Network Resilience Under Epidemic Attacks: Deep Reinforcement Learning Network Topology Adaptations

Qisheng Zhang (presenter) [1] Jin-Hee Cho [2]
Terrence J. Moore [3]

[1,2]Department of Computer Science, Virginia Tech

[3]US Army Research Laboratory

IEEE GLOBECOM 2021, December 2021

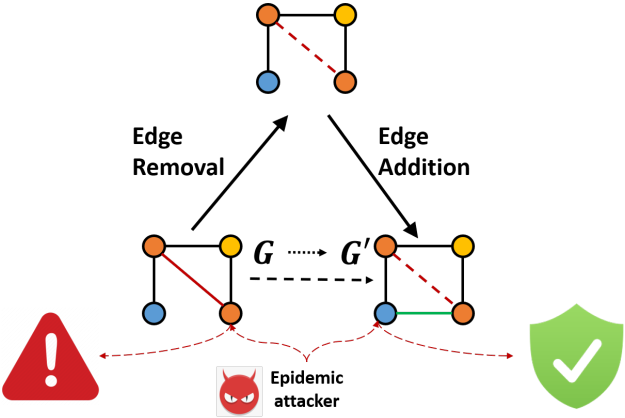
COLLEGE OF ENGINEERING
COMPUTER SCIENCE
VIRGINIA TECH.

Outline

- **Introduction**
- **Related Work**
- **Problem Statement**
- **System Model**
  - Network Model
  - Node Model
  - Attack Model
- **Proposed Framework**
  - Vulnerability Ranking of Edges and Nodes (VREN)
  - Fractal-based Solution Search (FSS)
  - DRL-based Budget Adaptation
- **Experimental Setup**
- **Numerical Results and Analyses**
- **Conclusions**

Motivation

- Achieving network security and network resilience by network topology adaptation under software polyculture environment.



Key Contributions

- Proposed a network topology adaptation technique to achieve network resilience in terms of maximizing system security, network connectivity, and system service availability.
- Presented two algorithms to support the DRL agent to efficiently identify an optimal adaptation budget strategy to meet the two system goals.
  - VREN: Vulnerability Ranking algorithm of Edges and Nodes
  - FSS: Fractal-based Solution Search algorithm
- Conducted extensive experiments to investigate the impact of three different types of objective functions to our proposed DRL scheme.
- Found that a larger size of the giant component is not necessarily aligned with higher service availability.
- Observed that a higher fraction of compromised nodes can increase actual service availability due to the existence of more paths available between nodes.

Related Work

- **Deployment of diversity-based network adaptations**
  - Metric-based: graph coloring based software allocation/assignment [1]
  - Metric-free: software assignment [2]; network topology shuffling [3]
- **DRL-based network topology shuffling**
  - Addition: adding edges to networks [4]
  - Removal: removing edges from networks [5]
  - Shuffling: redirecting edges in networks [6] [7]
- **Limitations**
  - Lack of work studying optimal edge adaptations for resilient networks
  - Limited topology operations and objective functions
  - Slow convergence for DRL agents to identify optimal solutions

---

1 Borbor et al., 2019
2 Yang et al., 2016
3 Hong et al., 2016
4 Darvariu et al., 2020
5 Dai et al., 2018
6 Chai et al., 2020
7 Zhang et al., 2020

Problem Statement

- **Main idea**: optimize network security ($\mathcal{F}_C$) + connectivity ($\mathcal{S}_G$) + service availability ($\mathcal{P}_{MD}$)
- **Objective function** :

$$\arg\max_{b_A, b_R} f(G') - f(G), \quad s.t. \quad 0 \leq b_A + b_R \leq B, \tag{1}$$

$$G : \text{original network}$$
$$G' : \text{adapted network}$$
$$b_A : \text{addition budget}$$
$$b_R : \text{removal budget}$$
$$\textbf{O-SG}: f : G \mapsto \mathcal{S}_G(G) - \mathcal{F}_C(G)$$
$$\textbf{O-MD}: f : G \mapsto \mathcal{P}_{MD}(G) - \mathcal{F}_C(G)$$
$$\textbf{O-SG-MD}: f : G \mapsto \mathcal{S}_G(G) + \mathcal{P}_{MD}(G) - \mathcal{F}_C(G)$$

System Model

- **Network Model**: A centralized system with one centralized controller
- **Node Model**
  - Activity indicator(IDS): $na_i = 1$(alive)/0(failed)
  - Compromise indicator: $nc_i = 1$(compromised)/0(not compromised)
  - Software version: $s_i \in [1, N_s]$, N_s: # of available software packages
  - Software vulnerability: $sv_i \in [0, 1]$ [8]
- **Attack Model**
  - Epidemic attacks: P_a
    - Perform two attack trials to infect its direct neighbors
    - Learn software versions along attacks
  - Packet drop attack
  - Packet modification attack

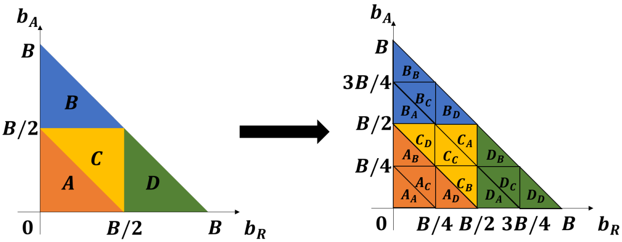
[8] The extent of a Common Vulnerabilities and Exposures (CVE) based on a Common Vulnerability Scoring System (CVSS)

Vulnerability Ranking of Edges and Nodes (VREN)

- Precision control by # of attack simulations
- Edge vulnerability level V_E: # of times it is used by attackers to compromise other nodes
- Node vulnerability level V_V: # of times it becomes an attacker (being compromised)
- Ranking system
  - R_E: edge ranking based on V_E in descending order
  - R_V: node ranking based on V_V in ascending order
- Adaptation based on budget constraints $[b_R, b_A]$
  - b_R: edge removal budget
  - b_A: edge addition budget

Fractal-based Solution Search (FSS)

- Reduce solution search space in edge addition and removal budgets
- Self-similar fractals
  - Centroid representation for each division
  - Logarithm complexity: $\lceil \log B \rceil$
    (B: the upper bound of the total adaptation budget)
- Discrete evaluation
  - Nearest integer points: (b_R, b_A)
    (b_R: edge removal budget, b_A: edge addition budget)



Proposed DeepNETAR Framework

- **DRL-based Budget Adaptation**
  - States
    - $s_t = (b_A^t, b_R^t, G_t')$
    - b_R^t: removal budget at time t; b_A^t: addition budget at time t; G_t': the network at time t
  - Actions
    - FSS: $a_t = \{A, B, C, D\}$, where $1 \leq t \leq \lceil \log_2 B \rceil$
  - Rewards
    - $\mathcal{R}(s_t, a_t, s_{t+1}) = f(G_{t+1}') - f(G_t')$, where f =O-SG/O-MD/O-SG-MD.

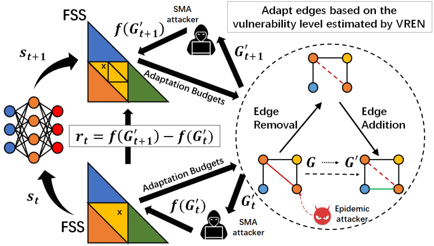


Figure 1: The overall architecture of the proposed DeepNETAR: The color of each node refers to a different software package installed in it.

Problem Statement (Recall)

- **Main idea**: optimize network security($\mathcal{F}_C$) + connectivity($\mathcal{S}_G$) + service availability($\mathcal{P}_{MD}$)
- **Objective function** :

$$\arg\max_{b_A, b_R} f(G') - f(G), \quad s.t. \quad 0 \leq b_A + b_R \leq B, \tag{2}$$

$$G : \text{original network}$$
$$G' : \text{adapted network}$$
$$b_A : \text{addition budget}$$
$$b_R : \text{removal budget}$$
$$\textbf{O-SG}: f : G \mapsto \mathcal{S}_G(G) - \mathcal{F}_C(G)$$
$$\textbf{O-MD}: f : G \mapsto \mathcal{P}_{MD}(G) - \mathcal{F}_C(G)$$
$$\textbf{O-SG-MD}: f : G \mapsto \mathcal{S}_G(G) + \mathcal{P}_{MD}(G) - \mathcal{F}_C(G)$$

Experimental Setup

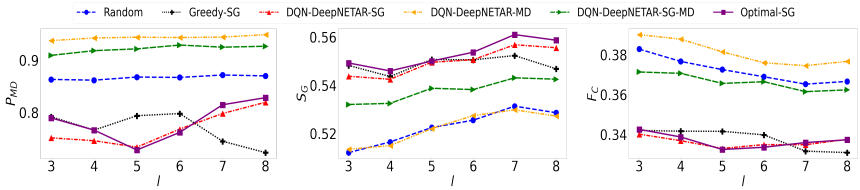
- Random Graph
  - ER: Erdős–Rényi random graph model
  - Number of nodes $N = 200$
  - Connection probability $p = 0.05$
- Attack Types Considered
  - Epidemic Attacks
    - Fraction of initial attackers in a network $P_a = 0.3$
  - Packet drop attack
    - Packet drop probability $P_d = 0.5$
  - Packet modification attack
    - Packet modification probability $P_m = 0.5$

Experimental Setup

Table 1: Key Design Parameters, Meanings, and Default Values

Param.	Meaning	Value
n_a	Number of attack simulations	500
n_r	Number of simulation runs	200
n_e	Training episodes of DRL-based schemes	1000
N	Total number of nodes in a network	200
k	Upper hop bound for edge addition	3
γ	Intrusion detection probability	0.9
P_{fn}, P_{fp}	False negative or positive probability	0.1, 0.05
P_d	Packet drop probability	0.5
P_m	Packet modification probability	0.5
λ	Constant used in packet forward failure rate	0.1
x	Degree of software vulnerability	0.5
p	Connection probability between pairs of nodes in an ER network	0.05
l	Number of software packages available	5
P_a	Fraction of initial attackers in a network	0.3
B	Upper bound of the total adaptation budget	500

Effect of Varying the Number of Software Packages Available (I) under an ER Network



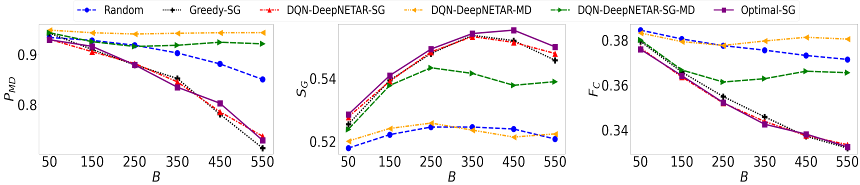
(a) Delivery of correct messages ($\mathcal{P}_{MD}$)

(b) Size of the giant component ($\mathcal{S}_G$)

(c) Fraction of compromised nodes ($\mathcal{F}_C$)

- As I increases, $\mathcal{F}_C$ drops, $\mathcal{S}_G$ and $\mathcal{P}_{MD}$ increase.
- DQN-DeepNETAR-SG has the lowest $\mathcal{F}_C$ and $\mathcal{P}_{MD}$.
- DQN-DeepNETAR-MD has the highest $\mathcal{F}_C$ and the highest $\mathcal{P}_{MD}$.
- DQN-DeepNETAR-SG-MD achieves a relatively high security level with the fairly good service availability.

Effect of Varying the Upper Bound of the Total Adaptation Budget (B) under an ER Network



(a) Delivery of correct messages ($\mathcal{P}_{MD}$) (b) Size of the giant component ($\mathcal{S}_G$) (c) Fraction of compromised nodes ($\mathcal{F}_C$)

- Higher B decreases $\mathcal{P}_{MD}$ and $\mathcal{F}_C$, but maximal $\mathcal{S}_G$ is obtained with different B under different schemes.
- Once the optimal budget is identified, higher B would slightly degrade the performance since higher B corresponds to a larger search space.

Conclusions & Future Work

Conclusions:

- Proposed a DRL-based framework, DeepNETAR, to handle multiple, competing objectives regarding system vulnerability, connectivity, and service availability.
- Proppосed DQN-DeepNETAR-SG-MD can better ensure security, connectivity, and service availability simultaneously with an appropriate evaluation function.
- Found that the size of the giant component, as a network connectivity metric, is more related to security rather than actual service availability under epidemic attacks.

Future Work Directions:

- Extend our single agent DRL-based approach to a multi-agent DRL-based approach for a large-scale network.
- Explore our work to a network shuffling-based moving target defense (MTD).

Any Questions?

Thank you!

Qisheng Zhang at

qishengz19@vt.edu

National Capital Region Campus

7054 Haycock Rd., Office 314

Falls Church, VA 22043

COLLEGE OF ENGINEERING
COMPUTER SCIENCE
VIRGINIA TECH.