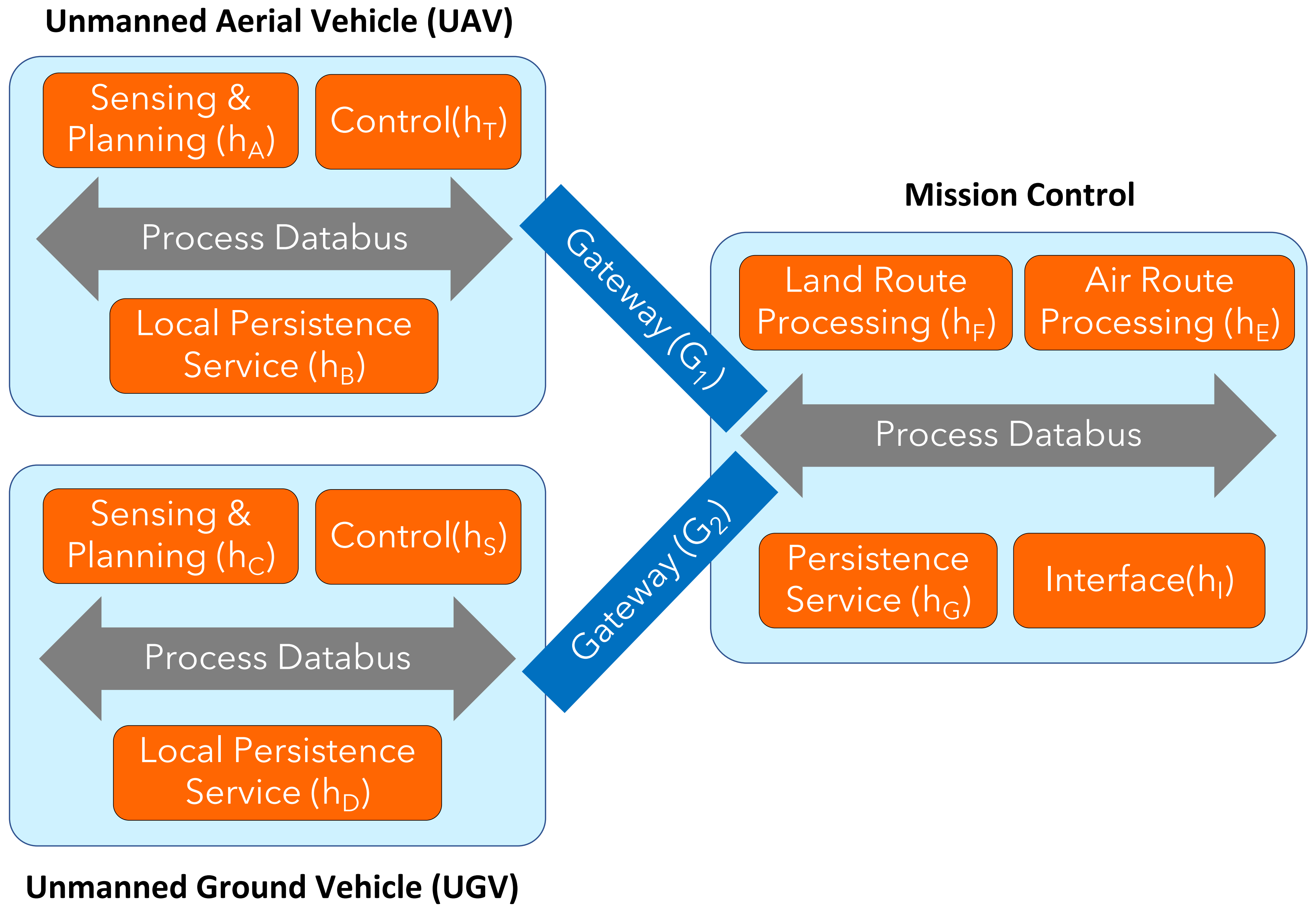
Securing Distributed System Configuration through Optimization and Reasoning on Graphs

Hamed Soroush, Shantanu Rane and Massimiliano Albanese

1

ABSTRACT: Evaluating the security impact of configuration changes on a distributed system is an inherently complex challenge. Existing solutions simplify the problem by optimizing only individual components while ignoring complex interdependencies amongst components. In contrast, we construct a graph-based model of the system and its vulnerabilities that captures such dependencies. Inspired by a model that assesses the impact of multi-step attacks [1], we show how to reason about security impact of configurations. We employ SMT solvers to derive configurations that minimize the impact of attacks while preserving system functionality.

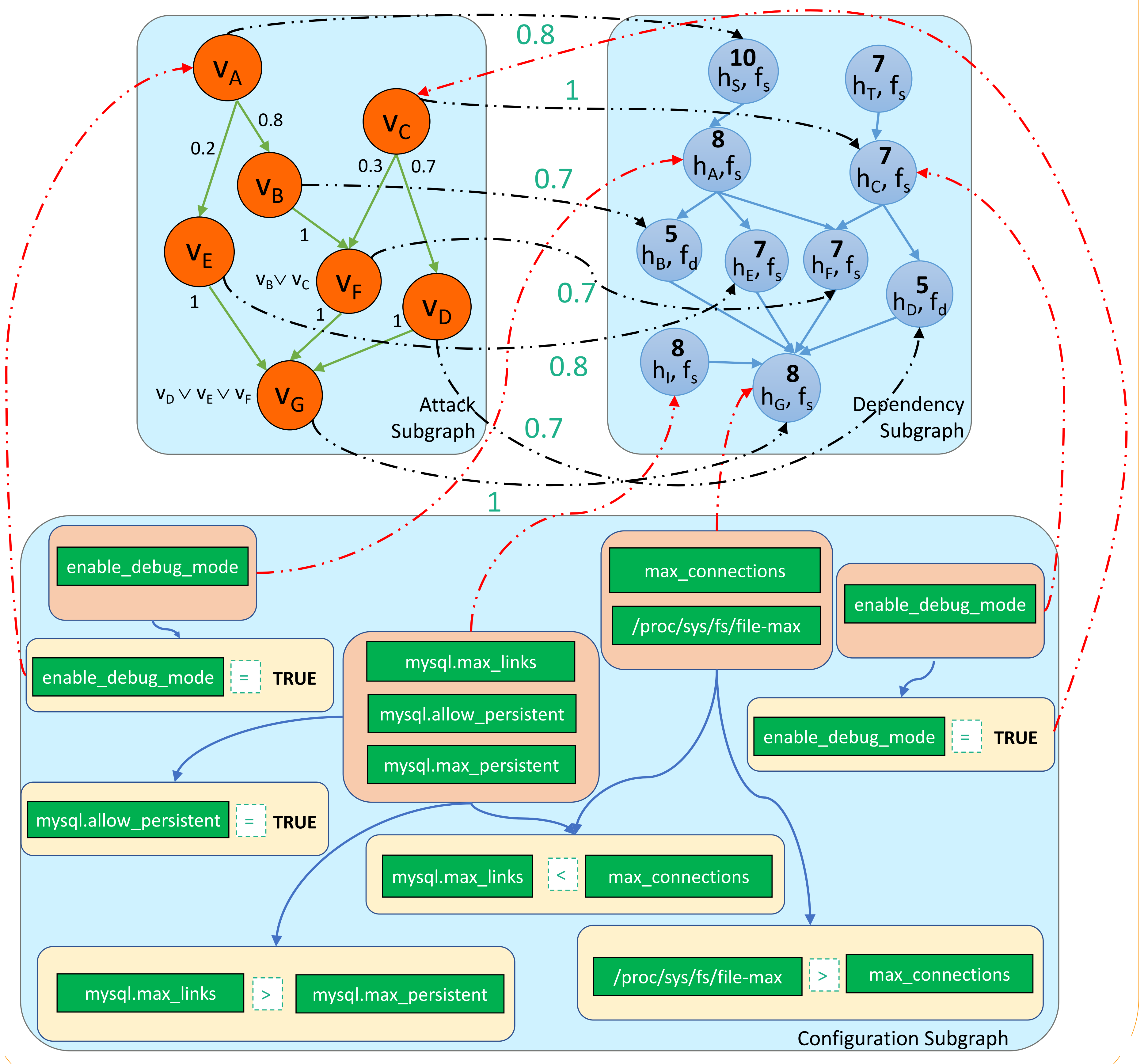
2 EXAMPLE SYSTEM:


Unmanned Aerial Vehicle (UAV)
Sensing & Planning (h_A)
Control(h_T)
Process Databus
Local Persistence Service (h_B)
Gateway (G_1)
Mission Control
Land Route Processing (h_F)
Air Route Processing (h_E)
Process Databus
Persistence Service (h_G)
Interface(h_I)
Gateway (G_2)
Sensing & Planning (h_C)
Control(h_S)
Process Databus
Local Persistence Service (h_D)
Unmanned Ground Vehicle (UGV)

Globally optimal security decisions cannot be made without dependency information: dependencies help in analyzing the cascading impact of both attacks and configuration changes.

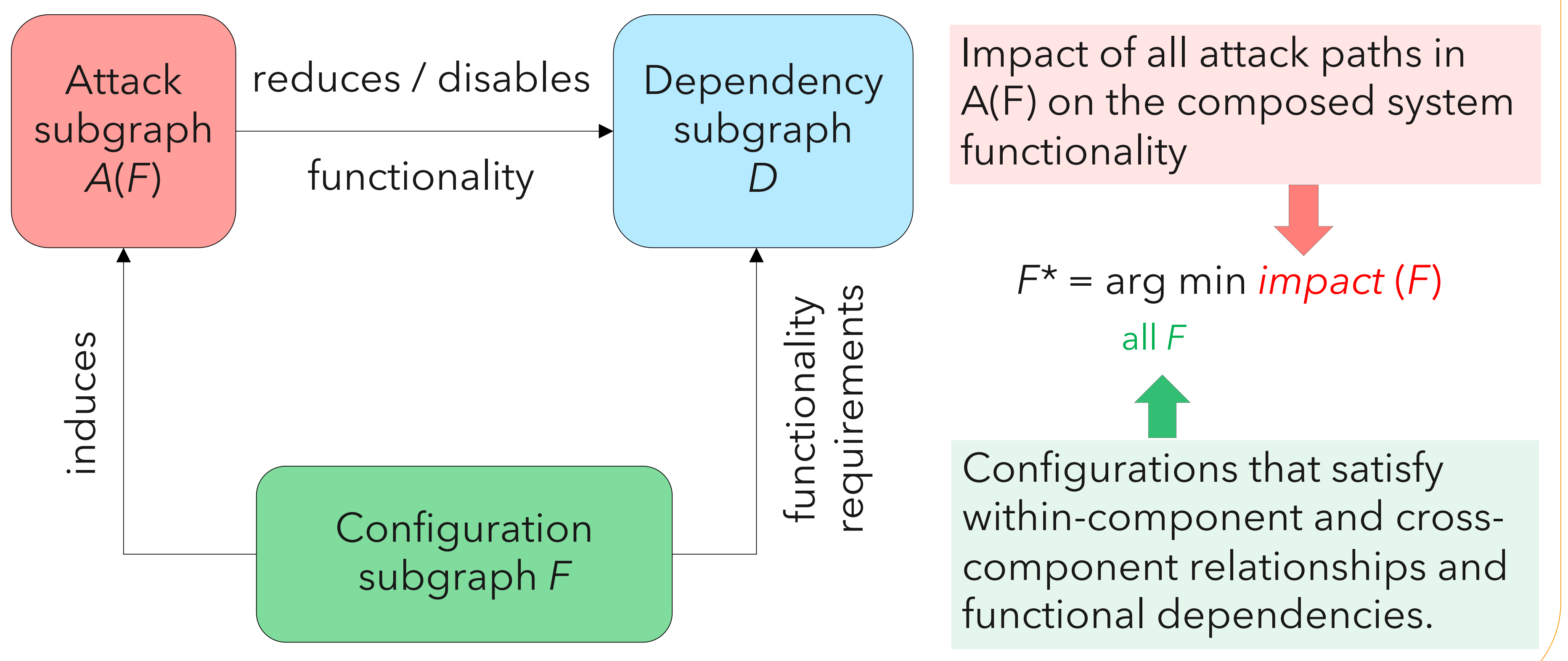
3 GRAPH-BASED MODELING APPROACH:

Express dependencies between configuration parameters, vulnerabilities, and functional components as a multi-layer graph.



4 PRELIMINARY RESULTS:

We built configuration, attack and dependency graphs for the above system in Neo4j, and solved the following optimization problem in Z3.



Impact of all attack paths in A(F) on the composed system functionality

$$F^* = \arg\min_{\text{all } F} \textit{impact}(F)$$

Configurations that satisfy within-component and cross-component relationships and functional dependencies.

5 ONGOING WORK:

- Automate the construction of configuration subgraphs from standard operating procedures and component specifications.
- Examine unsat core and tradeoff security against functionality.
- Provide evidence and explanation of secure configurations.

[1] M. Albanese and S. Jajodia, “A graphical model to assess the impact of multi-step attacks,” *Journal of Defense Modeling and Simulation*, vol. 15, no. 1, pp. 79–93, January 2018.

This work is funded by the US Department of Defense under the DARPA ConSec program. Any opinions, findings, and conclusions expressed in this material are those of the authors and do not necessarily reflect the views of the DoD or any other agency of the U.S. Government.