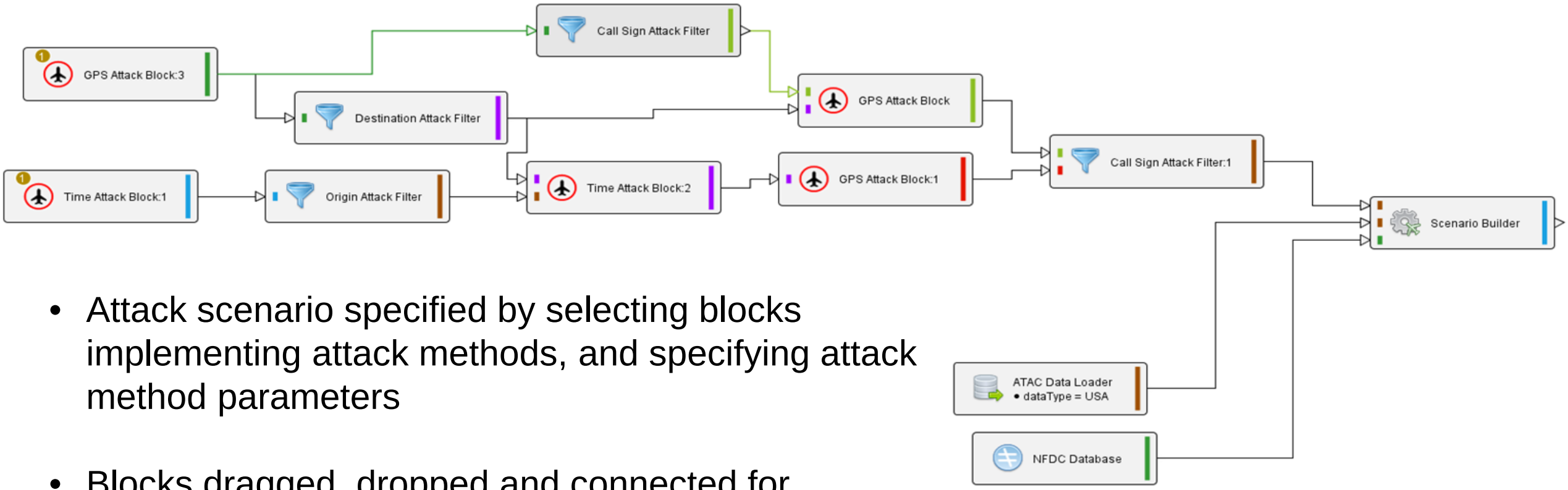
Attack Methods Developed

Attack Method	Outcome
Fake flight creation	• Stationary aircraft created at an airport • Fake aircraft flying great-circle trajectory from origin to destination • Fake aircraft created within a sector with destination airports • Copies of actual flights flying with a random offset
Flight deletion	• Flight data of actual flights removed with a probability
Flight-plan change	• Flight-plan altered by altitude change, origin destination swap, route data shuffling, route reversal, and by waypoint addition and deletion
Surveillance data attack	• Altered position, heading, speed or rate of climb • Drop data with a probability
Timestamp altered	• Timestamp altered by shuffling, reversing, replaying, modifying and dropping

Cyber Security Attack Emulation Procedure

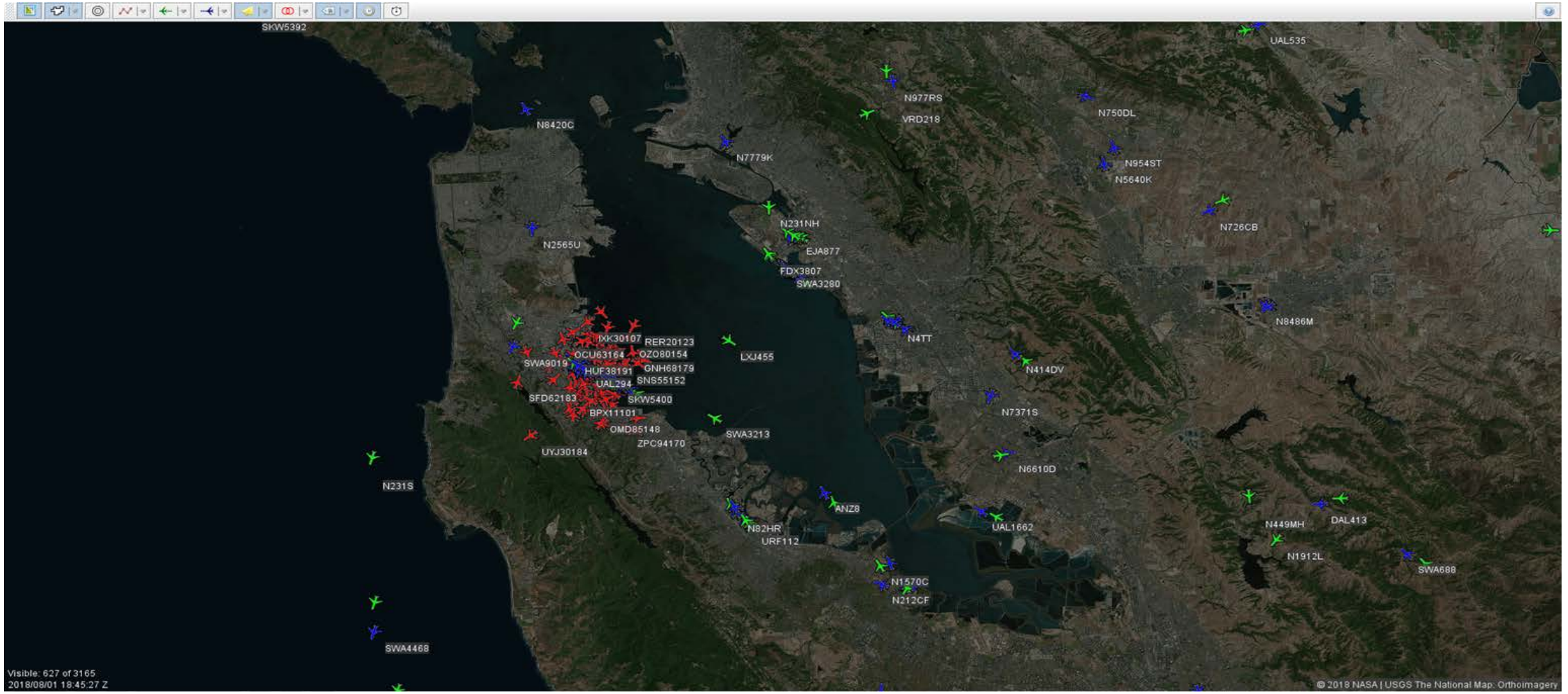


Traffic Scenario Creation using ATM Testbed Scenario Generation Capability



- Attack scenario specified by selecting blocks implementing attack methods, and specifying attack method parameters
- Blocks dragged, dropped and connected for scenario configuration using Testbed Simulation-Architect tool

Simulated Air Traffic on Testbed Viewer



Future Work

- Technical
  - Integrate scenario generation with simulation in the Testbed GUI-based Simulation-Architect tool
  - Test with Multi-Aircraft Control System, which is used for Human-in-the-Loop evaluations
  - Emulate attacks by altering weather data once the Testbed Viewer supports weather display

- General
  - Develop detection and mitigation strategies to counter the emulated attack scenarios
  - Develop metrics and criteria for evaluating resiliency and robustness of the solutions
  - Improve understanding of the ATM system vulnerabilities

The Big Picture for Future Work