



### Institutional Sign In

All



ADVANCED SEARCH

Conferences > 2024 International Conference...

# Game-Theoretic Method for Optimal Initial Allocation of Honeypots for Enhanced Network Security

Publisher: **IEEE**

[Cite This](#)



Hamidreza Asefi-Ghamari ; Murtadha Hssayeni ; Imad Mahgoub [All Authors](#) ...



53  
Full  
Text Views

## Alerts

[Manage Content Alerts](#)  
[Add to Citation Alerts](#)

### Abstract



Downl  
PDF

#### Document Sections

- I. Introduction
- II. Related Work
- III. Environment Model
- IV. Numerical Analysis
- V. Conclusion and Future Work

#### Abstract:

In this paper, we introduce a novel algorithm for the initial placement of honeypots. Our method is grounded in a two-person, zero-sum game framework that rigorously cons... [View more](#)

#### Metadata

##### Abstract:

In this paper, we introduce a novel algorithm for the initial placement of honeypots. Our method is grounded in a two-person, zero-sum game framework that rigorously considers various factors: the cost of deploying honeypots, the effectiveness of defense strategies, the expenses borne by attackers, the consequences of successful attacks, and the value of network nodes. The cornerstone of our approach is a reward function designed to incentivize defenders to focus on securing high-value nodes, thereby enhancing overall network security. Through comprehensive simulations that account for changing target nodes and node weights, our algorithm demonstrates superior adaptability and efficacy in bolstering defenses against sophisticated cyber threats in dynamic networks such as the Internet of Battlefield Things (IoBT) networks, filling a critical void in existing security paradigms.

**Published in:** 2024 International Conference on Smart Applications, Communications and Networking (SmartNets)

**Date of Conference:** 28-30 May 2024

**DOI:** 10.1109/SmartNets61466.2024.10577718

**Date Added to IEEE Xplore:** 05 July 2024

**Publisher:** IEEE

**Conference Location:** Harrisonburg, VA, USA

[Authors](#)

[Figures](#)

[References](#)

[Keywords](#)

[Metrics](#)

[More Like This](#)



▶ ISBN Information:

▼ ISSN Information:

☰ Contents

I. Introduction

In cybersecurity, combating Advanced Persistent Threats (APTs) remains a paramount concern [6], especially as they target higher-value network re-sources and exploit vulnerabilities through exten-sive reconnaissance. Honeypots have long been rec-ognized as valuable tools serving as decoys to mis-lead and trap attackers [1]. However, the strategic deployment of honeypots and optimizing their ini-tial placement remains complex issues. Optimal initialization of honeypot locations is crucial in coun-tering reconnaissance attacks because these attacks involve adversaries stealthily gathering information about a network's vulnerabilities. Defenders can mislead attackers about the network's true layout and weaknesses by strategically placing honeypots. This misdirection wastes the attacker's resources and provides defenders valuable intelligence about attack methods and intentions. Effective initial hon-eypot placement can turn the tables on attackers, transforming their reconnaissance phase into an opportunity for defenders to enhance their security posture and prepare for future attacks.

Authors	▼
Figures	▼
References	▼
Keywords	▼
Metrics	▼

More Like This

Game Theory in Internet of Things: A Survey  
 IEEE Internet of Things Journal  
 Published: 2022

A Game Theory Approach to Heterogeneous Resource Management: Work-in-Progress  
 2020 International Conference on Embedded Software (EMSOFT)  
 Published: 2020

Show More

**IEEE Personal Account**

CHANGE USERNAME/PASSWORD

**Purchase Details**

PAYMENT OPTIONS  
VIEW PURCHASED DOCUMENTS

**Profile Information**

COMMUNICATIONS PREFERENCES  
PROFESSION AND EDUCATION  
TECHNICAL INTERESTS

**Need Help?**

US & CANADA: +1 800 678 4333  
WORLDWIDE: +1 732 981 0060  
CONTACT & SUPPORT

**Follow**



About IEEE *Xplore* | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | IEEE Ethics Reporting | Sitemap | IEEE Privacy Policy

A public charity, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2024 IEEE - All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies.

**IEEE Account**

- » Change Username/Password
- » Update Address

**Purchase Details**

- » Payment Options
- » Order History
- » View Purchased Documents

**Profile Information**

- » Communications Preferences
- » Profession and Education

» [Technical Interests](#)

**Need Help?**

» **US & Canada:** +1 800 678 4333

» **Worldwide:** +1 732 981 0060

» [Contact & Support](#)

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2024 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.