지능형 시스템을 적용한 MTD 전략에 대한 연구 동향 분석

허남정[1], 이세한[2], 최상훈[3,*], 박기웅[3,†]
[1]세종대학교 시스템보안안연구실 (지능형드론 융합전공) 석사과정
[2]세종대학교 시스템보안연구실 (지능형드론 융합전공) 박사과정
[3,†] 세종대학교 정보보호학과 교수 (*연구교수)
uskawjdu@gmail.com, sehanlee141@sju.ac.kr, csh0052@gmail.com,
woongbak@sejong.ac.kr

An Analysis of Research Trends on MTD Strategy through Intelligent Systems

Nam-Jung Heo[1], Se-Han Lee[1], Sang-Hoon Choi[2], Ki-Woong Park[2,†]
[1]SysCore Lab. (Convergence Engineering for Intelligent Drone), Sejong University
[2,†] Dept. of Computer and Information Security, Sejong University

요 약

최근 인간의 인지 능력을 모방한 지능형 MTD 연구가 주목받고 있다. 지능형 MTD는 기존 전략에 성능 오버헤드를 줄이고 더 강력한 보안 시스템을 제공한다는 점에서 향후 미래 보안 기술로 예상된다. 본 논문에서는 지능형 시스템과 MTD 전략에 관한 연구들을 검토한다. 연구 논문에서는 지능형 MTD를 위한 관점 분류 연구에 초점을 맞춘다. 그 후, 해당 관점에 일치하는 추가적인 연구논문을 조사하여 향후 지능형 MTD의 연구 방향을 제시한다. 지능형 MTD는 동적 방어 체계의 효율성을 높이고 공격자의 공격에 적응하여 최적의 전략을 선택할 수 있는 방어 체계로서 미래 보안의 중요한 역할을 수행할 것이다.

1. 서론

최근 사이버 공격의 위협을 방지하고 사전 예방의 목적으로서 사이버 공격 목표를 교란시켜 공격자의 공격 효율성을 낮추는 사이버 보안 전략인 MTD (Moving Target Defense)가 많은 컴퓨팅 시스템에서 주목받고 있다 [1].

공격자들은 취약점을 파악하고 침입하는 과정에서 체계적인 사이버 킬체인(Cyber-Kill chain)을 따른다. 현재 대부분의 시스템 보안에서는 정적인 시스템을 가지고 있으며 정적 시스템은 재구성하는데 많은 시간과 노력이 필요로 하다. 따라서 공격자는 대상 시스템에 침입하여 취약점을 찾는데 충분한 시간을 들일 수 있다 [2].

반면 MTD 전략을 구현한 시스템은 동적으로 설계되어 있으며, 공격자가 시스템에 침투하여 취약점을 찾는 것을 어렵게 만든다. 이러한 MTD 전략을 통해 사이버 킬 체인을 무력화하고 지속적인 위협으로부터 시스템을 보호하는 데 도움이 된다 [3].

†교신저자: 박기웅 (세종대학교 정보보호학과 교수)

향상된 보안과 자동화된 시스템을 구현하기 위해서는 지능형 구조를 결합한 MTD 전략 기술은 매우 효과적이다. “지능형”이란 인간의 인지 작업을 자동화하는 것을 의미한다 [4]. Yingxu W, [5] 연구에 따르면, 지능은 계층적 지능 모델(HIM)을 분류될 수 있다. 이 모델에서 인지 지능은 비선형적인 특징을 가지며, 자율적인 추론에 의해 유도 및 추론 기반 행동을 생성할 수 있다.

인간의 인지 지능을 자동화한 지능형 MTD 전략이 규모가 크고 복잡한 작업을 처리할 수 있어 상당한 주목을 받고 있다. 기존 MTD 전략과 비교해 지능형 MTD는 비용 절감과 적응성 증가 등 향상된 보안을 얻을 수 있다. 하지만 지능형 MTD를 분류하는 포괄적인 관점에 대한 연구가 부족하다는 지적이 있다. 본 논문에서는 지능형 MTD에 연구 트렌드와 기술에 대하여 논의할 것이다 [6].

본 논문의 구성은 다음과 같다. 제2장에서는 MTD의 배경지식, 제3장에서는 MTD 전략 개요 대해 기술한다. 제4장에서는 지능형 MTD 관련 연구 조사 설명하고, 5장에서는 결론을 제시하고 향후 연

구 방향에 대해 논의한다.

2. 배경 지식

기존의 시스템 보안은 정적 시스템으로 설명된다. 반면, MTD 전략을 적용한 시스템은 동적 시스템으로 설명한다. <표 1>에서는 이러한 정적 시스템과 동적 시스템의 특징을 비교한다. 정적인 시스템은 단순하지만 재구성이 어려운 반면, 동적 시스템은 복잡하고 재구성이 쉽다는 것이 특징이다 [7].

<표 1> 정적인 시스템과 동적인 시스템 비교

구분	정적 시스템	동적 시스템
시스템 재구성	많은 노력과 시간 필요	적은 노력과 시간 필요
제어 구조의 복잡성	단순한 제어구조	복잡한 제어구조

MTD(Moving Target Defense) 전략은 시스템의 속성을 주기적으로 변화시켜, 시스템의 공격 벡터를 공격자에게 예측할 수 없게 만드는 기술이다.

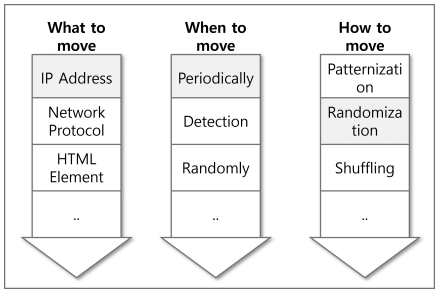
MTD 전략은 여러 연구를 통해 3가지의 관점을 가진다 [1, 8]. 이러한 관점들은 MTD 전략을 다양한 측면을 보다 명확하게 이해하는데 중요한 관점이 될 수 있다.

· **What to move** : 이 관점에서는 MTD 전략을 사용하여 보안 기술을 구현할 때, 어떤 구성 요소를 이동시키나 변경할지를 결정한다. IP 주소, MAC 주소, HTML 속성 요소 등이 포함될 수 있다.

· **When to move** : 이 관점에서는 MTD 전략을 사용한 보안 기술이 대상 구성 요소를 언제 이동시키거나 변경할지 결정한다. 이는 주기적으로 구성 요소를 변경할 수도 있으며, 공격 행위가 탐지되었을 때 변경할 수도 있다.

· **How to move** : 시스템의 구성 요소를 어떻게 이동하거나 변경할지를 결정한다. 구성 요소에 랜덤화, 패턴화를 적용하는 것을 포함한다.

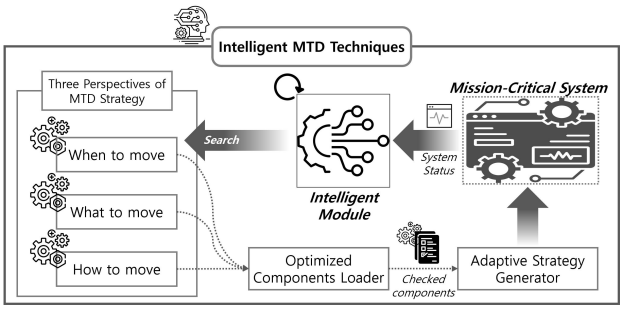
[그림 1]은 세 관점에서 각각 하나씩 선택하여 상호작용을 일으키는 MTD 전략의 예시이다.



(그림 2) MTD 전략의 3가지 관점.

예를 들어, 시스템의 시간에 흐름에 따라 주기적(When to move)으로 IP 주소(What to move)를 랜덤(How to move) 하게 변경하는 MTD 전략을 사용할 수 있다.

3. 지능형 MTD 전략 개요



(그림 3) 지능형 MTD의 동작 흐름.

[그림 2]는 지능형 MTD의 동작 흐름을 도식화한 것이다. 지능형 MTD 전략은 인간의 인지 지능을 자동화한다. 기존의 MTD 전략은 개발자가 수동으로 시스템의 구성 요소를 파악하고 시스템에 맞는 최적의 MTD 전략을 적용했다. 하지만 지능형 MTD에서는 시스템이 스스로 구성 요소를 파악하고 공격자의 행동 특성에 따라 방어 전략을 구축한다.

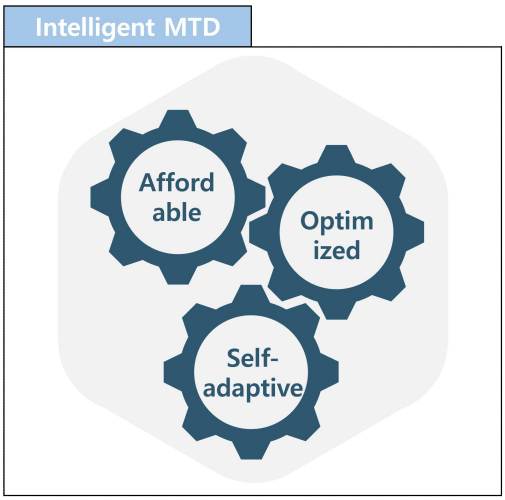
Rongbo et al. [6] 연구에서는 이러한 지능형 MTD를 Affordable, Optimized, Self-adaptive 로서 세 가지 관점을 제시한다.

· **Affordable:** MTD 기술을 적용하는 데 드는 배치 비용과 시스템의 오버헤드를 줄이는 것을 의미한다.

· **Optiomized:** 공격 유형, 시스템 구성, 시스템의 오버헤드 등 다양한 제약 조건을 고려하여 최적의 방어 전략을 스스로 선택한다. 이는 강화 학습 모델을 사용하여 제약 환경에서 어떤 행동을 취하면 방어에 성공할 수 있는지 보상을 주는 방식으로 사용할 수 있다.

· **Self-Adaptive:** 시스템이 공격자의 행동 특성에 적응하고 그에 따라 방어 전략을 조정한다. 이는 기계 학습 알고리즘을 사용하여 공격을 탐지했을 때 MTD를 적용하는 방식으로 사용할 수 있다.

이러한 세 가지 관점들은 [그림 3]과 같이 조화를 이루어져 동작했을 때, 지능형 MTD는 다양한 시스템의 제약 조건과 공격자의 행동 특성을 반영하여 최적의 MTD 전략을 스스로 선택할 수 있다.



(그림 4) 지능형 MTD의 3가지 관점.

4. 지능형 MTD 연관 최신 기술 연구 조사

본 장에서는 Rongbo et al. [6] 연구에서 제안한 세 가지 관점으로 최근 MTD 연구들을 <표 2>에서 분류한다. 지능형 MTD 전략의 인지 지능은 주로 비선형적인 특징을 가지고 있으며, 딥러닝 기반의 MTD 전략이 많이 사용된다.

Fengyuan et al. [9]은 1D-CNN 모델을 활용해 DoS 또는 네크워크의 침입을 탐지하고 IP 후킹을 적용하는 아키텍처를 제안한다. 해당 아키텍처는 CNN 모듈을 사용하여 네트워크 침입을 감지한 후, 기본 장식의 오버헤드 문제를 최소화하기 위해 IP 후킹을 적용한다.

Shardul et al. [10]은 HTML 요소를 지능적으로 랜덤화하는 새로운 MTD 기술을 제안하여, 사용자가 사용하기 편리하면서 효과적으로 웹봇을 방어할 수 있게 한다. 기존 방식인 CAPTCHA 시스템은 사용자가 문제를 해결하는 데 많은 시간과 노력을 사용하여 사용성이 떨어지는 문제가 있다.

Eitan et al. [11]은 강화 학습 알고리즘을 사용하여 다양한 공격 방식에 대응하는 최적의 방어 기술을 선택하는 전략을 제시한다. 더 나아가, 이 연구는 공격자의 공격 방식에 따라 스스로 최적의 MTD 전략을 선택하는 가능성을 보인다.

Zhuoyuan et al. [12]은 서버 상황에 따라 DDoS 공격에 적응적으로 대응할 수 있는 다중 에이전트 강화 학습 시스템을 제안한다. 고위험 클러스터와 잠재적 위험 클러스터라는 두 개의 서로 다른 클러스터를 설정하고, 에이전트가 공격받은 서버를 고위험 클러스터로 이동시킨 후 일정 시간 동안 공격이 없으면 잠재적 위험 클러스터로 다시 복귀시킨다.

Xiaoyu X et al. [13]은 공격자의 스캐닝 공격을 탐지하고 IP 호킹을 적용한다. 기존보다 시스템의 오버헤드를 줄이는 경량화된 CNN 모델을 제안한다.

Yuyang et al. [14]은 다목적 마르코프 결정 프로세스(MOMDP)를 사용하여 셔플링 기반 MTD의 오버헤드와 성능에 미치는 영향을 파악한다. 이후 셔플링 기반 MTD의 성능과 오버헤드의 사이의 균형을 이루는 최적의 전략을 제안한다.

<표 2> 지능형 MTD 세가지 관점 분류

Ref.	Aff	Opt	Self-Ada
[9]	X	X	√
[10]	√	X	X
[11]	X	√	X
[12]	X	X	√
[13]	√	X	√
[14]	√	√	X

5. 결론

본 논문에서는 지능형 MTD 분야의 최신 연구 동향을 검토한다. 그리고 Rongbo et al. [6] 연구에서 제안한 세 가지 관점을 기반으로 하여 추가적인 논문을 조사하였다. 현재 지능형 MTD 전략 연구들은 각자의 다른 연구 분야에 집중되어 있다. 이는 지능형 MTD에 대한 통합적인 연구 체계가 부족하다는 것을 의미한다. 단편적으로 흩어져 있는 MTD 연구들을 통합하고 분류할 수 있는 명확한 관점에 대한 추가적인 연구가 필요하다. 지능형 MTD 연구에 대해 완성 단계에 가까워지면, 시스템 보안 자동화에 있어 중요한 역할이 될 것이다.

사사정보

본 논문은 과학기술정보통신부의 재원으로 정보통신기획평가원(IITP)의 정보보호핵심원천기술개발(Project No. RS-2024-00438551, 50%), 정보통신방송혁신인재양성사업(Project No. 2021-0-01816, 30%) 및 국방ICT융합연구(Project No. 2022-11220701, 20%)의 지원을 받아 수행된 연구임.

참고문헌

[1] J.-H. Cho et al., “Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense”, IEEE Communications Surveys & Tutorials, vol.22 no.1, pp.709-745, 2020.

[2] M. Zhu, Z. Hu and P. Liu, “Reinforcement Learning Algorithms for Adaptive Cyber Defense against Heartbleed”, Proceedings of the First ACM Workshop on Moving Target Defense (MTD ‘14), 2014, pp.51-58.
[3] M. Khosravi-Farmad et al., “Moving Target Defense Against Advanced Persistent Threats for Cybersecurity Enhancement”, IEEE 8th International Conference on Computer and Knowledge Engineering (ICCKE), Mashhad, Iran, 2018, pp.25-26.
[4] Stephanopoulos G., and Han C., “Intelligent systems in process engineering: A review”, Computers & Chemical Engineering, vol.20, no.6-7, pp.743-791, 1996.
[5] Y. Wang et al., “On Autonomous Systems: From Reflexive, Imperative and Adaptive Intelligence to Autonomous and Cognitive Intelligence”, IEEE 18th International Conference on Cognitive Informatics & Cognitive Computing, Milan, Italy, 2019, pp.7-12.
[6] R. Sun et al., "A Survey on Moving Target Defense: Intelligently Affordable, Optimized and Self-Adaptive", Applied Sciences, vol.13, no.9, 2023.
[7] M. Zal, M. Michalski and P. Zwierzykowski, “Implementation of a Lossless Moving Target Defense Mechanism”, Electronics, vol.13, no.5, 2024.
[8] S.-H. Lee et al., “MTD-Diorama: Moving Target Defense Visualization Engine for Systematic Cybersecurity Strategy Orchestration”, Sensors, vol.24, no.13, pp.4389, 2024.
[9] F. Shi et al., “AHIP: An Adaptive IP Hopping Method for Moving Target Defense to Thwart Network Attacks”, 2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Rio de Janeiro, Brazil, 2023, pp.1300-1305.
[10] S. Vikram, C. Yang and G. Gu, “NOMAD: Towards non-intrusive moving-target defense against web bots” IEEE Conference on Communications and Network Security (CNS), 2013, pp.55-63.
[11] Eitam F. et al., “Defending via strategic ML selection”, arXiv preprint arXiv:1904.00737, 2019.
[12] Z. Li et al., “MARL-MOTAG: Multi-Agent Reinforcement Learning based Moving Target Defense to thwart DDoS attacks”, 2022 International Conference on Networking and Network Applications (NaNA), Urumqi, China, 2022.
[13] X. Xu et al., “An Adaptive IP Hopping Approach for Moving Target Defense Using a Light-Weight CNN Detector”, Security and Communication Networks, pp.8848473, 2021.
[14] Y. Zhou et al., “Cost-effective moving target defense against DDoS attacks using trilateral game and multi-objective Markov decision processes”, Computers & Security, vol.97, pp.101976, 2020.