2018 - PDR - 747-21D - Adaptive Threat Management Tool for Cyber-based Systems - Yahya Javed

CERIAS

The Center for Education and Research in Information Assurance and Security

Adaptive Threat Management Tool for Cyber-based Systems

Yahya Javed, Tawfeeq Shawly, Muhamad Felemban, and Arif Ghafoor

URL (http://multimedia.ecn.purdue.edu/AIMS.html)

Objective: Develop resilient Cyber-based System (CBS) by incorporating an adaptive threat management mechanism throughout the life cycle of such system from design through recovery from cyber attacks.

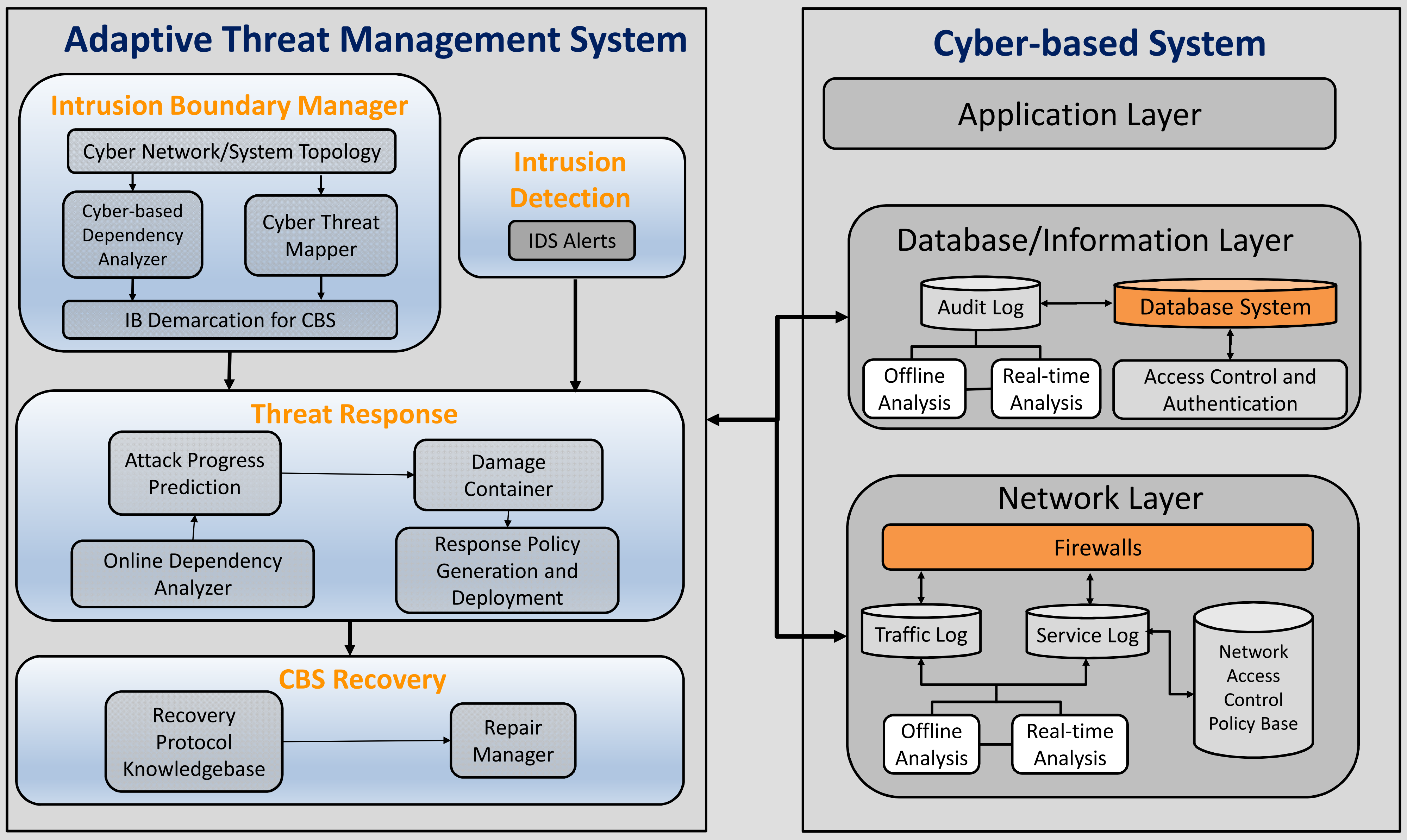
System Architecture

System Components

1. Intrusion Detection
2. Intrusion Boundary (IB) Manager
   - Damage confinement
   - Scalability
3. Threat Response
4. CBS Recovery

Proposed Solutions

1. **A**daptive **I**ntrusion **M**anagement **S**ystem (AIMS) for big datacenters
2. **A**daptive **T**hreat **M**anagement (ATM) for CBS


Adaptive Threat Management System

Intrusion Boundary Manager

Cyber Network/System Topology

Cyber-based Dependency Analyzer

Cyber Threat Mapper

IB Demarcation for CBS

Intrusion Detection

IDS Alerts

Threat Response

Attack Progress Prediction

Damage Container

Online Dependency Analyzer

Response Policy Generation and Deployment

CBS Recovery

Recovery Protocol Knowledgebase

Repair Manager

Cyber-based System

Application Layer

Database/Information Layer

Audit Log

Database System

Offline Analysis

Real-time Analysis

Access Control and Authentication

Network Layer

Firewalls

Traffic Log

Service Log

Network Access Control Policy Base

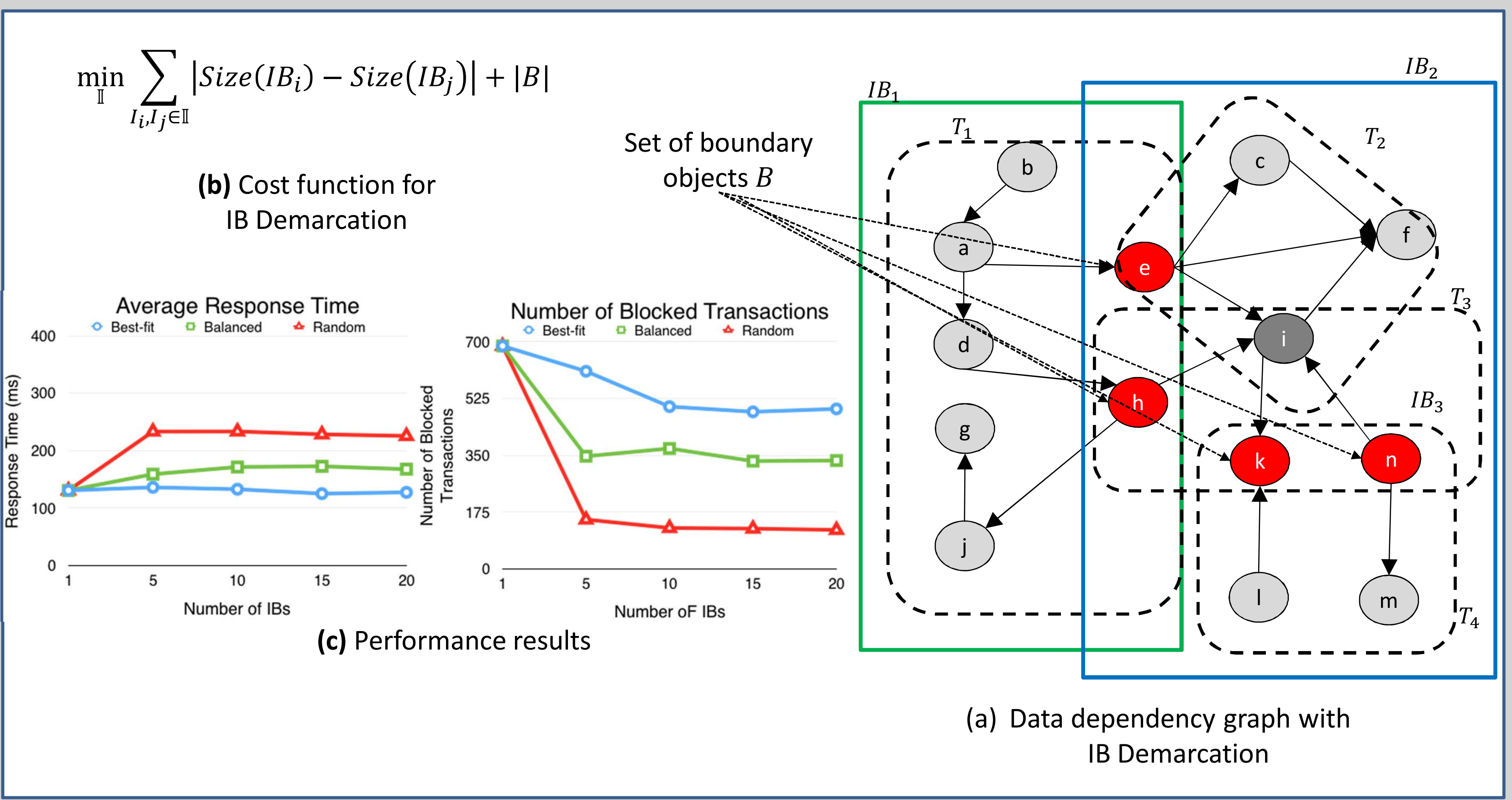
Offline Analysis

Real-time Analysis

AIMS

Solution Methodology

1. IB demarcation as a metrics-driven optimization problem for damage confinement
2. Development of an efficient intrusion response and recovery mechanism for malicious transactions
3. Development of malicious workload benchmarks for performance evaluation


$$\min_{\mathbb{I}} \sum_{I_i, I_j \in \mathbb{I}} |Size(IB_i) - Size(IB_j)| + |B|$$

(b) Cost function for IB Demarcation

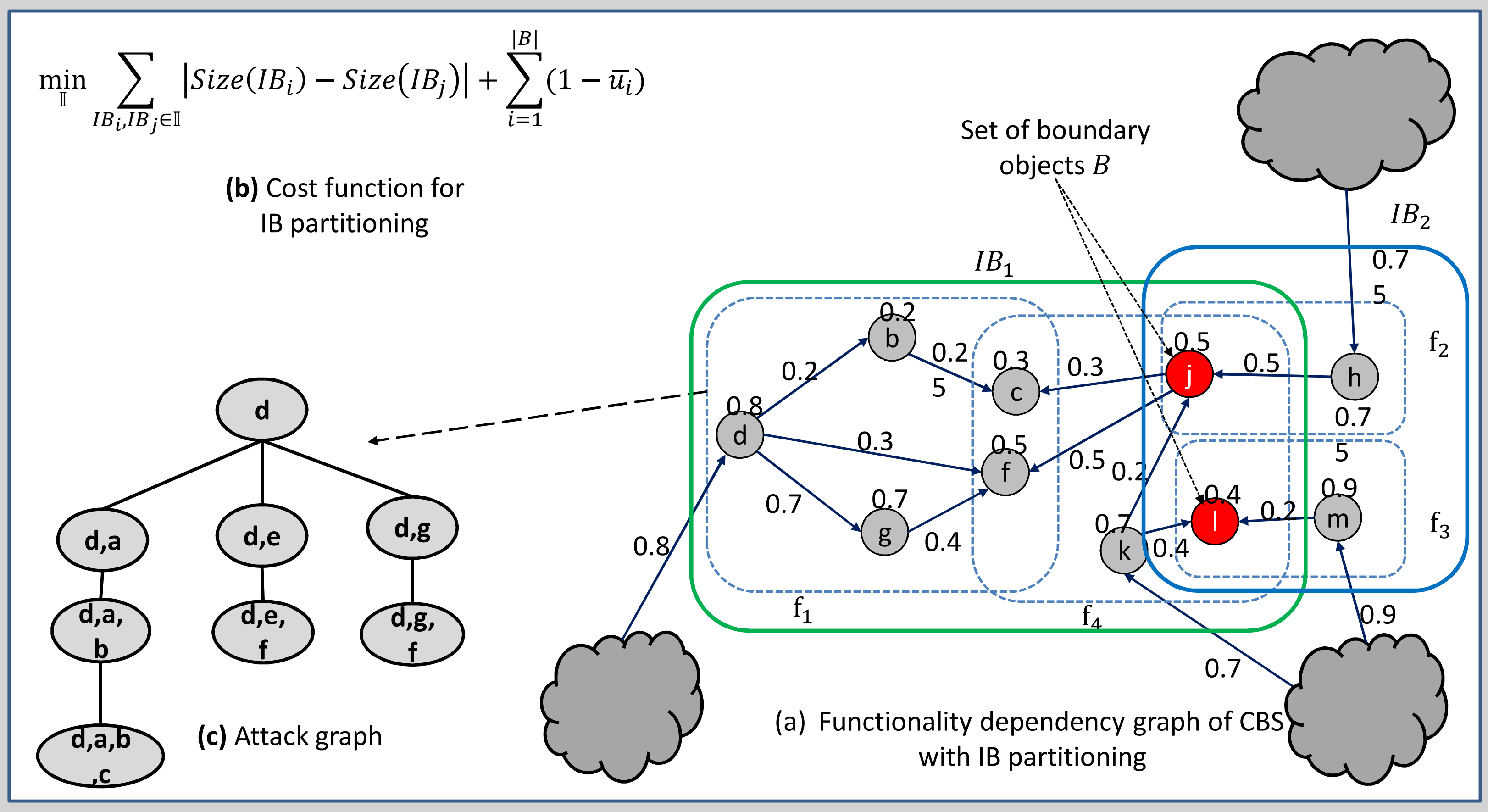
(c) Performance results

(a) Data dependency graph with IB Demarcation

ATM

Solution Methodology

1. Development of a real-time HMM-based intrusion detection
2. Development of firewall policy-based response and recovery playbook
3. Development of a risk-aware partitioning mechanism for scalable detection, response, and recovery
4. Development of an ATM prototype for testing and validation


$$\min_{\mathbb{I}} \sum_{IB_i, IB_j \in \mathbb{I}} |Size(IB_i) - Size(IB_j)| + \sum_{i=1}^{|B|} (1 - \bar{u}_i)$$

(b) Cost function for IB partitioning

(c) Attack graph

(a) Functionality dependency graph of CBS with IB partitioning

Acknowledgement: This work is supported in part by a grant from the Northrop Grumman Corporation and National Science Foundation Grant IIS-0964639.

PURDUE UNIVERSITY Discovery Park

CERIAS