

MODELING CYBERSECURITY POLICIES AT NUCLEAR POWER PLANTS VIA AXELROD ITERATED PRISONER'S DILEMMA INERTIAL TOURNAMENTS

Vinnitsia Institute of Trade and Economics of State University of Trade and Economics

Анотація

Кібербезпеку можна розглядати не тільки як процес виявлення загроз, а і як поведінкову надійність програмних компонентів та політик безпеки, які оцінюються шляхом багаторазових взаємодій у віртуальному тестовому середовищі, подібно до того, як працює антивірусне програмне забезпечення. Метою є виявлення поведінкових закономірностей, які сприяють безпечному та стабільному функціонуванню інформаційних систем атомної електростанції. Отримані результати свідчать, що взаємні та адаптивні поведінкові політики з інерційністю забезпечують вищий рівень довгострокової довіри порівняно зі стратегіями, які ґрунтуються виключно на безумовній довірі або надмірних обмеженнях.

Ключові слова: атомна електростанція, політика кібербезпеки, турніри Аксельрода, інерційна поведінка.

Abstract

Instead of treating cybersecurity exclusively as a process of threat detection, the behavioral reliability of software entities and security policies can be evaluated through repeated interactions in a virtual testing environment, similarly to how like antivirus software works. The objective is to identify behavioral patterns that contribute to secure and stable operation of nuclear power plant information systems. The results suggest that reciprocal and adaptive behavioral policies with inertia offer superior long-term trustworthiness compared with strategies based solely on unconditional trust or excessive restriction.

Keywords: nuclear power plant, cybersecurity policy, Axelrod tournaments, inertial behavior.

Introduction

Modern nuclear power plants rely on complex digital infrastructures that integrate industrial control systems, supervisory control and data acquisition platforms, safety monitoring subsystems, engineering workstations, and communication networks [1]. While digitalization improves operational efficiency and monitoring capabilities, it also increases exposure to cybersecurity threats [2]. Conventional cybersecurity mechanisms focus primarily on detecting malicious software, unauthorized access attempts, and abnormal network activity. However, many cyber incidents arise not from immediately identifiable attacks but from gradual violations of trust, unexpected software behavior, compromised updates, or interactions among components whose long-term operational effects are insufficiently understood [3]. Hence, this study proposes an alternative perspective based on Axelrod Iterated Prisoner's Dilemma tournaments [4, 5]. Subsequently, instead of treating cybersecurity exclusively as a process of threat detection, the proposed approach evaluates the behavioral reliability of software entities and security policies through repeated interactions in a virtual testing environment (like antivirus software). The objective is to identify behavioral patterns that contribute to secure and stable operation of nuclear power plant information systems.

Methods

The proposed framework represents software components, communication agents, update mechanisms, and security policies as autonomous entities participating in repeated interactions within a simulated environment. Each entity possesses a behavioral strategy that determines its response to other entities. Cooperative behavior corresponds to compliance with security protocols, transparent information exchange, proper authentication procedures, and adherence to operational constraints [3]. Defective behavior represents actions such as unauthorized privilege escalation, concealment of information, protocol violations, suspicious communication attempts, or other deviations from expected operation. The set of N admissible Axelrod strategies is denoted by $S = \{s_i\}_{i=1}^N$.

Before deployment into operational systems, candidate entities participate in an Axelrod-style tournament against a library of predefined behavioral profiles. These profiles include trusted components, faulty components, compromised agents, deceptive agents, and adaptive adversarial agents. During repeated interactions, each participant accumulates a performance score reflecting several evaluation criteria [6, 7]:

- 1) compliance with cybersecurity policies;
- 2) robustness against deceptive behavior;
- 3) stability of operation;
- 4) ability to maintain cooperation with trusted entities;
- 5) resistance to exploitation by malicious entities.

The tournament environment functions as an advanced behavioral sandbox. Rather than evaluating isolated actions, it examines how entities behave over extended sequences of interactions. The analysis focuses on three aspects:

1. Long-term trustworthiness of software entities.
2. Resilience of cybersecurity policies under repeated interactions.
3. Ability to identify potentially dangerous behavioral patterns before deployment.

This concept gives a natural interpretation of the population of strategies already present in the Axelrod framework. The main eight parts of the behavioral sandbox are:

- 1) trusted control modules;
- 2) legacy software;
- 3) newly installed updates;
- 4) third-party vendor software;
- 5) compromised components;
- 6) simulated malware;
- 7) adaptive attackers;
- 8) security policies themselves.

Denote the set of those parts above by Y . Then, given a period T of the virtual Axelrod tournament, each of the strategies in set S is run through the tournament, denoted by A with taking into account Y and some possible delays of response. The latter are gathered in a set denoted by D_N , where the subscript indicates that each admissible strategy can be attributed with an individual delay or inertial parameter. Then tournament A returns a subset

$$S^* = A(S, T, D_N, Y, \mathbf{P}(D_N); K, M) \text{ by } S^* \subset S, \quad (1)$$

where $\mathbf{P}(D_N)$ is a payoff matrix, K and M are the numbers of turns and repetitions, respectively, serving for tournament statistically stable results, and each strategy $s^* \in S^*$ maximizes the expected performance. It is worth mentioning that the strategies in subset $S^* \subset S$ by (1) are not precisely equally efficient (they all are approximately most efficient), and they valid for a real-time period not much exceeding period T .

The tournament by (1) then becomes a kind of behavioral stress test. Instead of asking “Is this software malicious?”, it asks “How does this software behave after 10, 100, or 1000 interactions with a diverse ecosystem of trusted and untrusted agents?” (i. e., therein $T = 10$, $T = 100$, $T = 1000$). That question is especially relevant for nuclear facilities, where many incidents originate not from a single malicious action but from an accumulation of interactions and trust relationships over time [1, 2, 8].

Results

The simulations demonstrate that entities exhibiting stable reciprocal behavior generally achieve the highest trustworthiness scores by the condition of reasonably longer and diverse inertial integer parameters in set D_N . Such entities consistently cooperate (where s^* is Grudger or WinStayLoseShift [5]) with compliant components while appropriately responding to suspicious or non-compliant behavior. Entities characterized by unconditional trust often become vulnerable to exploitation by deceptive participants [9]. Conversely, excessively restrictive entities may unnecessarily disrupt legitimate communications and reduce system efficiency (when s^* is Defector). The results expectedly indicate that balanced behavioral policies provide the most favorable compromise between security and operational continuity at nuclear power plants. The balance is additionally strengthened by probabilistically recombining the strategies in subset $S^* \subset S$ by (1) with regarding their relative frequencies. Such behavioral policies maintain cooperation among deserved-

ly trusted components while limiting opportunities for exploitation.

The tournament framework also reveals behavioral vulnerabilities that remain undetected during conventional functional testing. Certain entities perform correctly in isolated tests but gradually exhibit undesirable interaction patterns when exposed to prolonged sequences of encounters with heterogeneous participants. The findings suggest that repeated-interaction analysis can serve as an additional layer of cybersecurity assessment for critical infrastructure environments.

Discussion

The proposed approach extends the concept of cybersecurity testing from static verification toward behavioral evaluation. In contrast to traditional sandbox environments that primarily monitor executable actions, Axelrod tournaments assess how software entities behave under evolving interaction conditions. For nuclear power plants, where operational reliability is a critical requirement, understanding long-term behavioral characteristics is particularly important. Components that appear safe during short-term testing may reveal undesirable tendencies only after numerous interactions with other system elements.

The framework may also support cybersecurity policy design. Alternative authentication procedures, communication protocols, and access-control policies can be represented as tournament strategies and evaluated according to their ability to sustain secure cooperation while resisting exploitation. Furthermore, the methodology can be integrated with digital-twin environments used for modeling critical infrastructure systems. Such integration would enable cybersecurity specialists to evaluate candidate software updates and security configurations before introducing them into operational networks. Future research may incorporate machine-learning agents, adaptive attackers, evolving defense mechanisms, and multi-layer industrial control architectures to improve the realism of the simulations.

Conclusions

Axelrod Iterated Prisoner's Dilemma tournaments provide a novel framework for evaluating cybersecurity policies and software behavior in nuclear power plant environments. By treating cybersecurity assessment as a process of repeated interactions among autonomous entities, the proposed approach enables the identification of behavioral vulnerabilities that may not be visible during conventional testing. The results suggest that reciprocal and adaptive behavioral policies with inertia offer superior long-term trustworthiness compared with strategies based solely on unconditional trust or excessive restriction. Consequently, Axelrod tournaments may serve as a complementary tool, still being extremely simple, for strengthening cybersecurity assurance in critical nuclear infrastructure.

REFERENCES

1. International Atomic Energy Agency. *Computer Security of Instrumentation and Control Systems at Nuclear Facilities. Technical Guidance*. IAEA Nuclear Security Series No. 42-G. Vienna: IAEA, 2018.
2. Knapp E. D., Langill J. T. *Industrial Network Security. Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems* (Second Edition). Syngress, 2015.
3. Anderson R. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 3rd ed. Wiley, 2020.
4. Weibull J. W. *Evolutionary Game Theory*. MIT Press, 1997.
5. <https://github.com/Axelrod-Python/Axelrod>
6. Romanuke V. V. Compliance-and-defiance dilemma game best strategy for three and four agents. *Statistics, Optimization and Information Computing*, 2025, vol. 14, no. 5, pp. 415–433.
7. Gigerenzer G., Hertwig R., Pachur T. *Heuristics: The Foundations of Adaptive Behavior*. Oxford University Press, 2011.
8. Romanuke V. V. Optimal timing strategies in blockchain block proposals by one-bullet silent duels with one-third progression. *Information and Telecommunication Sciences*, 2025, vol. 16, no. 1, pp. 30–42.
9. Noordman C. R., Vreeswijk G. A. W. Evolving novelty strategies for the Iterated Prisoner's Dilemma in deceptive tournaments. *Theoretical Computer Science*, 2019, vol. 785, pp. 1–16.

Романюк Вадим Васильович — д-р техн. наук, професор, професор кафедри інноваційної економіки та цифрових технологій, Вінницький торговельно-економічний інститут Державного торговельно-економічного університету, Вінниця, Email: romanukevadimv@gmail.com

Romanuke Vadim Vasylyovych — Doctor of Technical Sciences, Professor, Professor of the Department of Innovative Economics and Digital Technologies, Vinnytsia Institute of Trade and Economics of State University of Trade and Economics, Vinnytsia, Email: romanukevadimv@gmail.com