CERIAS

The Center for Education and Research in Information Assurance and Security

PR-DRA: PageRank-based defense resource allocation methods for securing interdependent systems modeled by attack graphs

Mohammad Al-Eiadeh[1] and Mustafa Abdallah[2]

[1]*Purdue University in Indianapolis, Indiana, USA*

maleiad@iu.edu, abdalla0@purdue.edu

Introduction

- We focus on **developing proactive defense framework** to counteract the huge amount of different **cyberattacks** targeting **interconnected systems.**
- We utilize an evolutionary optimizer, called **Genetic Algorithm (GA)**, for identifying different potential **attack routes** that **attackers** are likely to **leverage** in their attacks.
- We use the popular **Google's PageRank (PR)** algorithm to determine the **significance** of each **asset node (critical asset)** and define the **security proportion** that should be **allocated** to **protect it.**
- We propose **four graph-theoretic** approaches to **mitigate attacks** like **stepping-stone**, **cascading failure**, **single node**, and **multi-stage attack** on interdependent systems.
- We **demonstrate** an **end-to-end framework** that combines **PageRank** with **four mitigation** methods for enhancing attack **resilience** and interdependent systems **protection**.

Motivation

- The **lack** of **efficient resource allocation** approaches has led to **wasted limited** resources and resulted in **low** or **poor protection**.
- Many studies operate by **guessing** or **assuming** the moves that **attackers** may consider and **act upon**, which is **difficult** to **predict** in real-world scenarios.
- Developing **efficient** resource allocation framework designed to **minimize cost**, **maximize protection**, and **reduce resource waste** would be **financially** beneficial for organizations.
- Developing **high-performance** resource allocation approach that operates **independently** from **guessing attackers' strategies** and provides high level of **security** is essential for **protecting interdependent systems**.

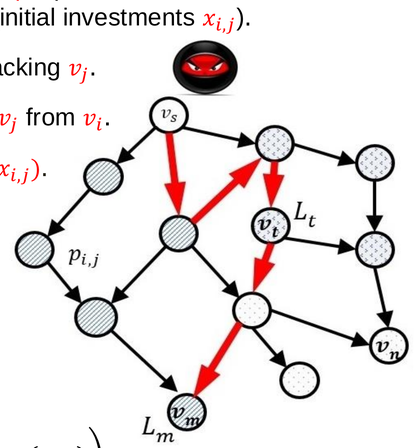
Our Contribution

- The research introduces an **end-to-end** framework for **allocating resources** to secure **interconnected systems**, **independent** of **initial guesses** about **attackers** or their **numbers**.
- The research uses **PR** algorithm, along with four allocation methods to improve system **security levels,** in which the **resources allocated** for specific asset is **proportional** to **its normalized rank**.
- Two different **metrics** are used to evaluate our methods: **PR + In-Degree Nodes**, **PR + Adjacent Nodes**, **PR + Markov Blanket**, and **PR + Min-Cut Edges**, across **four** real-world **systems** and **five baselines**.
- The source code of the **framework** is released to the community as **baseline approach** for **allocating resources** to secure interdependent systems and encourage further development with **new methods**.

Framework

Modeling Attack and Defense:

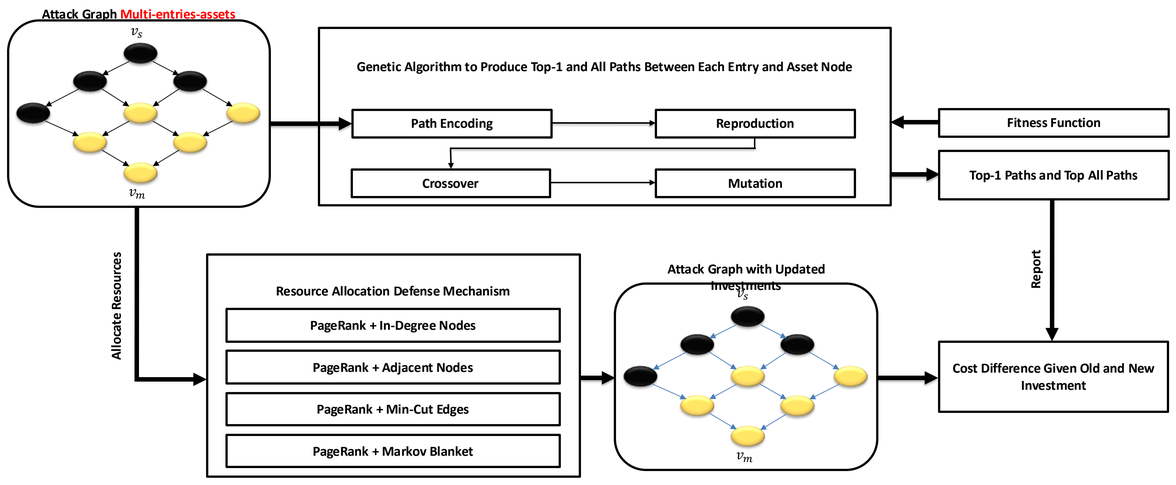
- The system is modeled using an attack graph $G = (V, E, W)$, where (V) represents entries, intermediates and assets, (E) represents attack links, and (W) represents weight (initial investments $x_{i,j}$).
- Direct edge $(v_i, v_j) \in E$ is occurred when v_i is revealed and then attacking v_j.
- Probability $\mathrm{p}_{i,j}(x_{i,j})$ indicates chance of an attacker breaching node v_j from v_i.
- The attack success probability on path P is given by $\prod_{(v_i,v_j)\in P} \exp(-x_{i,j})$.
- The defender D is responsible for protecting a set of assets $\mathrm{V_m} \subseteq V$.
- If asset $\mathrm{v_m}$ is compromised, the defender incurs a financial loss L_m.
- Resources are distributed on a set of edges $(v_i, v_j) \in E$



- The defender D_k minimizes the **cost function**:

$$C_k(x_k, x_{-k}) \triangleq \sum_{v_m \in V_k} L_m \left(\max_{P \in \mathbb{P}_m} \prod_{(v_i,v_j)\in P} p_{ij}(x_{i,j}) \right)$$

PageRank-based Security Resource Allocation Framework:

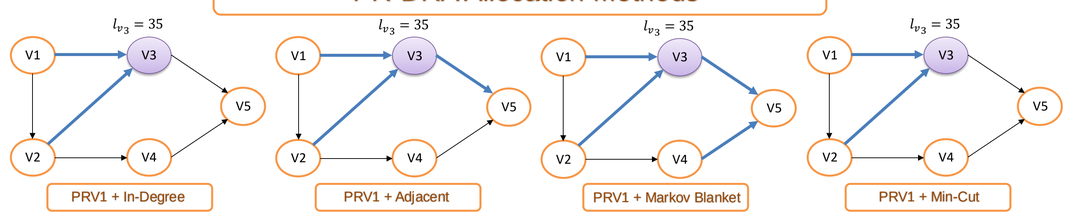


PR-DRA - Evaluation

Datasets

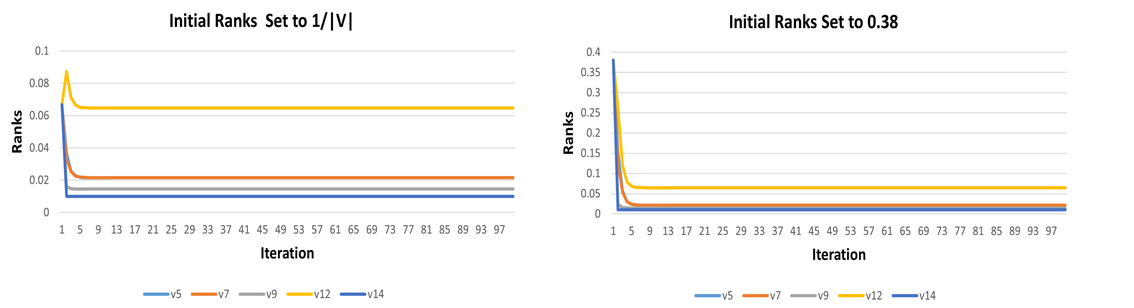
System	# Nodes	# Edges	# Critical Assets	Graph Type
SCADA	13	20	6	directed
DER.1	22	32	6	directed
E-Commerce	20	32	4	directed
VOIP	22	35	4	directed

PR-DRA Allocation Methods

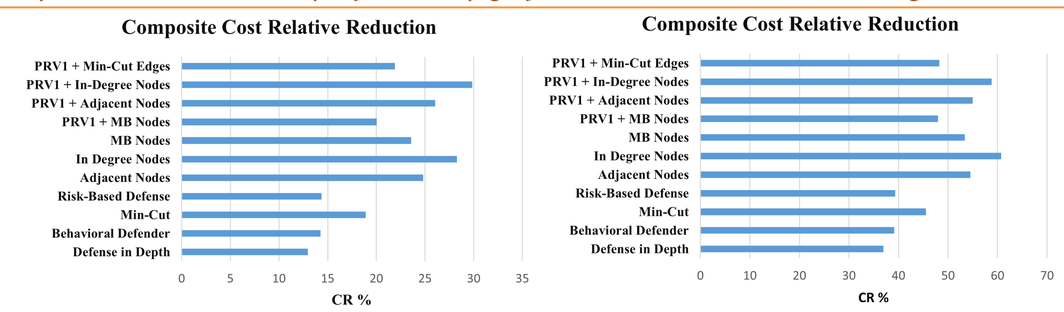


Results

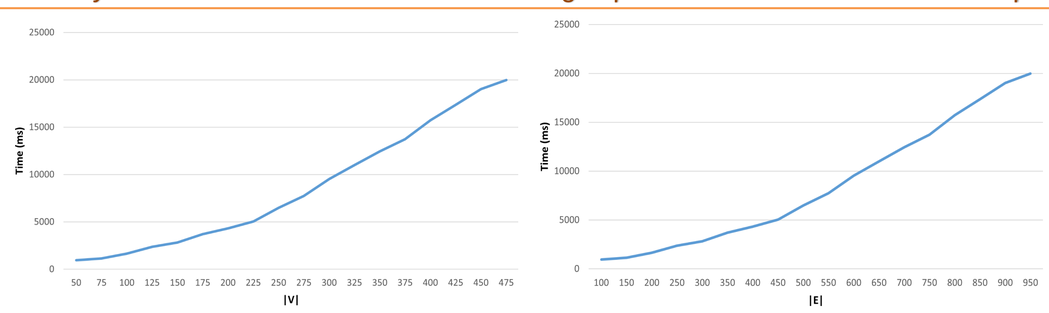
Convergence of the PageRank with Different Initial Guess for Different Attack Graphs



Comparison with Random (left) and 1s (right) Initial Investments Under Budget of 10 Units



Scalability for the Parallelized GA for Processing Top1 Attack Paths for Different Graphs



PRV1 vs PR(JGraphT) with In-Degree Under Random Initial Investments

Budget = 25 units

Dataset / System	PRV1	PR (JGraphT)
SCADA	**83.99**	79.95
DER.1	**98.07**	97.05
E-Commerce	71.8	**97.74**
VOIP	**94.69**	90

Budget = 10 units

Dataset / System	Optimized PR	PR (JGraphT)
SCADA	**63.76**	53.49
DER.1	**85.14**	80.86
E-Commerce	**94.94**	74.96
VOIP	**69.29**	66.52

Key Takeaways

- Creation of a novel **end-to-end resource allocation** framework for **mitigating** various attack types in order to **secure interdependent systems**, **regardless** of the **entry points** of attackers, and **ensuring** the **protection** of all **assets according** to their **importance**.
- **PR-DRA Framework still need improvements** to be applied in a production environment, but this work is **an important step in this direction**.
- PageRank's **reliance** on **node connectivity** is challenged in **complex networks**, where critical nodes may have **fewer connections** but **greater importance** (tackled by the optimized version).
- The resource allocation methods can be **improved** by adopting **hybrid independent defenders**, where **multiple defenders** use **different allocation** techniques in **parallel.**

Acknowledgement

This work was supported by AnalytixIN, Enhanced Mentoring Program with Opportunities for Ways to Excel in Research (EMPOWER); By the 1st Year Research Immersion Program (1RIP) Grants from the Office of the Vice Chancellor for Research at Indiana University–Purdue University Indianapolis; and in part by Lilly Endowment, Inc., by its support for the Indiana University Pervasive Technology Institute.

PURDUE UNIVERSITY

CERIAS