International Research Journal of Computer Science (IRJCS) ISSN: 2393-9842
Issue 08, Volume 08 (August 2021) https://www.irjcs.com/archives

APPLICATION OF GAME THEORY IN HIERARCHICAL NETWORK SECURITY

Ankita Sharma
TERI University, New Delhi, India
ankita.sharma.teri.93@gmail.com
Vibhu Sharma
Energy Engineer, Grumman|Butkus Associates
Chicago, IL, USA
sharmav9@icloud.com

Publication History
Manuscript Reference No: **IRJCS/RS/Vol.08/Issue08/AUCS10094**
Received: 15, August 2021
Accepted: 22, August 2021
Published:27, August 2021
Citation: Ankita,Vibhu(2021). Application of Game Theory in Hierarchical Network Security. International Research Journal of Computer Science, VIII, 221-226
doi: https://doi.org/10.26562/irjcs.2021.v0808.011
Editor: Dr.A.Arul Lawrence Selvakumar, Chief Editor, IRJCS, AM Publications, India

Abstract: Such hierarchical network structures, omnipresent in modern organizations, give rise to particular security challenges. In this paper, we study the application of game theory to model an attacker-defender game in these layered networks. In such models, aiming at optimal resource allocation, threat prediction, and adaptive defense, we discuss gametheoretic models of Stackelberg, Bayesian, and Signalling games among others. A survey of recent literature on hierarchical network security demonstrates both strengths and limitations of these models.
Keywords: Game Theory, Hierarchical Network Security, Cybersecurity, Attack-Defense Model, Resource Allocation, Stackelberg Game

I. INTRODUCTION

Large organizations, therefore, especially those in government, financial and critical infrastructure sectors, have an ever-increasing need for hierarchical network architectures. Hierarchical architectures are multilayer by nature, with different levels of access, each with different security considerations, thus segmenting the network into portions that have many varied security needs or vulnerabilities. Often, attackers take advantage of these multi-layer dependencies to create a breach from relatively lower-order systems to higher-valued assets. In this sense, game theory provides the best framework to model and analyze the dynamic process of strategic interactions between rational actors, thus enabling the modeling of such dynamics between attackers and defenders in hierarchical networks. Specifically, in a game-theoretic framework, the interaction between a defender and an attacker can be looked upon as a game, where it shows the best mode of defense strategies, resource allocation, and attack path prediction. Traditional game-theoretic application to cybersecurity has been done via zerosum games, Stackelberg games, Bayesian games, and signalling games that provide structured approaches for managing defense resources, predicting attack patterns, and reducing network vulnerabilities [1], [2].

II. HIERARCHICAL NETWORK SECURITY: CHALLENGES AND GAME THEORY'S ROLE

Hierarchical network structures segregate an organization's network into a number of levels, including executive, operational, and technical layers, each with different security requirements and vulnerabilities. These are very common in large organizations where variations in access permissions or data flow exist among different levels. Securing hierarchical networks poses a unique challenge since any one level of threat can easily cascade throughout the whole system.

A. Multi-layer Threat Propagation

That could be very true, since the interdependencies in a hierarchical network allow for the propagation of an attack from one level to the others. A breach in a low-level system can enable attackers to access critical information or systems in other layers, jeopardizing the entire network. Attackers frequently exploit this weakness by initiating their assault on the lower layers of nodes, which typically possess weaker defenses, with the objective of ultimately escalating their access. Game theory systematically addresses multi-layer threats, and under the Stackelberg game model, the defense can strategically allocate resources to outmaneuver the attacker by implementing effective remedies against multi-layer propagation. By employing game theoretic models, a defender can allocate resources to the most susceptible tiers, so mitigating the probability of upward threat propagation [2].

Table1. Hierarchical Network Security Challenges

Challenge	Description	Implication
Multi-layer Threat Propagation	Attack can spread across different network layers due to dependencies.	Increases overall risk of full network breach.
Resource Allocation Constraints	Limited security resources that must be distributed across various levels.	Leads to potential under-protection of layers.
Complex Defense Requirements	Different levels require tailored security based on access control and data sensitivity.	Requires adaptive, multi-faceted defense.

B. Constraints on Resource Allocation

Efficient protection of hierarchical networks necessitates the prudent distribution of limited resources throughout the various layers of the network. Conventional methods of resource allocation are inadequately suited to address the intrinsic complexity and dynamic characteristics of hierarchical structures.Attackers may strike at less critical layers that grant entry points to sensitive areas. Of course, some of the most appealing game-theoretic models, in particular Bayesian and Stackelberg games, have been put forward for determining the optimal resource allocation strategy among those layers. In Stackelberg games, the defender, being a leader, first commits to a certain allocation strategy; the attacker, being a follower, observes this and reacts correspondingly. The sequential approach given by Stackelberg games provides defenders with the ability to deploy resources in a manner that will deter expected attack strategies, especially on layers offering the greatest potential impact if breached [3].

C. Complex Defence Requirements

There are many different layers in hierarchical network security, each having its special security needs. Since the attacker's objective may vary depending on the layer attacked, the defense mechanism must be adaptive to evolve with the variations in attacker strategies [4]. For example, executive levels may require high data encryption and access control policies, while for the operation levels, the rapid detection and mitigation protocols should be implemented. Game-theoretic models, such as signalling games, help meet these requirements by distinguishing benign and malicious activities across layers. In a signalling game, the attacker and defender engage in a sequence of moves whereby each party understands the actions taken by the other. This model enables dynamic adjustments of the mechanisms of defense so that the accuracy of threat detection can be realized with as little false positives as possible [5].

III. GAME-THEORETIC MODELS FOR HIERARCHICAL NETWORK SECURITY

In a game-theoretic model, strategic frameworks are developed for analyzing and enhancing the defense mechanism at levels in networks. This kind of model gives a defender an opportunity to do the following: predict the behaviour of an attacker, use effective algorithms to allocate resources, and make decisions according to a priority list obtained from risk assessments at higher and lower levels of the network.

Table 2. Comparison of Game-Theoretic Models in Network Security

Game-Theoretic Model	Primary Use	Strengths	Limitations
Stackelberg Games	Resource Allocation	Sequential decision-making, anticipates attacker responses	Computationally complex in large networks
Bayesian Games	Attack Path Prediction	Manages uncertainty, effective in incomplete information scenarios	Assumes accurate prior probabilities
Signaling Games	Intrusion Detection	Enhances threat differentiation, adaptive detection	Prone to false signals in complex networks

A. Stackelberg Games for Resource Allocation

Stackelberg games have thus found wide applications within the realm of hierarchical network security due to their sequential structure, whereby the defender commits first, followed by the attacker.

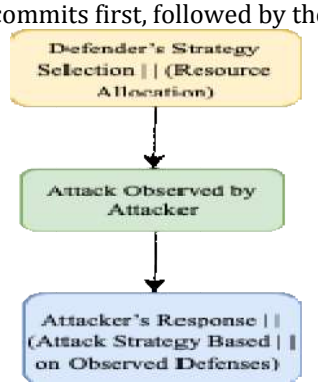

Fig 1. Decision-Making Process in Stackelberg Game for Resource Allocation

This model is particularly appropriate for resource allocation under hierarchical dependencies in the environment and enables defenders to allocate resources across layers of the network based on the likely attack paths seen as a response to the initial resource allocation.

In the Stackelberg game applied to network security, a defender optimally allocates resources between different layers. For example, highly sensitive layers may be better protected while other layers become less guarded, with the aim of minimizing overall expected damage. Figure 1 illustrates the play of a Stackelberg game against a hierarchical network structure. The defender's strategy in resource allocation takes into consideration the set of possible attack responses [6]. This approach has been effective in rather complicated hierarchical networks, such as those of financial and governmental systems, where structured resource allocation is often imperative. For example, Bedi et al. proposed the application of a Stackelberg model for dynamic cloud network resource allocation in order to enhance defense mechanisms against DDoS attacks [7].

B. Bayesian Attack Path Prediction Games

In a hierarchical network, defenders usually do not have any complete information about the attacker's capability and objective; hence, it always raises uncertainties in strategic planning. A Bayesian game will involve probabilistic assessment over different types of attackers; this will enable one to predict most likely attack paths and thus reinforce critical segments [8]. In Bayesian games, defenders update their beliefs regarding the attacker's strategy given the observed actions. The defenders then model the attacker's behaviour and target possibilities to prioritize security for network segments which could be more likely to be attacked. This is especially useful in hierarchical networks whose layers may be targeted in order to facilitate escalated attacks against higher layers. Bayesian games support the defenders in the concentration of resources on probable attack paths through proactive threat management enhancement [9]. Bayesian models find practical applications in critical infrastructure and high-security environments. Zhu and Başar [10]. illustrated the effectiveness of Bayesian game models with dynamic decision-making, wherein real-time updates on attacker behaviour could yield efficient defense against multi-layer network attacks.

C. Signalling Games for Intrusion Detection

The usefulness of signalling games in hierarchical networks refines intrusion detection systems by enhancing precision in identifying genuine threats. As a model, defenders and attackers send and interpret signals, like network activity or user behaviour, through multiple interactions; thus, defenders evaluate how likely network activities are due to malicious intentions and can respond accordingly [11]. Signalling games in hierarchical networks enable the defenders to make intrusion detection mechanisms appropriate for specific levels of the network, hence accuracy. For example, signalling games can protect critical assets by adapting the modification of detection thresholds on the high-priority layers. Consequently, it reduces false alarms while still allowing a high accuracy of detection. This approach is pretty convenient in those networks that bear sensitive information since differentiation between regular and malicious activity becomes crucial [12]. Pawlick et al. [13] applied the models of signalling games to network security, where one classifies threats according to a pattern observed in behaviour signature and reduces false positives within intrusion detection. An adaptive approach has given better detection rates in a case of layered and complex security systems.

IV. PRACTICAL APPLICATIONS AND FUTURE DIRECTIONS OF GAME THEORY IN HIERARCHICAL NETWORK SECURITY

While there is the prospect of more widespread use in hierarchical networks, the game-theoretic models remain useful abstractions for optimizing security strategies. Applied usage is expanding; further research aims to improve the scalability, adaptability, and predictive power of the models.

A. Current uses in Cybersecurity

1. Dynamic Resource Allocation: Stackelberg games are applied effectively in hierarchical networks for real-time resource allocation. Government and financial institutions that have usually faced diverse vectors of threats have adopted these models for dynamic resource allocations based on threat levels to protect their critical assets effectively [14].
2. Proactive Threat Prediction: Bayesian models will heighten the defender's threat prediction capabilities through the identification of possible attack paths and prepare actively against them. These are particularly useful in infrastructure networks, whereby the potential vectors of attack can be predicted to prevent critical breaches.
3. Adaptive Intrusion Detection: The use of signalling games in IDS systems leads to adaptability. It ensures that organizations will be able to detect more threats and do so accurately. Organizations might thus be able to calibrate their defenses at all layers of the network to allow for an improved intrusion detection rate without clobbering false positives[15].

Table 3. Applications of Game Theory in Cyber Security

Application Area	Game-Theoretic Model Used	Purpose	Sector Examples
Dynamic Resource Allocation	Stackelberg Games	Real-time distribution of resources	Finance, Government
Threat Prediction	Bayesian Games	Anticipate probable attack paths	Critical Infrastructure
Adaptive Intrusion Detection	Signaling Games	Improved threat identification and response	Military, High-Security Organizations

B. Future Research Directions

1. Integration with Machine Learning and AI: Integrating game-theoretic models with machine learning can further enhance accuracy and efficiency in resource allocation. Machine learning algorithms analyze large volumes of data to identify evolving attack patterns that can then inform the development of game-theoretic models through optimization of resource allocation strategies.
2. Enhanced Insider Threat Detection: In hierarchical networks, the threat of insiders is usually not addressed, but multi-level access can lead to serious harm. Game-theoretic models focusing on dynamics in insider behaviour can be useful for anticipating and mitigating the risk of insider threats in an environment with different levels of access for trusted users across the network [16].
3. Scalability of Algorithms for Large Networks: This will involve scaling game-theoretic models for large hierarchical networks. In this direction, efficient algorithms for Stackelberg and Bayesian games can help in improving the defenses for multi-layer networks with live-time solutions of resource allocation problems in a scalable manner without much computational overhead.
4. Human-Machine Interaction Models: Merging human factors into game-theoretic models can yield good dividends for security in hierarchical networks where human operators work in cooperation with automated systems. Understanding human decision-making in response to security threats may lead to effective security practices whereby defenders could account for both human intuition and algorithmic precision.

V. DISCUSSION AND LIMITATIONS

While promising, game-theoretic models for securing hierarchical networks have a number of serious limitations:

1. Computational Complexity: Most game-theoretic models applied in large hierarchical networks may be at the root of computational resource usage, hence limiting scalability due to their complexity [12].
2. Assumption of Rationality: Most game-theoretic models have an inbuilt assumption that attackers and defenders are fully rational, which may not be the case in terms of real adversarial behaviour.
3. Budget and Policy Constraints: There are organizations where such recommended resource allocations by design may not be practical due to either budget or policy constraints [13].

These limitations aside, game-theoretic analysis remains one of the handiest tools for bringing about improved cybersecurity in hierarchical networks by providing structured and strategic insights for defenders on resource allocation, threat anticipation, and planning defenses.

VI. CONCLUSION

Game theory offers structured ways to optimize resource allocation in improving hierarchical network security by predicting attack paths and adapting to defense mechanisms. With models such as Stackelberg, Bayesian, and signalling games, defenders are better prepared to deal with the complex, hierarchical nature of the challenges intrinsic to these networks. While usually limited by scalability and assumptions about attacker behaviour, game-theoretic models continue to evolve in sophistication and application.

REFERENCES

1. Alpcan, T., &Başar, T., *Network Security: A Decision and Game-Theoretic Approach*, Cambridge University Press, 2011.
2. Roy, S., Ellis, C. S., Shiva, S., Dasgupta, D., & Shandilya, V., "A survey of game theory as applied to network security," *43rd Hawaii International Conference on System Sciences*, 2010.
3. Manshaei, M. H., Zhu, Q., Alpcan, T., Başar, T., &Hubaux, J. P., "Game theory meets network security and privacy," *ACM Computing Surveys*, vol. 45, no. 3, 2013.
4. Lye, K.-W., & Wing, J. M., "Game strategies in network security," *International Journal of Information Security*, vol. 4, no. 1, pp. 71-86, 2005.
5. Pawlick, J., Johnson, B., & Zhu, Q., "A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy," *ACM Computing Surveys*, vol. 52, no. 4, pp. 1-28, 2018.
6. Zhu, Q., &Başar, T., "Game-theoretic approaches to dynamic decision making in cyber defense," in *Decision and Game Theory for Security* (Lecture Notes in Computer Science), vol. 7638, 2012.
7. Bedi, H., Roy, S., & Shiva, S., "Game theory-based defense mechanisms against DDoS attacks on cloud networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 2, pp. 321-332, 2017.
8. Liu, P., Zhu, Q., &Ahn, G.-J., "Hierarchical Stackelberg games for resource allocation in cyber-physical systems," *IEEE Transactions on Computers*, vol. 67, no. 4, pp. 592-603, 2018.
9. Rass, S., Schauer, S., König, S., &Schryen, G., "Defending against advanced persistent threats using game theory," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 2, pp. 236-251, 2019.
10. Nguyen, K., &Lucet, K., "Game-theoretic approaches to cybersecurity and the role of trust in networked systems," *Journal of Network and Computer Applications*, vol. 97, pp. 87-98, 2017.
11. Liu, P., & Zhu, Q., "A Stackelberg game approach for hierarchical security and privacy management in multi-layered networks," *Journal of Computer Security*, vol. 26, pp. 393-418, 2018.

